TRAKA32 USER GUIDE

UD0089

03/01/24

VERSION 4.1

1 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

2 TRAKA - INTELLIGENT ACCESS MANAGEMENT

2.1 WELCOME

Welcome to Traka

This user guide has been prepared in order to assist you with every aspect of Traka ranging from planning to advanced features of all the Traka systems.

The content of this guide is based upon the following software and firmware versions...

Software Version: 02.49.0000

8bit Firmware Version: 06.08.42 and below

16bit Firmware Version: 04.00.19 and below

2.2 TRAKA OVERVIEW

The Traka Item Management System has been designed to provide a quick and easy method of issuing and controlling keys. In addition, Traka provides instant information as to the current user of an item, the previous user as well as a complete history of the asset usage.

Traka can also restrict access to individual assets thus enabling cost effective and efficient management of keys, reducing losses as well as time and energy trying to locate misplaced or "taken home" assets.

The Key Cabinet systems consist of single or multiple security cabinets, each containing up to 360 electronic key fobs (iFobs). Each iFob contains a unique electronic security ID number. For most applications the keys are attached to the iFobs using security seals or key rings. Access to the cabinet is granted by the control pod, which only allows access to authorized users. The cabinet may have been specified with locking or non-locking iFobs (or a mixture of both). Locking iFobs require the user to press an adjacent button before the key will release.

2.3 COPYRIGHT

This manual and the programs to which it refers are copyrighted and all rights reserved. You are not permitted to:

- Copy this manual by any means
- Allow other people to have copies of the programs
- Use the programs on more than one machine at a time

Any such actions may be regarded as intent to defraud and action may be taken.

2.4 CAUTION

Great care has been taken to ensure that the Traka hardware and software works correctly but it is impossible to guarantee that there are no errors in a computer program or that hardware failures will not occur. Remember also that if someone enters the wrong information errors may also occur and careless use of the hardware can cause damage that no design can withstand.

Only you can check that the system works properly in your particular application both initially and on a regular basis.

We would ask you to consider how you would operate your business should you be unable to access the keys due to a hardware or software failure. We would also recommend you implement some contingency plan to cover such an occurrence.

For these reasons, Traka and their agents and distributors cannot assume liability or responsibility for any consequences under any circumstances arising from the use of the Traka equipment and programs. The product is sold only on the basis of this understanding. If this is not acceptable to you then please return the equipment and software prior to its use for commercial purposes for a complete refund.

2.5 CONTACT

Should you need assistance with your Traka products, please feel free to contact us by any of the means below. If however you purchased you Traka products through a distributor and you require assistance then please contact your distributor first.

Please ensure you have the following information to hand when you contact Traka...

- System Serial Number(s) - e.g. TKC 12345 - Can be found in the System Details window.
- Firmware Version(s) - e.g. V06.07.30 - Can be found in the System Details window.
- Software Version - e.g. V2.10.0000 - Can be found in the System Details window.
- Database Type - e.g. Access/SQL etc

Web Addresses

From our main website you can access our technical support website where you keep up to date with all the latest downloads and information.

Traka Website: http://www.traka.com

Email

If you have any questions regarding any aspect of Traka please feel free to email us.

Enquiries: info@traka.com

Support: support@traka.com

Telephone and Fax

If you have any questions regarding any aspect of Traka please feel free to call between the hours of 09:00 and 17:30 GMT/BST.

Telephone: **+44 (0)1234 712345**

Technical Support Helpline

Telephone: **0333 355 3641**

Postal Address

You can also write to us.

Address:

Traka
30 Stilebrook Road
Olney
Buckinghamshire
MK46 5EA
United Kingdom

An ASSA ABLOY Group Company

2.6 WARRANTY TERMS AND CONDITIONS

Traka UK Warranty and Annual Maintenance and Support Agreement

Traka cabinets are provided with a 12-month warranty, starting on the day of installation. During this warranty period Traka will provide parts and labour to repair any fault caused though manufacturing defect.

After the expiry of the warranty period, an annual maintenance and support agreement may be purchased, which covers the cost of parts and labour to repair on a planned next working day response any fault caused through normal use of the equipment. In addition the maintenance and support contract includes an annual system check and free upgrades to the PC software. The annual charge for this will be 15% (subject to distance) of the list price of the equipment covered.

Items covered by the Warranty and Annual Support Agreement

Hardware

All parts provided by Traka during the original installation. Where card or other readers are supplied by the Customer, these parts are specifically excluded from the warranty and maintenance. Items purchased subsequent to the original installation will be subject to an adjustment to the annual support agreement

Software

Traka will also provide free software upgrades as required during the period of the annual maintenance. Furthermore, Traka will provide a login to our technical support web site where information on the latest upgrades is available and where the latest software may be downloaded. Software upgrades are supplied on a self-install basis and requests for Traka to install the software are not included within the warranty or annual support agreement.

Response Times

Traka offer a 9:00 to 5:30 support facility and guarantee a same or next working day response to any reported fault. Where site visits are required, Traka will whenever possible attend on the next working day. Working days are Monday to Friday excluding Bank holidays.

Exclusions

Traka will not be responsible for any fault or damage or configuration change that occurs as a result of:

1. Inadequate user training
2. Software reconfiguration
3. Use of the software on a non-supported version of the Windows operating system
4. Customer re-installation on a different version of the operating system
5. Accidental damage
6. Vandalism, sabotage or terrorism
7. Noncompliance with the Customers responsibilities as detailed below

If a warranty or support visit is required to repair systems damaged as a result of these exclusions, Traka reserve the right to place a lower priority on the call and cannot guarantee the same response times to repair such failures.

If response to repair any fault or to reconfigure any settings is required due to these exclusions Traka will charge at their usual site visit rates.

If as a result of the site visit, the system failure was subsequently found to be caused by these or other exclusions, Traka will charge for both parts and labour at the prevailing rates.

Use of the equipment and Backing up the data

The Customers responsibilities are to:-

1. Ensure that the Traka hardware and software is used in a proper manner by competent trained employees only and in accordance with the Traka User Guides.

2. Provide the Traka support engineer full access to the Traka cabinet and Traka32 software. This may include making available access keys and passwords.

3. Ensure that the Traka cabinets are regularly communicated to the support PC and that the Traka32 database is regularly backed up.

4. Not alter or modify the hardware or software in any way whatever nor permit it to be combined with any other system without the prior written consent of Traka.

5. Not request, permit or authorise anyone other than Traka to provide any maintenance services in respect of the hardware or software while the maintenance agreement is in effect and not subject to notice of termination.

6. Co-operate fully with Traka personnel in the diagnosis of any error or defect.

7. Ensure in the interests of health and safety that Traka personnel while on the Customers premises for the purpose of this agreement are either at all times accompanied by a member of staff familiar with the premises and safety procedures or trained in respect of the site health and safety procedures.

Limitation of Liability

Traka shall not be liable for any direct, indirect or consequential loss or damage howsoever caused, arising from this agreement, the software, the hardware, its use, application support or otherwise, except to the extent which it is unlawful to exclude such liability.

Database

Traka shall not be liable for any direct, indirect or consequential corruption or loss of data arising from modification to the Traka database not conducted using the proper Traka32 tools provided. Any reparation to a Traka database required to be carried out by a Traka Engineer, where the database structure has been tampered with using other software programs (non-Traka software programs) such as Microsoft Access or Microsoft SQL Server will be charged for accordingly. Minimum fixed cost of reparation is **£150.00**

Virus

Traka warrants that it will use all reasonable endeavours to ensure that the software is supplied free of computer viruses and has undergone rigorous virus checking procedures prior to delivery in line within current best practices.

3 INSTALLATION

3.1 PLANNING

3.1.1 POSITIONING

Planning the position of the Traka systems is a very important part of the installation process and is time well spent as poor planning will result in problems later down the line.

The positioning of the Traka System is usually determined by who is going to use the system the most. From experience, things to take into account are:-

- **24 hour access**
  Traka systems should be positioned conveniently for the required users.

- **Busy periods**
  Places such as corridors or offices that have a high volume of traffic should be avoided.

- **Height of the system**
  Please take into consideration any disabled people that may have to use the Traka system.

- **Administration and serviceability**
  Ideally you should locate a PC Workstation that will be running a copy of Traka32 as close as possible to the Traka System as this will make system administration much easier.

- **Security**
  Traka is not designed as a high security safe, it is designed to control and monitor the issue of keys. The security of the location should be provided by the customer, so please don't position the Traka systems in an exposed or vulnerable location.

- **Indoor use only**
  Traka systems are designed to be used in ambient, dry conditions, not in an exposed location.

- **Type of wall**
  Traka systems can be quite heavy, typically weighing 40kg+ and therefore need a strong wall to fix to. Fixings are not included and so when selecting the appropriate fixings it's essential they are strong enough to retain the Traka System and to ensure that they do not pull out from the wall.

  NOTE: The wall (and any wall covering) to which the Traka System is fixed must be made of low flammability material (at least 94 UL-5V flammability class equivalent). Please ensure that any flammable materials, for example wall paper, are completely removed before fixing the cabinet to the wall.

- **Biometrics Reader**
  If the system is fitted with a biometrics reader, position the system so that users can stand in a comfortable and natural position when using the reader. Do NOT position in direct sunlight as this can affect the performance of the reader when scanning a fingerprint.

3.1.2 STANDALONE SYSTEMS

Standalone Traka systems are supported with easy to use Windows software called Traka32. The software does not need to be running every time you use Traka but it is essential that it is used to configure and maintain Traka. Therefore the computer ideally needs to be permanently connected using a serial RS232 or modem connection in close proximity to the Traka system.

Please refer to the RS232 and Modem sections.

Other things to take into account when Networking Traka are as follows:-

Database location
You will need to consider where the Traka database is to be located – either on the local hard drives of a workstation or preferably on a server.

Backing up the database
As Traka is building a long-term history of keys used, it is essential that the data is regularly backed up. By locating the database on a server, this may make the backup procedures easier to manage. However, when the data is stored locally, Traka includes regular reminders to back up the database. We suggest that you make backing up part of your office procedures.

3.1.3 NETWORK SYSTEMS

Networked Traka systems are supported with easy to use Windows software. The software does not need to be running every time you use Traka but it is essential that it is used to configure and maintain Traka. Therefore the computer ideally needs to be permanently connected using an RS485 or Ethernet network connection. If connected to your Ethernet, you will need a Traka Ethernet Device (TED). A static IP Address must be programmed into the TED so that the Traka system will be accessible from anywhere over the network.

Please refer to the RS485 and Ethernet sections.

Other things to take into account when Networking Traka is as follows...

Multiple users
Each Traka cabinet is supplied with a single software license for installation on a single computer. If you wish for more than one computer to access the database (assuming that you have a suitable network) you will need to purchase additional user licenses. If you wish these can be purchased after the initial installation as the software provides a 90 day evaluation period during which you may legitimately use the software. However, after the 90-day period it will cease to operate without a special release code that can only be provided by Traka.

Database location
You will need to consider where the Traka database is to be located – either on the local hard drive of a workstation or preferably on a server.

Backing up the database
As Traka is building a long-term history of keys used, it is essential that the data is regularly backed up. By locating the database on a server, this may make the backup procedures easier to manage. However, when the data is stored locally, Traka includes regular reminders to back up the software. We suggest that you make backing up part of your office procedures.

3.1.4 DATABASE OVERVIEW

Traka32 can work with two database formats, Microsoft Access and Microsoft SQL.

Microsoft Access

Access is ideal for standalone or small network users with small amounts of data. It is very simple to install and maintain through the Traka32 software.

Microsoft SQL

SQL is ideal for large network users providing a robust database. SQL is more complex to install and maintain than Access and will require an SQL Administrator.

3.1.5 COMMUNICATIONS

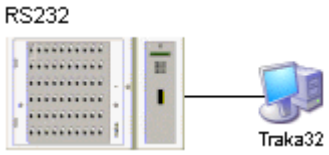
3.1.5.1 COMMUNICATIONS OVERVIEW

Each Traka System is administered from one or more copies of the Traka32 software. There are several ways of communicating between the Traka32 software and the Traka Systems...

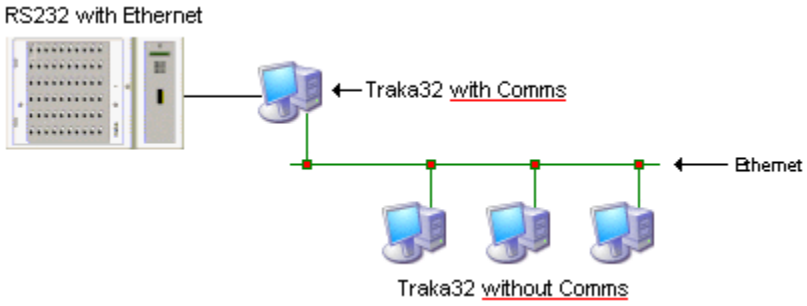
Comms Type	Traka32 Software	Traka32 Hardware
RS232	Single Copy	Single System
RS485	Single Copy	Up to 30 Systems
Modem	Single Copy	Unlimited Systems
Ethernet	Up to 255 Copies	Unlimited Systems

3.1.5.2 RS232

RS-232 (or serial as it is also known) is the simplest form of communications between the Traka32 software and a Traka System. This is most commonly used where only a single Traka System is administered by a single copy of the Traka32 software.

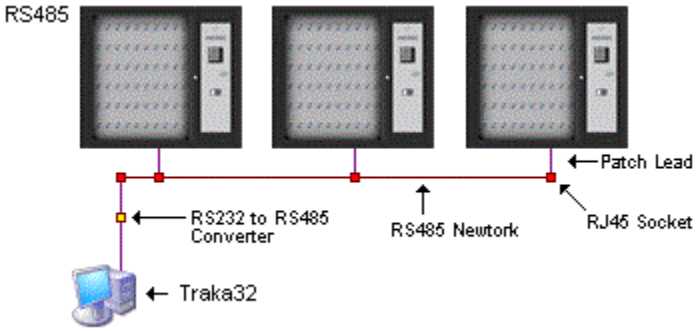


It is also possible to combine the RS232 communications with Ethernet to allow a single Traka32 client to administer the Traka Systems and as many additional 'view only' Traka32 clients as is required.

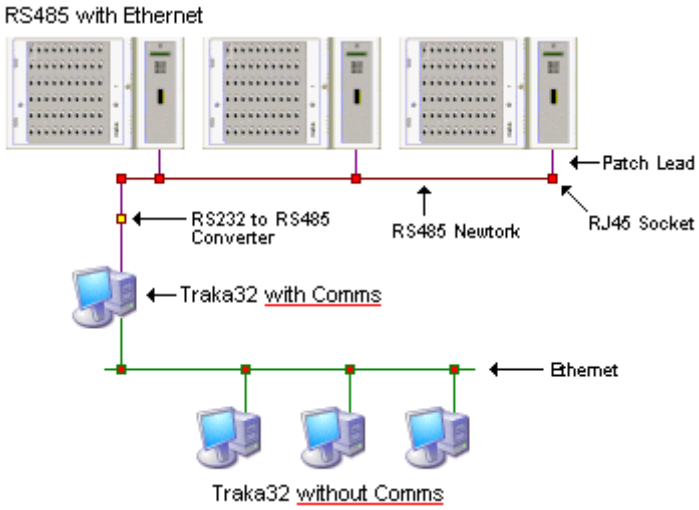


3.1.5.3 RS485

RS-485 is most commonly used where multiple Traka Systems are administrated from a single copy of the Traka32 software.

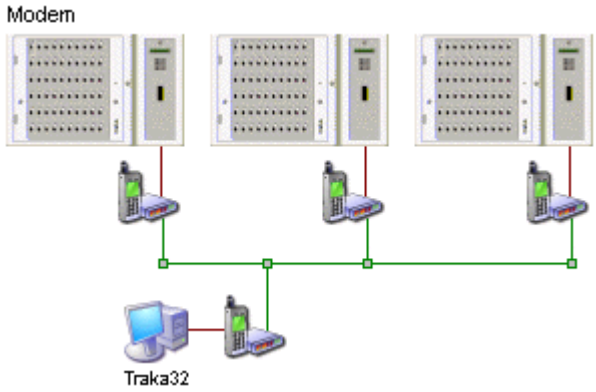


It is also possible to combine the RS485 communications with Ethernet to allow a single Traka32 client to administer the Traka Systems and as many additional 'view only' Traka32 clients as is required.



3.1.5.4 MODEM

A modem can be used to communicate to a remote Traka Systems.



Please refer to your modem user guide.

3.2 ETHERNET

Ethernet is the most popular form of communication allowing multiple Traka Systems to be administered from multiple copies of the Traka32 software using an existing Ethernet.

At present Traka uses a **Traka Ethernet Device** (TED) to connect to connect a Traka System to an Ethernet. There are currently two types of TED available...

Moxa

Xport

Each device has to be configured to talk across the network you are installing Traka onto. Before configuring each device you will need to obtain some information from the Network Administrator of the network you are installing onto. Each device will require the following information from the Network Administrator...

- Static IP Address
- Subnet Mask
- Default Gateway

3.3 HARDWARE INSTALLATION

3.3.1 ANTI STATIC PRECAUTIONS

When installing or maintaining the Traka systems you must take appropriate precautions against static discharge. This normally involves connecting yourself to an earth source via a wrist strap, so that any static generated is immediately discharged to earth. Failure to take static precautions may damage the Traka equipment. This damage may not manifest itself immediately but may cause the unit to fail in the future. If you have queries about static precautions please do not hesitate to contact your supplier who can advise on anti-static procedures and equipment.

3.3.2 WHAT YOU SHOULD HAVE

Every care is taken to ensure all parts necessary are shipped with your order. If you find any items missing from the checklist below please contact Traka immediately.

- Traka System – Your Traka system will be supplied with the correct number of receptor strips or locker compartments as per your order. Each receptor socket (if applicable) will have an iFob in place. For RFID lockers, RFID tags will be included with your system.
- Master Lock Keys – Traka is supplied with a set of keys, which operate the lock to the control panel and emergency door release.
- Back up battery (UK deliveries only).

Depending on the way in which you have chosen to administer your Traka System you will be supplied with the appropriate communication parts:

RS232

- A supplied length of cable with 9 pin 'D' plugs at either end.

RS485

- An 'RS232 to RS485 Converter' with patch lead for the PC.
- A patch lead for each Traka system.
- RS485 network cable category 5. (Supplied on request.)
- RS485 network ports category 5 RJ45. (Supplied on request.)
- RS485 installation guide.

Modem

- Modem. (This may be pre-installed in the Traka system.)
- Modem power cable and communication cable.
- Modem user guide.
- Modem installation guide.

Ethernet

If you are supplied with a Moxa Ethernet adaptor you should have the following…

- Moxa Serial Port Server. (This may be pre - installed in the Traka system.)
- Moxa Serial Port Server support CD.
- Moxa Serial Port Server user guide.
- Moxa Serial Port Server installation guide.
- A patch lead (supplied on request).

If you have an onboard XPort Ethernet adaptor you should have the following…

- XPort Serial Port Server installation guide.
- A patch lead (supplied on request).

3.3.3 WHAT YOU WILL NEED

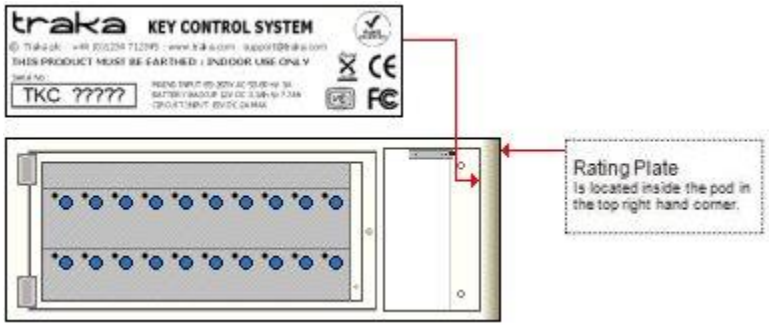
Prior to you installing the Traka System, you should ensure that the items below are in place and functioning before you continue.

- A mains power supply – The Traka system should be powered by an isolated Non Switched fused 13-amp spur with a 3-amp fuse fitted. It is not recommended that you simply plug Traka into a local power socket.
- A computer – Please check the minimum PC requirements before making a selection. If you are using a modem to communicate to your system then the PC will require a modem.
- Suitable Fixings and Tools – Suitable fixings must be chosen to support the weight of the Traka cabinets.
- Networking – If you are networking your system using Ethernet you will need to have a convenient RJ45 wall socket close to the Traka system that is patched into your network.

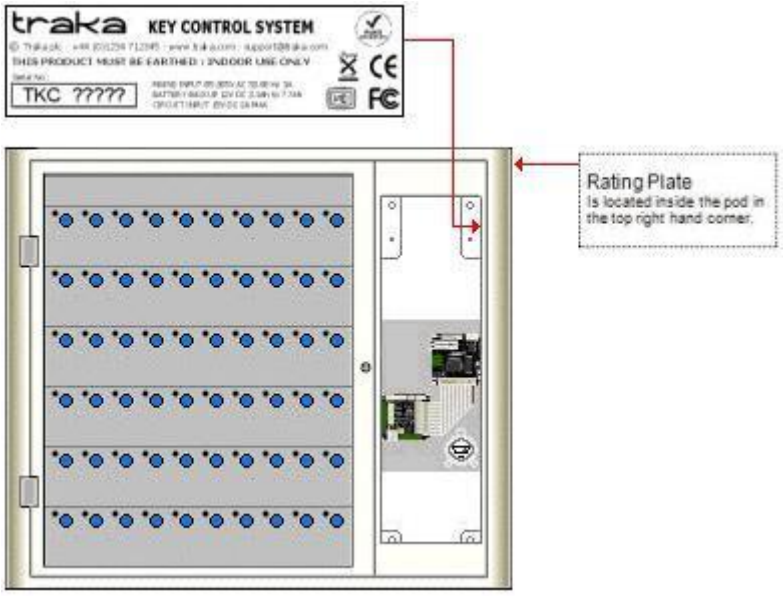
3.3.4 SERIAL NUMBER / RATING PLATE

All Traka Systems are fitted with a Serial Number / Rating Plate. This can be found in the following location...

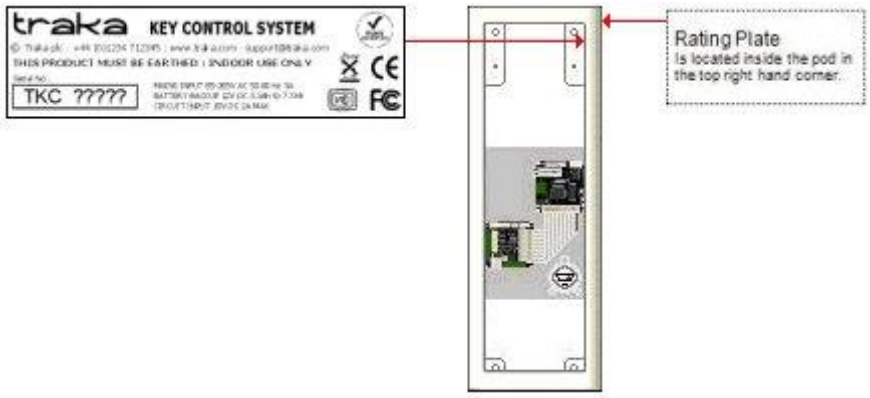
For the Traka **M-Series** the Rating Plate is located on the inside, you will need to remove the control panel in order to view the Rating Plate. Additionally there will be another label on the outside of the S-Series on the right hand side stating were you can find the Rating Plate.



For the Traka **S-Series** the Rating Plate is located on the inside, you will need to remove the control panel in order to view the Rating Plate. Additionally there will be another label on the outside of the S-Series on the right hand side stating were you can find the Rating Plate.



For Traka Products such as the **L-Series, Lockers and Access control Pods**, the Rating Plate is located inside the Pod. You will need to remove the control panel in order to view the Rating Plate. Additionally there will be another label on the outside of the Pod on the right hand side stating were you can find the Rating Plate.



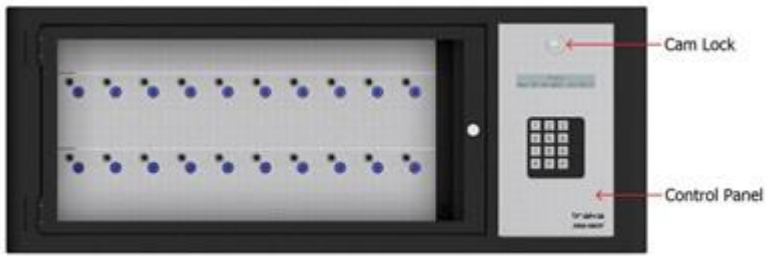
3.3.5 M-SERIES

3.3.5.1 M-SERIES PREPARATION

Before attaching an M-Series Traka system to the wall you will need to remove various parts in order to access the various fixing holes. Please refer to the anti static precautions before preparing the system.

NOTE: Any plastic protective film should be removed after installation in order to protect the stainless steel finish and polycarbonate door.

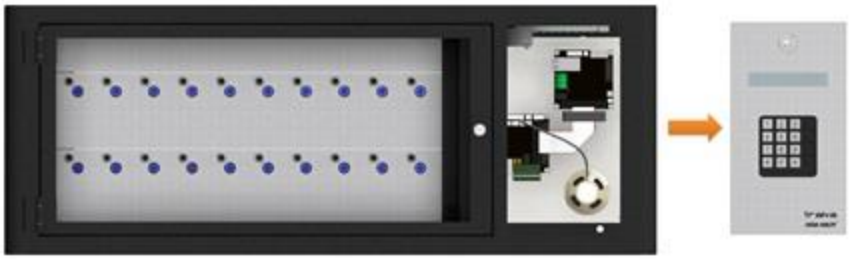
1. Carefully unpack your Traka unit and ensure all the necessary parts are there using the check list.
2. The Control Panel is hooked in at the bottom and locked at the top. Using the Master Key, unlock the Cam Lock.



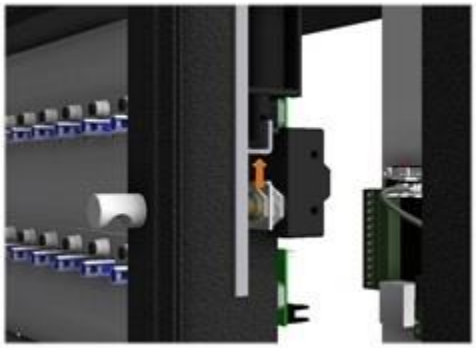
3. Carefully begin to remove the Control Panel. You will see that there are several wires connected to the control panel. Carefully disconnect the following wires noting where and how they connect.
    - Keypad Cable
    - LCD Cable
    - Earth Cable
    - Reader Cable (if applicable)

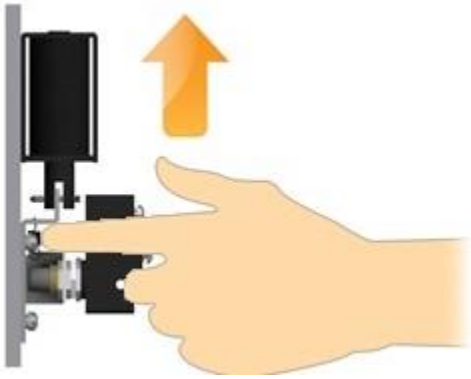
    NOTE: For more details on the various PCB connections, please refer to the 8bit Control PCB Diagrams or 16bit I/O PCB layout section of the Traka32 Help Guide.

4. Completely remove the control panel and put in a safe place until needed.

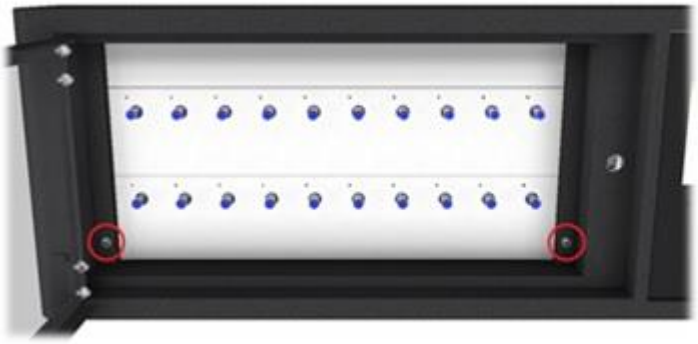


5. Reach inside and open the door manually by moving the door lock catch up.



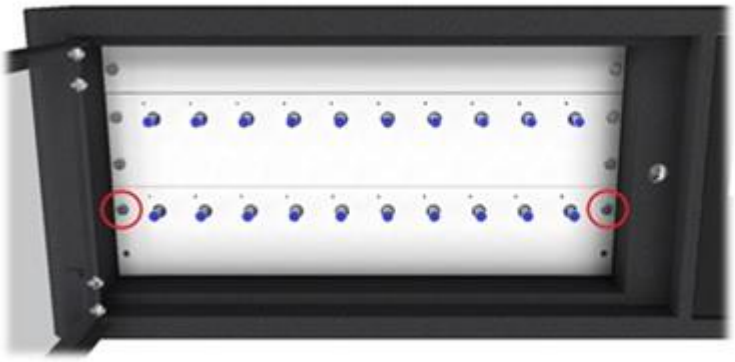


6. Using a 4mm Allen Key, remove the Cover Panel screws one at a time and remove the cover panels.



7. Using a large flat bladed screwdriver, carefully remove the blanking strip at the top and remove the two receptor strips and carefully disconnect the receptor ribbon cable. Put the receptor strips in a safe place until needed, noting where they came from as they must be returned to the same location.

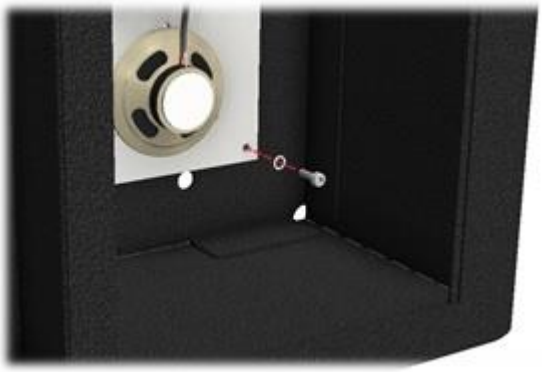
   NOTE: It is essential that the receptor strips are replaced in the same location from which they were removed otherwise the system will not function correctly.



8. Disconnect the following cables from the Control PCB taking note of how and where they connect.
   - Door Lock Cable
   - Power Cable
   - Receptor Cable

   NOTE: For more details on the various PCB connections, please refer to the 8bit Control PCB Diagrams or 16bit I/O PCB layout section of the Traka32 Help Guide.

9. Using an Allen Key remove the 4 screws to remove the 16bit Control PCB Plate or the 8bit Control PCB (depending on your system type).



10. The above preparation will have now revealed the 4 fixing holes that can be used to fix the system to a suitable wall with suitable fixings.

11. Now refer to the M-Series Installation section.

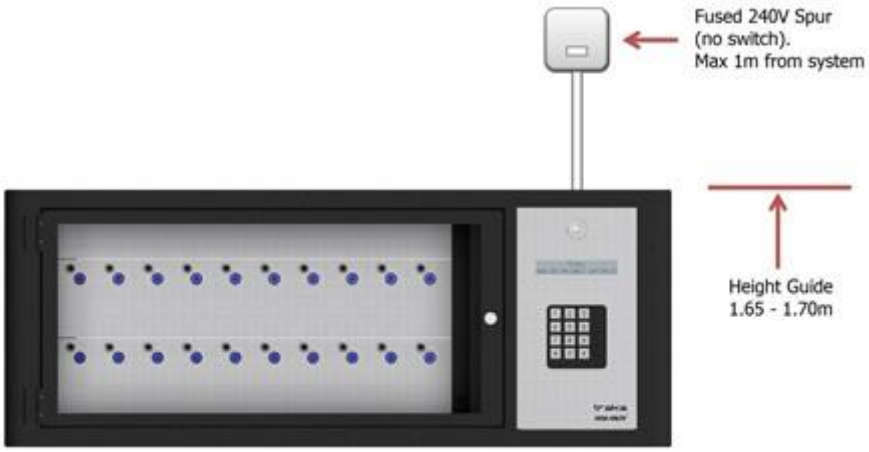
3.3.5.2 M-SERIES INSTALLATION

Before attaching an M-Series Traka system to the wall you will need to remove various parts in order to access the various fixing holes, please refer to the M-Series Preparation section.

NOTE: Traka systems can be quite heavy, typically weighing 40kg+ and therefore need a strong wall to fix to. Fixings are not included and so when selecting the appropriate fixings it's essential they are strong enough to retain the Traka System and to ensure that they do not pull out from the wall.

NOTE: The wall (and any wall covering) to which the Traka System is fixed must be made of low flammability material (at least 94 UL-5V flammability class equivalent). Please ensure that any flammable materials, for example wall paper, are completely removed before fixing the cabinet to the wall.

1. Locate the system on the wall where you want it to go. As a guide the top of the system should be 1.65 – 1.70 meters from the floor and should no further than 1 meter from the mains spur.



2. Mark and drill the four fixing holes and attach the system to the wall using the appropriate fixings.

3. 20mm knockout holes are provided in the top and bottom of the cabinet. The power supply and communication cables should be brought to the top or the bottom of the system via 20mm trunking.

   NOTE: Please refer to the mains power supply section for the power supply connection details and the relevant communication installation section for the communications connection. Do not switch on the system at this point.

4. Once securely fixed to the wall and the mains and communications cables have been run to the system, the items removed for installation can be replaced.

5. Replace the 16bit Control PCB Plate or 8bit Control PCB (depending on your system type) and reconnect the following cables.

   - Door Lock Cable
   - Power Cable
   - Receptor Cable
   - Comms cable (such as network or RS232 etc.)

     NOTE: For more details on the various PCB connections, please refer to the 8bit Control PCB Diagrams or 16bit I/O PCB layout section of the Traka32 Help Guide.

6. Replace all the receptor strips reconnecting the receptor ribbon cable. Using a large flat bladed screwdriver, secure the receptor strips in place with the fixings and removed earlier.

   NOTE: It is essential that the receptor strips are replaced in the same location from which they were removed otherwise the system will not function correctly.

7. Using a 4mm Allen Key, replace the Cover Panels one at a time with the fixings removed earlier. Once the cover panels have been replaced then close the door (if fitted).

8. Hook the Control Panel into the bottom of the Pod. Whilst holding the control panel, re-connect the following wires to the Control PCB.

    - Earth Cable
    - Power Cable
    - Receptor Ribbon Cable
    - Reader Cable (Optional)

    NOTE: For more details on the various PCB connections, please refer to the 8bit Control PCB Diagrams or 16bit I/O PCB layout section of the Traka32 Help Guide.

9. Insert the Battery into the base of the Pod and connect to the Control PCB.

10. Switch the On/Off switch on the 8bit Control PCB or 16bit I/O PCB to **On**.

    You should hear a double beep and the LCD should light up and start to display text. If this does not happen then switch Off the On/Off switch and double check your connections.

11. Finally, close the Control Panel carefully and lock with the Master Key. The Control Panel should fit easily, if not check that no wires have become caught or trapped between the Control Panel and the cabinet.

12. Now refer to the Commissioning section.

3.3.6 S-SERIES

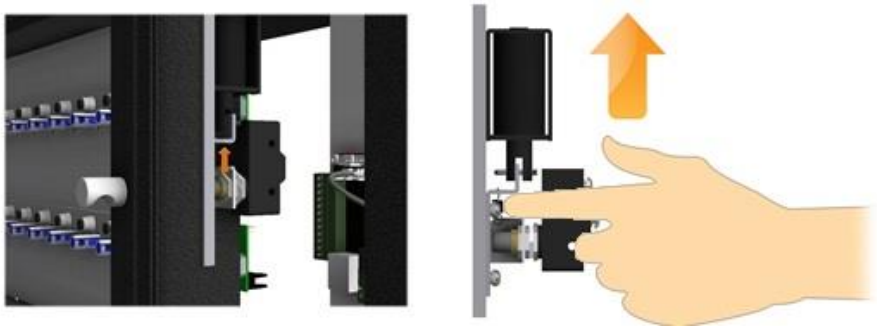
3.3.6.1 S-SERIES PREPARATION

Before attaching an S-Series Traka system to the wall you will need to remove various parts in order to access the various fixing holes. Please refer to the anti static precautions before preparing the system.

NOTE: Any plastic protective film should be removed after installation in order to protect the stainless steel finish and polycarbonate door.

1. Carefully unpack your Traka system and ensure your all the necessary parts are there using the checklist.
2. The Control Panel is hooked in at the bottom and locked at the top. Using the Master Key, unlock the Control Panel Cam Lock.

3. Tilt the Control Panel forward and reach inside and open the door manually by moving the door lock catch up.



4. Undo the plastic **Wing Bolt** then close and lock the Control Panel. You will now be able to swing **open the Control Panel Door**.

5. Disconnect the Receptor Ribbon cable and Door Lock cable from the 8bit Control PCB or 16bit I/O PCB respectively.

6. Disconnect the Green & Yellow Earth cable connector linking the Receptor Frame to the main cabinet.
7. Using a 2.5mm Allen Key, remove the screws holding the Receptor Frame in place.
8. Carefully slide the Receptor Frame to the right to free from the main cabinet and remove.

   NOTE: The receptor frame is heavy especially when fully loaded with keys.

9. The above preparation will have now revealed the 6 fixing holes that can be used to fix the system to a suitable wall with suitable fixings.

10. Now refer to the S-Series Installation section.

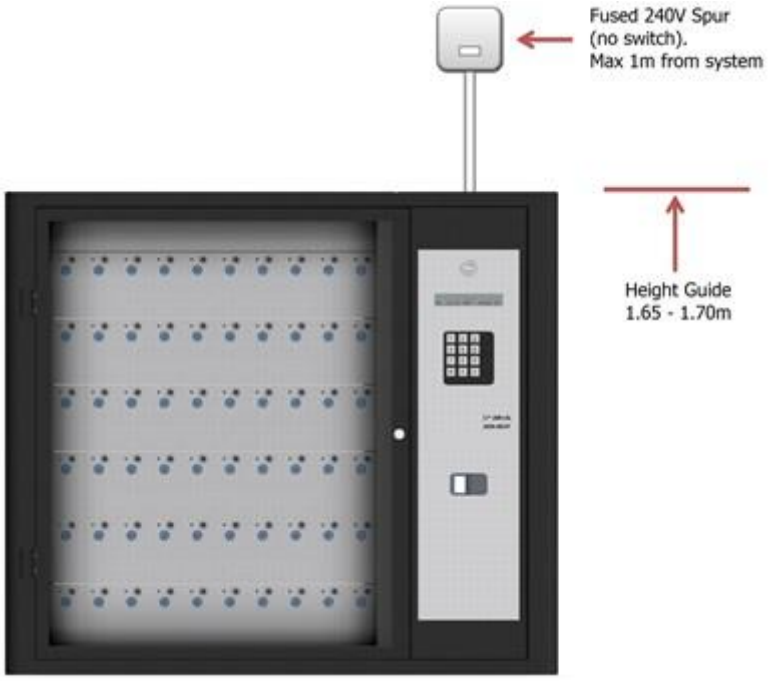
3.3.6.2 S-SERIES INSTALLATION

Before attaching an S-Series Traka system to the wall you will need to remove various parts in order to access the various fixing holes, please refer to the S-Series Preparation section.

NOTE: Traka systems can be quite heavy, typically weighing 40kg+ and therefore need a strong wall to fix to. Fixings are not included and so when selecting the appropriate fixings it's essential they are strong enough to retain the Traka System and to ensure that they do not pull out from the wall.

NOTE: The wall (and any wall covering) to which the Traka System is fixed must be made of low flammability material (at least 94 UL-5V flammability class equivalent). Please ensure that any flammable materials, for example wall paper, are completely removed before fixing the cabinet to the wall.

1. Locate the system on the wall where you want it to go. As a guide the top of the unit should be 1.65 – 1.70 meters from the floor and should no further than 1 meter from the mains spur.



2. Due to the weight of the system we suggest the top central hole is marked and drilled first. The system can then be supported on this one whilst the others are marked and drilled.

3. 20mm knockout holes are provided in the top and bottom of the cabinet. The power supply and communication cables should be brought to the top or the bottom of the system via 20mm trunking.

   NOTE: Please refer to the mains power supply section for the power supply connection and the relevant communication installation section for the communications connection. Do not switch on the system at this point.

4. Once securely fixed to the wall and the mains and communications cables have been run to the system, the items removed for installation can be replaced.

5. Carefully replace the Receptor Frame into the cabinet and slide to the left to connect to the main cabinet.

   NOTE: The receptor frame is heavy especially when fully loaded with keys.

6. Using a 2.5mm Allen Key, replace the screws holding the receptor frame in place.

7. Re-connect the Receptor Ribbon cable and Door Lock cable to the 8bit Control PCB or 16bit I/O PCB respectively.

   NOTE: For more details on the various PCB connections, please refer to the 8bit Control PCB Diagrams or 16bit I/O PCB layout section of the Traka32 Help Guide.

8. Re-connect the Green & Yellow Earth cable connector.

9. Insert the Battery into the base of the Pod and connect to the 8bit Control PCB or 16bit I/O PCB.

10. Switch the On/Off switch on the 8bit Control PCB or 16bit I/O PCB to **On**.

    You should hear a double beep and the LCD should light up and start to display text. The cabinet will continue to beep whilst the door is open (if fitted). If this does not happen then switch Off the On/Off switch and double check your connections.

11. Close the Control Panel Door.

12. The Control Panel is hooked in at the bottom and locked at the top. Using the Master Key, unlock the Control Panel Lock.

13. Tilt the Control Panel forward and re-fit the plastic Wing Bolt.

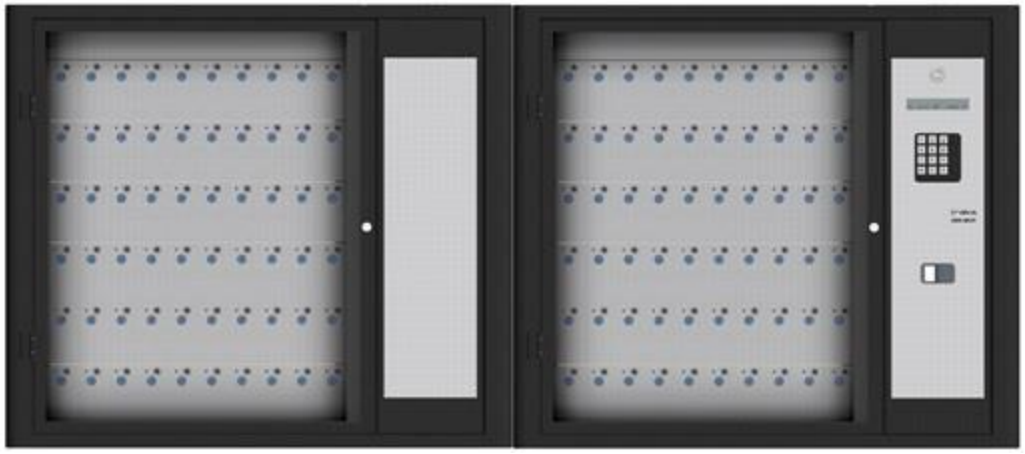
14. Close and lock the Control Panel.

15. Close the door.

16. Now refer to the Commissioning section.

3.3.6.3 S-SERIES EXTENSION CABINETS

Additional cabinets can be installed with or added later to the S-Series Traka system. For example...



or...

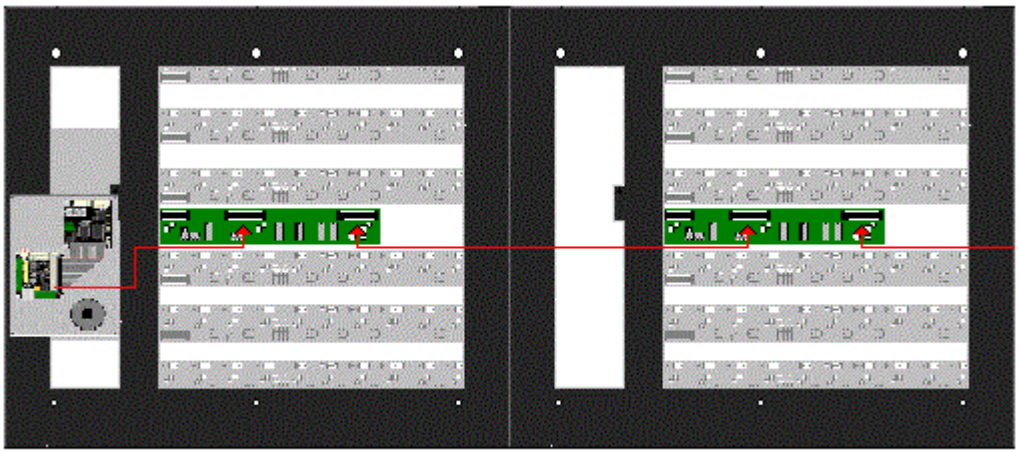
The S-Series extension cabinets are installed in exactly the same way as the standard S-Series cabinets except for the way in which they connect. Please refer to the preparation and installation sections on how to mount an S-Series cabinet on the wall along with the details below on how to connect the cabinets together.

The cabinets are connected via a series of Interface PCBs. Using a 34 way ribbon cable you can connect the cabinets as follows...

1. Connect the Control PCBs Receptor Connector to the first Interface PCBs Input Connector.
2. Connect the **first** Interface PCBs **Output** Connector to the **second** Interface PCBs **Input** Connector.

NOTE: Cables running between systems must be passed through the cut-outs in the sides of the cabinets. If no cut-out exists (older systems), a suitable size hole must be cut in the side of the cabinet. Cables must not be passed behind the cabinet as they could be damaged when trapped against the wall.

3. If you have more extension cabinets then continue to connect the **Output** to **Input** of the remaining Interface PCBs.



The Control PCB is shown for connection purposes but is located inside the cabinet.

NOTE: When connecting the Interface PCBs it is important to check the following...

- **Cabinet Selector settings.** Please refer to the Interface Selector Settings section of the Traka32 Help Guide for details on the correct settings.
- **Cabinet Jumper settings.** Please check there is only a link across the **J1** jumper on the last cabinet in the series. All the other cabinets must **not** have the link across J1.

Please refer to the 8bit Control PCB Diagrams or 16bit I/O PCB layout and Interface PCB Diagram of the Traka32 Help Guide to locate the various connections.

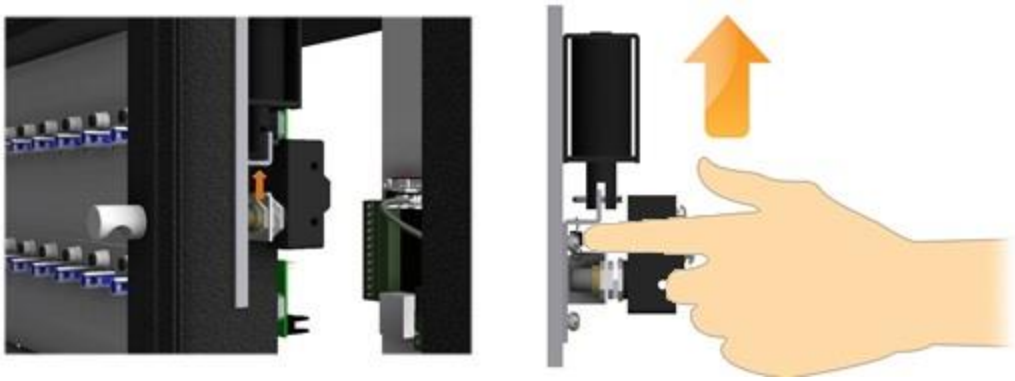
3.3.6.4 S-SERIES SERVICING

To access the internal part of the S-Series Traka System follow the procedure below...

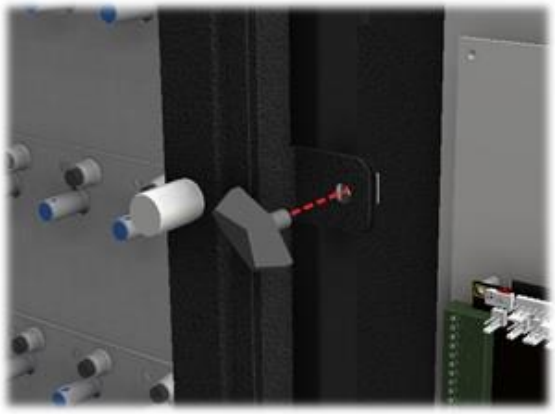
To open the Control Panel Door...

1. Ensure the system is disconnected from the mains power before continuing.
2. The Control Panel is hooked in at the bottom and locked at the top. Using the Master Key, unlock the Control Panel Cam Lock.

3. Tilt the Control Panel forward and reach inside and open the door manually by moving the door lock catch up.



4. Undo the plastic Wing Bolt then close and lock the Control Panel. You will now be able to swing open the Control Panel Door.



To further open the Receptor Frame...

5. Fit the Receptor Frame Hinge into the locating slots at the top and bottom of the cabinet by inserting the top first and then the bottom.

6. Using a 2.5mm Allen Key, remove the bolts holding the receptor frame in place.

7. Carefully slide the frame to the right aligning the holes in the Receptor Frame Hinge with those in the frame itself.

8. Fit two plastic Wing Bolts attaching the Receptor Frame Hinge to the Receptor Frame.

9. Slowly open the Receptor Frame.

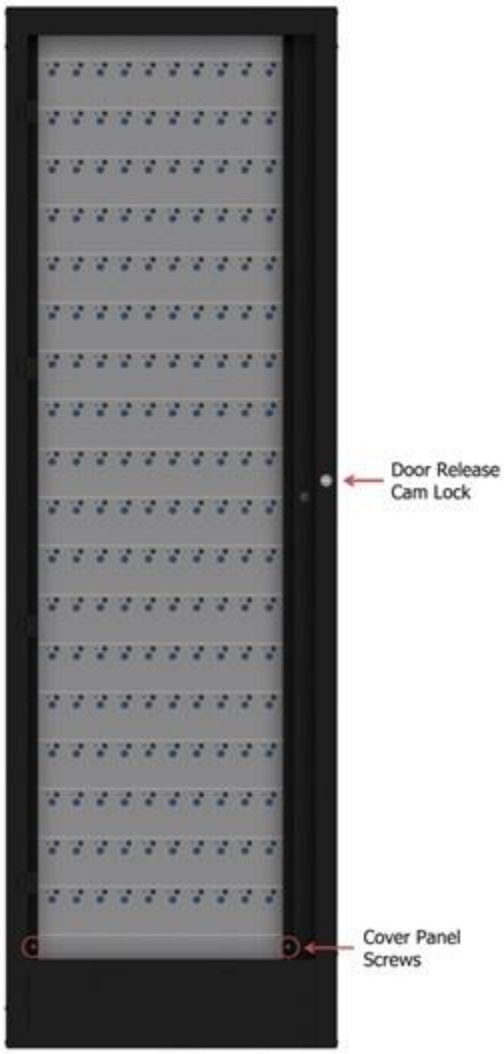
3.3.7 L-SERIES

3.3.7.1 L-SERIES CABINET PREPARATION

Before attaching an L-Series Traka system to the wall you will need to remove various parts in order to access the various fixing holes. Please refer to the anti static precautions before preparing the system.

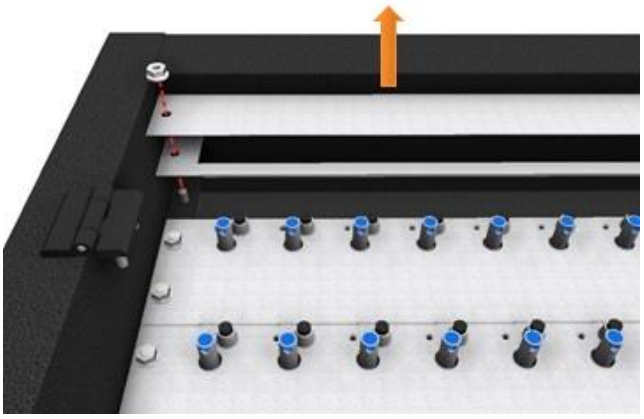
NOTE: Any plastic protective film should be removed after installation in order to protect the stainless steel finish and polycarbonate door.

1. Carefully unpack your Traka system and ensure all the necessary parts are there using the check list.
2. The L-Series system comes in two parts, the Pod and the Cabinet. Start with the cabinet(s) and install the Pod last.
3. Using the Master Key open the door (if fitted) using the Door Release CAM Lock.



4. Using a 4mm Allen Key, remove the Cover Panel Screws one at a time and remove the cover panels.

5. Using a 10mm Nut Spinner, carefully remove the top and bottom 1U blanking panels.



6. The above preparation will have now revealed 5 fixing holes.

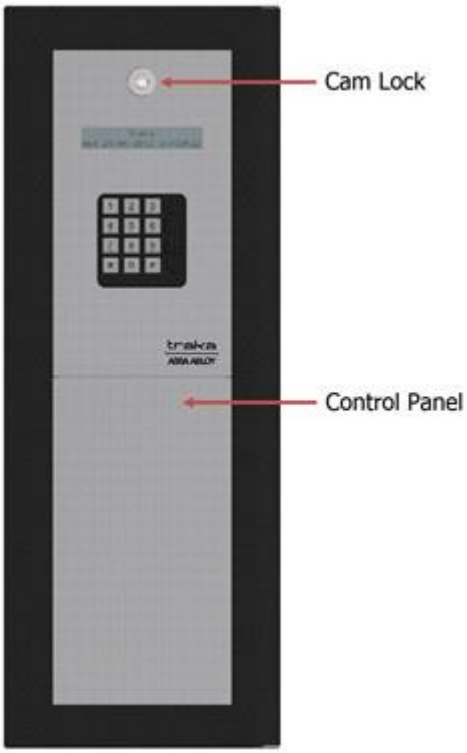
7. You will find the following cables hanging in the back of the cabinet. Carefully thread these cables through the pre-drilled hole in the right hand side of the cabinet.
    - Receptor Ribbon Cable
    - Door Switch/Solenoid Cable
    - Earth Cable
8. Now refer to the L-Series Pod Preparation section.

3.3.7.2 L-SERIES POD PREPARATION

Before attaching an L-Series Pod to the wall you will need to remove various parts in order to access the various fixing holes. Please refer to the anti static precautions before preparing the pod.

NOTE: Any plastic protective film should be removed after installation in order to protect the stainless steel finish.

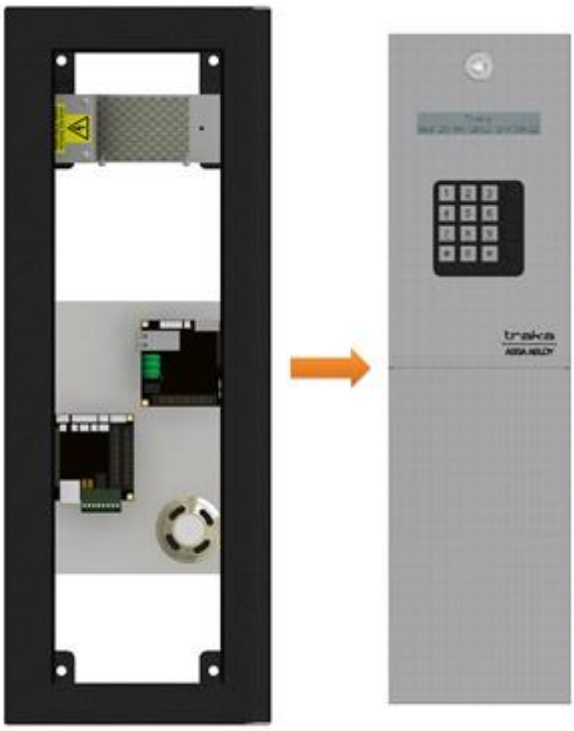
1. Carefully unpack your Traka Pod and ensure your all the necessary parts are there using the check list.
2. The Control Panel is hooked in at the bottom and locked at the top. Using the Master Key, unlock the Cam Lock.



3. Carefully begin to remove the Control Panel. You will see that there are several wires connected to the Control PCB that are attached to the control panel. Carefully disconnect the following wires noting where and how they connect.
    - LCD
    - Keypad
    - Card Reader (optional)
    - Earth Lead

NOTE: For more details on the various PCB connections, please refer to the 8bit Control PCB Diagrams or 16bit I/O PCB layout and 16bit Control PCB Layout sections of the Traka32 Help Guide.

4. Completely remove the control panel and put in a safe place until needed.



5. The above preparation will have now revealed the 4 fixing holes that can be used to fix the pod to a suitable wall with suitable fixings.

6. Now refer to the L-Series Installation section.

3.3.7.3 L-SERIES INSTALLATION

Before attaching an L-Series Traka system to the wall you will need to remove various parts in order to access the various fixing holes, please refer to the L-Series Preparation section first followed by the Pod Preparation section.

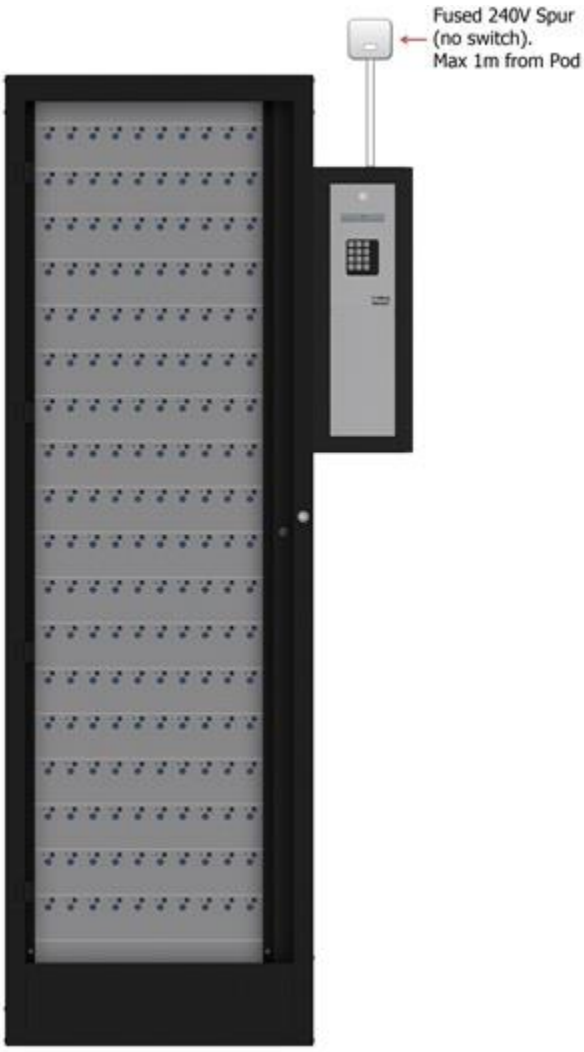
NOTE: Traka systems can be quite heavy, typically weighing 40kg+ and therefore need a strong wall to fix to. Fixings are not included and so when selecting the appropriate fixings it's essential they are strong enough to retain the Traka System and to ensure that they do not pull out from the wall.

NOTE: The wall (and any wall covering) to which the Traka System is fixed must be made of low flammability material (at least 94 UL-5V flammability class equivalent). Please ensure that any flammable materials, for example wall paper, are completely removed before fixing the cabinet to the wall.

1. Locate the cabinet on the floor and against the wall where you want it to go.

   NOTE: Remember to leave at least 350mm clear space on the wall to the right hand side of the cabinet to install the pod.

   TIP: The cabinet is designed to sit on the floor against a wall. Most internal wall will have a skirting board, if so then it is best to remove a 'cabinet's width section' of the skirting board so the cabinet will sit flush to the wall.



2. Mark and drill one of the top two holes in the cabinet. This will safely hold the cabinet in place allowing for fine adjustment whilst you install the pod.

3. Carefully thread the protruding cables from the right hand side of the cabinet into the pre-drilled hole in the left hand side of the pod. At the same time, position the pod on the wall flush to the right hand side of the cabinet.

NOTE: It is important to align these holes so that the receptor ribbon, door and earth cables can pass between the two without being caught or damaged.

Mark and drill the top two fixing holes in the pod and attach to the wall.

4. Adjust the pod and the cabinet so they are aligned correctly. Mark and drill the remaining holes in both the pod and the cabinet and secure to the wall.

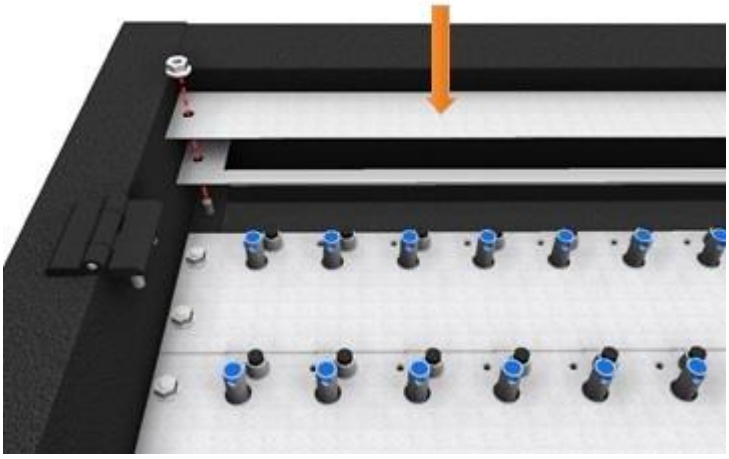
5. Connect the earth cable linking the cabinet to the pod.

6. 20mm knockout holes are provided in the top and bottom of the pod. The power supply and communication cables should be brought to the top or the bottom of the pod via 20mm trunking.

NOTE: Please refer to the mains power supply section for the powers supply connection and the communication installation section for the communications connection. Do not switch on the system at this point.

7. Once securely fixed to the wall and the mains and communications cables have been run to the system, the items removed for installation can be replaced.

8. Replace the blank receptor panels at the top and bottom of the cabinet.



9. Using a 4mm Allen Key, replace the Cover Panels one at a time with the fixings removed earlier. Once the cover panels have been replaced then close the door (if fitted).

10. Hook the Control Panel into the bottom of the Pod. Whilst holding the control panel, re-connect the following cables to the Pod and Control PCB.

    - Earth Cable
    - Power Cable
    - Receptor Ribbon Cable
    - Keypad Cable
    - LCD Cable
    - Reader Cable (if applicable)

NOTE: For more details on the various PCB connections, please refer to the 8bit Control PCB Diagrams or 16bit I/O PCB layout section of the Traka32 Help Guide.

11. Insert the Battery into the base of the Pod and connect to the 8bit Control PCB or 16bit I/O PCB respectively.

12. Switch the On/Off switch on the 8bit Control PCB or 16bit I/O PCB to **On**.

You should hear a double beep and the LCD should light up and start to display text. If this does not happen then switch Off the On/Off switch and double check your connections.

13. Finally, close the Control Panel carefully into the Pod and lock with the Master Key. The Control Panel should fit easily, if not check that no wires have become caught or trapped between the Control Panel and the Pod.

14. Now refer to the Commissioning section.

3.3.7.4 L-SERIES EXTENSION CABINETS

Additional cabinets can be installed with or added later to an L-Series Traka system.

The L-Series extension cabinets are installed in exactly the same way as the main L-Series cabinets except for the way in which they connect. Please refer to the preparation and installation sections on how to fix an L-Series cabinet to the wall along with the details below on how to connect the cabinets together.

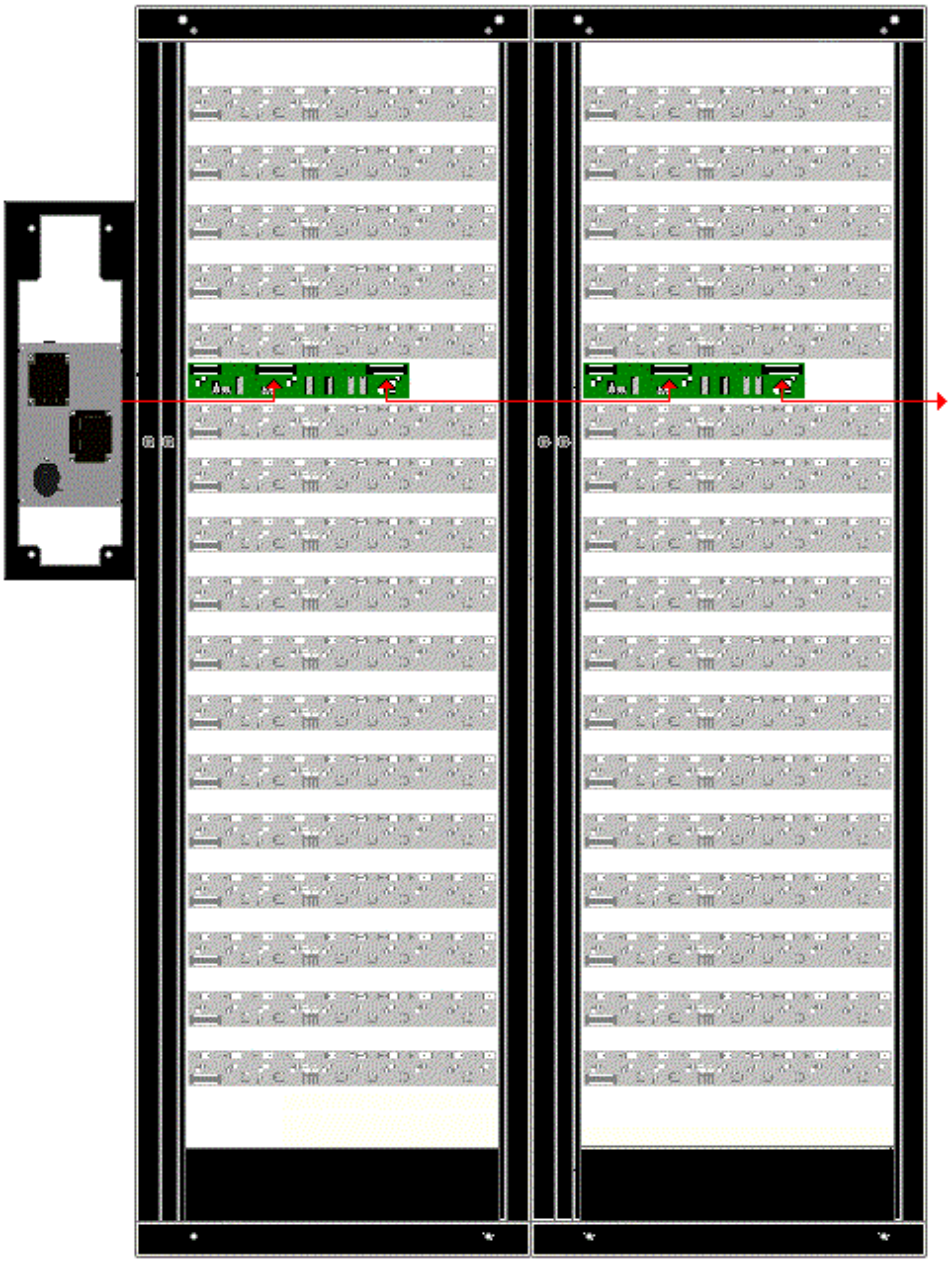
The cabinets are connected via a series of Interface PCBs. Using a 34 way ribbon cable you can connect the cabinets as follows...

1. Connect the Control PCBs Receptor Connector to the first Interface PCBs Input Connector.

2. Connect the first Interface PCBs Output Connector to the second Interface PCBs Input Connector.

NOTE: Cables running between systems must be passed through the cutouts in the sides of the cabinets. If no cutout exists (older systems), a suitable size hole must be cut in the side of the cabinet. Cables must not be passed behind the cabinet as they could be damaged when trapped against the wall.

3. If you have more extension cabinets then continue to connect the **Output** to **Input** of the remaining Interface PCBs.



NOTE: When connecting the Interface PCBs it is important to check the following...

- **Cabinet Selector settings.** Please refer to the Interface Selector Settings section of the Traka32 Help Guide for details on the correct settings.
- **Cabinet Jumper settings.** Please check there is only a link across the **J1** jumper on the last cabinet in the series. All the other cabinets must **not** have the link across J1.

Please refer to the 8bit Control PCB Diagrams or 16bit I/O PCB layout and Interface PCB Diagram of the Traka32 Help Guide to locate the various connections.

3.3.8 LOCKERS

3.3.8.1 TRAKA MODULAR LOCKERS

3.3.8.1.1 MODULAR LOCKER PREPARATION

NOTE: Traka Modular Lockers are designed specifically to suit a customer's requirements. Therefore the images displayed in this guide may differ to the system you are installing, however the same principles apply.

Before attaching a Traka Locker system to the wall you will need to remove various parts in order to access the various fixing holes. Please refer to the anti static precautions before preparing the system.

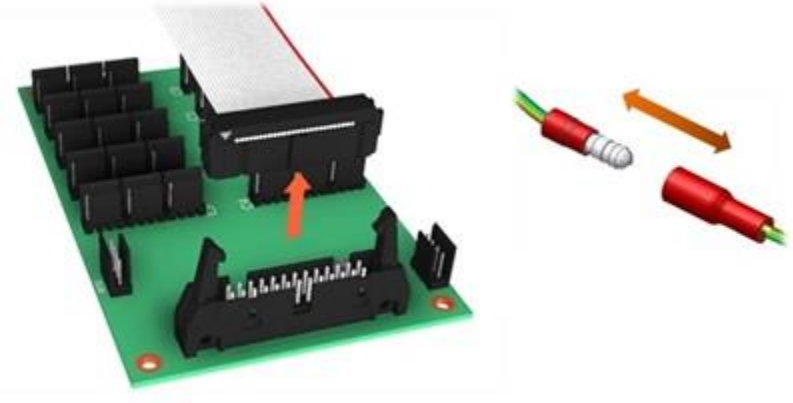
NOTE: Any plastic protective film should be removed after installation in order to protect the finishes.

Locker Preparation...

1. Carefully unpack your Traka Locker system and ensure all the necessary parts are there using the check list.
2. Using the Master Keys unlock the Cam Locks on each side of the locker and lift up the hinged Access Cover to expose the Interface boards and cables.

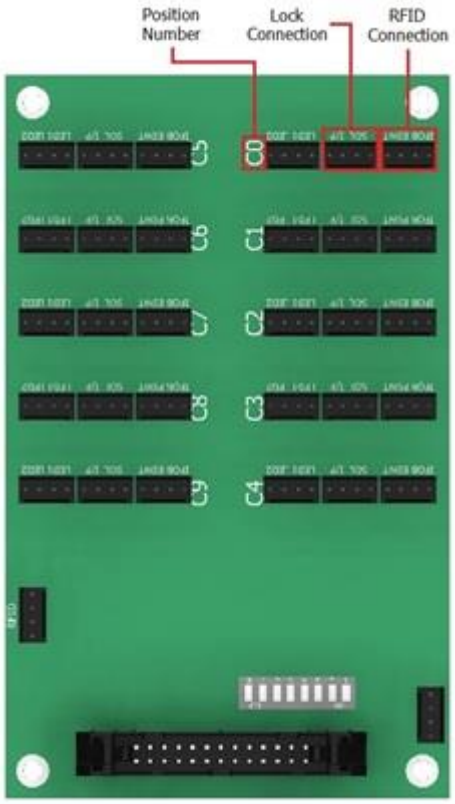
Beneath the cover you will see the locker PCBs connecting all of the lock cables and RFID cables (if applicable). If you have 10 compartments in each module there will be a locker PCB fixed to the top of every module. If you have less than 10 compartments in each module the PCBs will be positioned in the most suitable locations for connecting the cables.

3. To remove a module, disconnect the ribbon cable from the PCB (if applicable), and disconnect the earth cable connecting the module to the locker frame.



4. Depending on your system configuration it's possible that lock cables and RFID cables from adjacent modules may also be connected to the PCB. If this is the case then these cables must also be disconnected to allow the module to be freely removed.

All lock cables and RFID cables are labelled 0-9 according to the position number they connect to on the PCB (C0-C9). The diagram below shows the location of the lock and RFID cable connectors and the position number on the PCB.



5. To remove a module that does not have a PCB fixed to the top, follow the lock and RFID cables (if applicable) to the PCB they are connected to and disconnect. You will also need to disconnect the earth cable as described in the previous step.

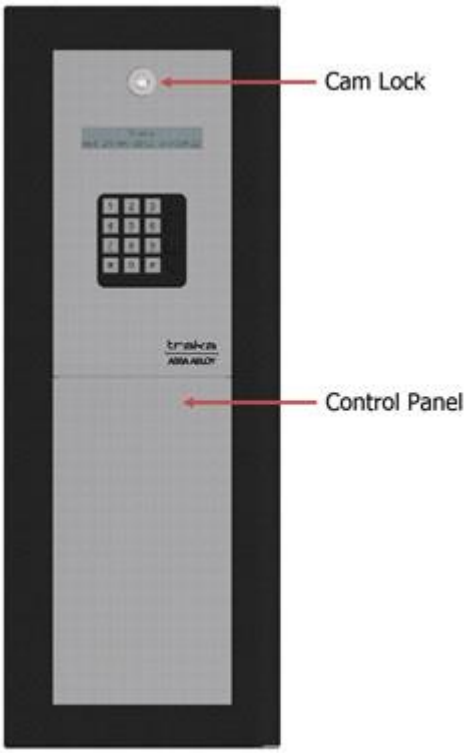
6. Carefully tilt the module forward and lift over the lip at the front of the frame to remove. Take care not to damage any cables when removing the modules.

NOTE: If your system has been designed with USB charging, depending on the size of your system it may have a USB Charging PCB fixed to the Locker Frame behind the modules. Each compartment will have a USB cable connected to the PCB. These must be disconnected in order to remove the module.

7. Removing all of the modules will expose the wall fixing points in the back of the frame. If your system has the option of charging in compartments the Power Bars or USB Charging PCBs will also be located in the back of the frame.

Pod Preparation…

1. The Control Panel is hooked in at the bottom of the Pod and locked at the top. Using the Master Key, unlock the Cam Lock.

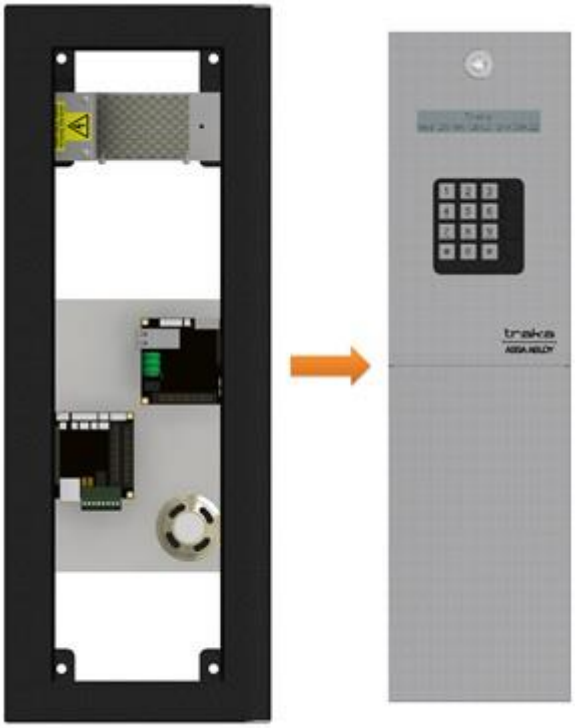


2. Carefully tilt the Control Panel towards you leaving the bottom hooked in. You will see that there are several cables connected to the PCB that are attached to the control panel. Carefully disconnect the following wires noting where and how they connect.

- LCD
- Keypad
- Card Reader (if applicable)
- Earth Cable

NOTE: For more details on the various PCB connections, please refer to the 8bit Control PCB Diagrams or 16bit I/O PCB layout section of the Traka32 Help Guide.

3. Completely remove the control panel and put in a safe place until needed.



4. The above preparation will have now revealed the 4 fixing holes that can be used to fix the pod to a suitable wall with the appropriate fixings.

5. Please now refer to the Modular Locker Installation section.

3.3.8.1.2 MODULAR LOCKER INSTALLATION

Before attaching a Traka Locker system to the wall you will need to remove various parts of the system in order to access the various fixing holes, please refer to the Modular Locker Preparation section.

NOTE: Traka systems can be quite heavy, typically weighing 40kg+ and therefore need a strong wall to fix to. Fixings are not included and so when selecting the appropriate fixings it's essential they are strong enough to retain the Traka System and to ensure that they do not pull out from the wall.

NOTE: The wall (and any wall covering) to which the Traka System is fixed must be made of low flammability material (at least 94 UL-5V flammability class equivalent). Please ensure that any flammable materials, for example wall paper, are completely removed before fixing the cabinet to the wall.

1. Attach the Pod to the Locker Frame using the supplied fixings and connect the earth cable linking the Pod to the Locker Frame through the cut-out.
2. Locate on the wall where you want the locker system to go, the Pod should be no further than 1 meter from the mains spur.
3. Mark and drill the fixing holes for both the locker frame and the pod and attach the system to the wall using the appropriate fixings.

4. Once securely fixed to the wall the mains and communications cables need to be run to the unit. 20mm knockout holes are provided in the top and bottom of the pod. The power supply and communication cables should be brought to the top or the bottom of the Pod via 20mm trunking.

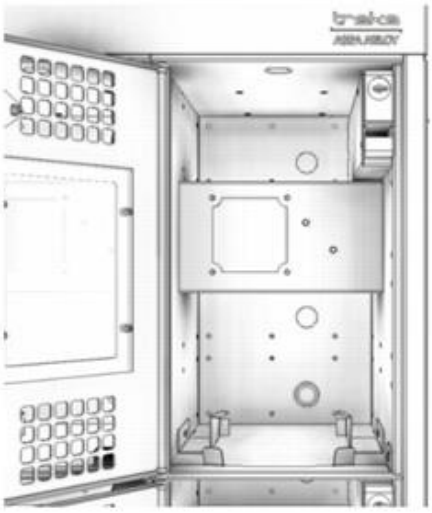
NOTE: Please refer to the mains power supply section for the power supply connection and the relevant communication installation section for the communications connection. Do not switch on the system at this point.

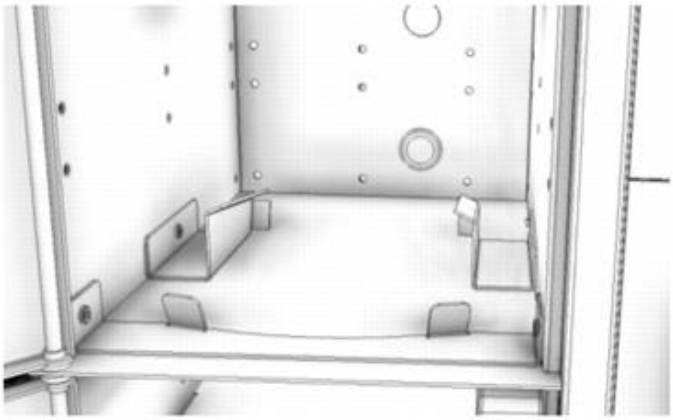
5. If your system has been designed with charging inside the compartments using mains chargers, it will have been fitted with Power Bars in the back of the Locker Frame. Much like the Pod, the Locker Frame has knockouts in the top for routing the Power Bar mains cables out to a suitable connection point.

Each Power Bar is pre-wired with a 3m length of mains cable. Route the cable through one of the knockouts using a grommet and suitable conduit as described in the previous section.

NOTE: The specification of the Power Bars will have been determined based on a specific type of charger and quantity intended to be used in the system. Details of this and the power requirements for the Power Bars can be found on the system drawing.

6. If the system requires chargers to be installed, the compartment will have been designed specifically to incorporate them. Depending on the design, you may be required to remove pre-fitted brackets inside the compartment to place in the chargers before refitting the brackets. Alternatively you may have been supplied with brackets not yet fitted. In either case the system drawing will show a detailed view of how the brackets are fitted to incorporate the charger. An example is shown below:





7. The modules that were removed in preparation can now be replaced and the all cables re-connected.

NOTE: It is essential that the modules are replaced in the same location from which they were removed otherwise the system will not function correctly.

8. Once all the modules have been replaced and the cables reconnected, you can close down the lid of the locker and lock it on both sides using the **Master Keys**.

9. Hook the Control Panel into the bottom of the Pod. Whilst holding the control panel, re-connect the following wires to the Control PCB.
    - LCD
    - Keypad
    - Card Reader (optional)
    - Earth Cable
    - Receptor Cable

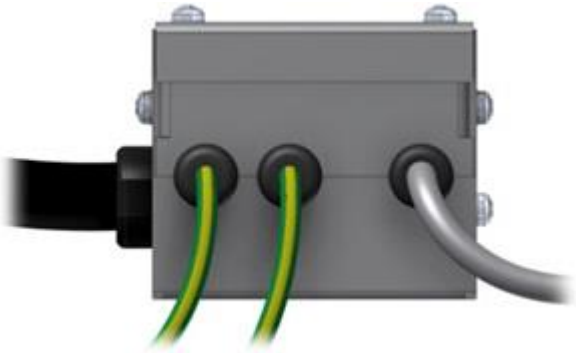
NOTE: For more details on the various PCB connections, please refer to the 8bit Control PCB Diagrams or 16bit I/O PCB layout section of the Traka32 Help Guide.

10. Insert the Battery into the base of the Pod and connect to the 8bit Control PCB or 16bit I/O PCB respectively.
11. Switch the On/Off switch on the 8bit Control PCB or 16bit I/O PCB to **On**.
12. You should hear a double beep and the LCD should light up and start to display text. If this does not happen then switch Off the On/Off switch and double check your connections.
13. Finally, close the Control Panel carefully into the Pod and lock with the Master Key.
14. The Control Panel should fit easily, if not check that no wires have become caught or trapped between the Control Panel and the Pod.
15. Please now refer to the Commissioning section.

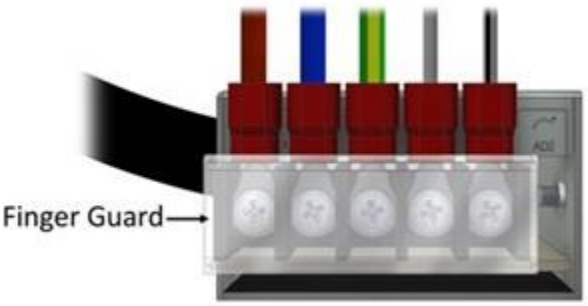
3.3.9 MAINS POWER SUPPLY & BATTERY INFORMATION

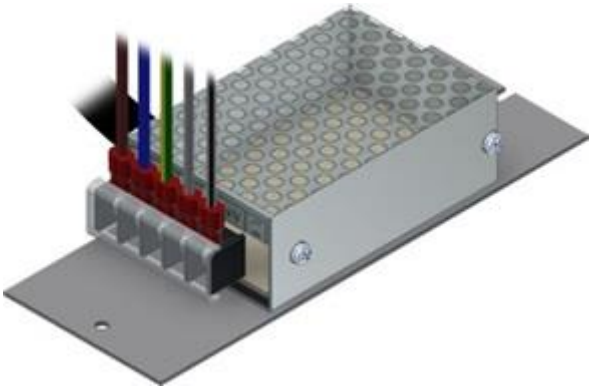
3.3.9.1 MAINS POWER SUPPLY ENCLOSURE

The Traka power supply is housed within a metal enclosure that ensures people cannot touch the live power terminals if they gain access to the systems electronics.



Older versions of the power supply aren't completely enclosed but do have a plastic guard covering the terminals as shown below.





3.3.9.2 CONNECTING THE MAINS POWER SUPPLY

GB - Traka Key Control and Intelligent Locker products are supplied without a plug and will need to be wired into a non-switched fused spur.

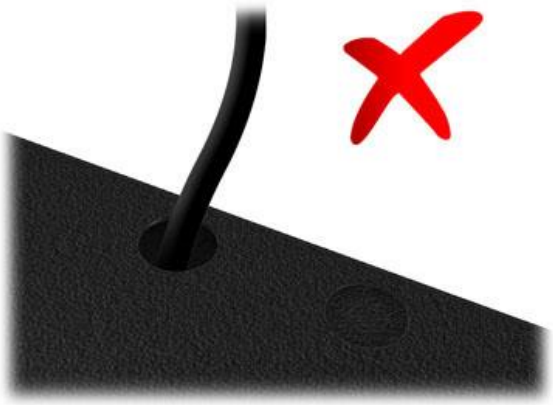
FR - Les armoires de gestion de clefs et les casiers intelligents sont fournis sans prise électrique, ils devront être raccordés à une boite de raccordement sans interrupteur et protégés par un fusible.

NOTE: Before wiring the Traka power supply mains lead into the non-switched fused spur, please ensure that the spur has been isolated at the main consumer unit or fuse box. If you have any doubt about connecting Traka to the mains power obtain expert advice before continuing.

The mains cord from the power supply will need to be fed through one of the knock out holes at the top or bottom of the control pod. It is important to use the rubber grommet provided to protect the cable from being cut by the metal work. The mains cable should also be run inside 20mm trunking to the non-switched fused mains spur.

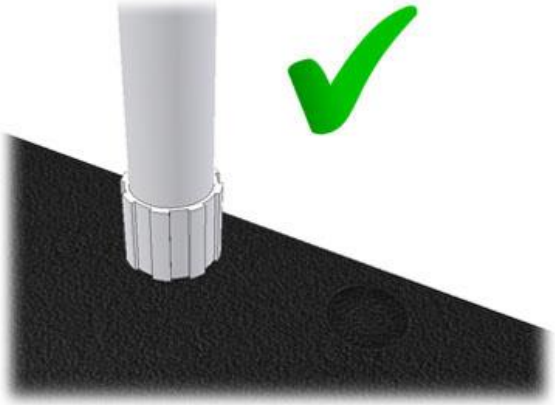
Incorrect

Mains cable run through a knock out without a cable gland or trunking.



Correct

Mains cable run through a knock out with a suitable cable gland and trunking.



NOTE: THIS APPLIANCE MUST BE EARTHED!

NOTE: The wires in this mains lead are coloured in accordance with the following code:

Green / Yellow:	Earth
Blue:	Neutral
Brown:	Live

If the coloured wires of the mains lead of this appliance do not correspond with the coloured markings identifying the terminals in your spur, proceed as follows:

- The wire which is coloured GREEN AND YELLOW must be connected to the terminal in the spur which is marked by the letter E or by the Earth symbol ⏚ or coloured GREEN or GREEN AND YELLOW.
- The wire which is coloured BLUE must be connected to the terminal in the spur marked with the letter N or coloured BLACK.
- The wire which is coloured BROWN must be connected to the terminal in the spur which is marked with the letter L or is coloured RED.

NOTE: A readily accessible mains disconnection device must be incorporated in the building installation wiring and this device must enable double pole disconnection and have a minimum of a 3mm contact gap. If you are installing the system outside of the United Kingdom or have any doubts about the installation, please contact Traka or a Qualified Electrician for mains wiring assistance.

3.3.9.3 BATTERY CONNECTION DETAILS

WARNING: All Traka Systems have two power sources, mains and battery. Before installing or servicing a Traka System, please ensure both mains and battery power sources are disconnected from the system.

This section will explain how to disconnect the battery from 8bit and 16bit systems.

Battery Disconnection

1. Open the control pod/panel of the system using the master key.
2. Locate the battery. Usually placed at the bottom of the control pod.
3. Disconnect the battery cable from the terminals as shown below.

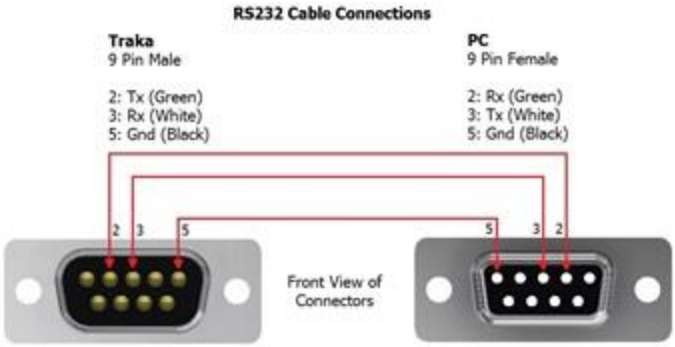
3.4 COMMUNICATION INSTALLATION

3.4.1 RS232 INSTALLATION

8bit RS232 Installation

1. Check that the jumper settings are set to **RS232** on the Control PCB. Please refer to the 8bit Control PCB Communication Jumper Settings section for details.

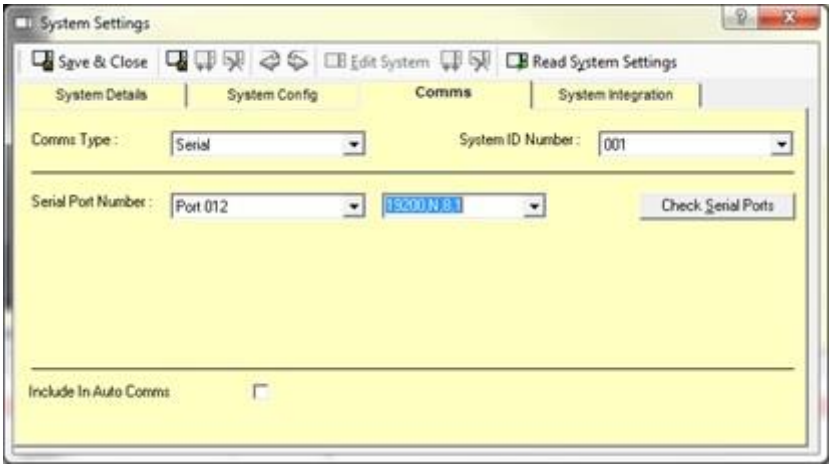
2. Simply use the RS232 cable (also known as serial cable) provided connecting the male end to the RS232 connector on the Traka Control PCB and the female end to an available serial port on the chosen PC. Please refer to the 8bit Control PCB Layout diagrams to locate the RS232 Connector.



3. In Traka32, right click on the Control Pod and select **Configure System**.

4. Select the **Comms** tab.

5. Select which serial port the RS232 cable is connected to on the PC and then specify the Baud Rate as **19200,N,8,1**.

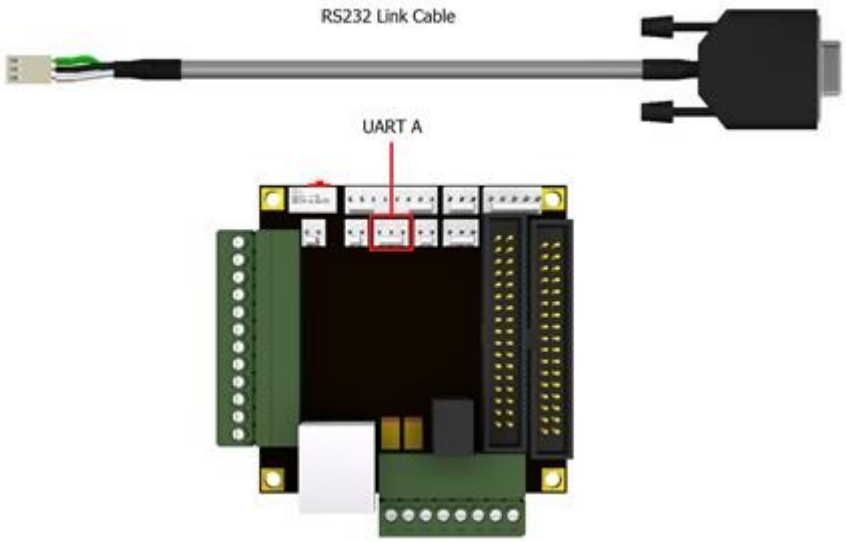


NOTE: The Baud Rate of 19200,N,8,1 is specified for Control PCBs fitted with a 7MHz Crystal. However, early versions of the 8bit Control PCB were fitted with a 3MHz Crystal. If your system is fitted with a 3MHz Crystal the Baud Rate must be set to 9600,N,8,1. To determine which Crystal is fitted to your PCB refer to the 8bit Control PCB Layout section.

6. Click **Save & Close**.

16bit RS232 Installation

1. Connect the supplied RS232 link cable to the UART A connector on the 16bit I/O PCB.

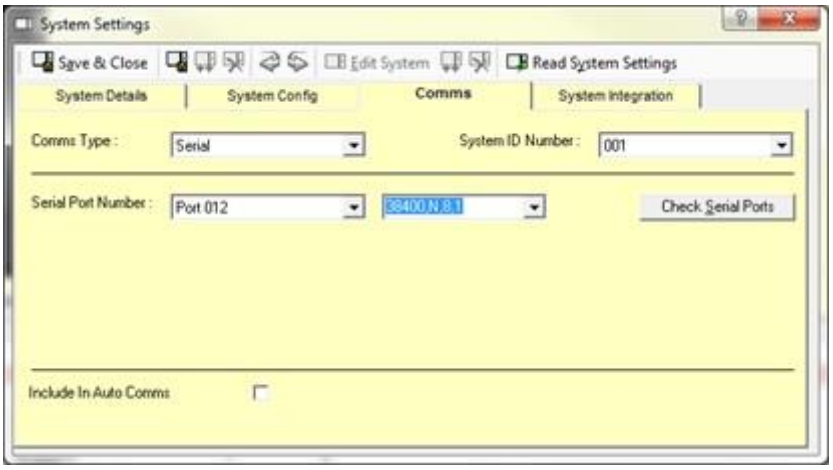


2. Using the supplied RS232 cable, connect the male end to the RS232 link cable, and the female end to an available serial port on the chosen PC.

3. In Traka32, right click on the Control Pod and select **Configure System**.

4. Select the **Comms** tab.

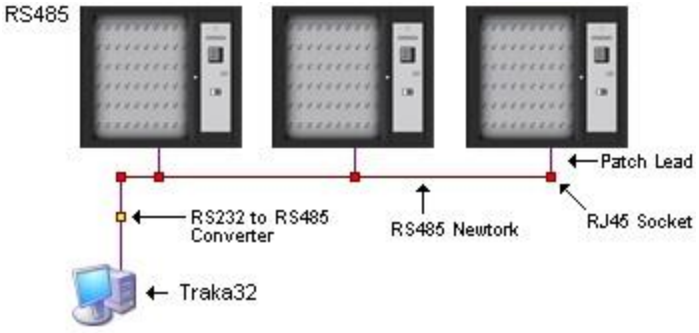
5. Select which serial port the RS232 cable is connected to on the PC and then specify the Baud Rate as **38400,N,8,1**.



6. Click **Save & Close**.

3.4.2 RS485 INSTALLATION

The main Traka network cable simply needs to run from the PC that controls the Traka network to each Traka in a daisy chain configuration...



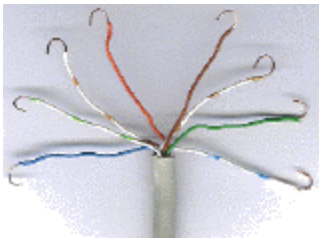
It is recommended that you install the RJ45 Wall ports behind the Traka Control Panels to prevent anyone from tampering with the connections. The Cat 5 cable should not span more than 500 metres in length and should not run alongside power cables.

Running the RS485 Cable

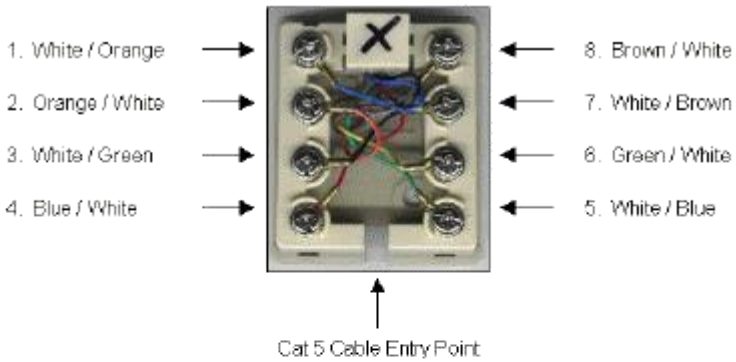
1. Run the Cat 5 UTP cable from the PC to the first Traka system in the chain leaving approximately 1 metre spare at each end.
2. Run additional lengths of Cat 5 UTP between the first Traka system and the next and do this for all additional Traka systems.
3. Attach the Wall Port to the wall behind the Control Panel at any convenient height so that the RJ45 socket faces upward, using the double-sided sticky pad or screws provided.

RJ45 Wall Port Connection

1. Strip 50mm of outer insulation at each end of the Cat 5 cable.
2. Untwist each pair and strip 5mm of each of the inner insulation.
3. Using a screwdriver, bend each copper end of the cables into a hook shape.



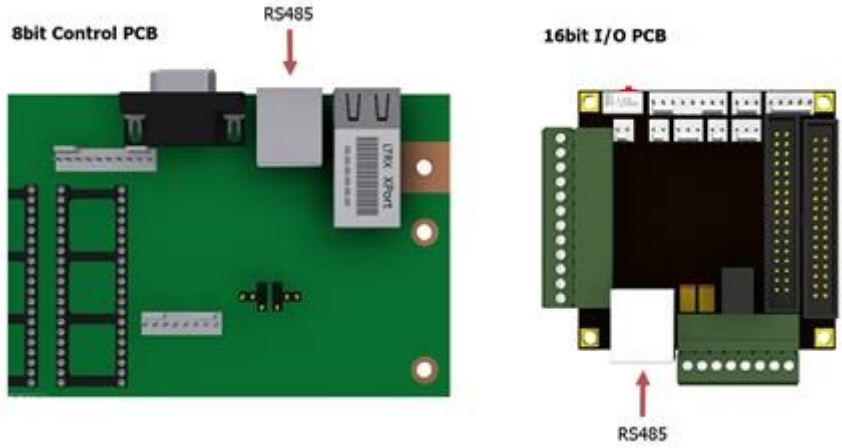
4. Connect as follows...



5. When all the connections are made, place the cover over the RJ45 Wall Port and connect the Traka and PC Patch Cables. Refer to the Configuration and Connection section below.

Configuration and Connection

1. Please refer to the Anti Static Precautions before configuring the Traka systems.
2. Using the Master Key, unlock the Control Panel and tilt forward to access the Control PCB.
3. Ensure the On/Off Switch on the Control PCB is set to **Off**. Refer to the 8bit Control PCB Layout or 16bit I/O PCB Layout diagrams to locate the On/Off Switch.
4. Connect the supplied patch cable between the RJ45 Wall Port and the RS485 Connector on the Control PCB. The diagram below shows the location of the RS485 Connector for both 8bit and 16bit systems.



5. If your system is 8bit the Comms Select jumper settings must be set to **RS485**. Refer to the 8bit Control PCB Communication Jumper Settings.
6. Switch the On/Off Switch on the Control PCB to **On**.
7. Finally, close the Control Panel carefully and lock with the Master Key.

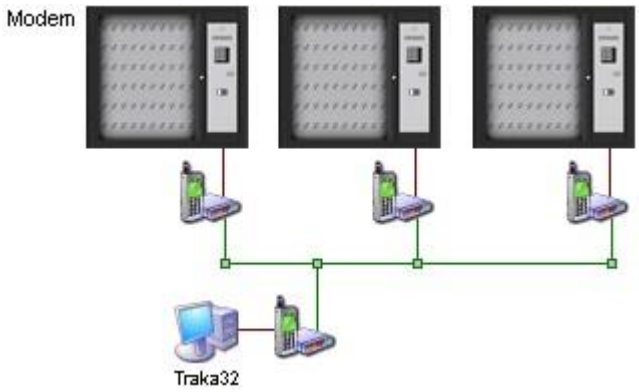
KK Systems K2 Converter DIP Switch Settings

Here are the default DIP Switch settings used on the KK Systems K2 RS-232 to RS-485 converter used on the cable connecting the PC to the RS485 network:

- K2 Off
- RXEN **On**
- TXEN **On**
- - Off
- - Off
- - Off
- OPT Off

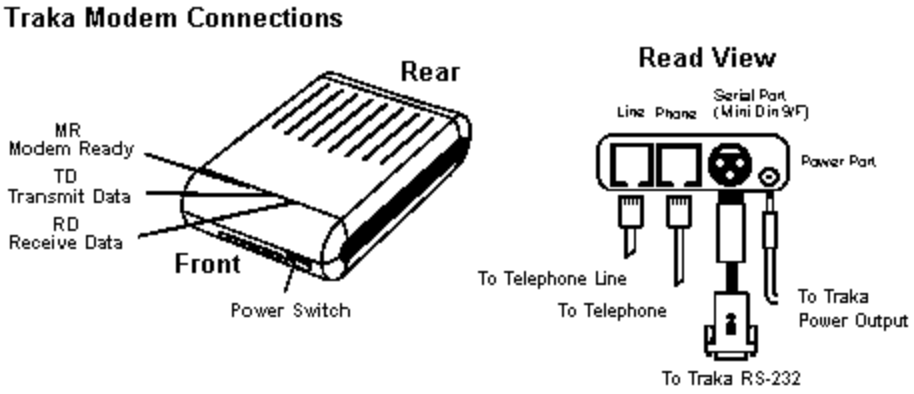
3.4.3 MODEM INSTALLATION

When using a modem with Traka you will require a Modem in each Traka system and one connected to your PC.

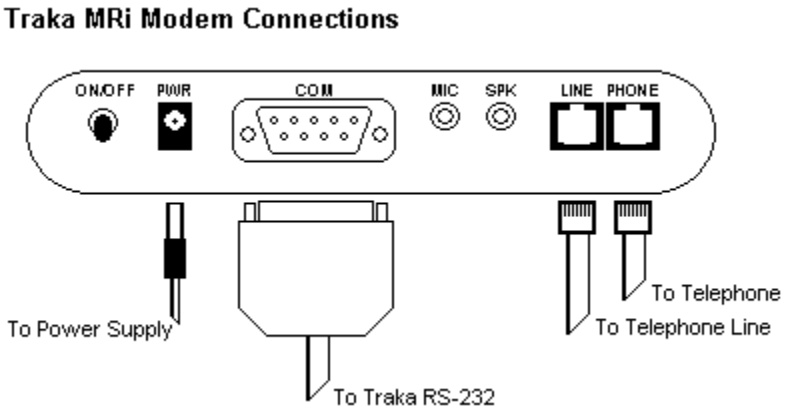


To install a modem in Traka please follow the instructions below. To attach a modem to your PC, please refer to the user guide supplied with your modem.

1. Please refer to the Anti Static Precautions before configuring the Traka systems.
2. Using the Master Key, unlock the Control Panel and tilt forward to gain access to the system electronics.
3. Ensure the On/Off Switch on the Control PCB is set to **Off**. Refer to the 8bit Control PCB Layout or 16bit I/O PCB Layout diagrams to locate the On/Off Switch.
4. Please refer to the following diagrams on how to connect the modem…



or…



5. Fit the modem behind the Control Panel of the Traka system, feeding the Modem Telephone Lead out through any of the cable knockout holes on the Pod/cabinet and connect to an Approved British Telecom Telephone Socket.

6. If your system is 8bit, ensure the jumper settings are set to **RS232** on the Control PCB. Refer to the 8bit Control PCB Communication Jumper Settings.

7. Connect the Serial Lead between the Modem Serial Port and the Traka RS232 Port.

8. Connect the Power Lead from the Modem Power Port to the Power Output connector on the Traka Control PCB or to an external power source depending on the modem type. Refer to the 8bit Control PCB Layout and 16bit I/O PCB Layout diagrams for details on the available power output connections.

9. Make sure the Modem Power Switch is switched **On** (Depressed).

10. Switch the On/Off Switch on the Control PCB to **On**.

11. Hold down the **0** key on the keypad. At the same time press and release the **Reset** button on the Control PCB. This will configure the modem with the correct communications settings and to auto answer.

12. When you release the Reset button you should hear **two beeps followed by a double beep**, this means the modem is configured successfully.

13. If you **hear two beeps followed by an error beep** then the modem did not configure correctly, re-check your connections and try again.

'Fail A' means the modem returned some unexpected data and '**Fail B**' or '**Fail C**' means the modem did not return anything at all. Check that the modem is connected correctly and power is present and the modem is switched on.

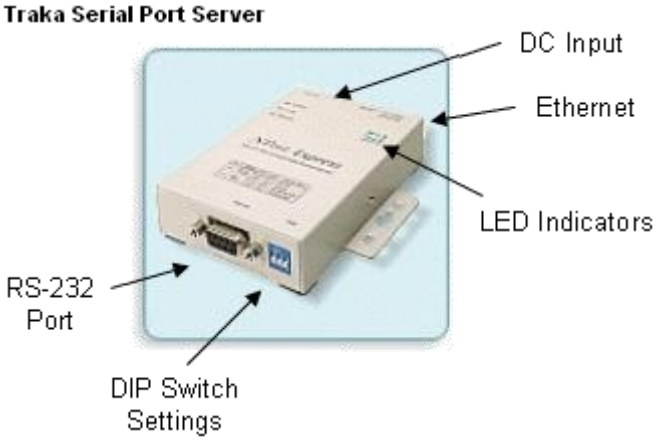
14. Finally, close the Control Panel carefully and lock with the Master Key.

3.4.4 ETHERNET INSTALLATION

3.4.4.1 MOXA

3.4.4.1.1 MOXA INSTALLATION

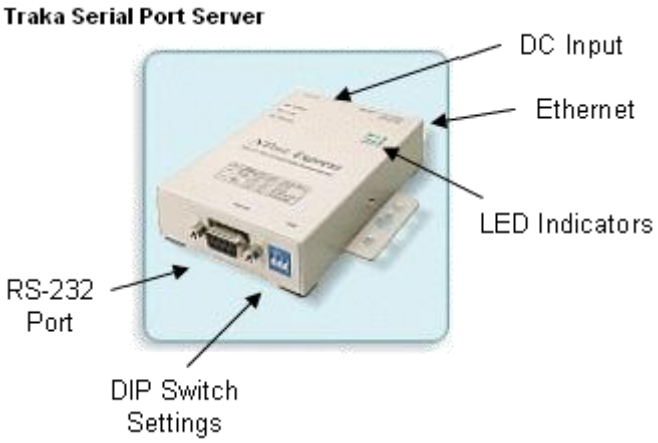
In order to set up and configure the Traka Moxa Ethernet Device (TMED) you must first connect them to the network and Traka.



1. Please refer to the Anti Static Precautions before configuring the Traka systems.
2. Using the Master Key, unlock the Control Panel and tilt forward to gain access to the system electronics.
3. Ensure the On/Off Switch on the Control PCB is set to **Off**. Refer to the 8bit Control PCB Layout or 16bit I/O PCB Layout diagrams to locate the On/Off Switch.
4. If your system is 8bit, ensure the jumper settings are set to **RS232** on the Control PCB. Refer to the 8bit Control PCB Communication Jumper Settings.
5. Fit the TMED behind the Control Panel of the Traka system, feeding the Patch Lead out through any of the cable knockout holes on the Pod/cabinet.
6. Connect the RS232 Port of the TMED to the RS232 Port of the Traka system using the cable provided.
7. Connect the **10/100M Ethernet Port** of the TMED to your Ethernet using a straight-through Ethernet cable. In some cases a cross-over cable may be required.
8. Connect the **DC-IN** of the TMED to the Power Output connector on the Traka Control PCB using the cable provided. Refer to the 8bit Control PCB Layout and 16bit I/O PCB Layout diagrams for details on the available power output connections.
9. Switch the On/Off Switch on the Control PCB to **On**.
10. Check that the **PWR** and **Link** lights are both **On**. If the PWR light is not on then re-check your connections. If the Link light is not on then re-check your connections and ensure that the network port that you have connected the TMED to is patched in correctly.
11. Close the Control Panel carefully and lock with the Master Key.
12. Now refer to the configuration section.

3.4.4.1.2 MOXA CONFIGURATION

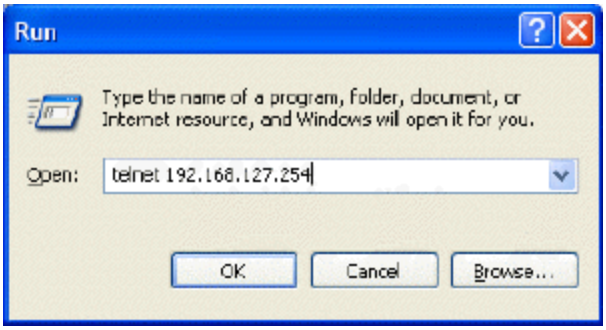
Before configuring a Traka Moxa Ethernet Device (TMED) you will need to obtain certain information from your Network Administrator. Please refer to the planning section for details.



Once you have obtained the configuration details you can configure the TMED. The TMED cannot be set up through the Traka32 software and has to be configured either by using Telnet or Moxa PComm Terminal Emulator. If you are not experienced with networks we suggest you ask your Network Administrator or Local Traka Engineer to set up the TMED.

Using Telnet

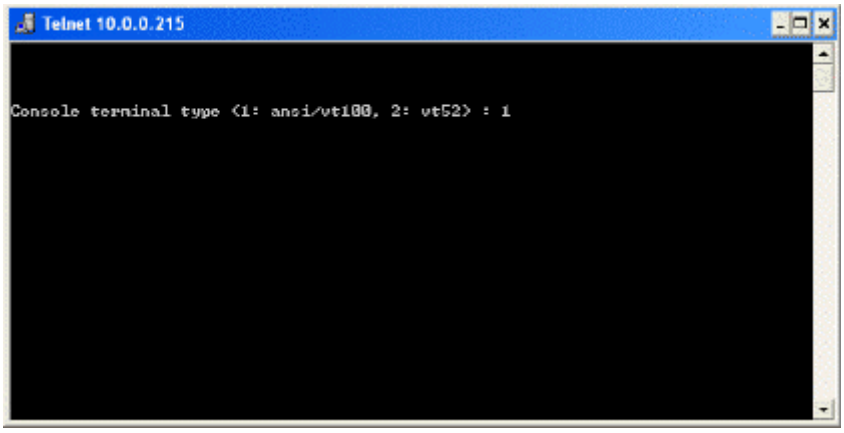
1. Check that the DIP Switch Settings on the TMED are all set to **Off**.
2. Check that the **PWR** and **Link** lights are both **On**. If the PWR light is not on then re-check your connections. If the Link light is not on then re-check your connections and ensure that the network port that you have connected the TMED to is patched in correctly.
3. From a workstation that is connected to the same network, click on **Run** from the Start button and the following window will appear...



In order to establish an initial connection with the TMED you must first telnet to the device using its default IP Address. The default IP Address can be found on the under side of the TMED. In the example this is **192.168.127.254.**

Type **telnet 192.168.127.254** followed by **Enter**.

4. When the Telnet window opens, using the keyboard type **1** followed by **Enter** to select ansi/vt100.



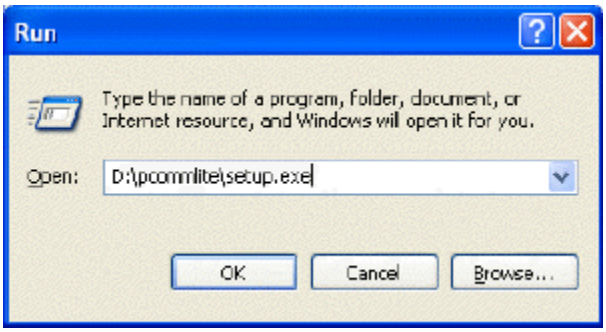
Please note, if the following text "Console terminal type (1: ansi/vt100, 2: vt52) : 1" does not appear on the screen then check the default IP Address is within range of the IP Address that you are running telnet from. The default subnet mask of the TMED is 255.255.255.0 with no gateway.

5. Next refer to the configuration section later in this topic.

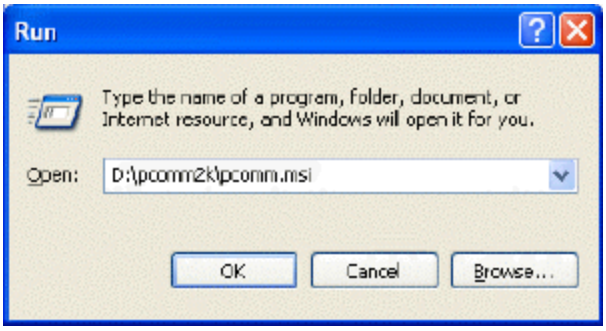
Using Moxa PComm Terminal Emulator

Before you begin you will need to have a PC in close proximity to the TMED and a fully connected 9-Pin Male to 9-Pin Female Serial Cable or fully connected 9-Pin Male to 25-Pin Female Serial Cable depending on your PC.

1. Please refer to the Anti Static Precautions before configuring the Traka systems.
2. Load the Moxa Software CD into your CD-ROM drive.
3. If your operating system is Windows 9x or NT run the Setup.exe on the CD located in the pcommlite directory e.g. D:\pcommlite\Setup.exe

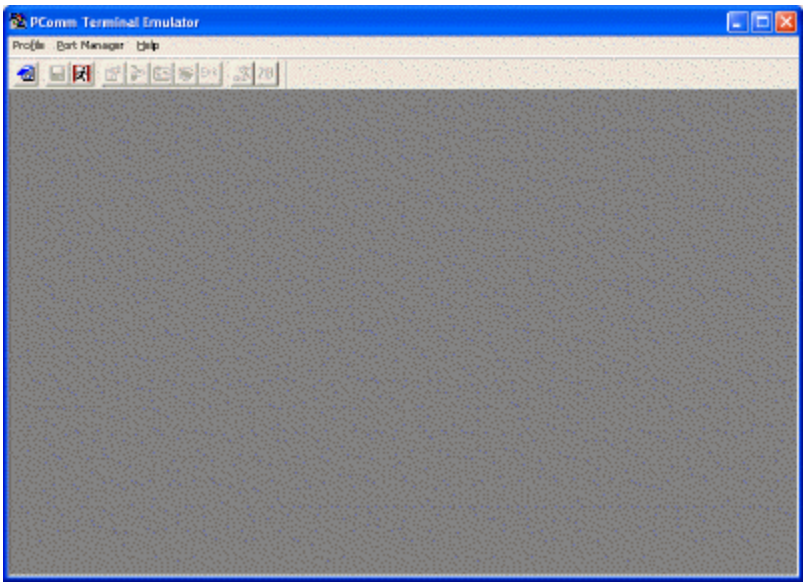


If your operating system is Windows 2000 run the pcomm.msi on the CD located in the pcomm2k directory e.g. D:\pcomm2k\pcomm.msi



4. Follow the on screen instructions.

5. Once installed, click on **Start>Programs>PComm Lite 2.5>Terminal Emulator**.



6. Using the Master Key, unlock the Control Panel and tilt forward to gain access to the system electronics.

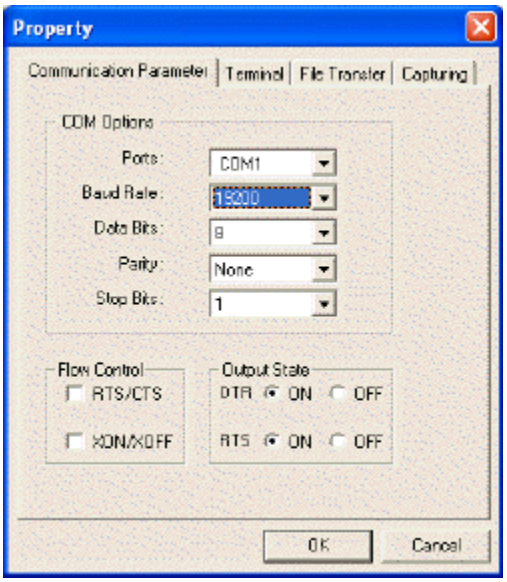
7. Disconnect the Traka from the RS232 Port of the TMED.

8. Connect the RS232 Port of the TMED to a spare RS232 Port on your PC using a 9-Pin Male to 9-Pin Female Serial Cable or 9-Pin Male to 25-Pin Female Serial Cable depending on your PC.

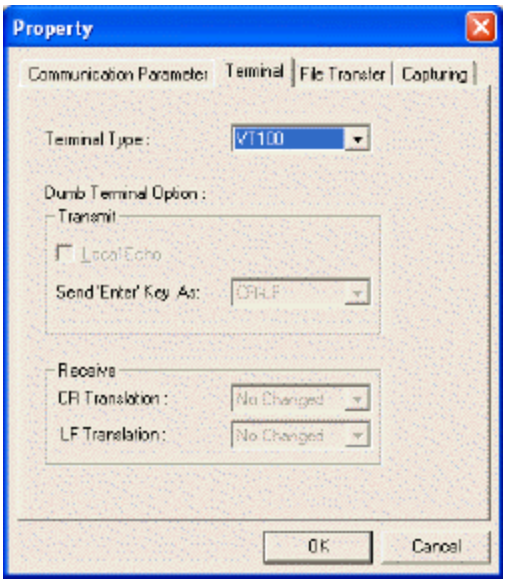
9. Check that the **DIP Switch Setting SW1** on the TMED is set to **On**.

10. Using the **PComm Terminal Emulator**, click on the **Port Manager** menu and then click on the **Open** icon.

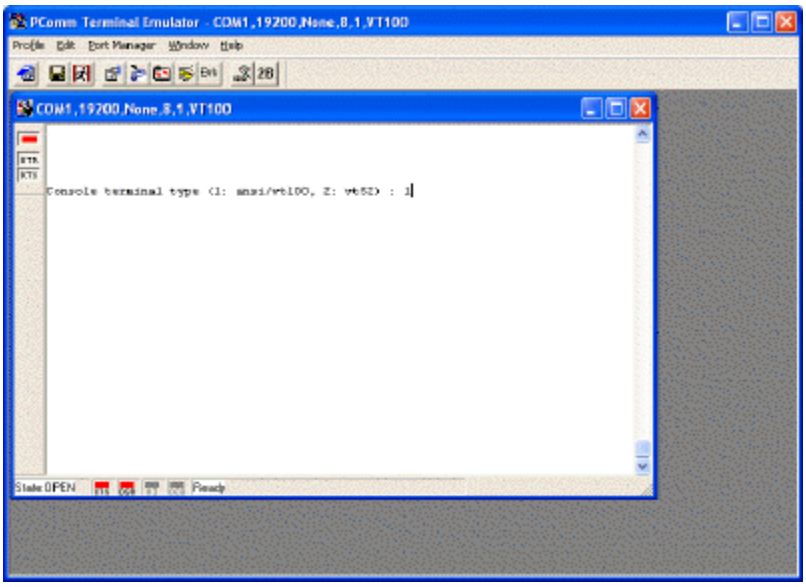
11. From the **Property** window's **Communication Parameter** page, select the appropriate **COM Port** for the connection e.g. COM1 and set the **Baud Rate** to **19200**.



12. From the **Property** window's **Terminal** page, select set the **Terminal Type** to **VT100**.



13. Again from the **Property** window, click on **OK** and after a few seconds the following screen should appear...

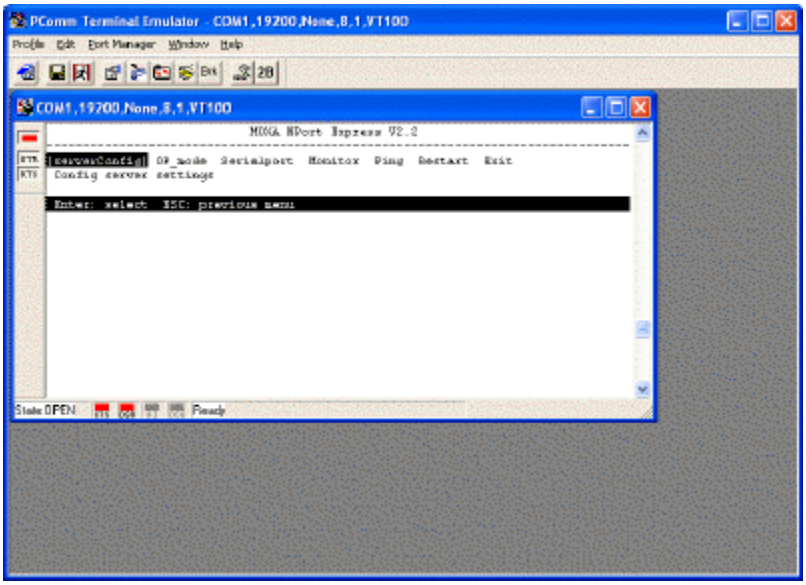


Please note, if the following text "Console terminal type (1: ansi/vt100, 2: vt52) : 1" does not appear on the screen then try powering down the TMED, waiting 5 seconds and powering back up again.

14. Next refer to the configuration section below.

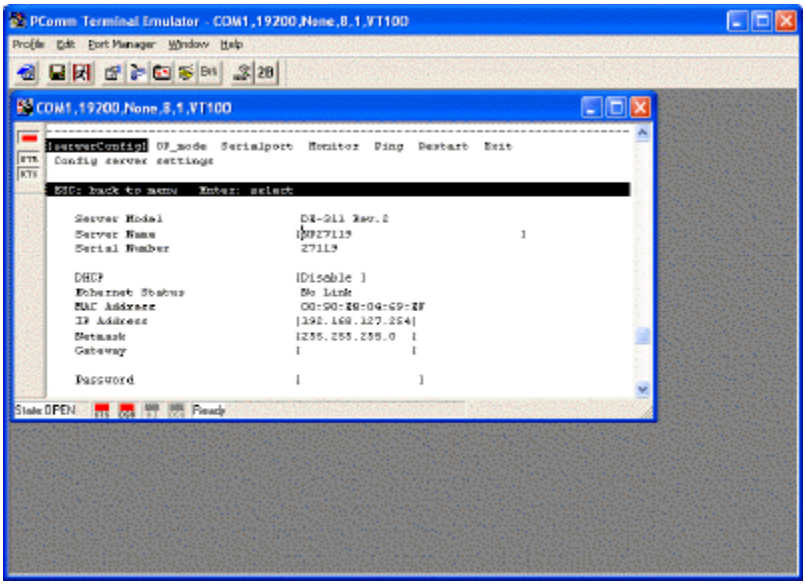
Configuration

1. Use the keyboard arrow keys to highlight **[serverConfig]** and press **Enter**.



If you are using telnet from Windows 9x and you cannot use the arrow keys, click on **Terminal** followed **Preferences** and set the **VT100 Arrows** option.

2. Using the keyboard set the following options...



   a. DHCP [Disable] (press enter to select options)

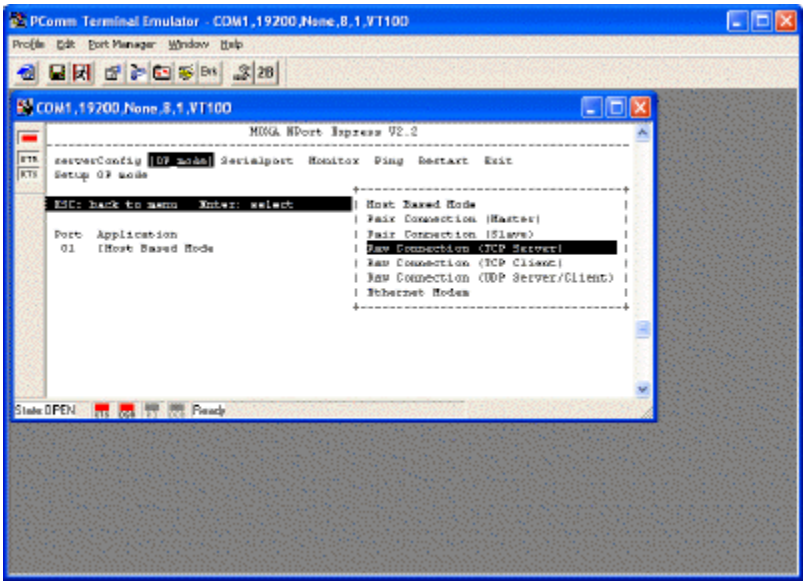
   b. IP Address [enter your IP Address here] (press space to clear unwanted text)

   c. Netmask [enter your Subnet Mask here]

   d. Gateway [enter your Default Gateway here]

3. When complete press **Esc** to return to the top menu.

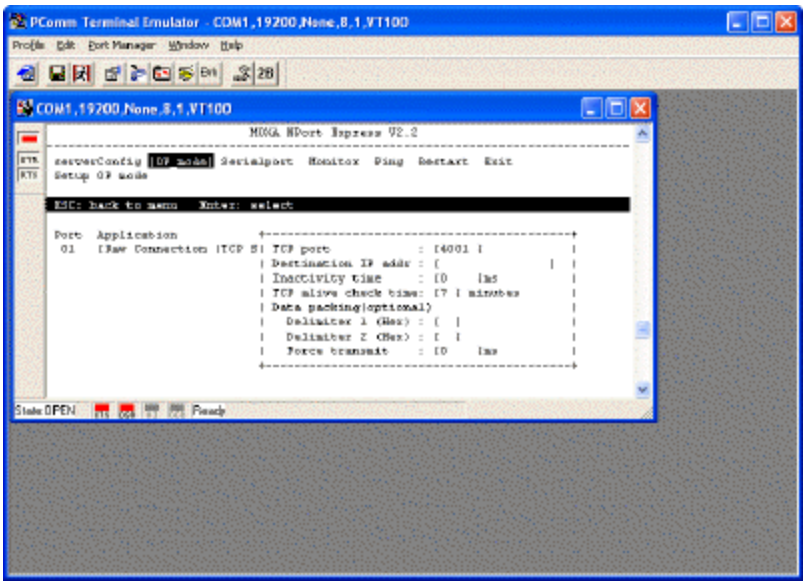
4. Use the keyboard arrow keys to highlight **[OP_Mode]** and press **Enter**.



5. Using the keyboard set the following options...

    a. Application [Raw Connection (TCP Server)] *press enter to select options*

6. Using the keyboard highlight **[Select for more settings]** and press **Enter**.

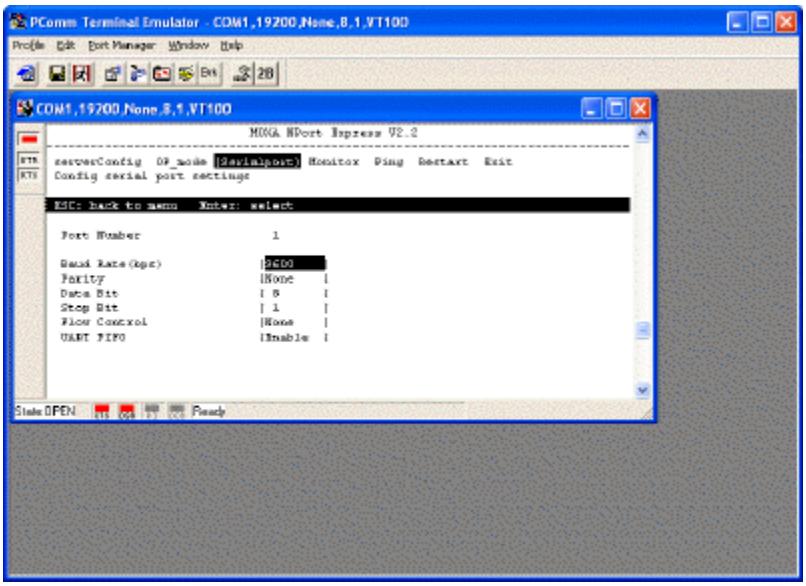


7. Using the keyboard set the following options...

    a. Make a note of the **TCP Port** number, as you need this to configure Traka32. It is usually **4001** but you can alter this if required.

8. When complete press **Esc** to return to the top menu.

9. Use the keyboard arrow keys to highlight **[Serialport]** and press **Enter**.



10. Using the keyboard set the following options...

    a. Baud Rate [9600] or [19200]

       Set [9600] if the Control PCB is fitted with a 3MHz crystal or set [19200] if the Control PCB is fitted with a 7MHz crystal. Please refer to the Control PCB Diagrams to locate the crystal type.

    b. Parity [None]

    c. Data Bit [8]

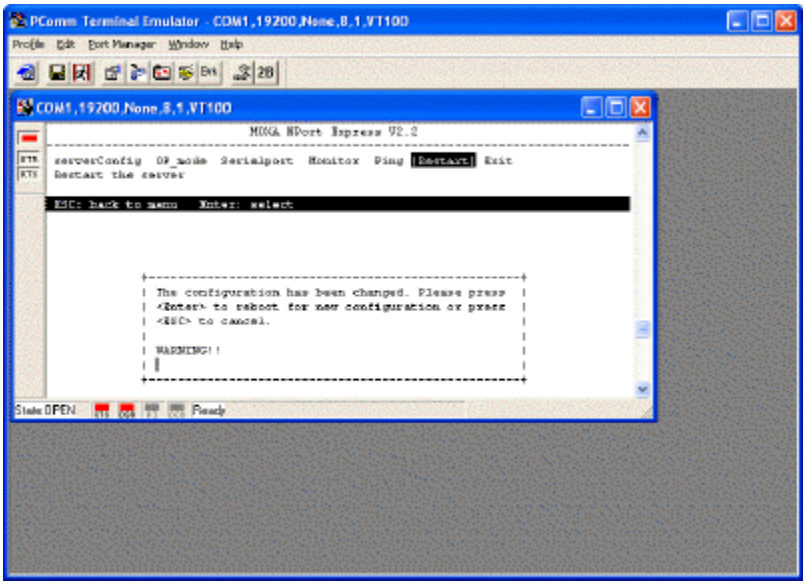
    d. Stop Bit [1]

    e. Flow Control [None]

    f. UART FIFO [Enable]

11. When complete press **Esc** to return to the top menu.

12. When you are happy the configuration is correct, use the keyboard arrow keys to highlight **[Restart]** and press **Enter.**



13. Press **Enter** again to confirm your changes.
14. Disconnect the TMED from your PC and re-connect to the Traka System.
15. Check that the **DIP Switch Settings** on the TMED are all set to **Off**.
16. Finally, close the Control Panel carefully and lock with the Master Key.

3.4.4.1.3 MOXA DIP SWITCH SETTINGS

SW1	SERIAL CONNECTION	SW2	SW3	INTERFACE MODE
ON	RS232 CONSOLE	-	-	-
OFF	DATA COMM	OFF	OFF	RS232
		OFF	ON	RS485
		ON	OFF	RS485 BY RTS
		ON	ON	RS485 BY ADDC

3.4.4.1.4 MOXA LED INDICATORS

LED NAME	LED FUNCTION
PWR	Red indicates that the power is on
Link	Orange indicates a 10Mbps Ethernet connection Green indicates a 100Mbps Ethernet connection
Ready	Green indicates SPS system is ready

3.4.4.2 XPORT

3.4.4.2.1 XPORT CONNECTIVITY & BANDWIDTH

Protocol: TCP/IP

Connectivity: 10/100Mb/s Auto Sense

IP Address: Static and must be supplied by the customer.

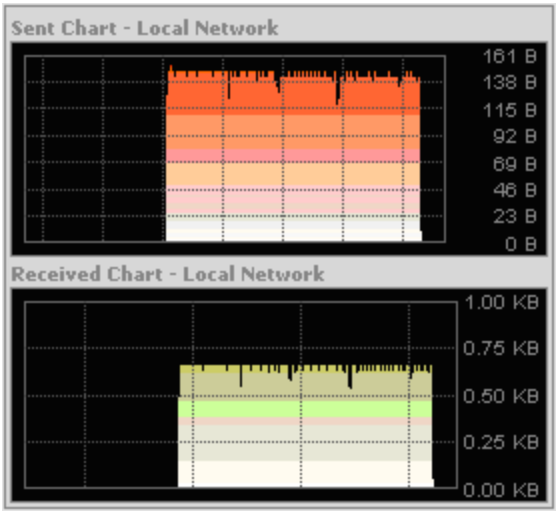
Port: The default is 10001 but can be changed as required.

NOTE: When using with the Remote Host option, each Traka System must use a different port number e.g. 10001, 10002, 10003 etc. Port 9999 is also used for configuration of the Traka Systems network adaptor but is not used day to day.

Bandwidth:

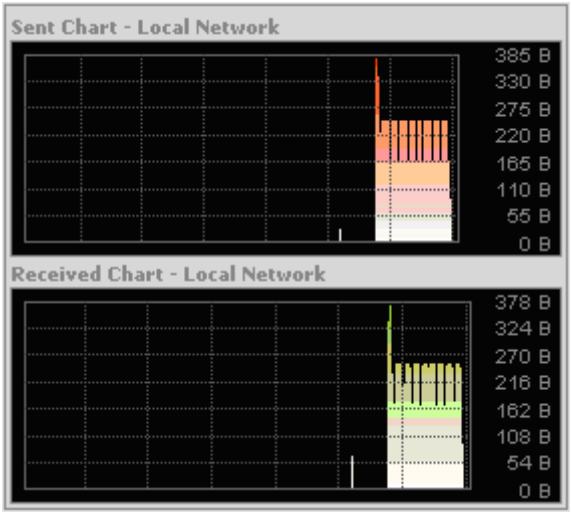
Read All System Data

This is the most common communication averaging 670 bytes per second. The graph shows the downloading of 2000 events which takes around 2 minutes.



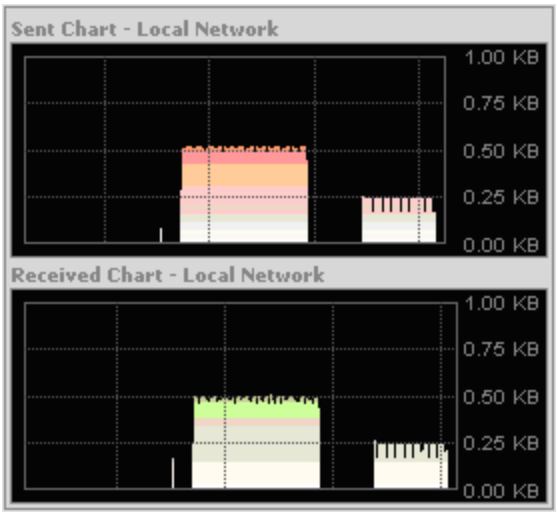
Synchronise System

Peak 384 bytes per second and then averaging down to 245 bytes per second when synchronising iFob and User records. The graph shows the uploading of 60 iFob and 100 user records and takes approximately 1 minute.



Firmware Upgrade

Peak 525 bytes per second and averaging down to 245 bytes per second when synchronising iFobs and User records.



3.4.4.2.2 XPORT INSTALLATION

The Traka XPort Ethernet Device (TXED) is an optional device that comes pre-installed on Control PCBs. If the device is not fitted, please contact Traka for advice.

In order to set up and configure the TXED you must first connect them to the network.

1. Please refer to the Anti Static Precautions before configuring the Traka systems.
2. Using the Master Key, unlock the Control Panel and tilt forward to gain access to the system electronics.
3. Set the On/Off switch on the Control PCB to **Off**.
4. If your system is 8bit, ensure the jumper settings are set to **Ethernet** on the Control PCB. Refer to the 8bit Control PCB Communication Jumper Settings.
5. Connect the **TXED** to your Ethernet using a straight-through Ethernet cable. In some cases a cross-over cable may be required.
6. Set the On/Off switch on the Control PCB to **On**.
7. Check that there is LED activity. If there is no activity, re-check your connections to the Control PCB, Wall Port, Patch Panels and Switch/Hub. For details of the LED indicators and their meanings refer to the XPort LED Indicators section.
8. Close the Control Panel carefully and lock with the Master Key.
9. Now refer to the Configuration section.

3.4.4.2.3 XPORT CONFIGURATION

Before configuring a Traka XPort Ethernet Device (TXED) you will need to obtain certain information from your Network Administrator. Please refer to the planning section for details.

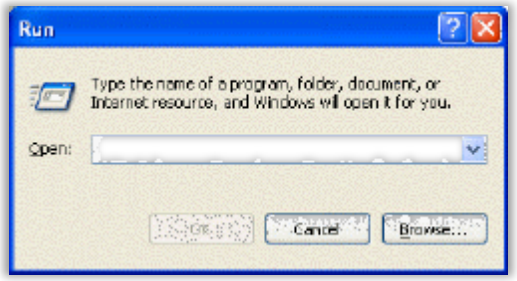
Once you have obtained the configuration details you can configure the TXED. The TXED can either be configured using Telnet or using the Diagnostics Tool within Traka32. If you are not experienced with networks we suggest you ask your Network Administrator or Local Traka Engineer to set up the TXED.

Using Telnet

NOTE: Windows Vista operating system does not have the Telnet client installed by default. Please refer to Installing Telnet on Windows Vista if using this operating system and have not already installed Telnet.

1. Check that there is LED activity on the device. If there is no activity, check that there is power to the Control PCB and that it is switched on and re-check your connections to the Control PCB, Wall Port, Patch Panels and Ethernet Switch Hub.

2. From a workstation that is connected to the network click on **Start**, **Run** and the following window will appear…



In order to establish an initial connection with the device we must use the ARP method to create an entry in the hosts ARP table. To do this, type the following in the Run window and click on **OK**…

arp -s IP-Address MAC-Address

The IP-Address is provided by your Network Administrator and the MAC-Address is printed on the label attached to the device as shown.

For example if you wanted to assign an IP-Address of **10.0.0.254** to a device with an MAC-Address of **00-20-4A-80-2C-A8**, then I would type the following in the Run window and click on OK…

arp -s 10.0.0.254 00-20-4A-80-2C-A8

3. Now we Telnet to the device using port 1 to create a temporary connection. To do this, again click on **Start**, **Run**, type the following and click on **OK**…

telnet IP-Address 1

Following the above example you would type…

telnet 10.0.0.254 1

NOTE: This temporary connection will fail quickly, but the device will temporarily change its IP Address to the one designated.

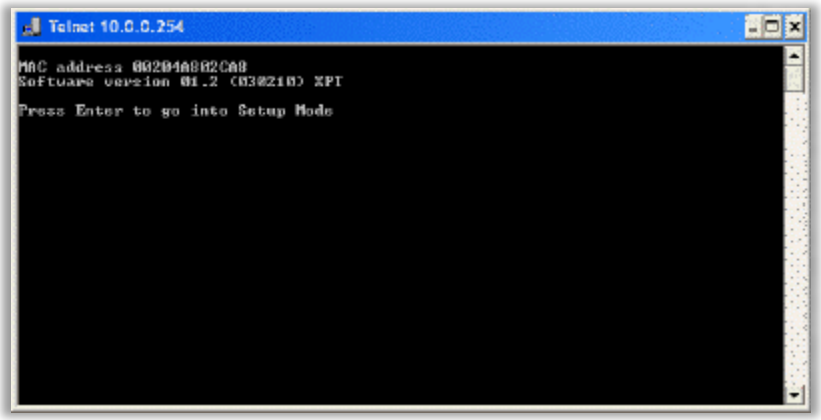
4. Finally we Telnet to the device using port 9999 enabling us to configure. To do this, again click on **Start**, **Run**, type the following and click on **OK**…

   telnet IP-Address 9999

   Again, following the above example you would type…

   telnet 10.0.0.254 9999

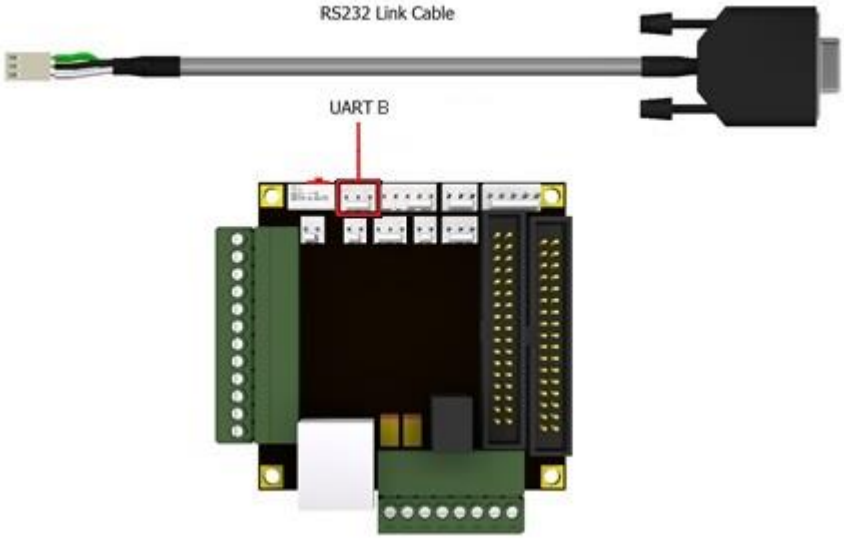
   When the following window appears, press **Enter** quickly to go into the Setup mode…



5. Now refer to the Configuration later in this topic.

Using Traka32 Diagnostics

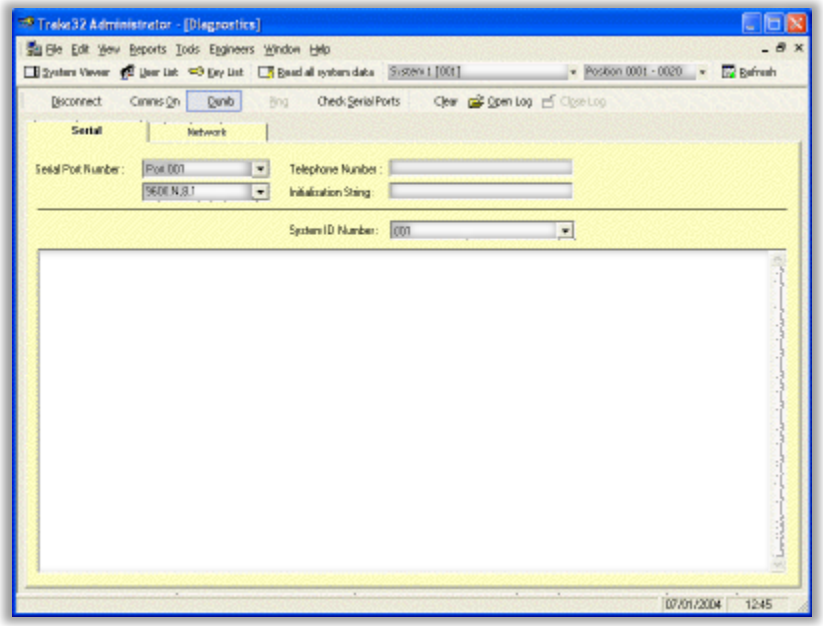
1. Please refer to the Anti Static Precautions before configuring the Traka systems.
2. Using the Master Key, unlock the Control Panel and tilt forward to gain access to the system electronics.
3. Set the On/Off switch on the Control PCB to **Off**.
4. If your system is 8bit, ensure the jumper settings are set to **Ethernet Config** on the Control PCB. Refer to the 8bit Control PCB Communication Jumper Settings. The 16-bit Control PCB auto-detects the communications method so no jumper settings are required to be configured.
5. Using an RS232 cable (also know as serial cable) connect the **Male End** to the RS232 connector on the Control PCB and the **Female End** to an available serial port on the chosen **PC**.
   - The **8-bit Control PCB** has a 9 pin D-Type (female) RS232 connector for connecting the RS232 cable to.
   - The **16-bit Control PCB** is supplied with a short 3 pin Molex to 9-pin D-Type (female) cable for connecting an RS232 cable to. This connects to **UART B** on the 16-bit I/O PCB.



6. Open the Traka32 software by double clicking on the  icon.

7. If you are prompted for a login, please login as an **Engineer**. Please refer to the Engineers section for further details.

8. Click on the **Engineers** menu followed by **Diagnostics**.



9. Click on the **Serial** tab, if not already selected.

10. Select the appropriate **Serial Port**.

11. Do one of the following depending on your hardware...

    - For an **8-bit Control PCB,** set the **Serial Port Settings** to **9600,N,8,1.**
    - For a **16-bit Control PCB,** set the **Serial Port Settings** to **38400,N,8,1**.

12. Click on the **Traka** toolbar button to toggle it to **Dumb**.

13. Click on the **Connect** button, this will open the serial or network port.

    (Note that if successful the Connect button changes to Disconnect)

14. Click the cursor into the main text box where `Communication Off` is usually displayed.

15. Select one of the following procedures depending on your hardware...

    - **8-bit Control PCB**

        a. Make sure Caps Lock is Off.

        b. Click on the **Clear** button to clear the screen below.

        c. Hold down the **X** key on the PC keyboard and set the On/Off switch on the 8-bit Control PCB to **On.**

        d. The following information should appear within a couple of seconds

        ```
        MAC address 00204A802CA8
        Software version 01.2 (030210) XPT
        Press Enter to go into Setup Mode
        ```

        e. Press **Enter** quickly to go into the Set-up mode.

        f. Now refer to the Configuration section further below.

        g. When complete, close the Diagnostics window in Traka32.

        h. Disconnect the RS232 cable.

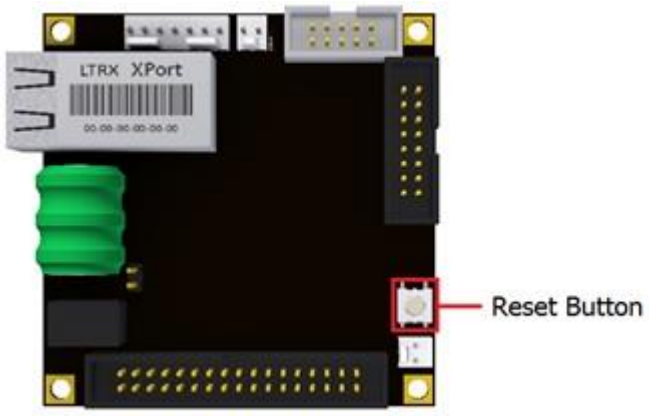
        i. Set the jumper settings on the 8-bit Control PCB to **Ethernet**. Please refer to the Communications section for details of the jumper settings.

        j. Finally, close the Control Panel carefully and lock with the Master Key.

    - **16-bit Control PCB**

        The 16-bit Control PCB needs to be placed in XPort mode from the Setup Menu. To do this...

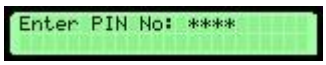
        a. Press and hold the Reset Button on the 16bit Control PCB, then press and hold the '#' key on the Keypad.

        b. Keeping hold the '#' key, release the Reset Button and the following message will appear...

c. Release the '#' key and you will be asked to enter a PIN No. The PIN No. is the last 4 digits of the system serial number.

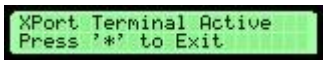


d. Enter the PIN No. and press '#'. You will then see the Setup Menu..

e. Press the '1' key for System.

f. Press the '3' key for Comms.

g. Press the '4' key to Enter the XPort Terminal...



h. On the PC screen the following should appear within a couple of seconds...

```
MAC address 00204A802CA8
Software version 01.2 (030210) XPT
Press Enter to go into Setup Mode
```

NOTE: Unlike the 8-bit Control PCB, there is no need to press X or Enter as the 16-bit Control PCB will do this automatically.

i. Now refer to the Configuration section below.

j. When complete, close the Diagnostics window in Traka32.

k. Disconnect the RS232 cable.

l. Press '*' on the keypad to exit the XPort terminal.

m. Press '*' 3 more times to exit the Setup Menu.

n. Finally, close the Control Panel carefully and lock with the Master Key.

Configuration

When entering the configuration menu, the following summary will be displayed…

1.
```
MAC address 00204A802CA8
Software version 01.2 (030210) XPT

Press Enter to go into Setup Mode

*** basic parameters
Hardware: Ethernet TPI
IP addr 0.0.0.0, no gateway set

*************** Security ***************
SNMP is enabled
SNMP Community Name: public
Telnet Setup is enabled
TFTP Download is enabled
Port 77FEh is enabled
Web Server is enabled
ECHO is disabled
Enhanced Password is disabled

*************** Channel 1 **************
Baudrate 19200, I/F Mode 4C, Flow 00
Port 10001
Remote IP Adr: --- none ---, Port 00000
```

```
Connect Mode : C0 Disconn Mode: 00
Flush Mode : 00

************** Expert *****************
TCP Keepalive : 45s
ARP cache timeout: 600s

************** E-mail *****************
Mail server: 0.0.0.0
Unit :
Domain :
Recipient 1:
Recipient 2:

*** Trigger 1
Serial Sequence: 00,00
CP1: X
CP2: X
CP3: X
Message :
Priority: L
Min. notification interval: 0 s
Re-notification interval : 0 s

*** Trigger 2
Serial Sequence: 00,00
CP1: X
CP2: X
CP3: X
Message :
Priority: L
Min. notification interval: 0 s
Re-notification interval : 0 s

*** Trigger 3
Serial Sequence: 00,00
CP1: X
CP2: X
CP3: X
Message :
Priority: L
Min. notification interval: 0 s
Re-notification interval : 0 s

Change Setup:
0 Server configuration
1 Channel 1 configuration
3 E-mail settings
5 Expert settings
6 Security
7 Factory defaults
8 Exit without save
9 Save and exit Your choice ?
```

1. Type **0** (Server configuration) followed by **Enter**.

2. Type each part of the IP Address followed by **Enter**. If you do not want to change a value, just press **Enter** to skip.

   ```
   IP Address : (000) 10.(000) 0.(000) 0.(000) 254
   ```

3. If you wish to configure a Gateway, type **Y** and type each part of the Gateway Address followed by **Enter**, otherwise type **N**.

   ```
   Set Gateway IP Address (N) Y
   Gateway IP addr (000) 10.(000) 0.(000) 0.(000) 201
   ```

4. Select the appropriate subnet mask from the following table and type the corresponding number of **Host Bits** followed by **Enter.**

   Standard IP Network Netmasks…

Network Class	Network Bits	Host Bits	Netmask
A	8	24	255.0
B	16	16	255.255.0.0
C	24	8	255.255.255.0

   Netmask Examples...

Netmask	Host Bits	Netmask	Host Bits
255.255.255.252	2	255.255.255.0	8
255.255.255.248	3	255.255.254.0	9
255.255.255.240	4	255.255.252.0	10
255.255.255.224	5	255.255.248.0	11
255.255.255.192	6	255.128.0.0	23
255.255.255.128	7	255.0.0.0	24

   ```
   Netmask: Number of Bits for Host Part (0=default) (0) 8
   ```

5. Select if it is required to protect the Telnet Configuration capability with a password.

   Type **N** for no password.

   ```
   Change telnet config password (N) N
   ```

   Type **Y** to enable / change a password and then enter a password. The password cannot have more than 4 characters as standard unless the **Enable Enhanced Password** option is enabled.

   ```
   Change telnet config password (N) Y
   Enter new Password: 1234
   ```

6. Type **1** (Channel 1 configuration) followed by **Enter**.

7. Again, type each value one at a time followed by **Enter** setting to the following values. If you do not want to change a value, just press **Enter** to skip.

8. For the **Baudrate**, type **9600** for an 8bit Control PCB fitted with a **3MHz** crystal, type **19200** for an 8bit Control PCB fitted with a **7MHz** crystal, or type **38400** for a 16bit system followed by **Enter.** Please refer to the 8bit Control PCB Layout to locate the crystal type.

   ```
   Baudrate (9600) ? 19200
   ```

9. For the next two settings please keep the default settings as shown below. If you do not want to change a value, just press **Enter** to skip.

   ```
   I/F Mode (4C) ?
   Flow (00) ?
   ```

10. Make a note of the **Port No**, as you need this to configure Traka32. It is usually **10001** but you can alter this if required.

11. If you will be using the XPort Remote Host feature on more than one Traka System, a different Port No. must be set for each system for example, System 1: 10001, System 2: 10002, System 3: 10003 and so on.

    ```
    Port No (10001) ?
    ```

12. Set the **ConnectMode** to **C0**. If you will be using the XPort Remote Host feature, and you are running 8bit firmware versions 6.07.20 to 6.07.22 then set the ConnectMode to **D4**. If you are running 8bit firmware versions 6.07.23 or above set the ConnectMode to **D7**.

```
ConnectMode (C0) ?
```

13. For all other settings please keep the default settings as shown below. If you do not want to change a value, just press **Enter** to skip.

```
Remote IP Address : (000) .(000) .(000) .(000)
Remote Port (0) ?
DisConnMode (00) ?
FlushMode (00) ?
DisConnTime (00:00) ?:
SendChar 1 (00) ?
SendChar 2 (00) ?
```

14. If extra security is required, certain functionality can be disabled. Optionally type **6** (Security) followed by **Enter**.

15. For the first two settings please keep the default settings as shown below. If you do not want to change a value, just press **Enter** to skip.

```
Disable SNMP (N)
SNMP Community Name (public):
```

16. To disable the Telnet Configuration capability, set the Disable Telnet Setup option to **Y**. **WARNING:** Once this option is disabled, the only way to re-configure the XPort device is to use the Diagnostics Tool within Traka32.

```
Disable Telnet Setup (N) Y
```

17. For the next two settings please keep the default settings as shown below. If you do not want to change a value, just press **Enter** to skip.

```
Disable TFTP Firmware Update (N)
Disable Port 77FEh (N)
```

18. To disable the Web Server Configuration capability, set the Disable Web Server option to **Y**.

```
Disable Web Server (N) Y
```

19. For the next setting please keep the default settings as shown below. If you do not want to change a value, just press **Enter** to skip.

```
Disable ECHO ports (Y)
```

20. If a more complex password is required to protect the Telnet and/or Web Server Configuration capability, set the Enable Enhanced Password to **Y**. It is also possible to change the password if there is already one set.

```
Enable Enhanced Password (Y) Y
Change the Password (N) 123456789
```

21. For the final setting please keep the default settings as shown below. If you do not want to change a value, just press **Enter** to skip.

```
Disable Port 77F0h (N)
```

22. When you are happy with the configuration, type **9** (Save and exit) followed by **Enter**.

23. The device will automatically re-boot ready for use with the new settings. This will take approximately 10 to 20 seconds.

3.4.4.2.4 XPORT LED INDICATORS

Part Number XP1001000-01 (Shipped prior to August 2004)...

Left LED	Right LED	Meaning
Off	Off	No Link
Off	Solid Amber	100BASE-Tx Half Duplex Link
Off	Blinking Amber	100BASE-Tx Half Duplex Link with Activity
Off	Solid Green	100BASE-Tx Full Duplex Link
Off	Blinking Green	100BASE-Tx Full Duplex Link with Activity
Solid Amber	Off	10BASE-T Half Duplex Link
Blinking Amber	Off	10BASE-T Half Duplex Link with Activity
Solid Green	Off	10BASE-T Full Duplex Link
Blinking Green	Off	10BASE-T Full Duplex Link with Activity

Part Number XP1001000-03 (Shipped after August 2004)...

Left LED	Meaning
Off	No Link
Solid Amber	10BASE-T Link
Solid Green	100BASE-Tx Link

Right LED	Meaning
Off	No Link
Blinking Amber	10BASE-T Link
Blinking Green	100BASE-Tx Link

3.4.4.2.5 AES256 ENCRYPTION

AES-256 Encryption prevents data from being captured when travelling over the network wire between the Traka32 application and the customer database. This will prevent unauthorised access to personal information that could inherently provide unauthorised access to high security keys held in the Traka key cabinets.

NOTE: Traka32 version 02.09.0009 or above is required, plus an XPort with the Encryption compatibility.

How to tell the difference between normal XPorts and XPorts with Encryption compatibility?

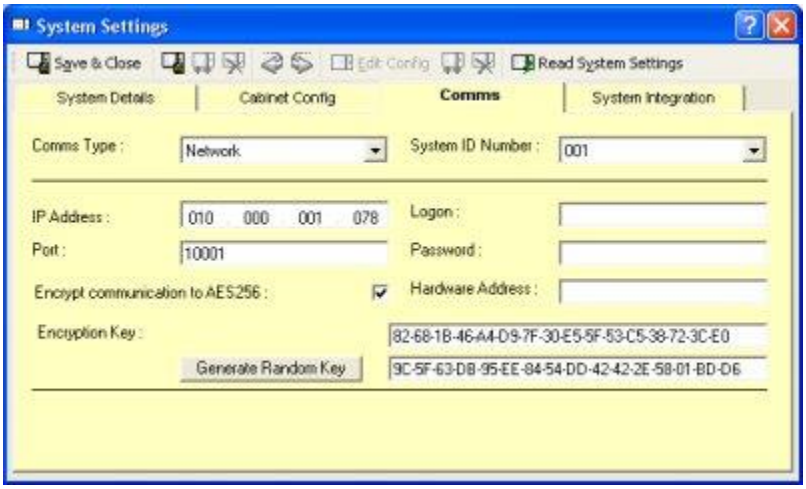
There is a part number printed on the side of every XPort. The 6th digit will show whether or not the XPort is configured for Encryption.

Standard: XP1001000-03R

Encryption : XP1002000-03R

How to set up and use AES256 Encryption

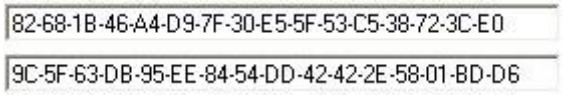
1. To enable AES256 Encryption right click your Traka System from the System Viewer and select Configure System. Then select the Comms tab.



2. Ensure the IP Address and Port Number of the XPort are entered into the appropriate fields, then tick the 'Encrypt communications to AES256' tick-box.

3. Click the 'Generate Random Key' button to generate a random AES256 encryption key. This will appear in the 2 adjacent text boxes.

4. The Encryption Key is made up of a combination of the 2 text boxes.



   Make a note of the Encryption Key and click the button.

5. The Encryption Key will then need to be entered into the XPort via Telnet. In the bottom left of your PC, click the Windows Start button and select the 'Run' feature. In the Run window, type 'cmd' and click OK.

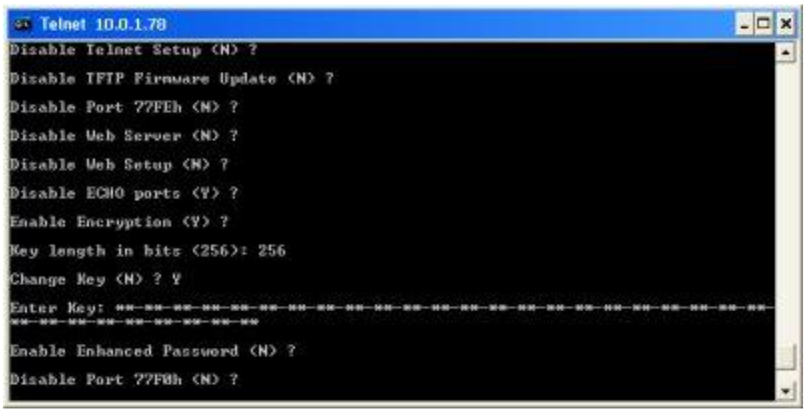
6. Telnet to the XPort, for example 'telnet 10.0.1.78 9999'. From the main menu.

    a. Select option 6 Security

    b. Press the Enter key until you are prompted to the '**Enable Encryption (N) ?**'

    c. Press (Y) then Enter key to enable encryption

NOTE: You can change this to N to turn off encryption however Traka32 will require the 'Encrypt communications to AES256' tick-box to be un-ticked before it will communicate.



    d. You will then be prompted to enter '**Key length in bits (0)**'. Type in 256 then press the Enter key. This will set the encryption to AES256.

    e. You will then be prompted '**Change Key (N) ?**' Press (Y) then press the Enter key to change key.

    f. You will then be prompted to '**Enter Key**:'.

    g. Type in the Encryption Key which was earlier entered into the Traka32 system settings.

    **-
    --**

    Notes:
    i. You do not need to type the dashes, the XPort will put these in for you.
    ii. The XPort is not case sensitive!
    iii. The Encryption Key cannot be viewed or read from the XPort

    h. Press Enter twice more and you will be taken back to the Telnet main menu.

    i. Select option 9 Save and Exit to save the changes.

    j. Once configured, navigate back to Traka32 and test the communications by simply Setting the Date & Time to ensure it communicates correctly. If there is a problem with your communication, be sure you have followed the pervious steps correctly.

3.4.4.2.6 E-MAIL

3.4.4.2.6.1 XPORT EMAIL OVERVIEW

The Traka XPort Ethernet Device (TXED) can be used to send e-mails directly from a Traka System in certain circumstances.

The ability to send e-mails is fairly limited but useful none the less. The device can send a pre-defined message to a maximum of two recipients whenever an event occurs. The device can programmed with up to a maximum of three events to respond too.

For example...

- The Traka System could send an e-mail to security@traka.com if the door of the Traka system was left open.
- The Traka system could send an e-mail to building.maintenance@traka.com if there was a power failure on the Traka System.

NOTE: The XPort Email option will only be functional if the firmware of the selected system has XPort Email enabled and the XPort device has been correctly configured. To configure the XPort device to send e-mails, please refer to the XPort Email configuration section.

3.4.4.2.6.2 XPORT EMAIL CONFIGURATION

To configure the Traka XPort Ethernet Device (TXED) to send e-mail, follow the procedure below.

1. Connect to the XPort device using either Telnet or the Diagnostics Tool within Traka32.

   NOTE: If you are not experienced with networks and e-mail we suggest you ask your Network Administrator or Local Traka Engineer to set up the XPort.

2. When entering the configuration menu, the following summary will be displayed...

```
MAC address 00204A802CA8
Software version 01.2 (030210) XPT

Press Enter to go into Setup Mode

*** basic parameters
Hardware: Ethernet TPI
IP addr 0.0.0.0, no gateway set

*************** Security ***************
SNMP is enabled
SNMP Community Name: public
Telnet Setup is enabled
TFTP Download is enabled
Port 77FEh is enabled
Web Server is enabled
ECHO is disabled
Enhanced Password is disabled

*************** Channel 1 **************
Baudrate 19200, I/F Mode 4C, Flow 00
Port 10001
Remote IP Adr: --- none ---, Port 00000
Connect Mode : C0 Disconn Mode: 00
Flush Mode : 00

*************** Expert *****************
TCP Keepalive : 45s
ARP cache timeout: 600s

*************** E-mail *****************
Mail server: 0.0.0.0
```

```
Unit :
Domain :
Recipient 1:
Recipient 2:

*** Trigger 1
Serial Sequence: 00,00
CP1: X
CP2: X
CP3: X
Message :
Priority: L
Min. notification interval: 0 s
Re-notification interval : 0 s

*** Trigger 2
Serial Sequence: 00,00
CP1: X
CP2: X
CP3: X
Message :
Priority: L
Min. notification interval: 0 s
Re-notification interval : 0 s

*** Trigger 3
Serial Sequence: 00,00
CP1: X
CP2: X
CP3: X
Message :
Priority: L
Min. notification interval: 0 s
Re-notification interval : 0 s

Change Setup:
0 Server configuration
1 Channel 1 configuration
3 E-mail settings
5 Expert settings
6 Security
7 Factory defaults
8 Exit without save
9 Save and exit Your choice ?
```

3. Type **3** (E-mail settings) followed by **Enter**.

4. Type each part of the **Mail Server's IP Address** followed by **Enter**. If you do not want to change a value, just press **Enter** to skip.

```
Mail server (0.0.0.0): (000) 10.(000) 0.(000) 0.(000) 20
```

5. Type the **Unit Name** of the Traka system followed by **Enter**. This will form the first part of the e-mail address e.g. reception@traka.com.

```
Unit name (): reception
```

6. Type the **Domain Name** of the Traka system followed by **Enter**. This will form the second part of the e-mail address e.g. reception@traka.com.

```
Domain name (): traka.com
```

7. Type the e-mail address of the first **Recipient** followed by **Enter**.

```
Recipient 1 (): djw@traka.com
```

8. Optionally type the e-mail address of the second **Recipient** followed by **Enter**. A second recipient e-mail address does not have to be specified.

```
Recipient 1 (): support@traka.com
```

9. Type the **Trigger 1**, **Serial Sequence** followed by **Enter**.

   ```
   Serial Sequence (00,00): 69,<Alarm_Code>
   ```

   This must be entered in the following format. Type **69,** followed by an alarm code. For example, to send an e-mail if when alarm code 6 (iFob Forced From System) occurs type **69,06**.

   NOTE: Two digits must be entered for the alarm code. For example enter 69,06 and not 69,6. Please refer to the Alarm section for a full list of alarm codes and descriptions.

10. For the next three settings please keep the default settings as shown below. If you do not want to change a value, just press **Enter** to skip.

    ```
    CP1 [A/I/X] (X):
    CP2 [A/I/X] (X):
    CP3 [A/I/X] (X):
    ```

11. Type the **Trigger 1**, **Message** followed by **Enter**. This would typically be the description of the alarm code. For example, if you wish to send an e-mail for alarm code 6, enter the description 'iFob Forced From System'.

    ```
    Message (): iFob Forced From System
    ```

12. Enter the **Trigger 1**, **Priority** level followed by **Enter**. Enter **H** for high priority or **L** for low priority.

    ```
    Priority (L): L
    ```

13. For the next two settings please keep the default settings as shown below. If you do not want to change a value, just press **Enter** to skip.

    ```
    Minimal notification interval (0 s):
    Re-notification interval (0 s):
    ```

14. Repeat steps 7 to 11 for **Trigger 2** and **Trigger 3**.

15. When you are happy with the configuration, type **9** (Save and exit) followed by **Enter**.

16. The device will automatically re-boot ready for use with the new settings. This will take approximately 10 to 20 seconds.

3.4.4.2.7 REMOTE HOST

3.4.4.2.7.1 XPORT REMOTE HOST OVERVIEW

As part of the auto communications available within Traka32, 'Remote Host' forms one of the many options. The remote host option will only work with Ethernet communications.

The remote host option is very similar to the other forms of auto communications. The main difference with remote host is that the Traka Systems establish the communications with Traka32 rather than Traka32 establishing the communications with the Traka Systems.

This has two major advantages...

1. **Reliability & Speed**

   When a copy of the Traka32 software is opened, the software registers itself with each Traka system that is included in the remote host group. Each Traka system can have three copies of the Traka32 software registered at any one time. So whenever the Traka system has data waiting to be sent to the Traka32 software, it has more chance of getting there quickly. The more copies of Traka32 that are running and configured for remote host the more efficient and reliable the whole system becomes.

   For example, if one of the registered copies of the Traka32 software is busy or an error has occurred, the Traka system will try to communicate with one of the other copies of the Traka32 software.

   If all the copies of Traka32 are busy, the Traka system will re-try the communications every 60 seconds.

2. **Multiple Administration**

   One disadvantage with the Online Auto communications is that in Ethernet Installations a network port is constantly opened between the Traka32 software and the Traka System. Only one network port can be opened on a Traka system at any one time. This means that if one copy of the Traka32 software is Online, no other copies of the Traka32 software can communicate with the Traka system.

   The Remote Host Auto Communications resolves this issue as the Traka System has the ability to open a network port to the Traka32 software whenever it needs to download data. This leaves the network port closed for the majority of the time ready for other copies of the Traka32 software to connect to whenever user, iFob or keys information is updated.

In addition to the remote host communications, the Read All System Data function is not affected and can still be used as normal. The remote host feature should be the preferred choice of auto communications and should be used whenever large amounts of data need to be downloaded automatically.

NOTE: The XPort Remote Host option will only be functional if the firmware of the selected system has the XPort Remote Host enabled and the XPort device has been correctly configured. To configure the XPort device, please refer to the XPort configuration section.

There are only two differences on the XPort Remote Host configuration from the standard settings...

1. For 8bit firmware versions 6.07.20 to 6.07.22 set the ConnectMode to D4 instead of C0.
2. For 8bit firmware versions 6.07.23 and above set the ConnectMode to D7 instead of C0.
3. Set a different Port No. for each system. For example, System 1: 10001, System 2: 10002, System 3: 10003 and so on.

3.4.4.2.7.2 XPORT REMOTE HOST SETUP

In order to use Remote Host you must follow the steps below...

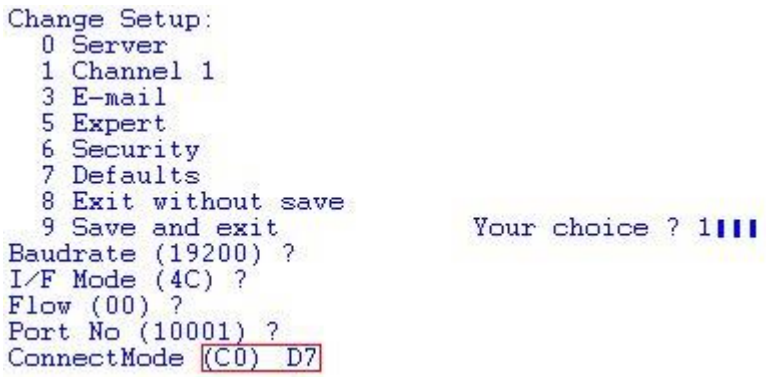
1. The 'Remote Host' option must be enabled in the firmware of the desired system/s.

2. If you already have an existing Traka system/s with previously configured XPorts, then you will need to change the Connect Mode of the XPort.

   To change the Connect mode, from the Traka32 software select **Engineers>Diagnostics**. From the Diagnostics window select the **XPort Utilities** tab and click the **Search** button. A list of active XPort devices will be displayed along with the MAC address of each XPort and the device's IP address.

3. Locate your XPort device either by the MAC Address or the IP address, then click it once to highlight it and select the **Telnet** button. You will notice on the right hand side of the screen that you have connected to the XPort. You will be prompted to press the **Enter** button. Next press the number **1** button and then the **Enter** button. You are now in the 'Channel 1' setup menu. Press the **Enter** button until you get to the 'Connect Mode'.

   The 'Connect Mode' will be set up as C0 and needs to be changed to **D7**. Simply enter **D7** and select **Enter**.

4. Enable remote host comms type in **File>Properties>Comms>Remote Host** (interval is optional, and is not for remote host, only for standard autocomms).

5. Right click on the Control Panel and select **Configure system>Comms**, and then tick the 'Include in autocomms' option.

6. Click **Save & Close** and then close and re-open Traka32.

3.4.4.3 LANTRONIX UDS2100

For some applications it is necessary to use the Lantronix UDS2100 dual serial to Ethernet device server. This is provided as an alternative to the standard Lantronix XPort device. The difference between the UDS2100 and the XPort is that the UDS2100 has 2 serial ports available (as opposed to just one). Also, unlike the standard XPort device, the UDS2100 is not soldered directly to the Control PCB. The 2 serial port connections are connected to the UART A and UART B connections on the Control PCB, and the power is taken from the Power Output connector on the Control PCB.

Configuration

Configuration is carried out in the same way as the XPort Configuration but with the addition of configuring the second Serial Port. Follow the Xport Configuration section, and after configuring the settings for Channel 1 follow the steps below.

1. Select **2** from the main menu followed by **Enter** to configure the settings for Channel 2.
2. Use the Enter key to navigate through the menu, only entering values against the following fileds:
    a. **Baudrate:** Enter the correct Baudrate, for example 8bit 3MHz = 9600, 8bit 7MHz = 19200, 16bit = 38400.
    b. **Port No:** For channel 2 this is almost always **10002**. Note the difference here, Channel 2 uses port 10002 and not 10001.
    c. **I/F Mode:** This should have a default value of **4C**, ensure this is correct.
    d. **Connect Mode:** This should have a default value of **C0**, ensure this is correct.
    e. **Flush Mode:** This should be configured with the value **F7** to enable packing.
3. Once you have navigated through this menu you should return to the main menu.
4. Enter **9** to **Save and Exit**, followed by **Enter** to confirm. This will commit the changes you have made.

3.4.4.4 INSTALLING TELNET ON WINDOWS VISTA

Telnet Client can be used to configure a Traka Ethernet Device (TED) across an Ethernet. However it is important to note that by default, Telnet is not installed with Windows Vista, but you can install it by following the steps below.

To install Telnet Client...

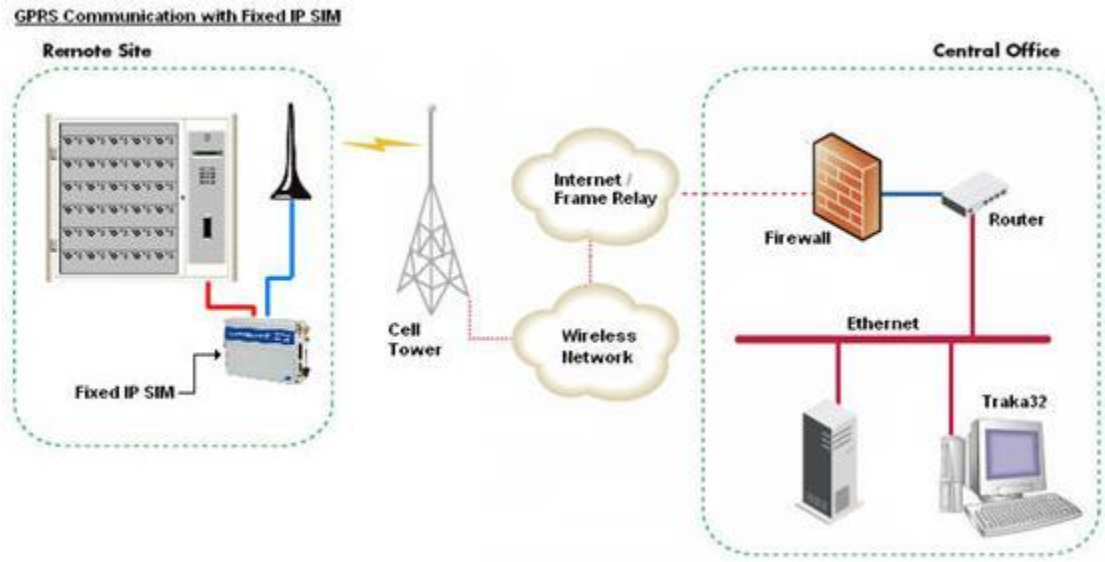
1. Click the **Start** button, click **Control Panel**, click **Programs**, and then click **Turn Windows features on or off**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

2. In the **Windows Features** dialog box, select the **Telnet Client** check box.

3. Click **OK**. The installation might take several minutes.

3.4.5 GPRS COMMUNICATION

With the increasing need to administer Traka Cabinets remotely, it is now possible to communicate to your Traka cabinet via GPRS.



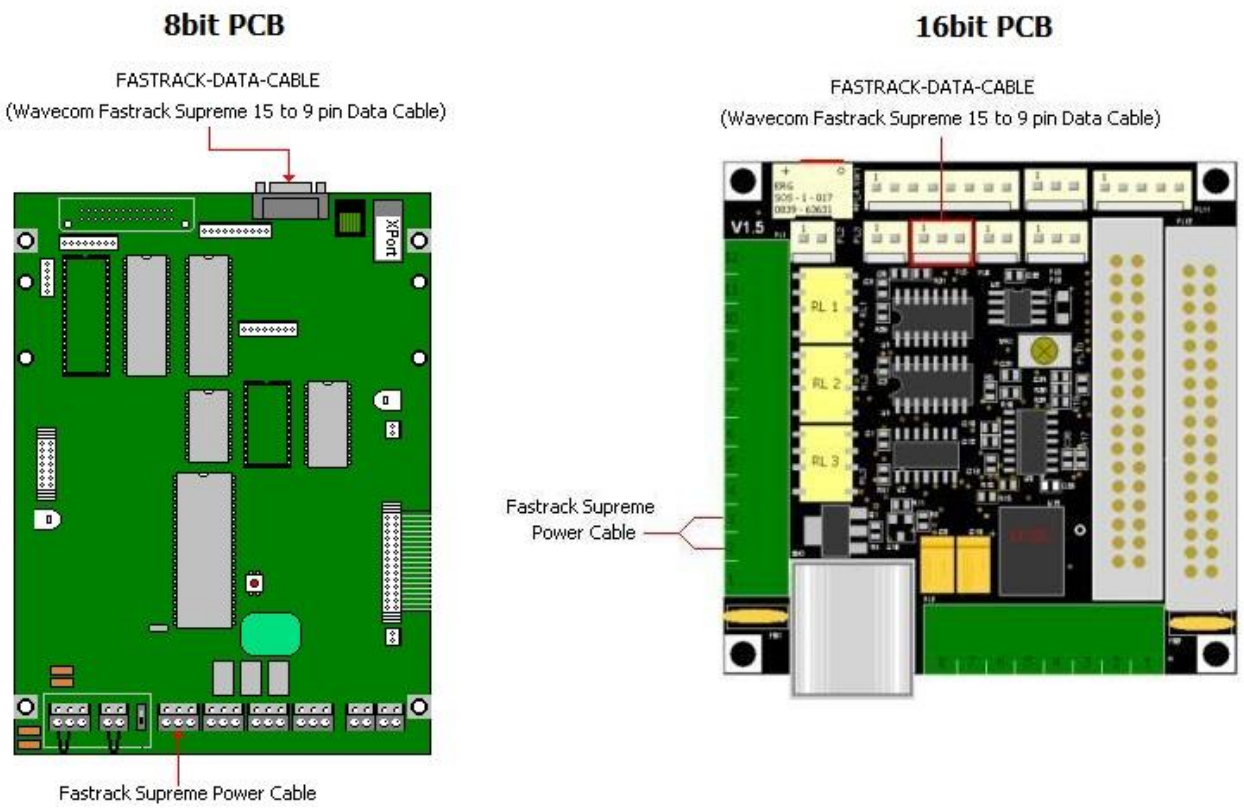
NOTE: This does not currently work with the SMS Text messaging capability on the Traka systems.

Hardware

The GPRS Communication hardware consists of...

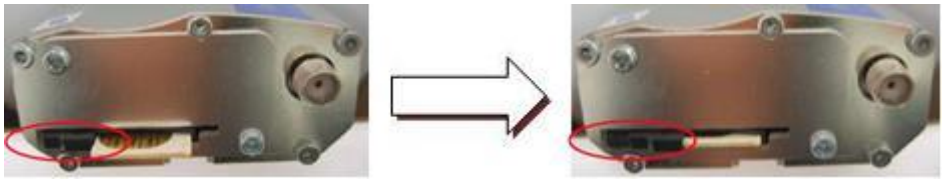
- 1 x FASTRACK-S10 or FASTRACK-S20 (Wavecom Fastrack Supreme 10 or 20)
- 1 x FASTRACK-DATA-CABLE (Wavecom Fastrack Supreme 15 to 9 pin Data Cable)
- 1 x FASTRACK-PSU (Wavecom Fastrack Supreme Power Supply for connecting to a PC only)
- 1 x AO100/SMAM/5M (Large Wall Mount Antenna with 5m of Cable)
- 1 x NULL MODEM Converter

When you receive your Traka cabinet the GPRS Module will already be connected to the control board, you will need to disconnect the GPRS Fastrack Supreme Data Cable to program your individual SIM card settings. Use the images below to disconnect the data cable accordingly.



Once disconnected form the control board you will need to plug the Data cable in to a spare port on your PC (if you do not have a serial port for the Data cable you will need a Serial to USB converter which Traka can supply for you). If you wish to use a separate power supply instead of the control boards power output, then this can be wired and configured at a later stage. For now, leave the power cable plugged in to the control PCB.

Next insert your SIM card into the end of the Fastrack Supreme Module. Ensure that the 'SIM Card Lock' is moved to the right and is holding the SIM card in place.

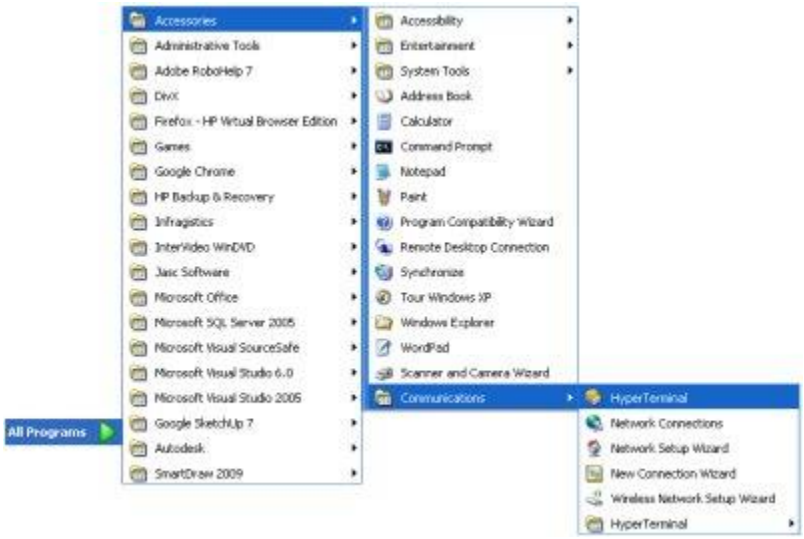


GPRS Configuration

NOTE: This document assumes prior knowledge of HyperTerminal.

To configure the GPRS Fastrack Supreme Module to read your specific SIM Card details you need to open the Windows HyperTerminal application.

1. From your Windows start button in the bottom left of the computer screen click **Start>All Programs>Accessories>Communications>HyperTerminal.**



2. You will be confronted with a message which recommends that you make the HyperTerminal your default telnet program. Select the desired option and continue.

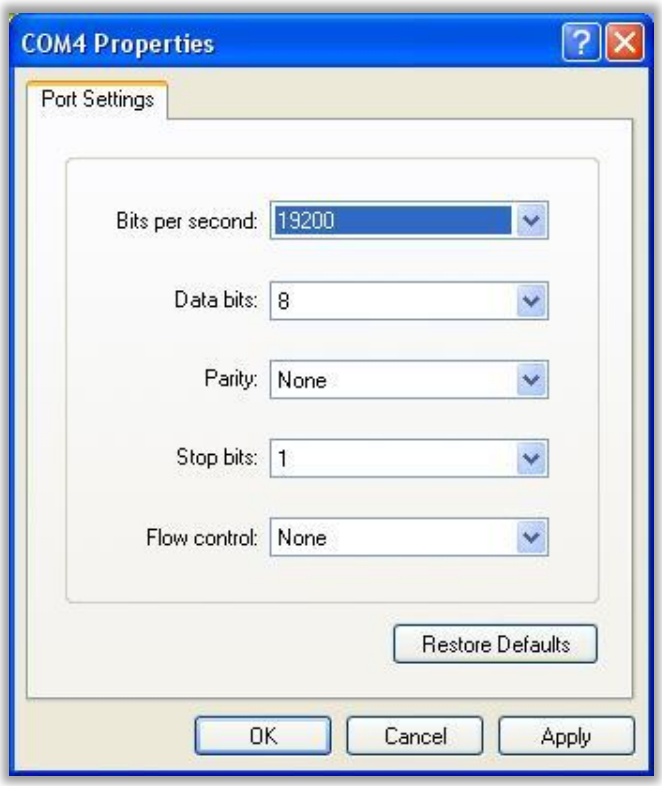
3. You will then be asked to give the connection a description name and you will also have the choice of different icon images displayed at the bottom.

4. In the next window configure the HyperTerminal to connect to the COM port that the Fastrack Supreme is connected to.

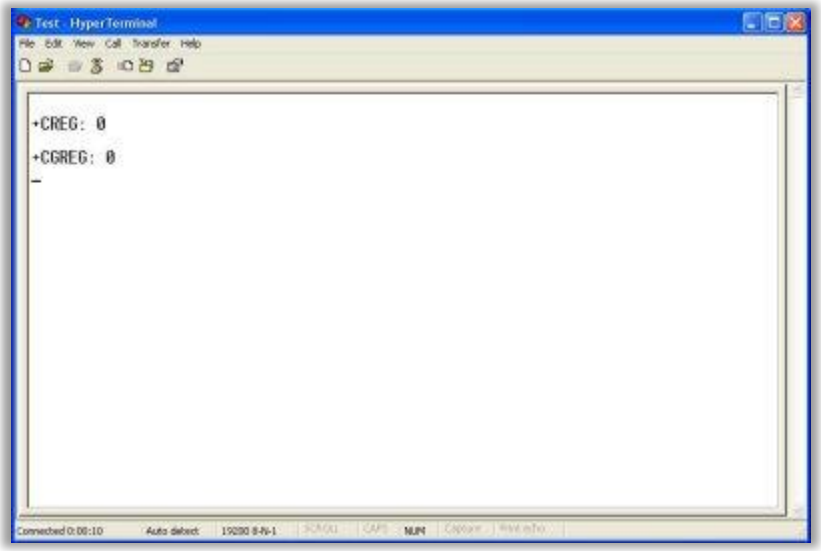
5. After selecting the appropriate COM port, set the Baud Rate to either 19,200 (8bit) or 38,400 (16bit) depending on what control board you have. Ensure all the other settings are as follows.

   Baud Rate: 19,200 or 38,400
   Data Bits: 8
   Parity: None
   Stop Bits: 1
   Flow Control: None

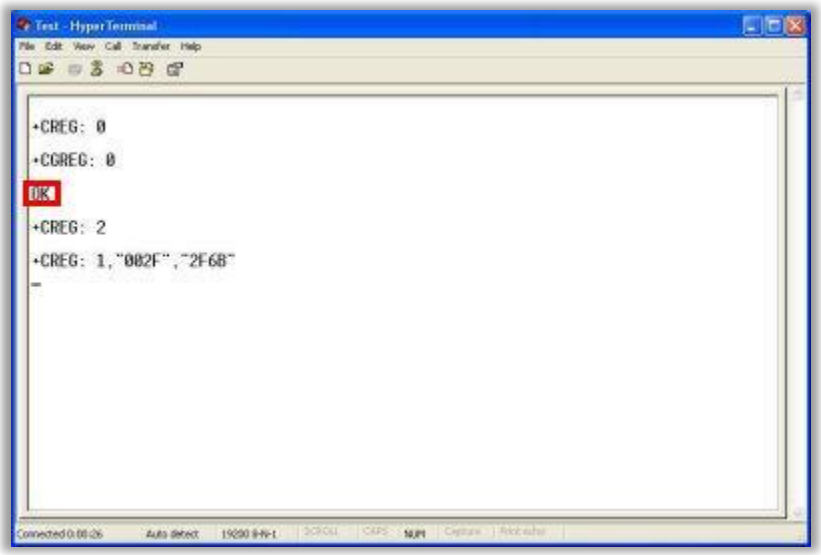
6. When the appropriate setting have been entered click 'OK' and a blank HyperTerminal window will open.



7. Switch on the GPRS module by powering on the 8bit/16bit control board. You will see the following text appear in the HyperTerminal.



8. Then quickly type +++ and then wait 1 second to enter 'Command Mode'. If successful, the Fastrack Supreme should output 'OK'.



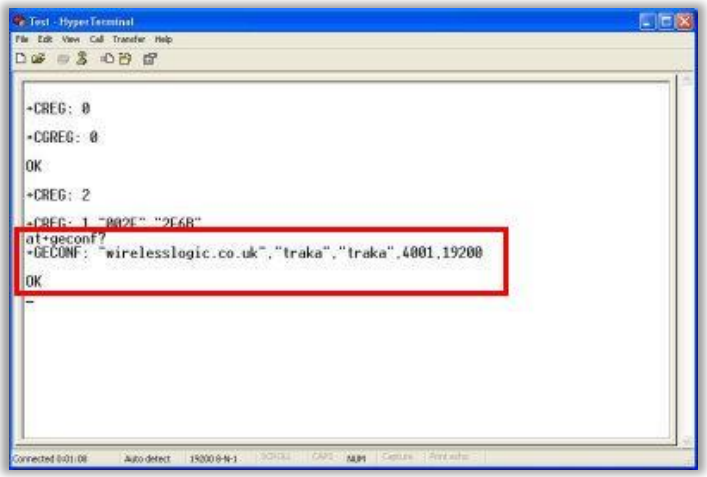
9. Certain parameters need to be configured in order to connect to the GPRS network. These details will be supplied with the Fixed IP Address SIM Card. To enter the APN, Username, Password and Port Number enter the following information:

   AT+GECONF="<APN>","<USERNAME>","<PASSWORD>",<PORT>[,<UART_BAUDRATE>]

10. The baud rate will depend on the Control PCB e.g. 8bit 7MHz = 19,200, 16bit = 34,800 etc. The example below shows the details provided with the Traka development SIM card:

    E.g.: AT+GECONF="wirelesslogic.co.uk","traka","traka",4001,19200

TIP: To find out what the current settings are, type AT+GECONF? and the Fastrack Supreme should output the settings (See Below).



11. Power down the Fastrack Supreme and power back up. Upon power up, the Fastrack Supreme should output:

    +CREG: 0
    +CGREG: 0

    On power up the Fastrack Supreme will then automatically connect to the GPRS network ready for communication. Provided there is an antenna connected and a signal received, once a connection has been made the Red LED on the module will start to flash.

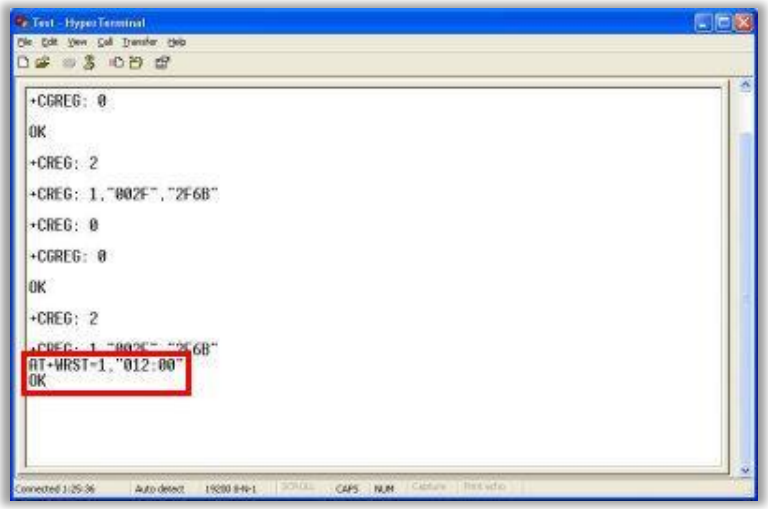
Network Timer

On busy cellular networks, the network provider will sometimes (depending on network demand) disconnect dormant connections automatically if no data is sent for long periods of time, e.g. 12, 24, 48, 72 hours etc. One method of overcoming this is to restart the modem every few hours, so that if it has been disconnected it will re-connect. The modem has a built in timer that can be set with a start value e.g. 12 hours. When the modem is powered up, the timer ticks down until it reaches 0 and then the modem restarts. Once restarted the counter goes back to 12 hours, ticks down again and so on. No settings are lost during a restart. The Traka default Network Timer is 12 hours. To change the auto restart timer…

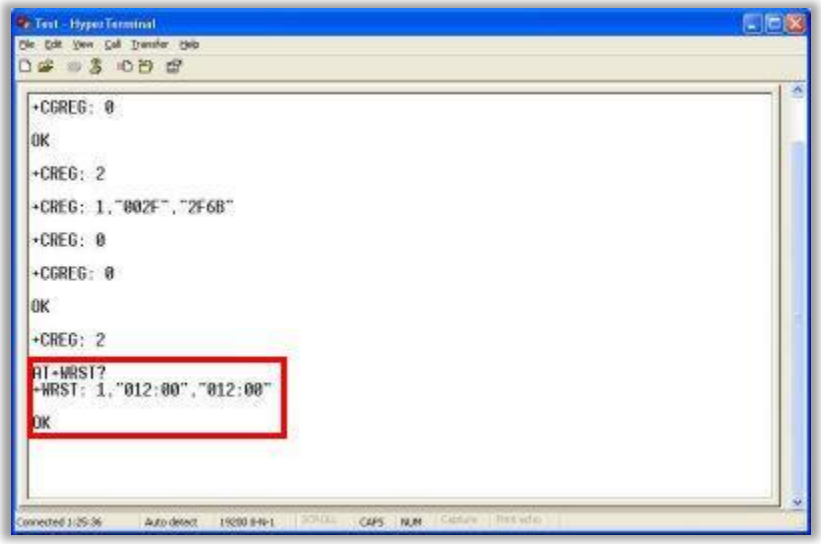
1. In the HyperTerminal, quickly type +++ and the wait 1 second to enter command mode. If successful, the Fastrack Supreme should output OK. To alter the automatic reset parameters type:

   AT+WRST=1,”012:00”

   The above example shows that the modem will auto reset every 12 hours. The first 3 digits “012” indicates hours, then a “:” and the last 2 digits “00” means minutes. If for example you wanted to reset the modem every 30 minutes you would type “000:30”.



TIP: To find out what the current settings are, type AT+WRST? and the Fastrack Supreme should output the settings.



NOTE: To disable the auto restart type AT+WRST=0.

2. Once entered, type AT+CFUN=1, the Fastrack Supreme will restart and the countdown timer will begin. Once restarted, the Fastrack Supreme should output:

   +CREG: 0
   +CGREG: 0

3. You may now close the HyperTerminal and disconnect the data cable from the PC and reconnect it to the Traka cabinet. If you desire to use an separate power supply for the Fastrack Supreme you may now connect it up accordingly.

NOTE: If you for example you setup a 24 hour auto restart and the last power cycle or restart was done at 3pm, the modem will reset itself at 3pm each day. If this is likely to be a period in which heavy communications occur, it is better to re-cycle the power to the modem during a non-busy period.

NOTE: When the modem auto restarts, it is not intelligent enough to know if it's currently communicating and so if you are in the middle of communicating and the restart timer hits 0, the communications will cut off. This may cause an Internal Error in Traka32, however no data will be lost. Simply retry the command and it will resume.

Traka32 Software

NOTE: (for 8bit Users Only) Before attempting to communicate, ensure the 8bit Control PCB Communication Jumper Settings are set to RS232.

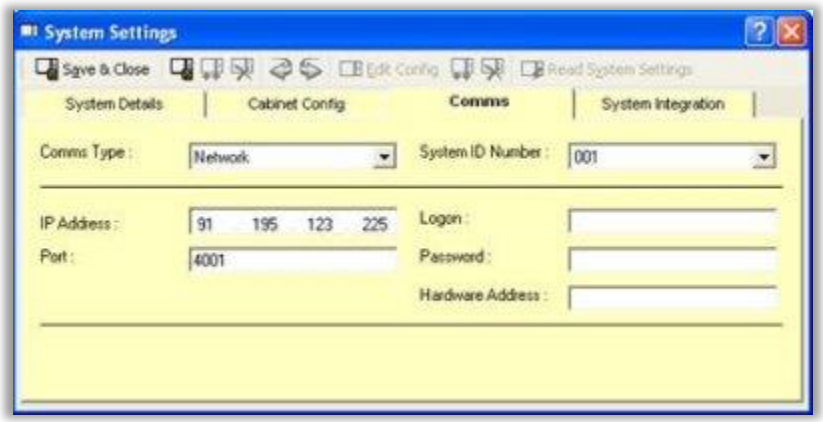
The Fixed IP Address SIM Card will have been supplied with Public IP Address. To configure Traka32 to talk to the Fastrack Supreme, set the Communications Settings to Network and set the IP Address to be the Public IP Address. The Port Number should be set to that specified in the GPRS Configuration section. The example used for this document was 4001.

1. In Traka32 right click the image of your cabinet and select **Configure System**.

2. The System Settings window will now appear. Select the **Comms** tab and enter your information accordingly.

   The example below shows the details provided with the Traka development SIM card:

   IP Address: 91.195.123.225
   Port: 4001



NOTE: The PC running Traka32 will have to be connected to the Internet in order to communicate with the Fastrack Supreme. This may also require configuration of a firewall to allow this to work.

3.5 SOFTWARE INSTALLATION

3.5.1 TRAKA32 MINIMUM PC REQUIREMENTS

Traka32 requires a minimum of 650MB free space from your host machine. This is the same for every operating system Traka supports to date. The Traka CD also contains 64-bit versions of the Sagem USB Fingerprint reader and Desktop Programmer.

NOTE: If installing any of the below versions of SQL Server and Traka32 on the same server, it is recommend that an extra 1GB RAM is added to the values above.

32bit & 64bit Windows Operating Systems

Operating System	Minimum Processor Speed (Ghz)	Recommended Processor Speed (GHz)	Minimum RAM	Recommended RAM
Windows 7	1.0	2.5+	2GB	3GB+
Windows 8	1.0	2.5+	2GB	4GB+
Windows 10	1.0	2.5+	2GB	4GB+
Windows 11	1.0	2.5+	2GB	4GB+

64bit Windows Operating Systems

Operating System	Minimum Processor Speed (Ghz)	Recommended Processor Speed (GHz)	Minimum RAM	Recommended RAM
Windows Server 2012 (Including R2)	1.4	2.5+	2GB	4GB+
Windows Server 2016	1.4	2.5+	2GB	4GB+

NOTE: Windows 11 is compatible with both SQL Server 2019 and SQL Server 2022.

3.5.2 TRAKA32 LICENCE

The Software supplied under this agreement shall be subject to the following terms and conditions…

1. Definitions

   "Company" shall mean ASSA ABLOY Ltd trading as Traka and shall include the Company's successors and assigns.
   "Customer" shall mean the person, firm or company with whom this agreement is made.
   "Software" shall mean all Software licensed under these conditions.

2. Licence

   The Company hereby grants a non-exclusive, non-transferable licence to use the Software specified on one computer processing unit for every user licence purchased.

3. Patents, Designs and Copyright

   The Company retains all proprietary interests and rights in and over the Software and all trade secrets, patent rights and ideas in relation thereto remain the exclusive property of the Company.

4. Copying

   The Customer agrees not to disclose the contents or code of the Software to any third party. The Customer may take copies of the Software, but only for the purpose of back-up security and agrees that these shall also be kept confidential.

5. Delivery

   Unless otherwise agreed in writing, any delivery or performance dates specified by the Company are approximate only and time shall not be of the essence for delivery.

6. Prices and Payments

   All prices are quoted exclusive of VAT or other statutory taxes.

   The Company shall have the right to charge the Customer for any expenses incurred as a result of discharging its obligations under this Agreement, unless otherwise specified.

   The Customer shall pay the amounts due under this Agreement within thirty days from the date of the Company's invoice. The Company reserves the right to charge interest on any overdue amount at the rate of 2% per month from the date at which the amount becomes overdue. If payment in full is not made in accordance with the Agreement the Company may require the Customer to return the Software together with all known copies and Software protection devices, without prejudice to any other remedy which may be available to the Company. The risk in the goods shall pass to the Customer on delivery but all items remain the property of the Company until payment is received in full.

7. Maintenance and Support

   The Company agrees to provide the Customer with maintenance and support under the terms of it's warranty for the 12 months following the date of installation. At the completion of this 12 month period, the licence will continue to remain in force; but ongoing maintenance and support will only be provided by the payment of an Annual Maintenance Fee, always providing that the Fee specified has been received by the Company. The services shall be as follows…

   a. Provide the Warranty service as specified in (10) below.

   b. Provide the Customer with a copy of any programs issued by the Company as new release, which may includes upgrades as well as additional features and facilities.

   c. Provide a telephone help line support during the normal working hours of the Company.

8. Annual Maintenance Fee

   The Annual Maintenance Fee specified will, if chosen, be payable upon expiry of the first year following installation of the Traka system and at yearly intervals thereafter. Payment of such invoices shall be as specified above. The payment of the invoice will entitle the Customer to the services specified under Clause 8 (maintenance and support) for a further year from the date of the Annual Maintenance invoice.

9. Warranty Service

   The Company believes that to the best of its knowledge the Software has been thoroughly tested for freedom from arithmetic or logical defects in the Software and that it will function as stated in the user manual. As there is no means of ensuring the total absence of defects in the Software, the Company agrees to use all reasonable endeavours to correct free of charge any such defects in the Software discovered by the Customer during the period of the Warranty, provided always that…

   a. The Customer promptly notifies the Company of any defect which it believes to exist.

   b. The Customer provides the Company with all details and information which may assist in diagnosing and correcting the defect.

   c. The Customer provides any facilities which the Company may reasonably request to aid the diagnosis and/or correction, and co-operates with the Company in these activities.

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

      The correction service under this clause does not apply if…

      i. The defect is attributable to failure or breakdown or interference of any third party, or software or hardware not supplied subject to this agreement.

      ii. The Customer is in breach of this Agreement with the Company.

      iii. The Customer fails to operate the Software properly or fails to follow the instructions or recommendations of the Company with respect to the Software.

      iv. The defect is due to the input of invalid or inaccurate data by the Customer.

      v. The Customer interferes with, modifies, or fails to secure the Software.

10. Training

    Other than the supply of the standard documentation included with the Software, no additional formal training is provided by the Company unless otherwise agreed by the Customer and the Company.

11. Limit of Liability

    The Company and the Customer agree to indemnify each other against any liability in respect of injury (including death) or loss or damage to property which results from the act, default or negligence of itself, its employees or agents to a maximum of £2,000,000.

    The Company accepts no liability for any losses, whether direct or consequential, however caused, arising directly or indirectly from the use of the Software.

12. Disposal

    The Customer undertakes that, upon the cessation of the use of the Software for whatever cause, or upon termination of this Agreement, it will return to the Company, all known copies of programs, Software protection devices, documents or other material in its possession on whatever media they are recorded, or otherwise dispose of them as the Company may direct.

13. Force Majeure

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

14. Termination

    Either party shall have the right to terminate this Agreement if the other party is in material breach of this Agreement and fails to rectify such breach within 30 days of receipt of notification thereof in writing, from the injured party. Termination shall not affect any other rights of the injured party.

15. Law

    This Agreement is governed by the laws of England and Wales and the parties submit to the jurisdiction of the Courts of England and Wales.

16. Entire Agreement

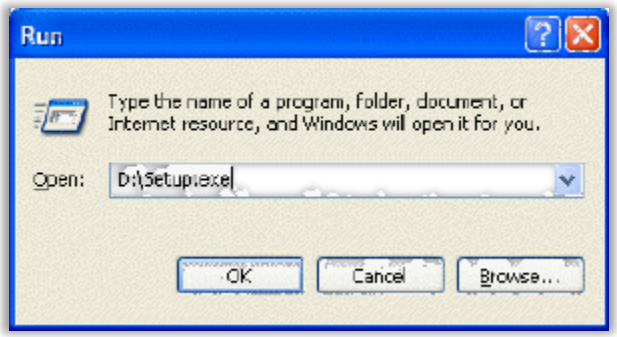
    The parties agree that these terms and conditions (together with any other terms and conditions expressly incorporated in the Agreement) represent the entire agreement between the parties relating to the licence of the Software, and that no statements or representations made by either party have been relied on by the other in agreeing to enter into the Agreement.

3.5.3 TRAKA32 INSTALLATION

Before installing the Traka32 software, please check that the PC you are going to install the software on meets the minimum requirements otherwise you may face problems during the installation or use of the software. Please refer to the minimum PC requirements section for more details.

1. Insert the Traka32 CD into the CD-ROM drive.
2. After a few seconds the set-up wizard should run automatically.

   If not, click on **Start>Run** and type **D:\Setup.exe** followed by **Enter** (replacing the D with the appropriate CD-ROM letter).



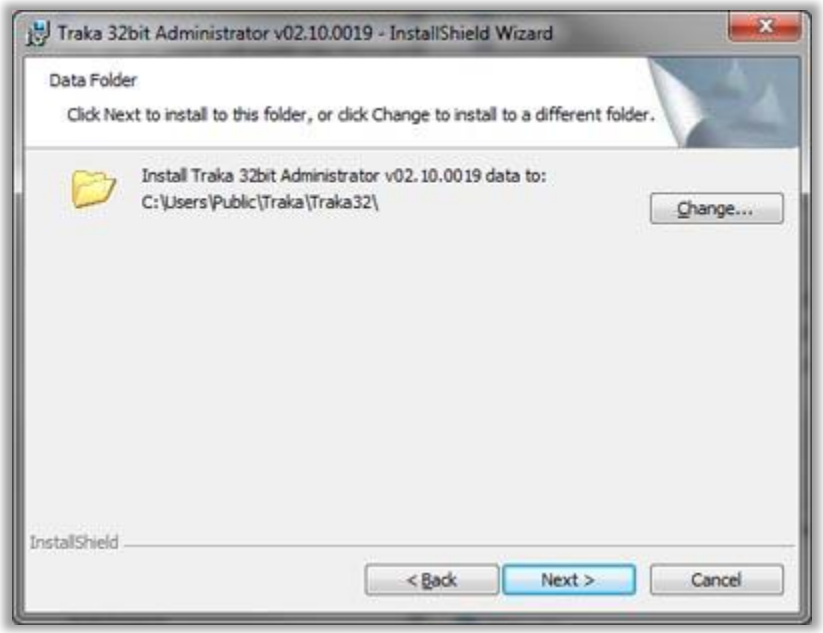
3. The set-up wizard will guide you through the installation.

Installation Locations For Traka32 Software

When installing Traka32 you can specify the file locations for the Destination Files and the Writable Files (Data Files).

Setting the path to the Writable files folder

At a certain point in the installation you will be presented with the following window.



From here click the **Change** button to browse to select the desired location for the writable files. Continue with the installation and click finish.

- If you are installing software version 02.08.0003 and above, on to a Windows XP or Vista platform, once installed you must ensure that the permissions of the **Traka32 Program Files** (C:\Program Files\Traka Limited\Traka32) are set to...

  Read & Execute
  List Folder Contents

  ...as the Traka32 software will need to create and delete temporary files during the communication process.

- The **Traka32 Data Files/Writable Files** (C:\Users\Public\Traka\Traka32) will require the permissions set to...

  Full Control

  or at least

  File Create
  File Delete
  Modify
  Read & Execute
  List Folder Contents
  Read
  Write
  Read

  ...as information will be written to the database and locking files will need to be created and deleted from the directory.

  Also Read & Write permissions must be granted for the following **registry** key and sub keys...

  HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Traka32

You now have the ability to change where the writable folders are kept. By default Traka32 always looks for the following folders in **C:\Users\Public\Traka\Traka32**:

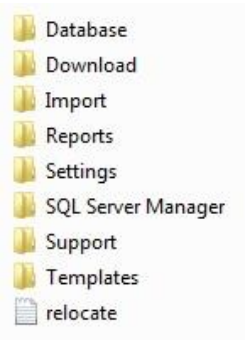
Download
Reports
Settings
Support

Some customers do not allow files to be updated on the local computers 'C:' drive so you can now copy the folder structure to another location and point Traka32 to use the new location.

1. To set this up simply navigate to the folder where you installed the writable files e.g. **C:\Users\Public\Traka\Traka32** and copy the folder structure into the location you wish to move the folders to.

   NOTE: Do NOT delete the original files from the installation, only copy them to a new location.

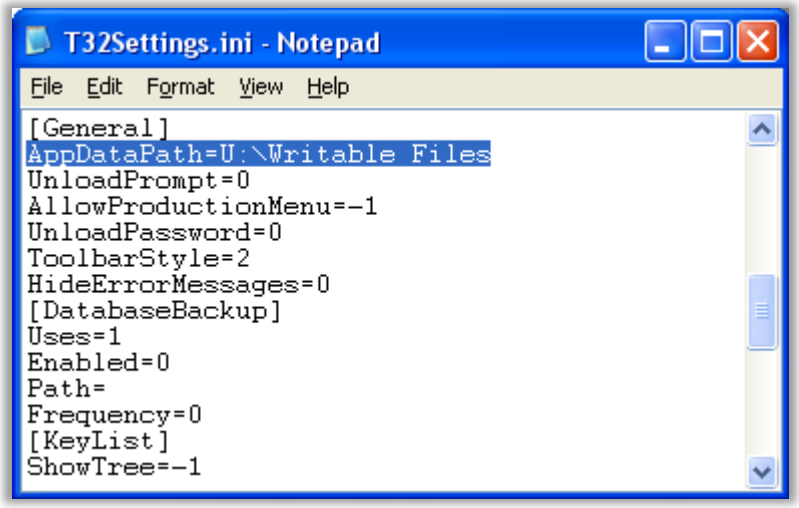
   The structure needs to be the same as the structure as it was in the original installation location. The structure is as follows...



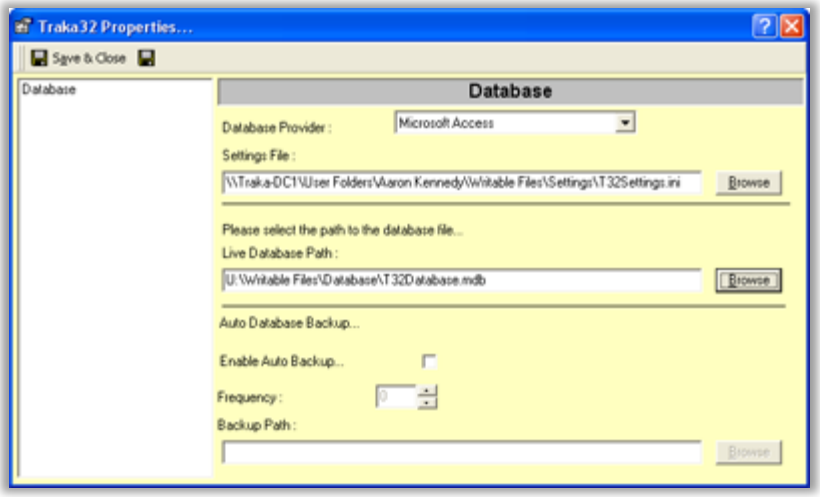
NOTE: The settings.ini file (inside the Setting folder) can be moved to another location outside of the other writable files, for example, if you moved the Database, Download, reports etc to the D:\ drive then you can move the settings.ini file to a different location.

2. After placing the files in their new location explore the Settings folder and open the **settings.ini** file.

3. In the **[General]** section of the settings.ini file add the following line '**AppDataPath=**' followed by the new location you have moved the file to. Ensure that you do not add any additional incorrect characters to the location name, as you may receive an error on start up.



4. Open Traka32 whilst holding F11 on your keyboard to open the Traka32 Properties window. Point the database & settings files to their new locations by clicking the browse button.



5. Click the **Save & Close** button and use Traka32 as normal.

3.5.4 TRAKA32 REGISTRATION

When you run the Traka32 software for the first time you will be asked for a software registration code.

Traka32 is registered on a concurrent user basis, so effectively you have to register your database. Once you have registered the Traka32 software you can install as many copies of the software as you wish but you will only be allowed to have a certain number of copies loaded at any one time.

You do not have to register Traka32 immediately as you can evaluate the software for 90 days. Simply click on the **Evaluate** button to continue loading the software. During the evaluation period you will have full use of the software.

When you are ready to register the software please contact Traka by telephoning +44 (0)1234 712345 between the hours of 08:30 and 17:30 GMT/BST or by email to support@traka.com quoting the following...

- Application
- Version
- Software Code

You will be given a 20 digit unlock code. Enter the unlock code and click on **Register** to complete the registration process.

NOTE: Older versions of Traka32 used to be registered on a copy by copy basis. If you have version 01.05.0003 or earlier of the Traka32 software you will have to register every copy you install.

3.5.5 DATABASE INSTALLATION

3.5.5.1 MICROSOFT ACCESS DATABASE INSTALLATION

Whenever a copy of Traka32 is installed on a Workstation, a blank database will be installed. If you are upgrading a previous installation the current database will not be overwritten. The default file path for the database is 'C:\Users\Public\Traka\Traka32\Database\T32Database.mdb'.

Moving the database

It is strongly recommended that if you are setting up a networked Traka system that you move the database from its default location to a file server that can be accessed by all the required workstations and is regularly backed up.

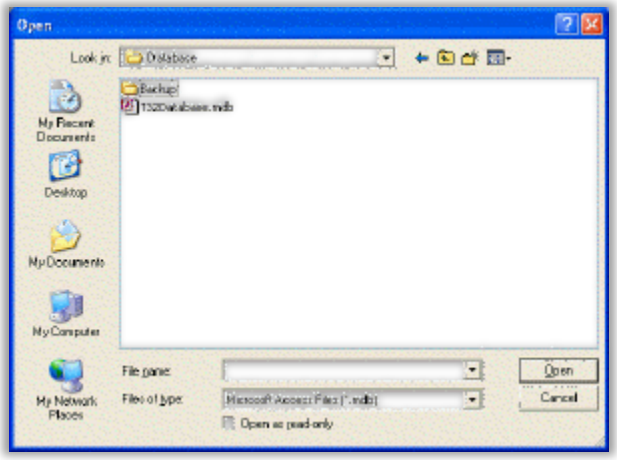
To do this, simply move the database from its default location of 'C:\Users\Public\Traka\Traka32\Database\T32Database.mdb' to your chosen network location using Windows Explorer.

NOTE: If you are installing the database on to a Windows XP platform, the database directory will require the permissions set to 'Full Control' as information will be written to the database and locking files will need to be created and deleted from the directory.

Setting the database path

1. Load the Traka32 software by double clicking on the  icon. When you run Traka32 for the first time you will be prompted for a database path.

2. Click on **OK** to set the database path.



3. You will be presented with an open window, select the path to the database and click on **Open**.

4. Traka32 will continue to load. Please note that after setting the database path, Traka32 will take longer to load than normal as an integrity check will be made on the database.

For further details including setting up Software Access please refer to the Software Access using a Microsoft Access Database section.

3.5.5.2 MICROSOFT SQL

3.5.5.2.1 MICROSOFT SQL SERVER OVERVIEW

In addition to Microsoft Access, Traka32 supports all versions of Microsoft SQL Server as the database back-end. Microsoft SQL Server delivers security, reliability and scalability for customers with multiple cabinets and/or installations of the client software.

NOTE: Ensure you are using a version of SQL Server as recommended by Microsoft for your version of Windows Operating System.

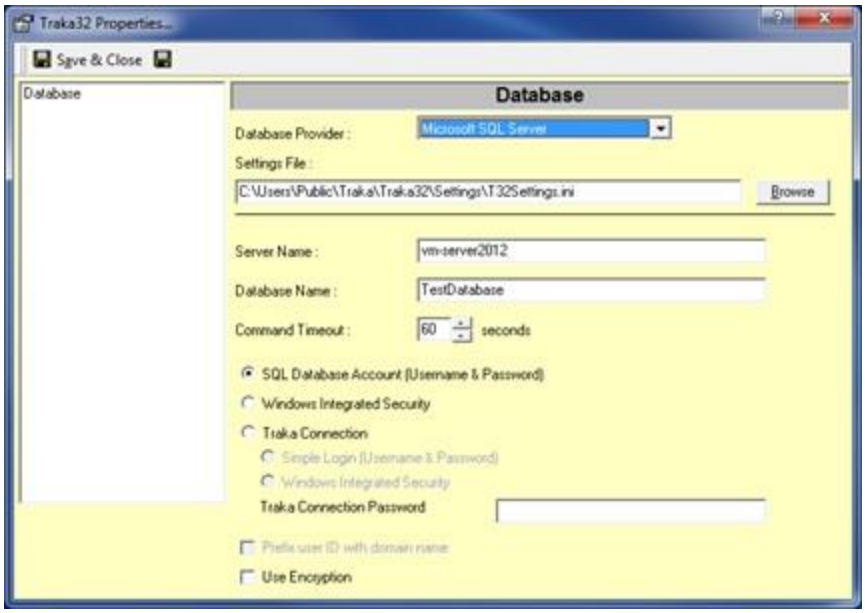
For further details on setting up Software Access please refer to the Software Access using a Microsoft SQL Server Database section.

3.5.5.2.2 INTEGRATED SECURITY

When a user logs into Traka32 that is connecting to a SQL Server, the user must have the appropriate authorisation to connect to the database. This is in order to maintain the highest level of security of the SQL Server and the database.

When Traka32 connects to a SQL Server it has to authenticate the user in one of the following ways...

The type of authentication used can be defined in the Database Properties window in Traka32. To open the Database Properties window hold F11 and open Traka32.



- **SQL Database Account (Username & Password)**

  When a user connects with a specified login name and password, SQL Server performs the authentication itself by checking to see if a SQL Server login account has been set up and if the specified password matches the one previously recorded. If SQL Server does not have a login account set, authentication fails and the user receives an error message.

- **Windows Integrated Security (also known as Windows Authentication Mode)**

  Integrated Security allows a user to connect through a Microsoft Windows (domain) user account.

  SQL Server achieves login security integration by using the security attributes of a network user to control login access. A user's network security attributes are established at network login time and are validated by a Windows domain controller. When a network user tries to connect, SQL Server uses Windows-based facilities to determine the validated network user name. SQL Server then verifies that the person is who they say they are, and then permits or denies login access based on that network user name alone, without requiring a separate login name and password.

- **Traka Connection (recommended)**

  Using the Traka Connection option, Traka32 connects to the SQL Server using an encrypted password. This means that a user is unable to connect directly to the back end database.

  Simple Login (Username & Password): The user's ID and password are set up in the User Details form in Traka32. The user must then use their Traka32 User ID and password to run Traka32.

  Windows Integrated Security: The user's Windows login ID is matched against their Traka32 software login ID. The user must then use their Windows login ID and password to run Traka32. If you tick the checkbox Prefix user ID with domain name, then when a user starts Traka32 the user record will be matched against the domain and Windows login ID.

- **Additional SQL Server Connection String Parameter**

  A new Key called 'AppendToConnectionString' can optionally be added to the [Database] section of the T32Settings.ini file.

  For example:

  ```
  [Database]

  Provider=2

  SQLServer=TrakaServer

  DatabaseName=Traka32

  AppendToConnectionString=MultiSubnetFailover=True
  ```

  From the above example, the text "MultiSubnetFailover=True" will be appended to the end of the normal SQL connection string. If this key is not found then the connection string will be the same as normal.

  Any text can be added into this field as required.

3.5.5.2.3 SQL CONNECTIVITY & BANDWIDTH

Protocol: TCP/IP

Port: The default is 1433.

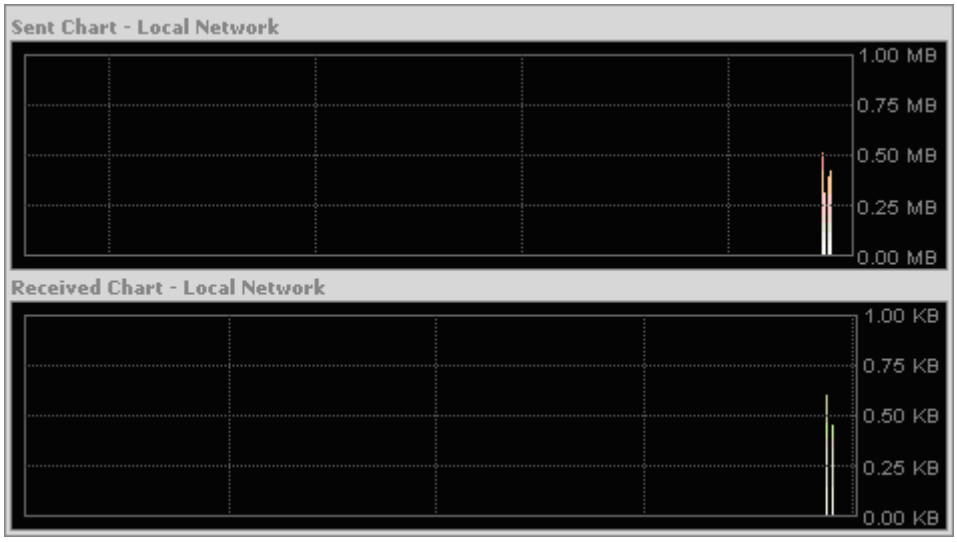
Encryption: Traka32 version 02.05.0024 currently uses Microsoft ADO version 2.7 to connect to either a Microsoft Access or Microsoft SQL Server database. Microsoft has not published any information on the encryption levels of ADO 2.7 so it is not possible for to provide any information therefore it is assumed that there is no encryption currently incorporated in the database connection between Traka32 and SQL Server.

Bandwidth: The minimum acceptable bandwidth is 4M bits (512K bytes) per second. (See below)

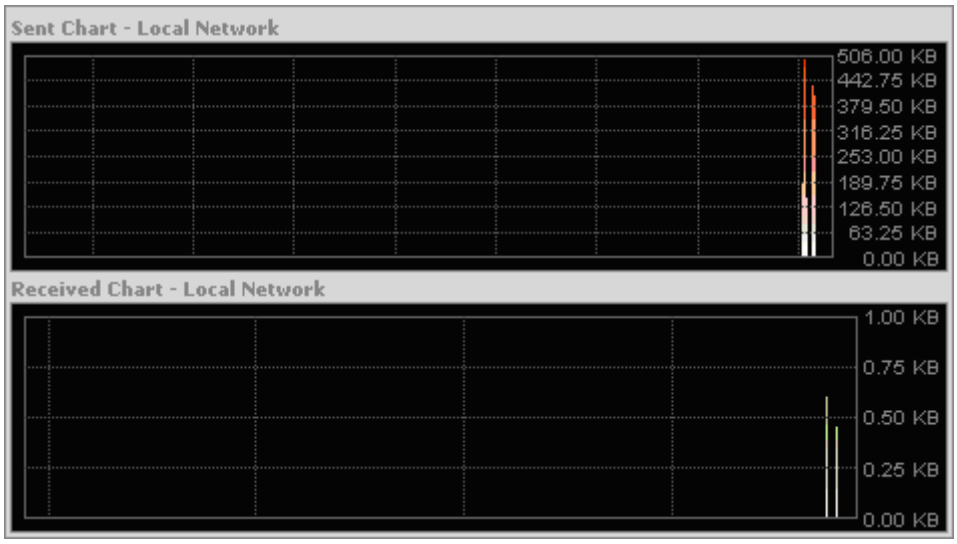
Key List

This is based upon 5,278 Key Records being displayed in the Traka32 key list. This transposes to 1,698.51K bytes of data being sent by the SQL Server to Traka32.

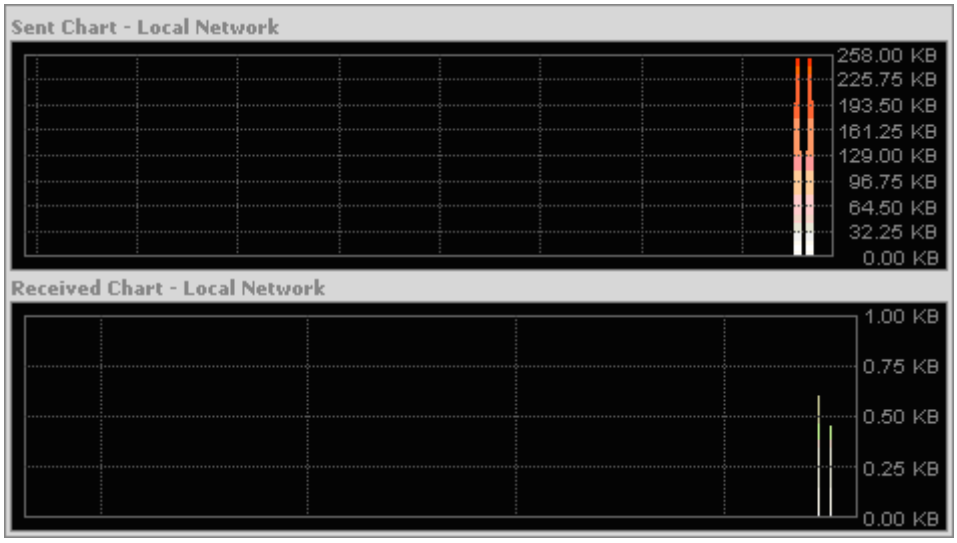
With an unrestricted 100M bits (12,800K byte) per second connection it takes 5 seconds to transfer the data.



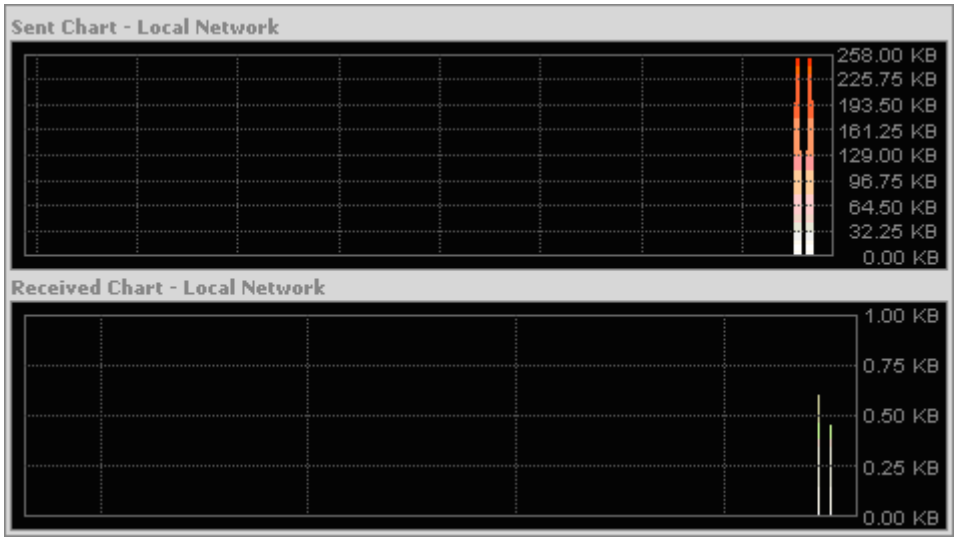
With a restricted 4M bits (512K byte) per second connection it takes 8 seconds to transfer the data.



With a restricted 2M bits (256K byte) per second connection it takes 11 seconds to transfer the data.



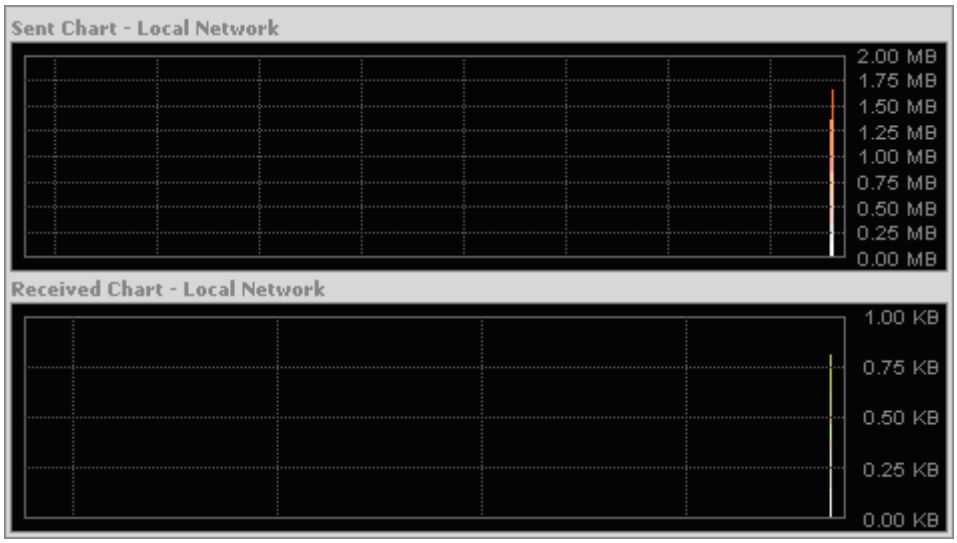
With a restricted 0.5M bits (64K byte) per second connection it takes 31 seconds to transfer the data.



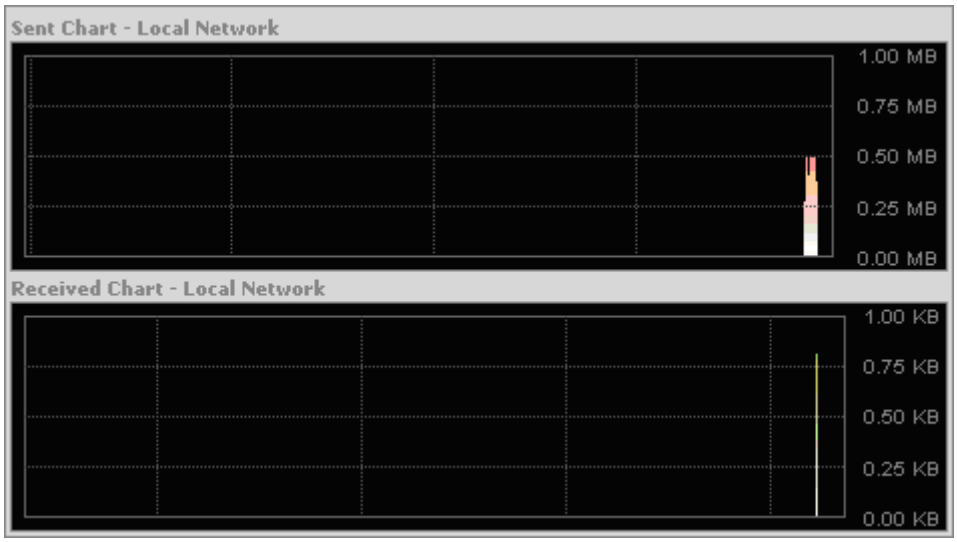
Standard Event Report

This is based upon 23,600 Event Records being displayed in the Traka32 crystal report viewer. This transposes to 3,139.84K bytes of data being sent by the SQL Server to Traka32.

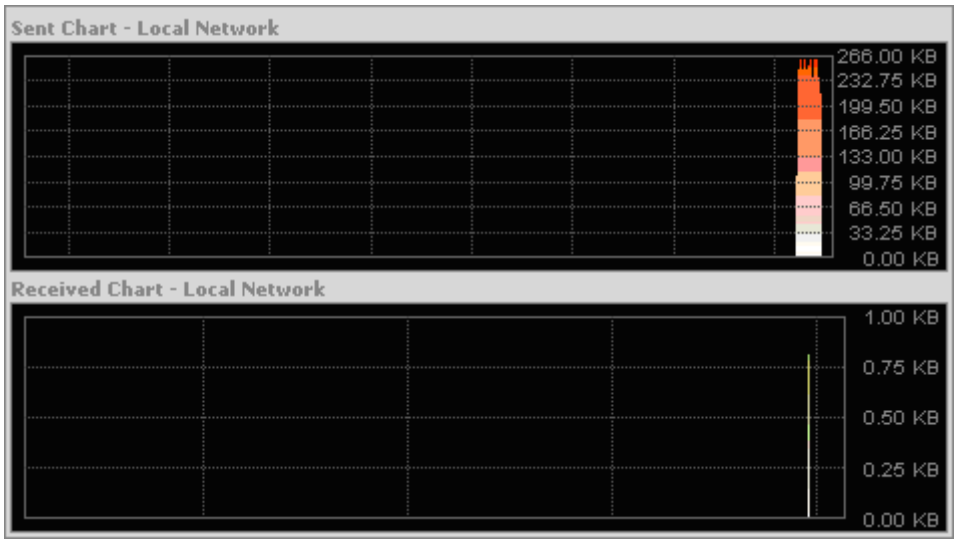
With an unrestricted 100M bits (12,800K byte) per second connection it takes 2 seconds to transfer the data.



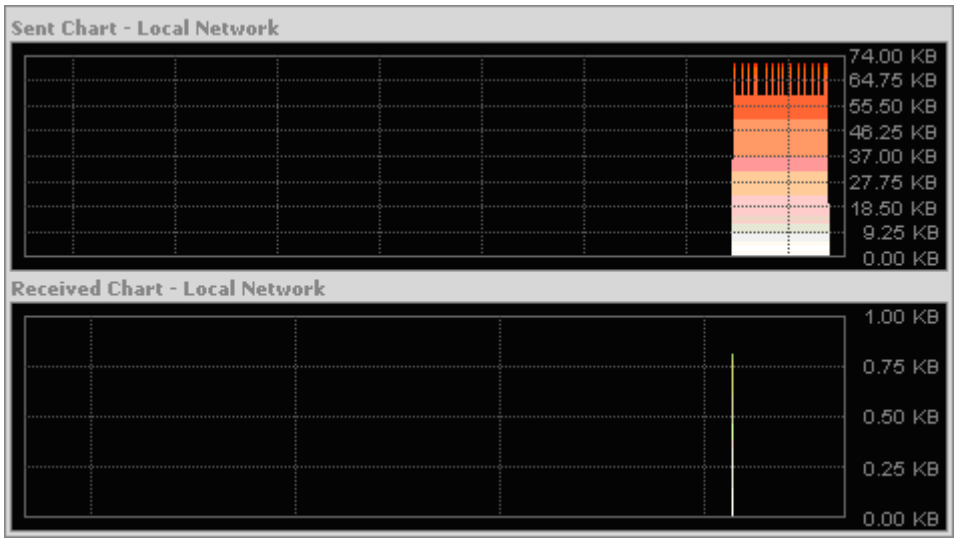
With a restricted 4M bits (512K byte) per second connection it takes 6 seconds to transfer the data.



With a restricted 2M bits (256K byte) per second connection it takes 12 seconds to transfer the data.



With a restricted 0.5M bits (64K byte) per second connection it takes 45 seconds to transfer the data.



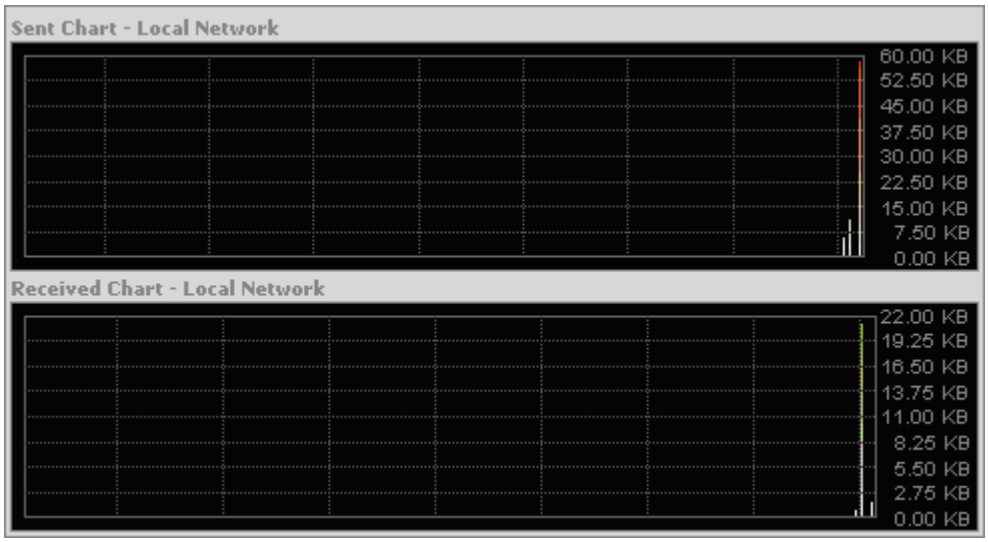
Editing a User Record

This is based upon opening and editing a single user record that has access to 2 Traka Systems. This transposes to 74.36K bytes of data being sent by the SQL Server to Traka32.

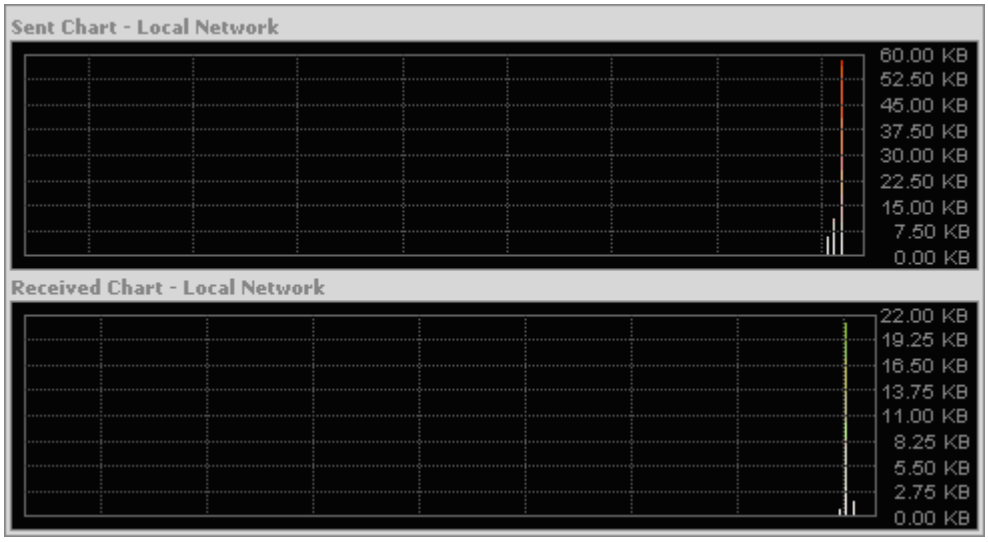
NOTE: This does not include any communication between Traka32 and the Traka Systems directly. Please refer to the XPort Connectivity & Bandwidth section for details.

When editing user records it takes minimal time to open the data within Traka32 and save the changes back to the database.

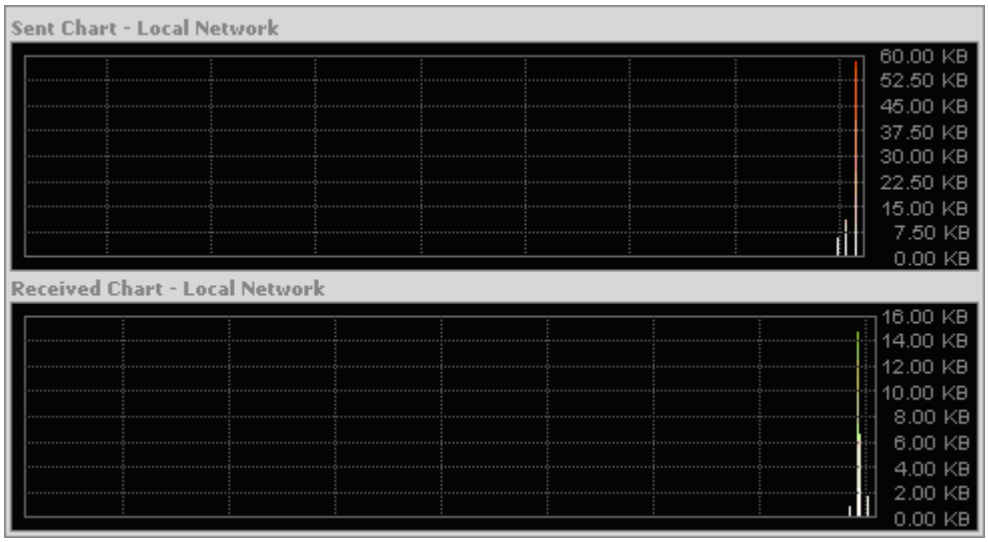
With an unrestricted 100M bits (12,800K byte) per second connection:



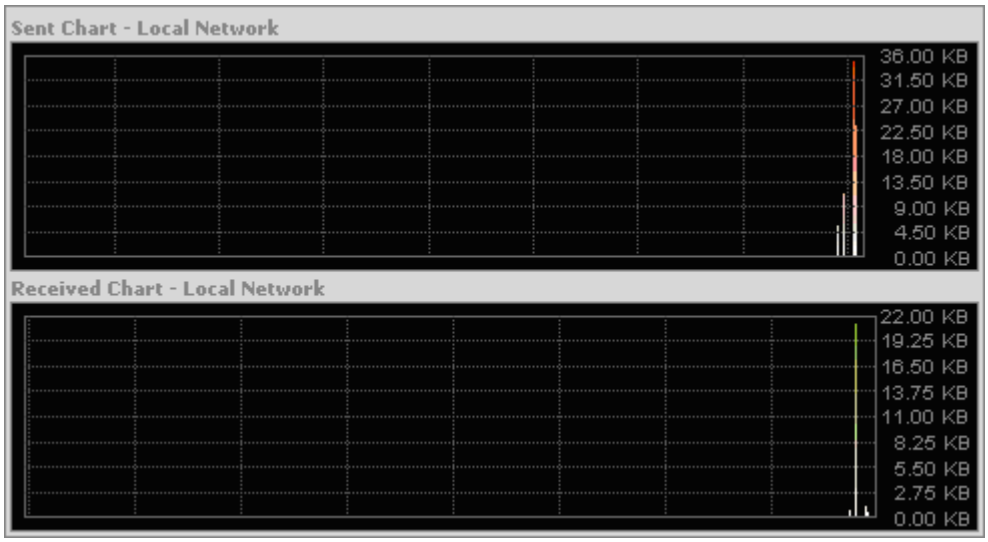
With a restricted 4M bits (512K byte) per second connection:



With a restricted 2M bits (256K byte) per second connection:



With a restricted 0.5M bits (64K byte) per second connection:



3.5.5.2.4 SQL SERVER

3.5.5.2.4.1 MICROSOFT SQL INSTALLATION

This section provides a guide for configuring an installation of Traka32 for use with SQL Server. It assumes the reader is already familiar with the Traka32 software, SQL Server Management Studio and SQL Server security.

Before Installing Traka32

1. Install and configure SQL Server.

   NOTE: Traka32 is compatible with all collation orders.

2. Create an empty database in SQL Server for Traka32 to use. The standard name for the database is T32Database.

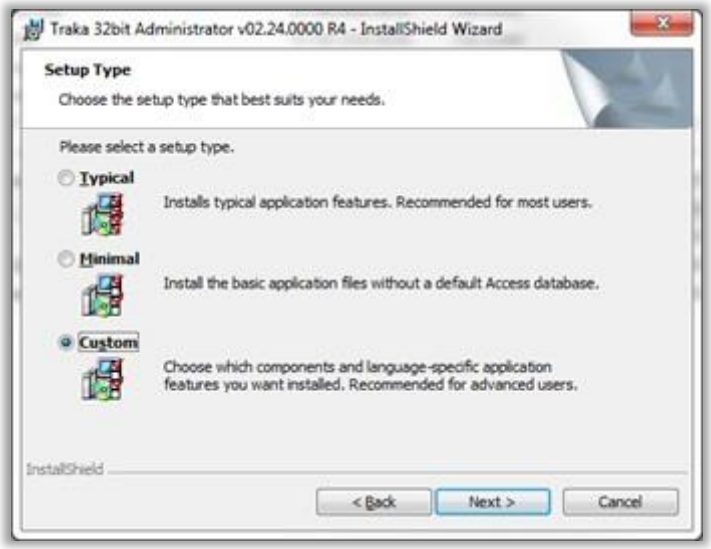
   NOTE: It is left to the Database Administrator (DBA) to determine suitable file locations, sizes and backup/restore policies.

Installing Traka32 and Server Tools

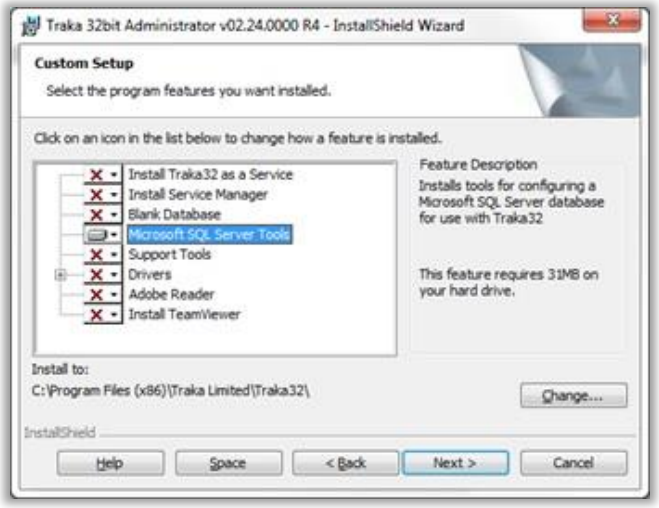
1. Run the Traka32 installation as usual.

   The installation for managing SQL Server does not have to be located on the same machine as SQL Server itself however the Traka SQL Server Manager requires the SQL DMO Object Library to work.

2. At the **Setup Type** dialog, select the **Custom** option:



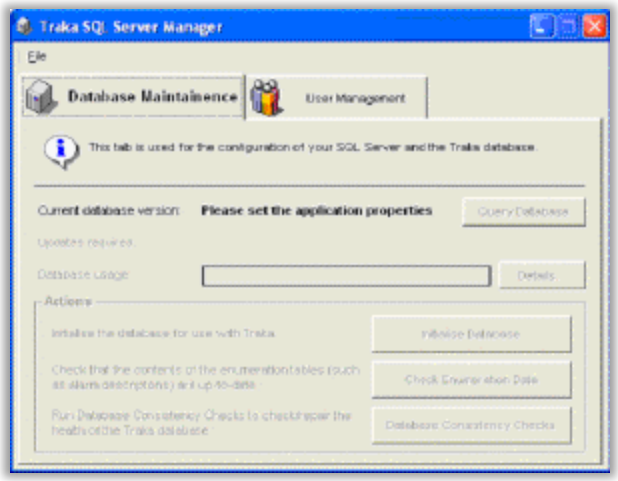
3. Remove the **Blank Database** from the setup and include Microsoft SQL Server Tools:



4. Complete the set-up as usual. When the installation has finished, uncheck the **Launch application now checkbox** and click on **Finish**.

Connecting to SQL Server and Creating a Database

1. Click **SQL Server Manager** from the **Traka** program group in the **Start** menu to open the Traka SQL Server Manager:



2. Select **File>Properties**.

3. Click the selector button (...) next to the **SQL Server** box and select the installation of SQL Server where the Traka database is located and click **OK**:

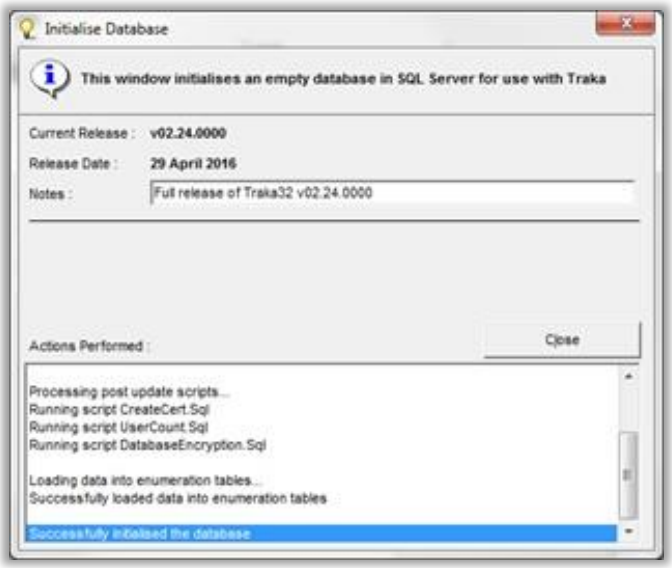
4. If you are using Integrated Security or SQL Connection Encryption tick the appropriate boxes.

5. Click the selector button (...) next to the **Traka Database** box, noting that if **Integrated Security** is not being used, you will be prompted for your SQL logon details and select the appropriate database and click the **OK** button:

6. Check the **Query the state of the Traka database when the application starts** checkbox, and then click **OK**.

7. Click the **Initialise Database** button:

8. Confirm the **Current Release** is correct and click the **Initialise Database** button. The actions performed should be displayed as follows:



9. Close this dialog and the main window should appear as follows:

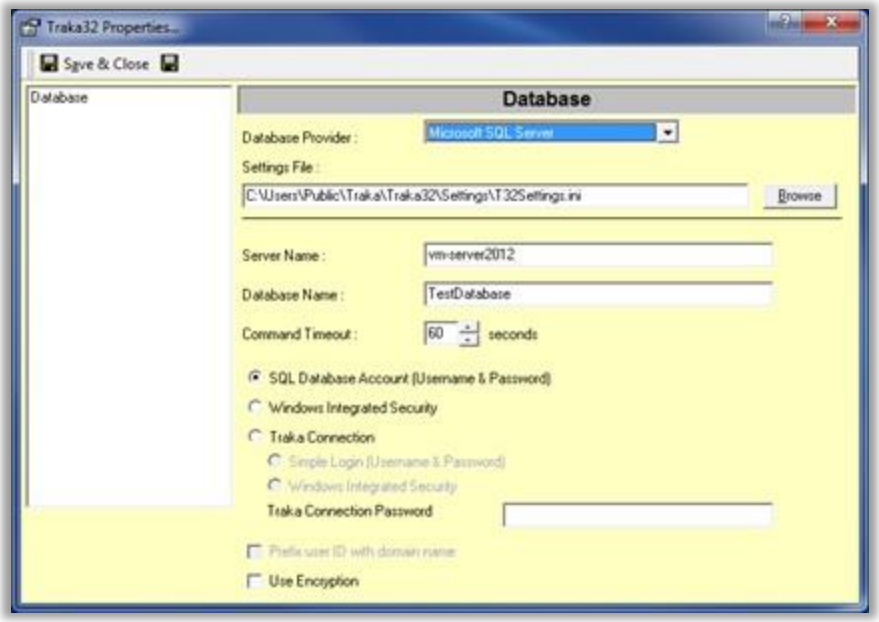
10. The initialisation is now completed and the database is ready for use with Traka. The Manager tool can also be used to query the state of the database by clicking the **Details...** button, which displays an overview of the state of SQL Server and the Traka database. Database consistency checks and basic user management can also be undertaken from the Manager.

    NOTE: Whilst the extended functions in the Manager work, it is recommended that all management tasks, including user management, are undertaken from SQL Server Management Studio.

    The **Check Enumeration Data** button can be used at any stage to ensure that the data held in the enumeration tables is consistent, although this should not be required during normal operation.

Configuring and Starting Traka32

1. Before Traka can be started, it needs to be pointed to SQL Server. To achieve this, single-click the Traka32 icon on the desktop, press-and-hold the **F11** key, and then double-click the Traka32 icon. The **Traka32 Properties...** dialog should appear (you can release F11 key when it does):



2. Change the **Database Provider** to **Microsoft SQL Server** and enter the appropriate **Server Name** and **Database Name**.

3. Adjust the **Command Timeout** value in seconds accordingly. The default command timeout value is 60 seconds. If you experience **Command Timeout Error** messages then increase the command timeout values in increments of 10 until the errors no longer appear.

   NOTE: It is not recommended that you enter a command timeout value below 30 seconds.

4. If you are using Integrated Security, select the appropriate option from those available.

5. Click **Save & Close**.

6. Re-start Traka32 by double-clicking the Traka32 icon on the desktop.

   If required, you will be prompted for your SQL Login details. At this stage, this will need to be the built-in "sa" login or a user who is mapped to the database owner.

7. The Traka32 interface should now appear with no systems defined.

3.5.5.2.4.2 ACCESS TO SQL MIGRATION

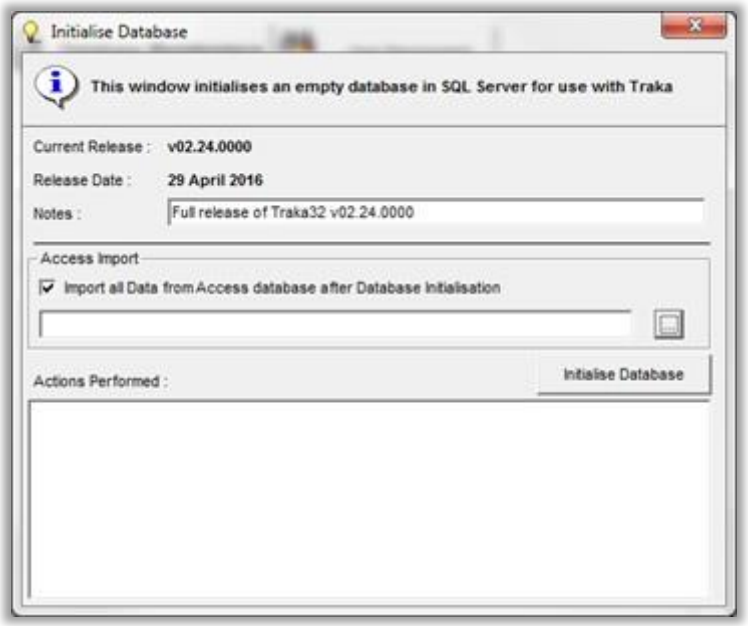
This topic describes how to import data to a Traka SQL Database from a single Traka Access Database. It assumes the reader is already familiar with the Traka32 software, SQL Server Enterprise Manager and SQL Server security.

Before You Start

- If you wish to import multiple Access databases to one SQL database please contact Traka as this topic does NOT cover this scenario.
- The version of the Traka32 software that is used with the Access database MUST be the exact same version as that being used with the SQL database. If the versions are different, upgrade the Traka32 software that is used with the Access database to the same version as going to be used with SQL prior to migrating. You must also run the Traka32 software so the database checks are made. This is to ensure the Access and SQL database structures are the same.
- When upgrading from Access to SQL server you will receive another 90 days evaluation period to cover the time needed to get another unlock code.

Installation

1. During the initialisation of the database as described in the Microsoft SQL Installation topic, the below screen will appear. Tick the option to **Import all Data from Access database after Database Initialisation**.



2. Click the (...) button to browse to and select the existing Access Database. Once selected click **OK**.
3. Select **Initialise Database**.
4. Continue with the process in the Microsoft SQL Installation topic to configure Traka32 to point to the new database.

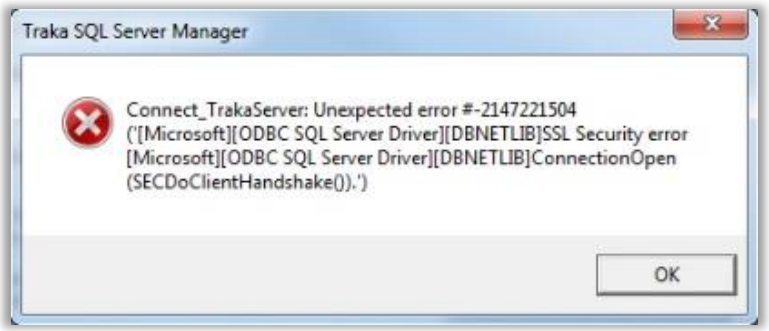
3.5.5.2.5 TRAKA SQL SERVER MANAGER V2

There is an additional v2 version of the Traka SQL Server Manager program. This version is only required if you are creating or updating the Traka32 database schema or you are starting with a new installation of the Traka32 software and the TLS 1.0 protocol has been turned off on your server.

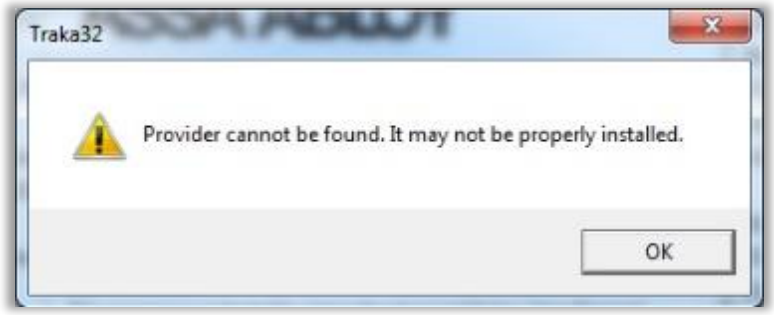
NOTE: Traka32 version 02.39.0000 or higher will be required if installing Traka SQL Server Manager v2.

1. Ensure that the Support for Non TLS 1.0 enabled servers option is selected within Traka32 Properties. Please refer to section 3.9.1 for more information.

If TLS 1.0 is turned off on the server that hosts the SQL Server Database and you attempt to connect Traka32 using the default connection properties, the following message will be displayed:



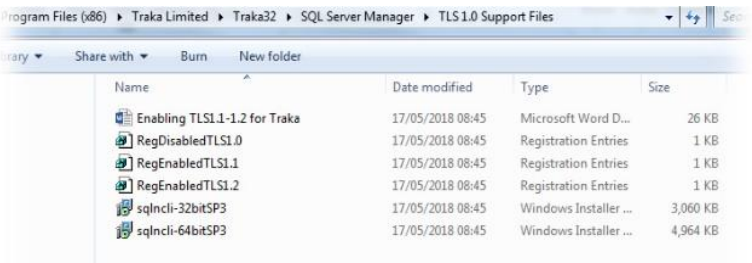
If you have selected the **Support for non-TLS 1.0 enabled servers** option, and when connecting to the database, you receive the following message:



You will need to install one of the following Native Clients; **Sqlcli-32bitSP3** or **Sqlcli-64bitSP3.** The installation files will be located in the Traka32 directory within the TLS 1.0 Support files.

The installation files will be located in the Traka32 directory, within the TLS 1.0 Support files.

2. Launch either the 32bit or 64bit installation, depending on your Operating System.



3. Follow the on-screen instructions for the installation.

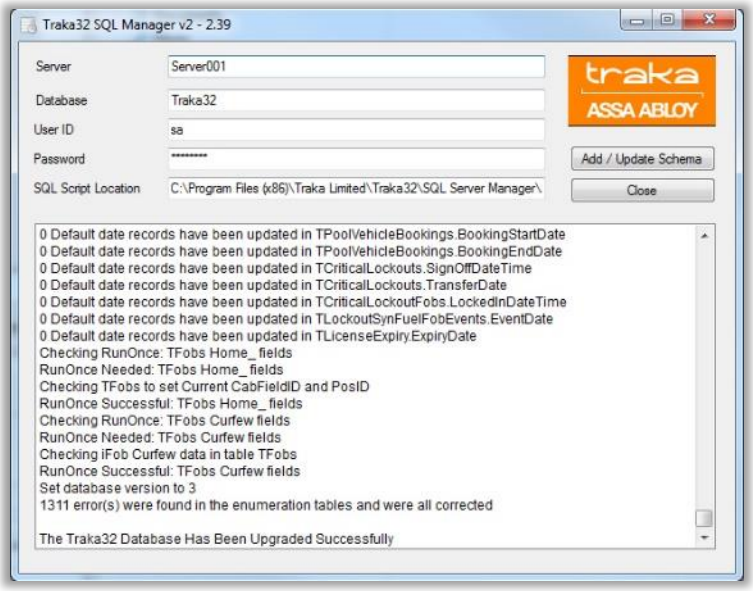
NOTE: Ensure that .Net Framework 4.6.2 is installed.

Once the installation has completed, the SQL Server Manager v2 can be located from the Start menu.

4. Launch the SQL Server Manager v2.
5. Complete the on-screen information as required. You can choose to use an existing database or create a new database by simply entering a new name.

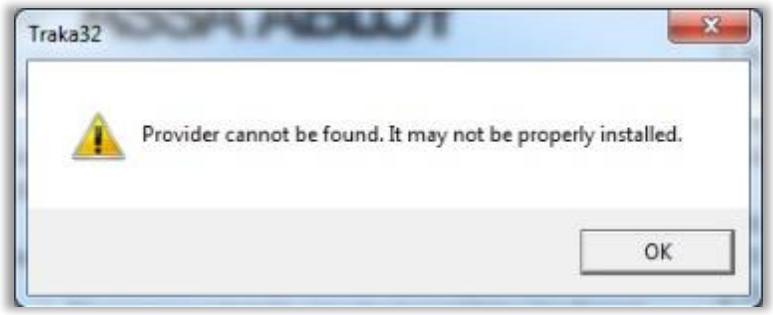
NOTE: If Traka32 hasn't been installed in the default location, you will be required to change the path to where the SQL scripts have been installed prior to adding or updating the database schema.

6. Select **the Add/Update Schema** button to apply the changes.



If you are not upgrading or installing Traka32 and TLS 1.0 is turned off, refer to section 3.9.1 and ensure that Support for Non TLS 1.0 enabled servers option is selected.

If the Native client has not been installed when you launch Traka32, you will receive the following error message:



Refer to note 2 of this section for details on installing the SQL Server 2012 Native Client.

3.6 COMMISSIONING

3.6.1 COMMISSIONING OVERVIEW

Hopefully by this stage you will have installed your Traka systems and have at least one copy of the Traka32 software installed. If not please refer to the following sections...

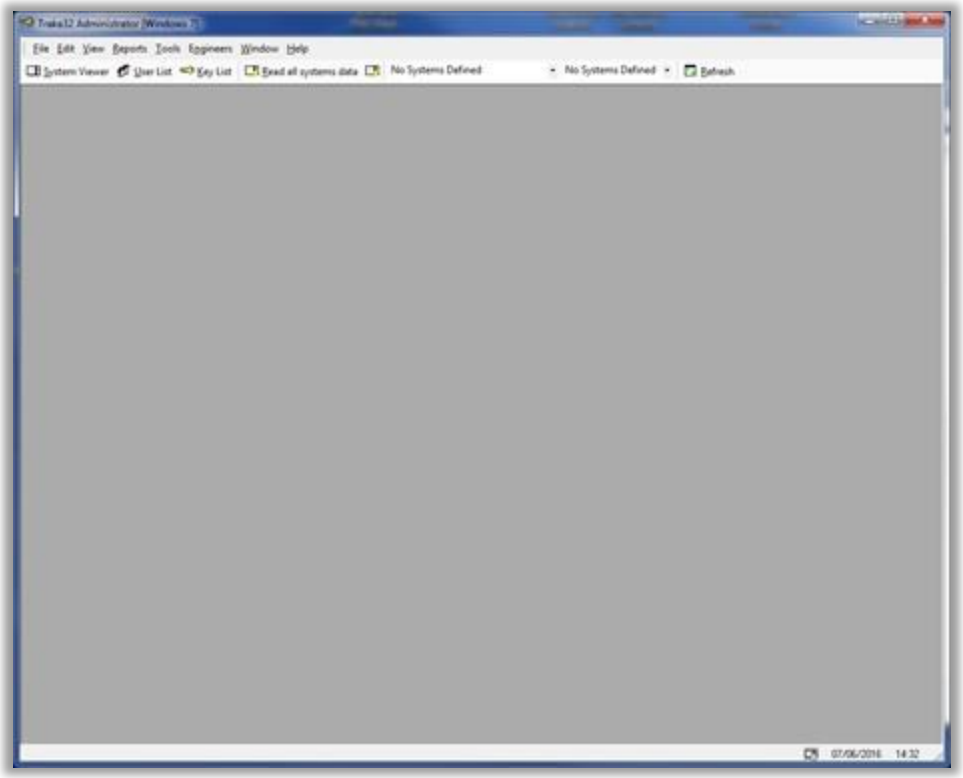
- Planning
- Hardware Installation
- Communication Installation
- Software Installation

The commissioning stage will take you through the configuration and testing of the Traka systems using the Traka32 software. Once this stage has been completed you can then start to use your Traka systems.

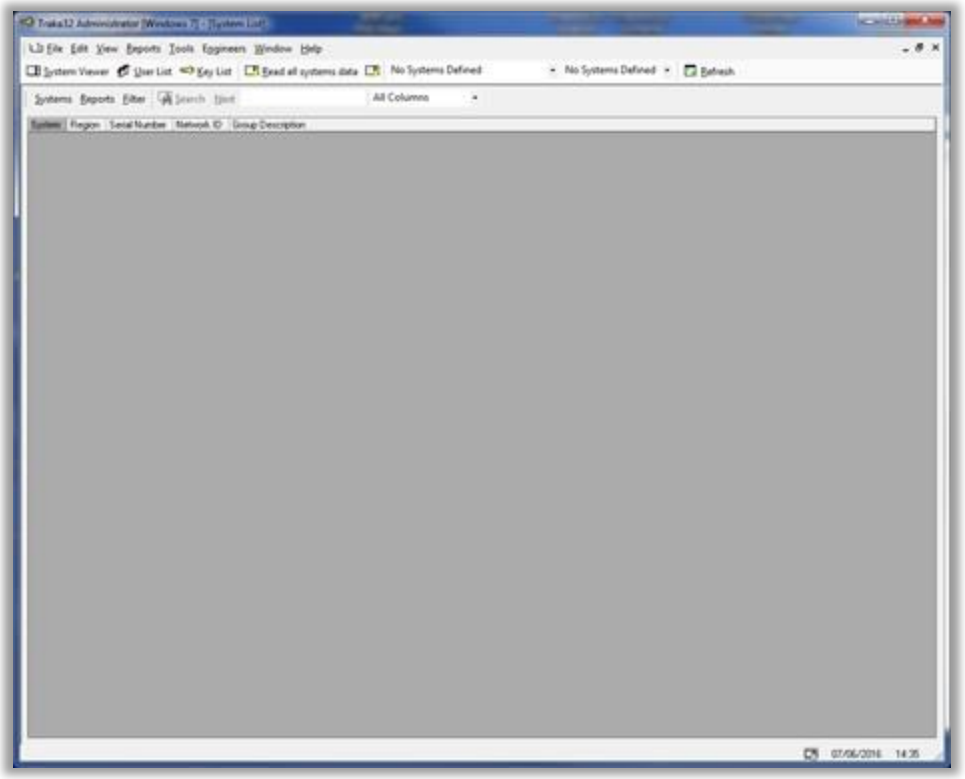
3.6.2 CONFIGURING SYSTEMS

Before you can start administering your Traka Systems from the software, the system details must be defined. Once defined, you will be able to configure the iFobs, Key and User details and start to use the Traka System to its full potential.

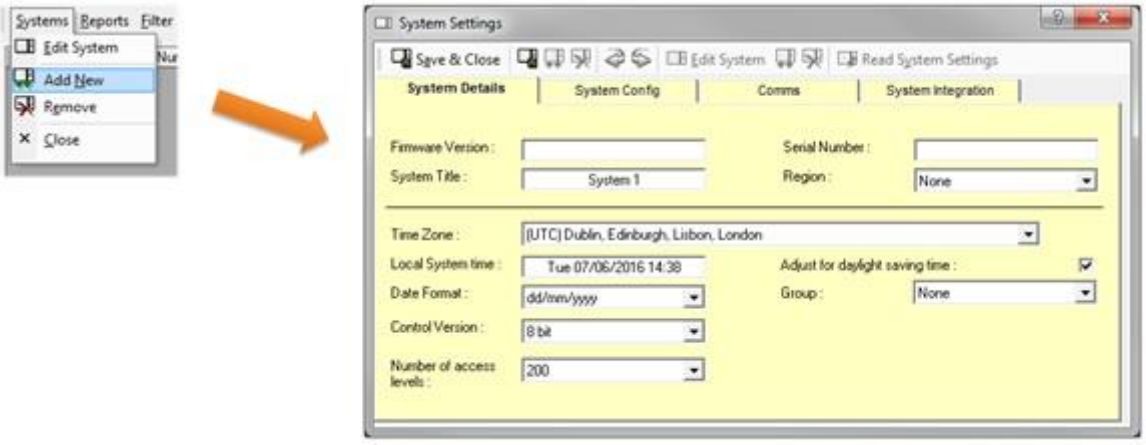
1. Load the Traka32 software by double clicking on the  icon.
2. If you have not registered your software yet, please refer to the Traka32 registration section.
3. If you have not configured your database path yet, please refer to the database installation section.
4. When Traka32 has loaded for the first time you will be presented with a grey screen.



5. Click on the **Tools** menu followed by **Configure Systems** and you will be presented with the System List.



6. Click on the **Systems** Menu followed by **Add New** and you will be presented with a new System Settings window.



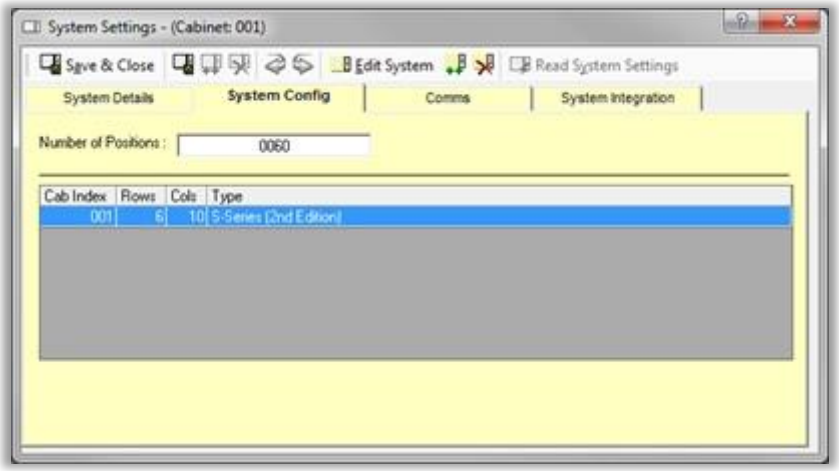
7. Enter a **System Title** to represent the system you are adding for example Reception or Basement.

8. Enter the **Serial Number** of the system for reference. This can be found on the inside of the Pod and starts TKC, for example TKC10123.

9. Set the **Time Zone**, **Daylight Saving** and **Date Format** as required.

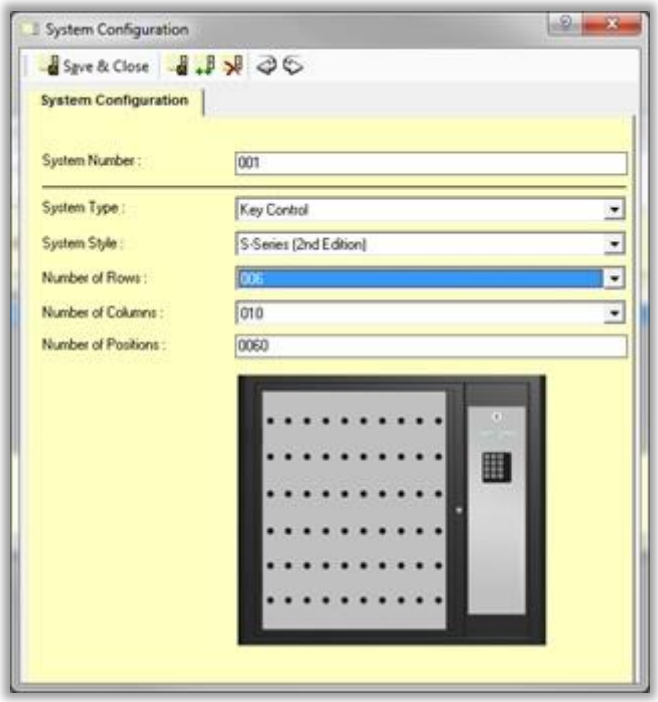
10. Set the **Control Version** to **8bit** or **16bit** depending on the hardware fitted to your Traka System.

11. Click on the **System Config** tab.



12. You will see a list of cabinets that are attached to the system. A system comprises of a control pod and one or more cabinets. By default there is one cabinet that has 6 receptor strips or rows. You must alter the cabinet configuration to match that of your physical system as follows.

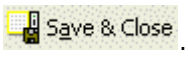
    To edit the default cabinet, either double click on the cabinet in the list or click on **Edit System**.



    Simply edit the **Number of Rows** and **Columns** to match that of the Cabinet in the System.

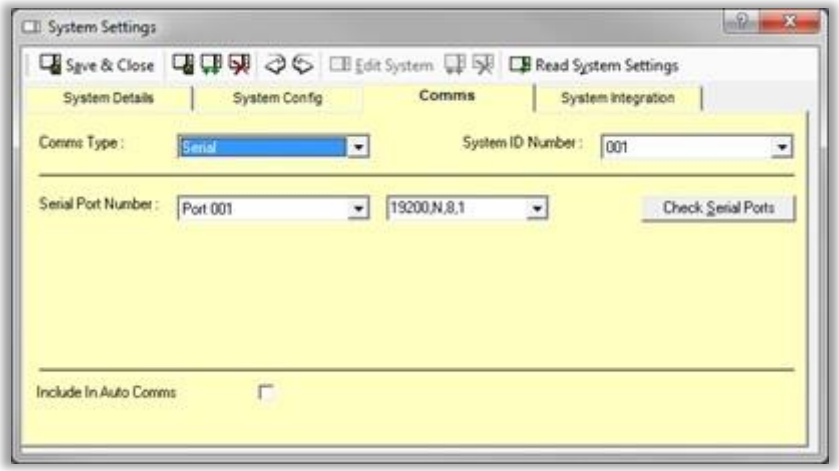
    To Add a Cabinet, click on  .

    To Remove a Cabinet, click on  .

    To save the changes, click on  or 

.

13. Click on the **Comms** tab.



14. You will see a **Comms Type** drop down menu. From this you can select:

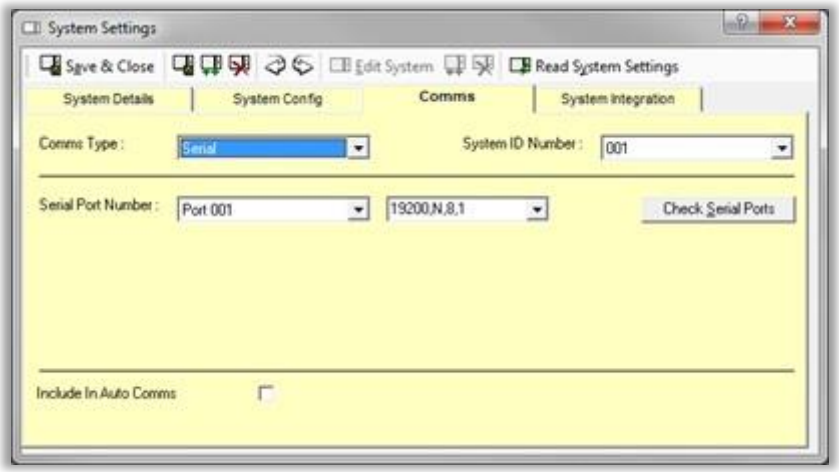
    a. Serial for RS232 or RS485.

    b. Modem.

    c. Network for Ethernet.

15. Select the appropriate communication setting.

16. If you have chosen **Serial**, select the following options:



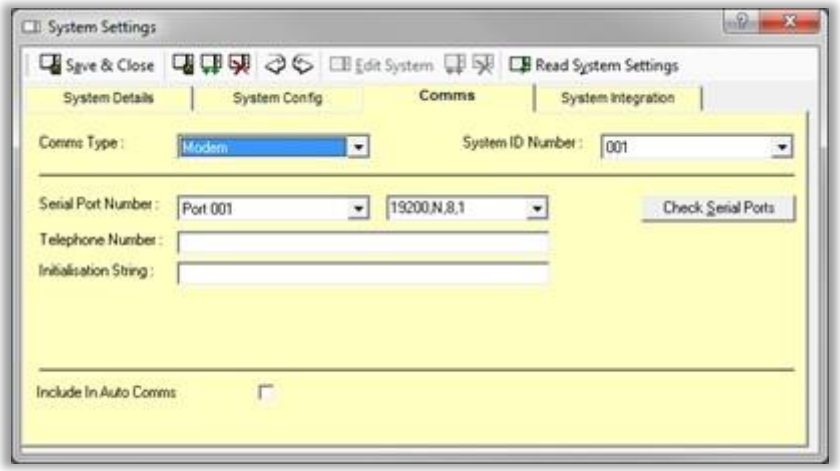
    a. **Serial Port**
    Select the Serial Port of the PC that you have connected the Traka System to.

    b. **Serial Port Settings**
    Select the appropriate serial port settings.

    For an **8bit** system the setting depends upon the type of **crystal** your Traka system has been fitted with. Set **9600,N,8,1** if the 8bit Control PCB is fitted with a **3MHz** crystal or set **19200,N,8,1** if the 8bit Control PCB is fitted with a **7MHz** crystal. Please refer to the 8bit Control PCB Diagrams to locate crystal type.

    For a **16bit** system the default setting is **38400,N,8,1.** The 16bit hardware can also be configured for 19200,N,8,1 or 9600,N,8,1 if required.

17. If you have chosen **Modem**, select the following options:



a. **Serial Port Number**
Select the Serial Port of the PC that you have connected the Traka System to.

b. **Serial Port Settings**
Select the appropriate serial port settings.

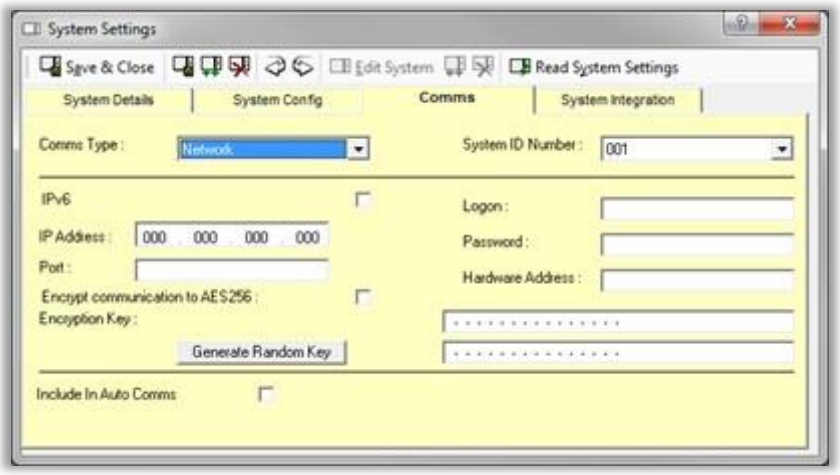
For an **8bit** system, the setting depends upon the type of **crystal** your Traka system Control hardware has been fitted with. Set **9600,N,8,1** if the 8bit Control PCB is fitted with a **3MHz** crystal or set **19200,N,8,1** if the 8bit Control PCB is fitted with a **7MHz** crystal. Please refer to the 8bit Control PCB Diagrams to locate crystal type.

For a **16bit** system the default setting is **38400,N,8,1.** The 16bit control hardware can also be configured for 19200,N,8,1 or 9600,N,8,1 if required.

c. **Telephone Number**
Enter the telephone number of the modem you wish to dial.

d. **Initialization String**
Please refer to your modem user guide to work out the appropriate initialization string. The default setting is **ATV0X4N1L1Q0&M0%C0&K0\N0** and should apply to most modems.

18. If you have chosen **Network**, select the following options:



a. **IP Address**
Enter the IP Address of the Ethernet device.

b. **Port**
Enter the Port number of the Ethernet device, this is usually **4001** for the Moxa device and **10001** for the XPort device.

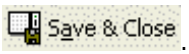
c. **Logon**
This is not currently required for the commonly used Ethernet devices but is available if a different type of device is required.

d. **Password**
Again this is not currently required for the commonly used Ethernet devices but is available if a different type of device is required.

e. **Hardware Address**
This field is for reference only to help with the administration of the Ethernet devices. The Hardware Address is also known as the MAC Address, for example 00-90-E8-04-31-38.

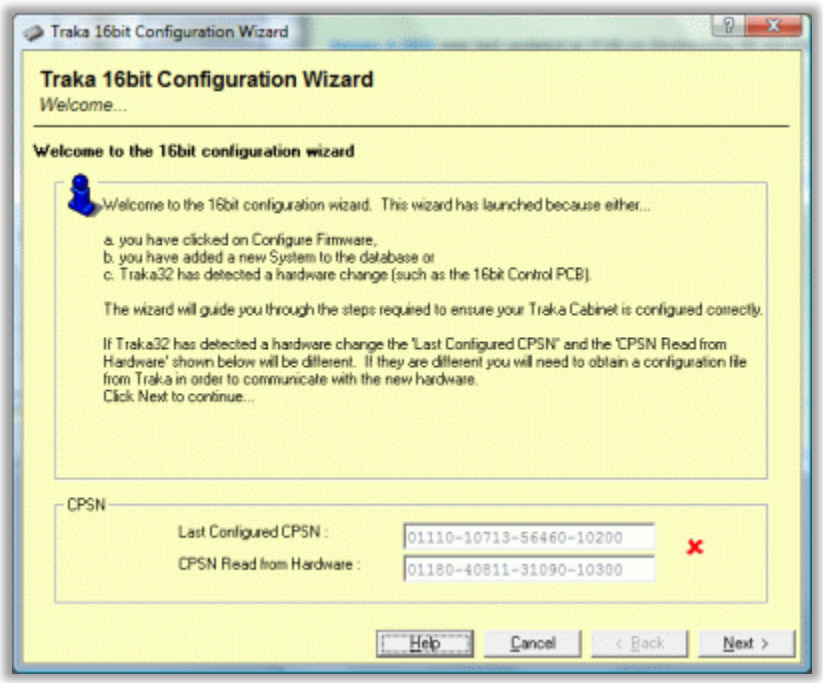
f. Select the **System ID Number** from the drop down menu. The System ID Number has to match that of the number programmed in the Traka System. For most systems this number will be 001. Please refer to the Configuration Menu section for details on setting the System ID.

g. Do not worry about the **System Integration** tab at the moment as this can be configured later.

19. When you are happy with your configuration click on  or 

.

20. If you have a 16bit Traka System, the 16bit Configuration Wizard will launch allowing the hardware to be registered and configured. Please refer to the Adding a 16-bit System section for more details.



21. Now refer to the Initialising Systems section.

3.6.3 ADDING A NEW 16BIT SYSTEM

When adding a new 16bit Traka System to a database, the **16bit Control PCB must be registered to the database with a configuration file**.

Because the 16bit application firmware is generic and not customer specific (like the 8bit firmware), a configuration file is required to customise the firmware for each system. The configuration file contains the configurable parts to the system such as the number of receptor strips and card reader settings as well as the cost options.

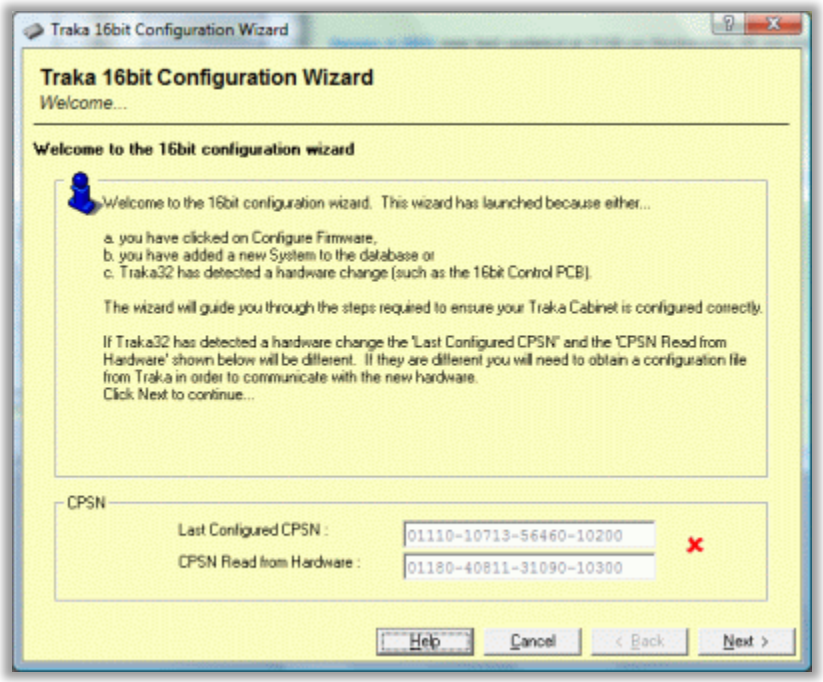
Without a configuration file, a Traka System can be used as normal, however no cost options will be enabled and the card reader settings will remain as they were last programmed into the Control PCB.

The communications between Traka32 and the Traka System will also be possible for up to 30 days, but every time communications is initiated, Traka32 will prompt for a configuration file first.

NOTE: When adding a new 16bit System, it is very important to set the Control Version in the System Settings window to 16bit.

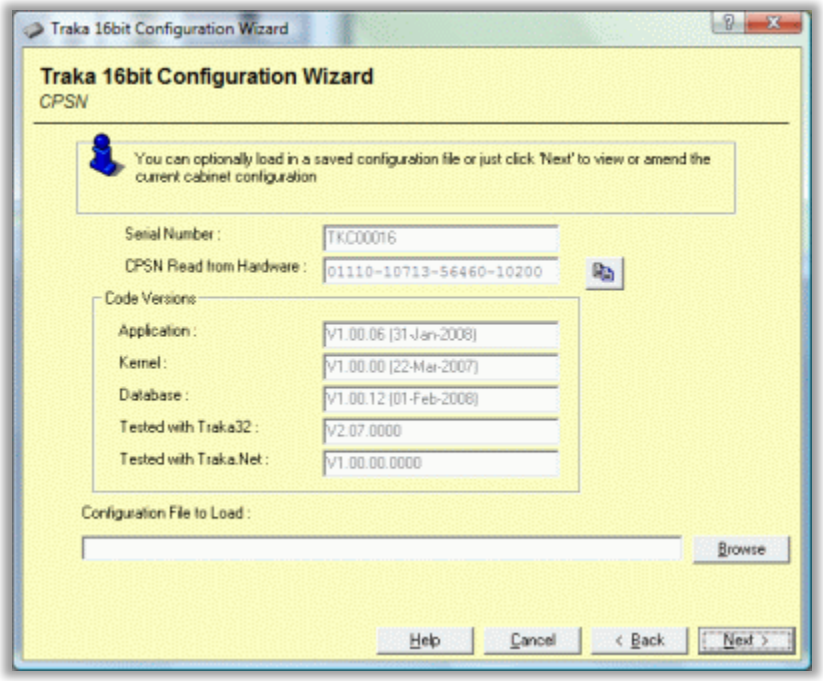
Adding a New 16 bit System

1. When adding in a new 16bit System and communicating for the first time, the 16bit Configuration Wizard will be displayed.



2. Click on **Next**.

3. The CPSN window is displayed confirming the Serial Number, CPSN Read from Hardware, the Hardware and Code versions and also the Traka32 version the firmware was tested with.



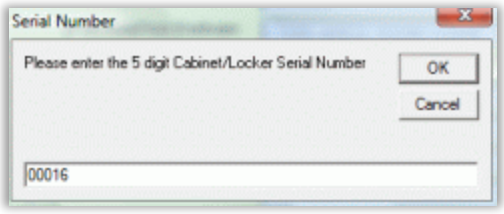
You will need to contact your distributor quoting the **CPSN Read from Hardware**. The distributor will them be able to e-mail you with a configuration file for your hardware.

TIP: Click the  **button to copy the CPSN to the clipboard for pasting into a file or email.**

4. Once you have obtained the configuration file from Traka or your distributor, **save** it to the machine from which you wish to load it.

5. Click **Browse** to search for the configuration file.

6. Enter the 5 digit serial number of the Traka system (excluding TKC,TIL etc).



7. Click **OK** and browse to the location the configuration file was saved to. Only configuration files matching that of the entered serial number will be available for selection.

   The configuration file name is structured as follows:

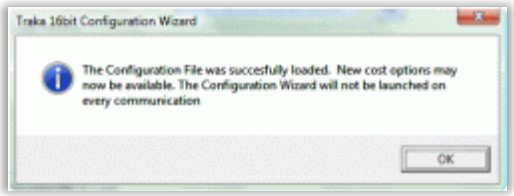
   <Serial Number> - <CPSN Number> - <Firmware Version>.TKCcfg

   For example, for a system with a serial number TKC12345, a CPSN of 01041006164704010200 and a firmware version of 1.00.00, the following file is required:

   12345 - 01041006164704010200 - 010000.TKCcfg

8. When you have selected the path to the configuration file, click on **Next**.

If the configuration file was correct a message will be displayed indicating the hardware will be licensed to the database and any cost options will become available. A message is displayed indicating the file has been successfully loaded.



NOTE: This indicates it has been loaded into the Traka32 database only at this stage and not yet applied to the cabinet.

If the configuration file was incorrect, check that you have the correct file via the file name and try again. An incorrect file may be because:

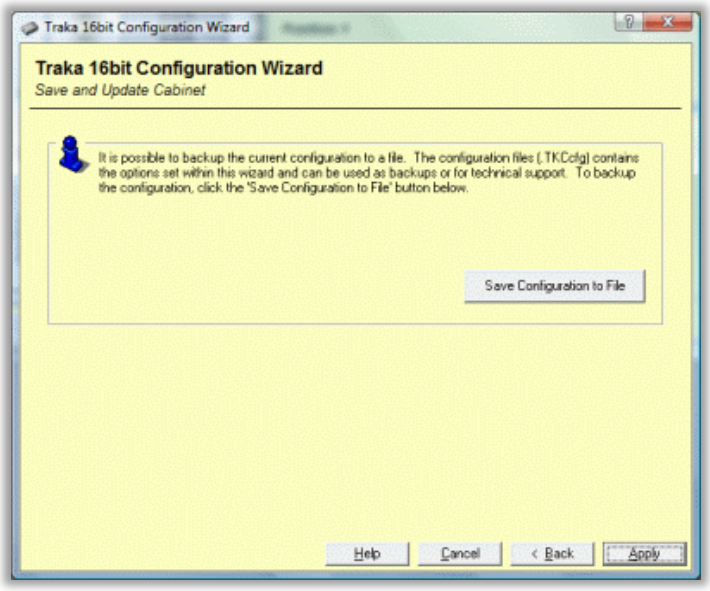
a. The CPSN did not match,

b. The Hardware Key did not match or,

c. The Firmware Version did not match.

9. Follow the wizard through, checking ALL the settings and amend as required. For details on the various settings, please refer to the Firmware Options & Settings section.

10. Finally click on **Apply** to load the configuration into the cabinet.



If you wish you may also save the current configuration (with any changes) to a File. Click the **Save Configuration File** button to do so and provide a suitable name for the file perhaps indicating any specific options that it contains.

11. Now that the new 16bit Control PCB's CPSN has been registered, you will be able to communicate as normal.

Also View:-

16bit System File Types

16bit Configure Firmware Wizard

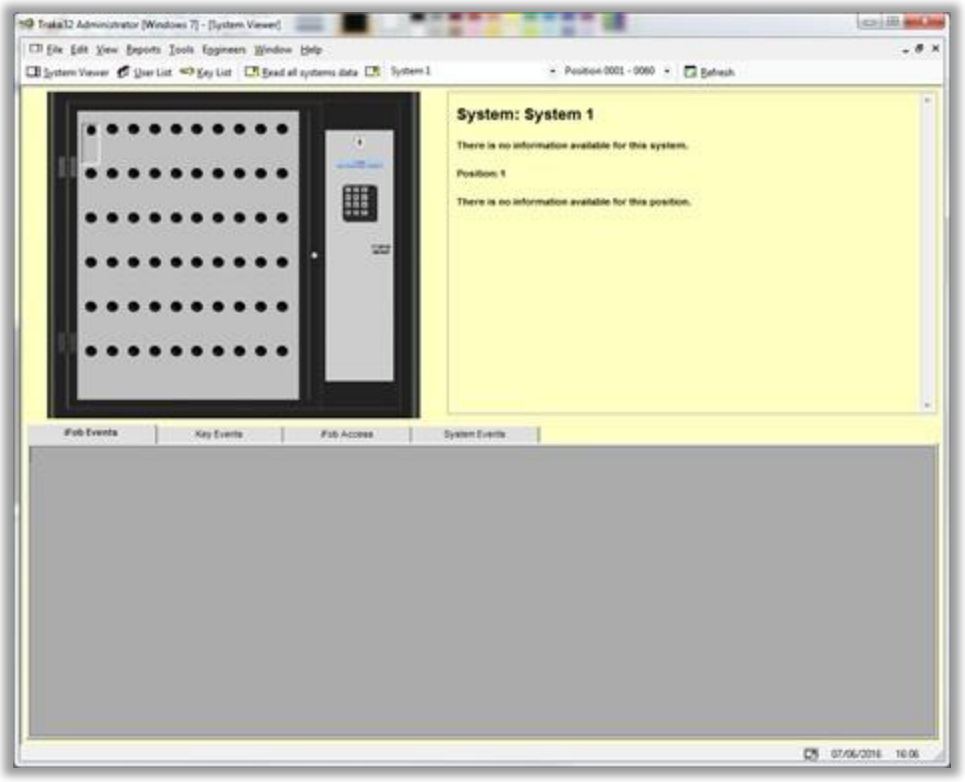
Changing Hardware

Changing Firmware Settings

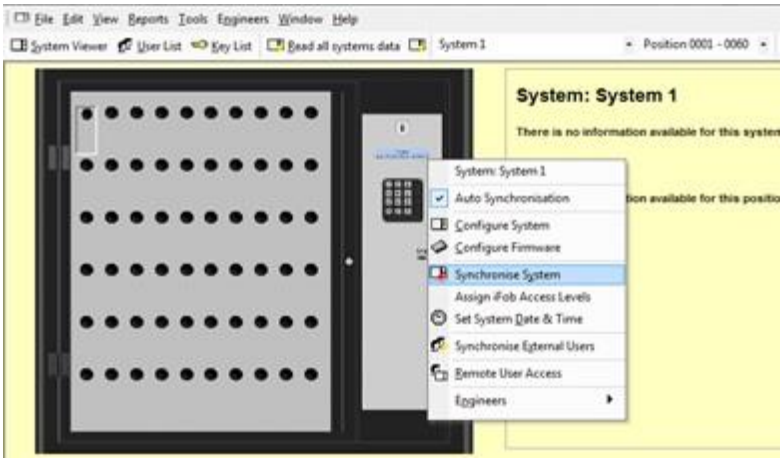
3.6.4 INITIALISING SYSTEMS

When Traka Systems are delivered the memory within the system can become corrupt especially if x-ray machines are used to check the packages. To ensure there is no corrupt data within the system you must reset the memory and set the date and time.

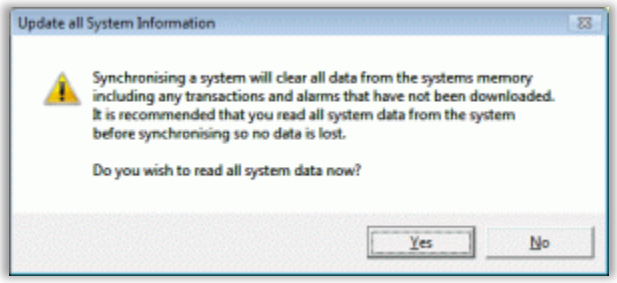
1. When you have configured the systems you can view the system by clicking on **View** followed by **System Viewer**. This is the default view that will be shown whenever the software is loaded.



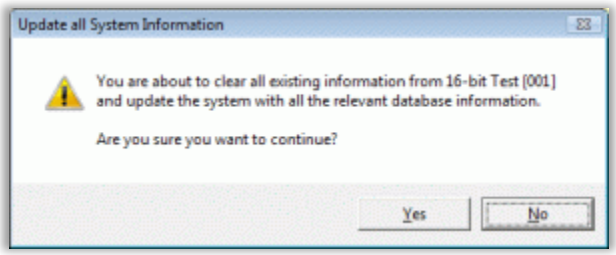
2. To reset the memory and set the date and time, simply click with the right mouse button over the picture of the system and click on **Synchronise System**.



3. You will be asked if you wish to read all system data. Click on **No**.



4. When asked if you are sure you want to continue, click on **Yes**.



5. The software will then communicate with the Traka System.

This should only take a few seconds. If the communications fails, check the communications settings and installation. If communications still fails you will need to contact your supplier for further help.

6. Now refer to the Configuring iFobs section.

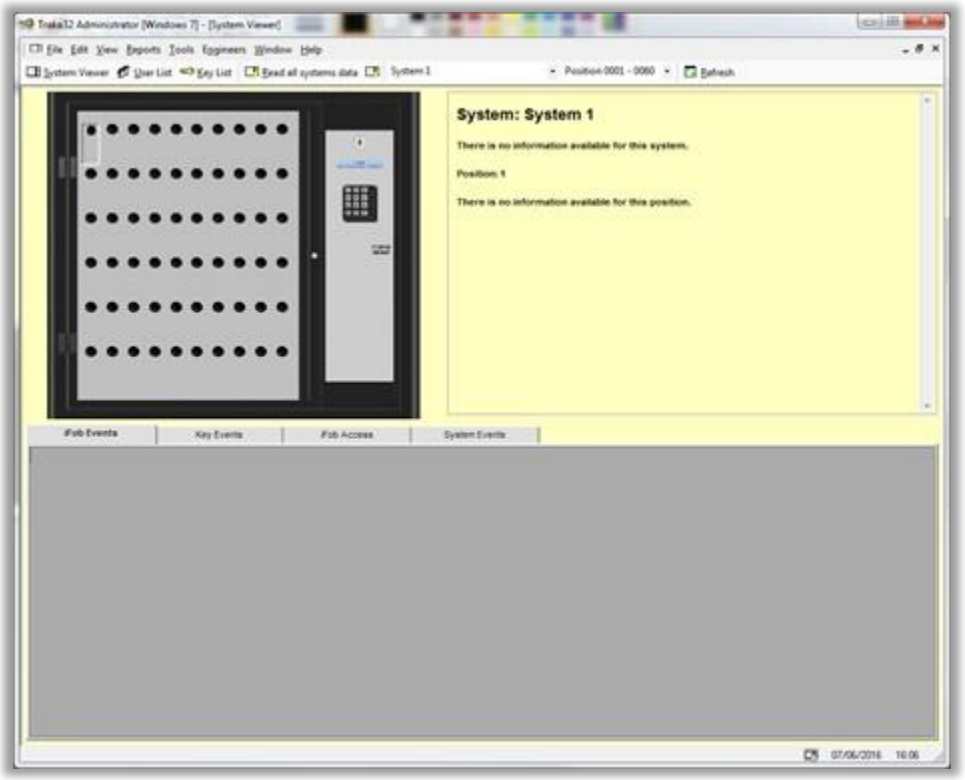
3.6.5 CONFIGURING IFOBS

The Traka Systems work on fixed iFob replacement basis which means the iFobs must be returned to the position from where they were taken (unless using the custom Random Return option - see note below). By default the system will not know where each iFob should go therefore the iFob serial numbers must be associated with the position in the system and the Traka32 software.

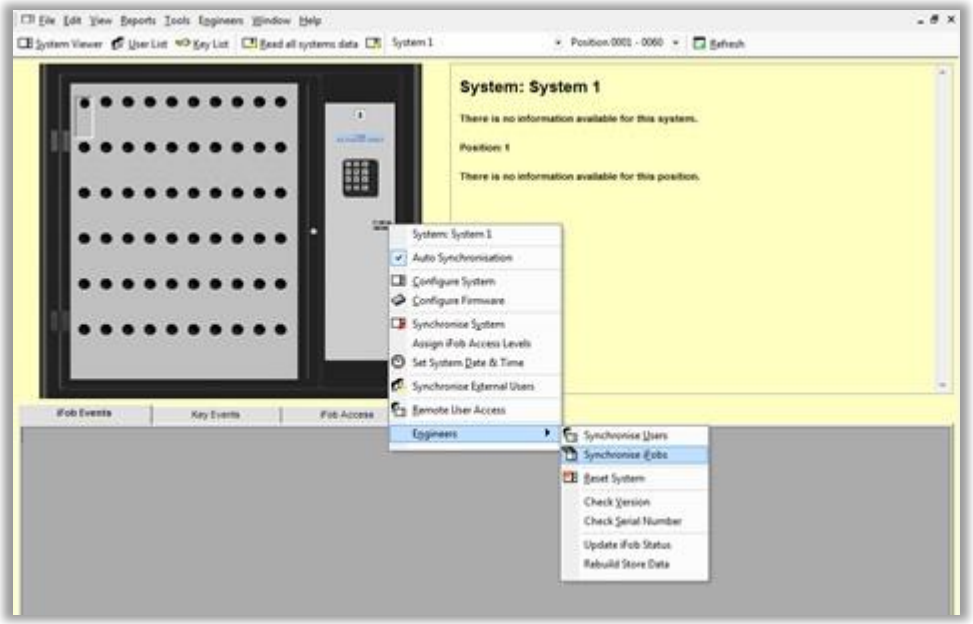
NOTE: If your system is setup for Random Return to Multiple Systems (RRMS) this process does not apply. Please refer to the Random Return to Multiple Systems Setup for more details. If your system is Random Return to a Single System (RRSS) continue to follow this process.

1. Ensure the Traka System is loaded with an iFob in every slot.

2. When you have configured the systems you can view the system by clicking on **View** followed by **System Viewer**. This is the default view that will be shown whenever the software is loaded.

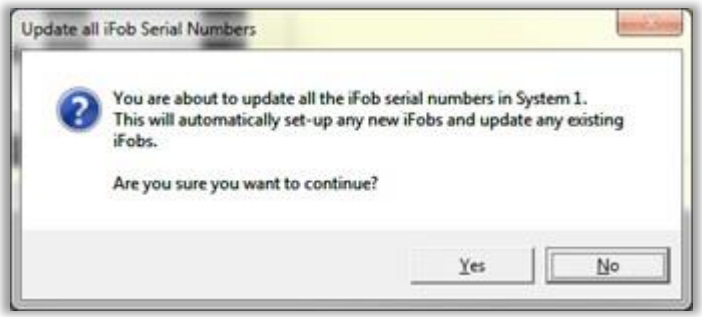


3. To configure the iFob serial numbers, simply click with the right mouse button over the picture of the system and click on **Engineers** followed by **Synchronise iFobs**.



4. You will be asked if you wish to download all transaction and alarms. Click on **No**.

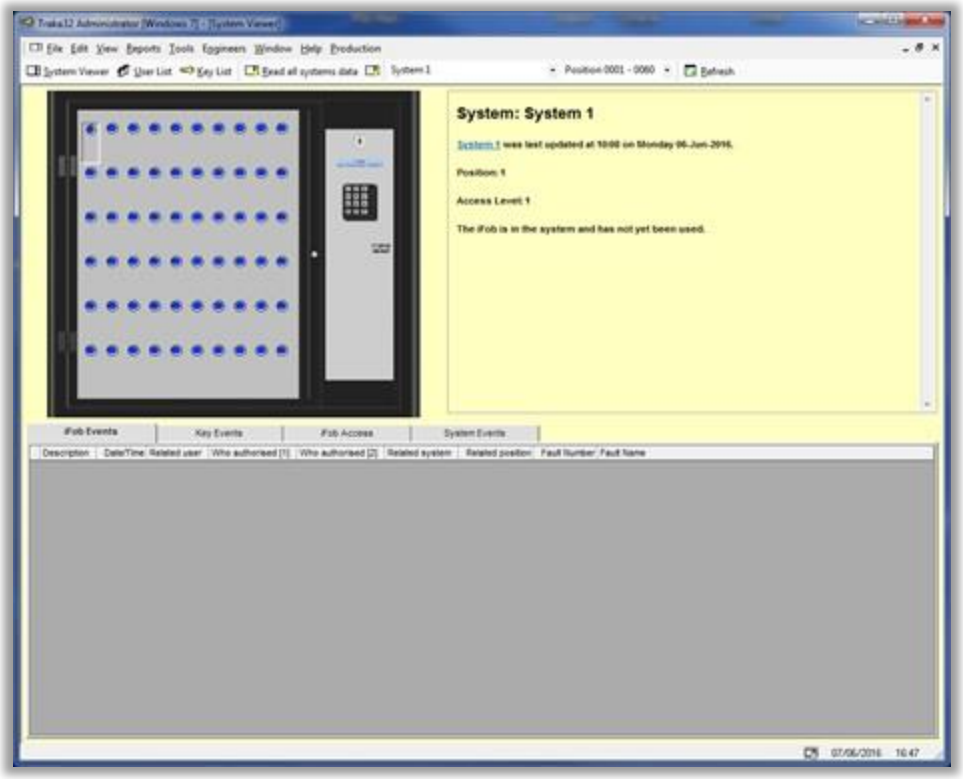
5. When asked if you are sure you want to continue, click on **Yes**.



6. The software will then communicate with the Traka System.

This should only take a few seconds. If the communications fails, check the communications settings and installation. If communications still fails you will need to contact your supplier for further help.

7. Your system viewer should now contain the iFobs.

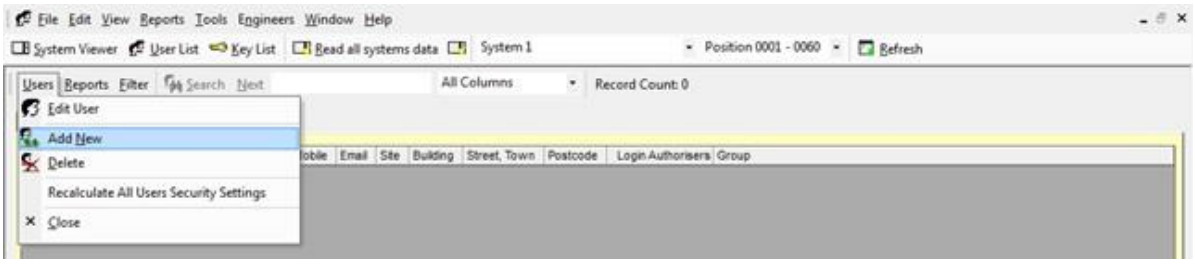


By default, all the iFob Access Levels will be set to 1 which is sufficient for testing and basic use. For more in-depth information on configuring the iFob access levels and access times please refer to the iFob Details section.

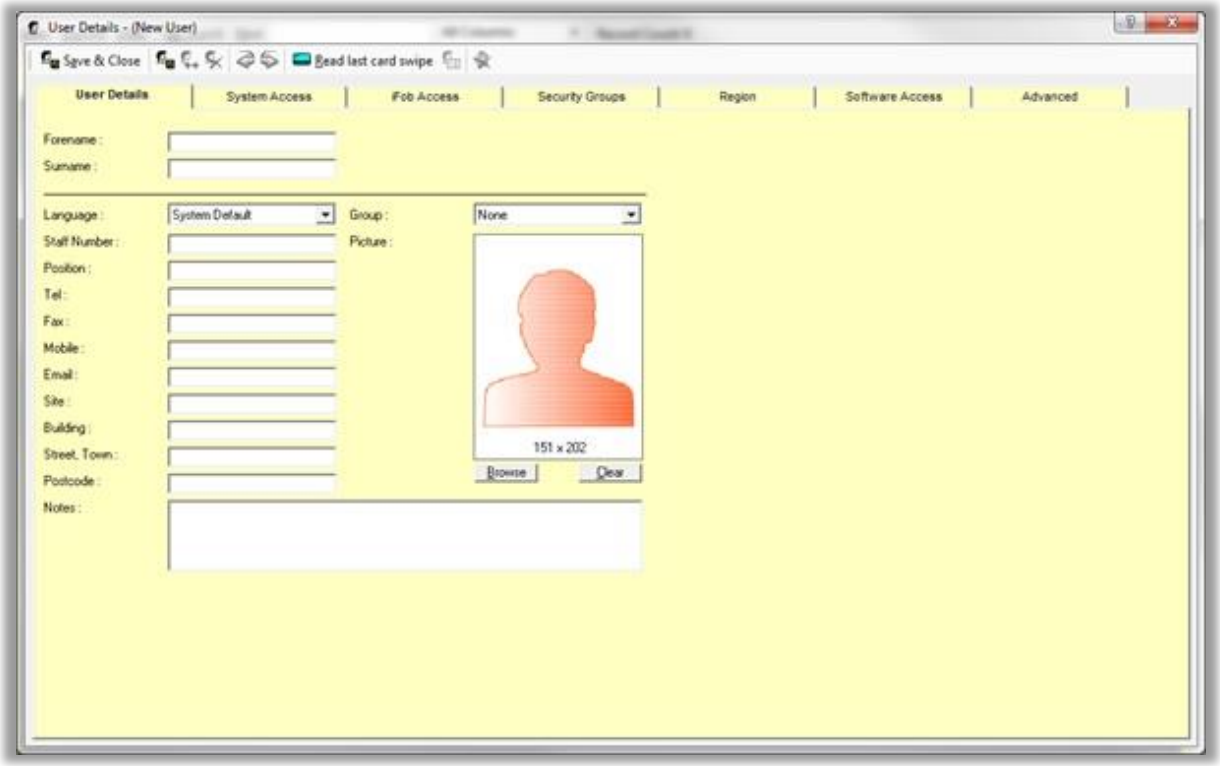
3.6.6 CONFIGURING A USER

1. Click on the **View** menu followed by **User List** and you will be presented with the User List.

2. Click on the **Users** menu followed by **Add New.**



3. You will be presented with a new User Details window.

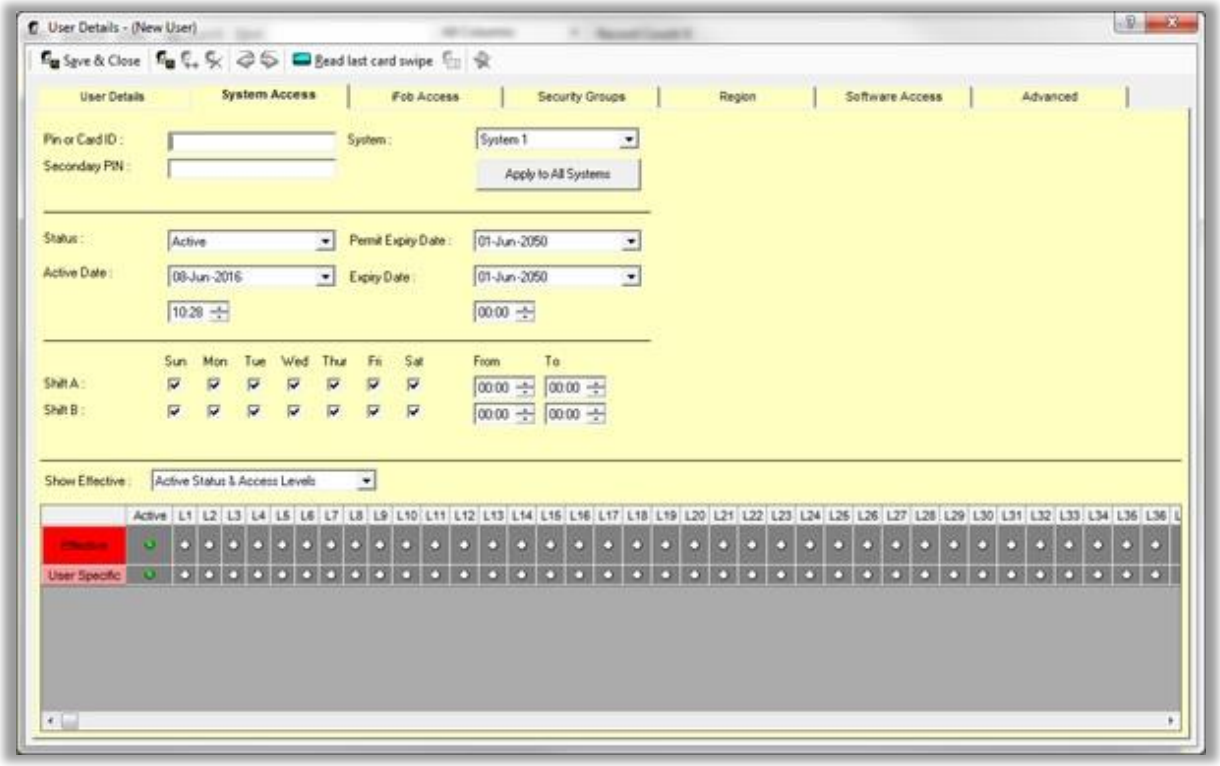


The user details tab allows you to input details about the users.

4. Enter a **Forename** and **Surname** for the user.

All the other fields in the User Details tab are for reference only and are not required for the commissioning stage. For more in-depth information on configuring the user details please refer to the User Details section.

5. Click on the **System Access** tab.



The system access tab allows you to define the user's access code, the period of validity and the times of access.

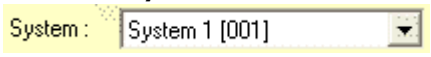
6. Enter a **PIN or Card ID** for the user.

   - For a Keypad entry Traka System, enter the Primary Personal Identification Number (PIN).
   - For a Card Reader entry Traka System, enter the Card ID.

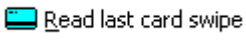
     If you do not know the Card ID:

     a. **Swipe the card** through the reader fitted one of the Traka systems. The Traka system should beep and display **ID Not Recognised** on the LCD, if not try swiping again.

        NOTE: Make sure no other user swipes their card until you have read the Card ID!

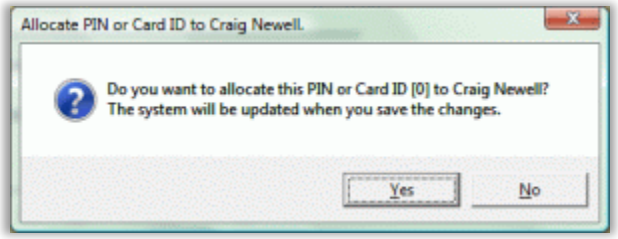
     b. **Select the system** that the card was swiped on from the 

drop down menu.

     c. **Read the last card swipe** by clicking on the 

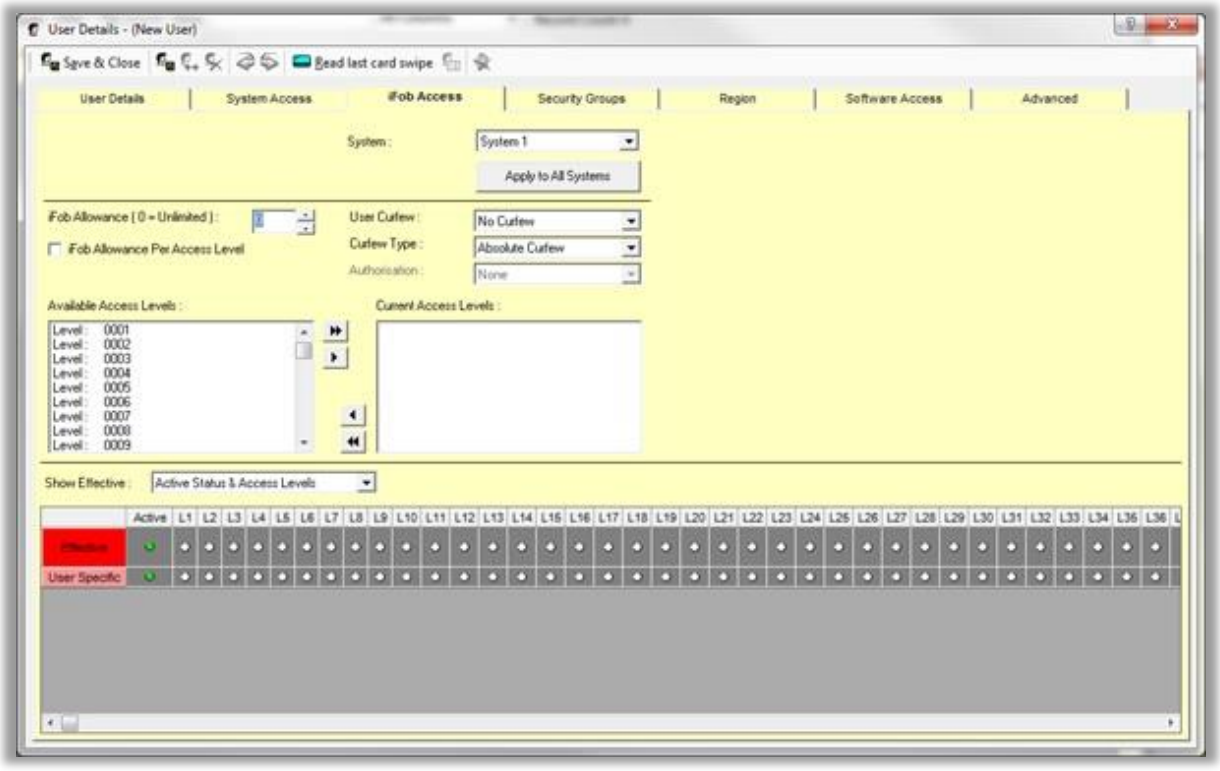
button.

     d. If successful, the Card Number will be displayed.

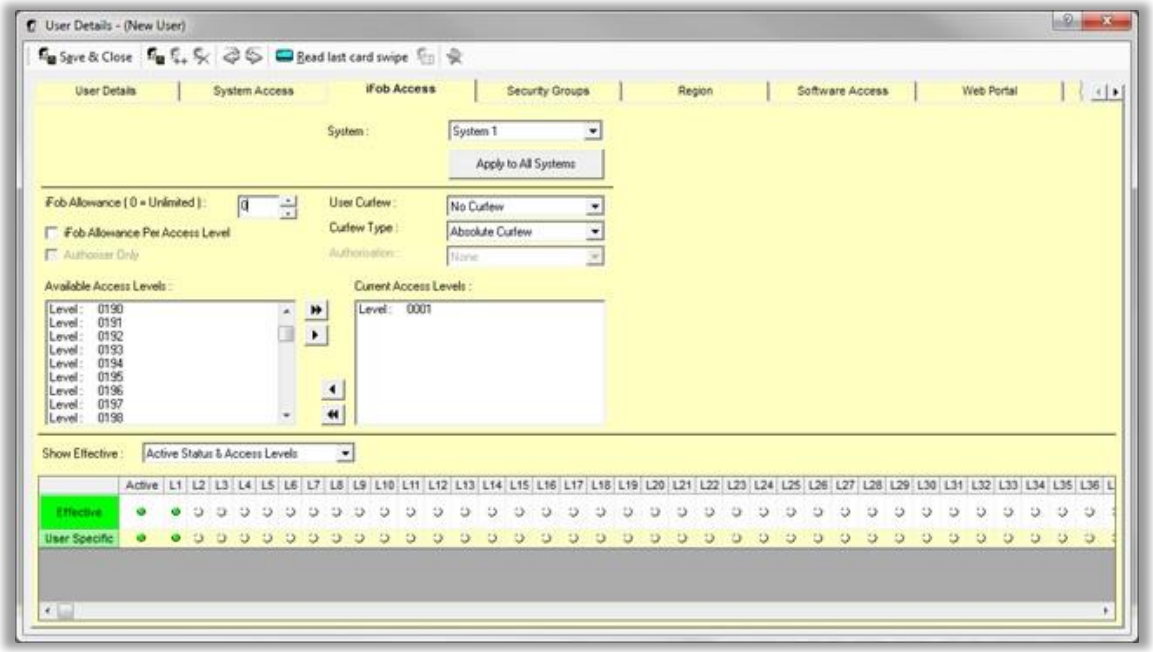


e. Click on **Yes** to allocate the Card Number to the user and you will see a series of **** in the PIN or Card ID field.

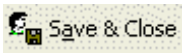
7. Click on the **iFob Access** tab.



8. In order to test the system you will need access to the iFobs. By default all iFobs are configured with Access Level 1 unless otherwise specified. Assign Access Level 1 to the user by selecting it from the Available Access levels list on the left and clicking the single right arrow to move it to the Current Access levels list. The 'Effective' status at the bottom will change from read to green to show that the user now has access to the system.



9. All the other fields and tabs in the User Details window are not required for the commissioning stage. For more in-depth information on configuring the user details please refer to the User Details section.

10. When you are happy with your configuration click on  or 

and the details will be written to the database and to the relevant Traka Systems.

11. Now refer to the Final Testing section.

3.6.7 FINAL TESTING

The final testing of the Traka System involves removing and returning the Traka iFobs.

1. Identify yourself to the Traka System.
2. For a Keypad entry Traka System, enter your Primary **Personal Identification Number** (PIN). Or for a Card Reader entry Traka System, **swipe your Card**.
3. Check that the door pops open (if fitted). If you have more than one cabinet attached to your system you will be asked to select which door you want to open, simply enter the door number on the keypad.

4. Check that LCD is displaying the correct name of the user that has logged in.

5. Starting at position 1, check that you can take and return each iFob in the system.
    a. If the position is a **Locking** position, press the black button against the iFob until you hear a beep.

Release the button, the solenoid that holds the iFob in place will activate and you should be able to remove the iFob. Check the LCD displays the correct position number.

6. If the position is a **Non-Locking** position, simply remove the iFob and check the LCD displays the correct position number.

NOTE: If you have a description set against an iFob, when you remove the iFob the description will be displayed on the LCD (Software version 02.10.0016 and above)

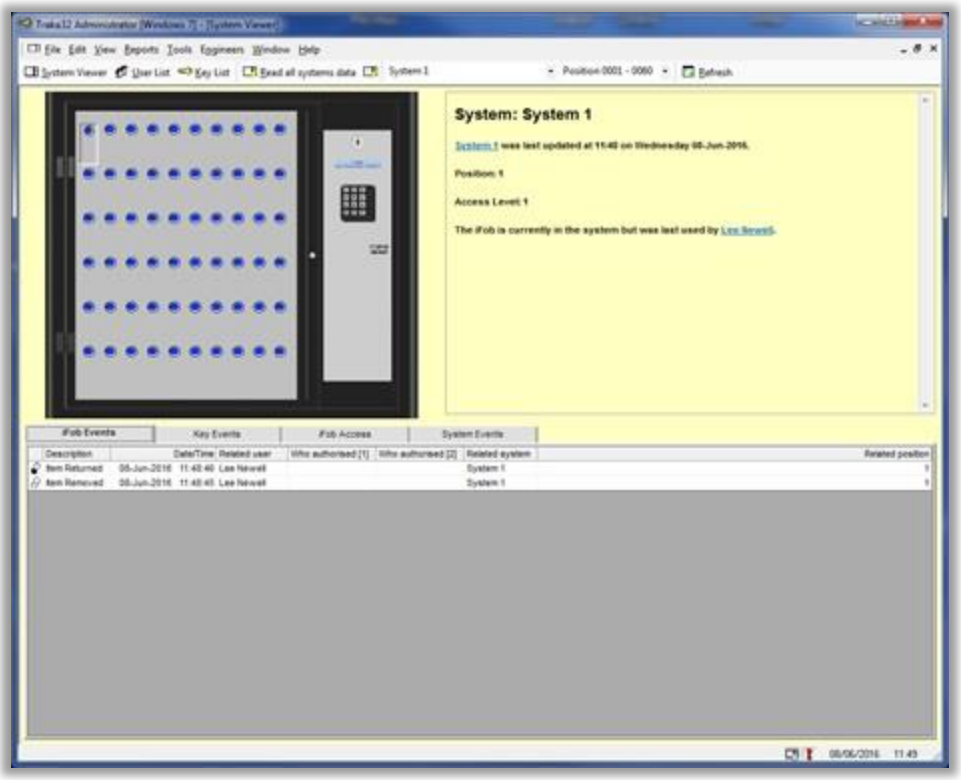
7. Repeat the process for each iFob in the system.

During this process it's possible that a time-out may occur and the system will display 'PLEASE CLOSE THE DOOR'. If this happens simply close the door and then log back into the system to continue testing the iFobs.

8. Once you have finished testing all of the iFobs in the system, close the door.
9. Return to the Traka32 software.
10. Select the appropriate system from the drop down menu.

11. Click on the button highlighted below to read data from the selected system.

12. Check that Traka32 downloads an appropriate number of transactions and that the transactions appear in the **iFob History** tab.

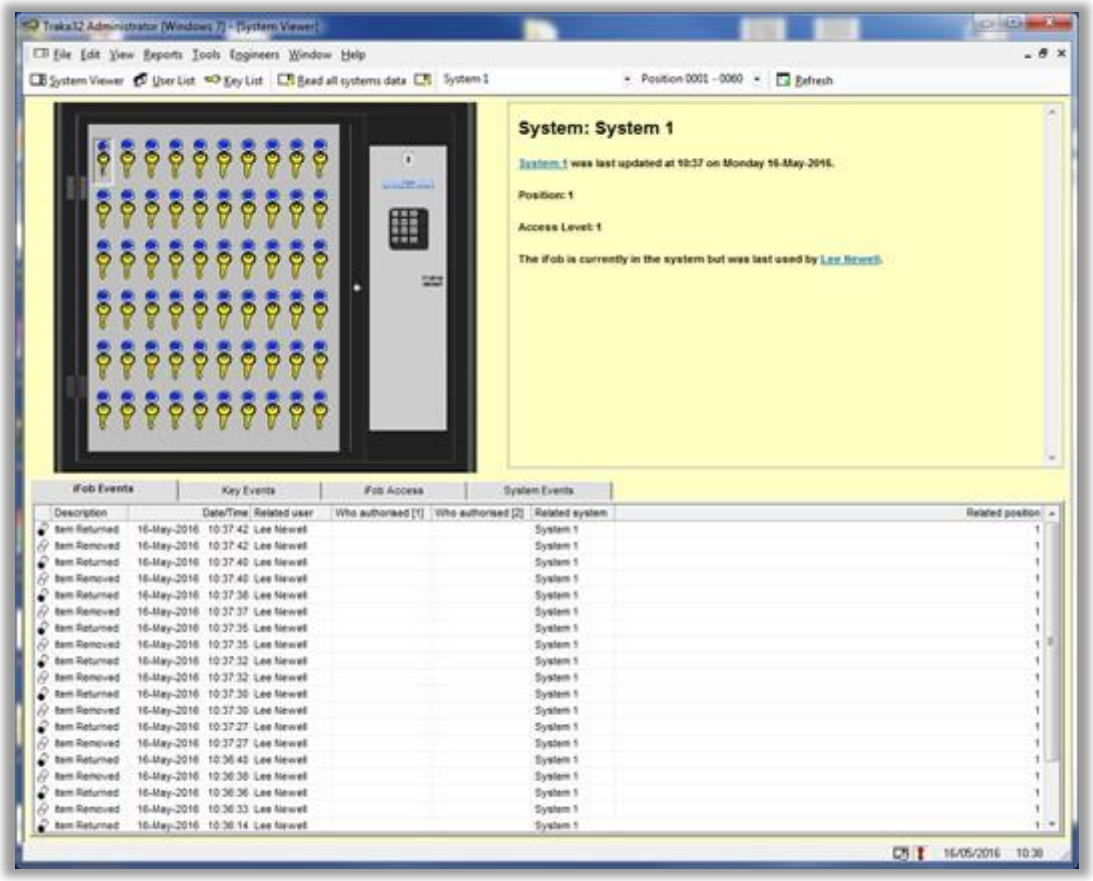


13. This completes the basic installation and testing. Please refer to the main user guide for more in depth information on the various features and options of Traka.

4 TRAKA32 SOFTWARE

4.1 TRAKA32 SOFTWARE OVERVIEW

All Traka products that use 8bit or 16bit hardware are supported by the Traka32 Windows software, this is essential to configure the Traka Systems. Traka32 allows you to view and manage your Traka system through an 'easy to use' software interface.



This software is installed on a local or remote PC and can be networked if required. It is not required for the software to be "on-line" and for most installations the software will be installed on an existing computer to be used when collecting data from the Traka Systems or when changing user or key/item details.

With so many opportunities to configure the system, it is important that this is completed using a computer screen - it would be impossible just using the Traka keypad and display.
The software is remarkably easy to use and shows graphically the details of the keys or assets held in the system and gives comprehensive user and key/item activity reports. The Traka system allows up to 200 access levels (8bit systems) and 2560 access levels (16bit systems) giving a huge range of possibilities of access for different grades of staff.

Traka32 can support 20,000 users on Key cabinets when used with 16bit Key cabinet firmware 03.00.16 and above and 50,000 users when used with 16bit Locker firmware version 03.00.16 and above.

Traka32 is written in Visual Basic and can use either a Microsoft Access, Microsoft SQL Server or an Oracle database. Please view below which versions are supported.

Access Database

Windows 7

Windows 8

Windows 10

SQL Database

Windows Server 2012

Windows Server 2012 R2

Oracle Database

Oracle 10G

Oracle 11G

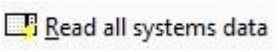
Traka32 must be run on a Windows XP or later computer. Traka32 is designed for multi-lingual support with several European languages already available.

4.2 READ ALL SYSTEMS DATA

The transactions, alarms and events reports available from the Traka32 software are only as up to date as the last time the system data was read.

To update the data from a single system, select the required system from the 

drop down menu and click on  (shortcut key F9).

To update the data from all systems, simply click on 

.

It is possible to configure the Traka32 software to automatically Read All System Data at regular intervals or a specific time of the day. Please refer to the **Auto Communication** in the Properties section for more details.

NOTE:

It is good practice to Read All System Data as often possible. If a problem was to occur with a Traka System valuable data may be lost if the data is not read.

Traka does have a limited amount of memory as with any system. If a Read All System Data is not done for a very long period the memory may become full. When the memory becomes full, it will start to overwrite the oldest information in order to keep the most recent information and data may be lost.

If a Traka System's LCD starts displaying the '**Memory Almost Full**' message, the alarm and/or transaction memory within the Traka System is nearing maximum capacity.

If a Traka System's LCD starts displaying the '**WARNING: MEMORY FULL!!**' message, the alarm and/or transaction memory within the Traka System has reached maximum capacity.

4.3 LANGUAGES

Languages on 8bit Systems

8bit systems currently can only display one language per system. Please see the below list of supported languages.

Languages on 16bit Systems

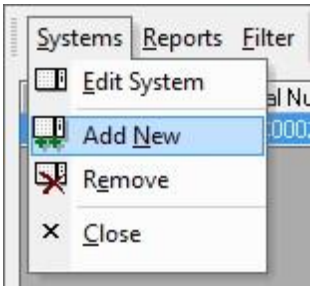
16bit systems have the ability to display a different language for each user in the database. This allows each user to login to the cabinet/locker and have their own language displayed whilst they use the system. Once they are finished and have stopped using the system, the cabinet/locker will revert back to displaying its default language until another language specific user begins to use the system. Please see below for supported languages.

- Czech
- English
- Finnish
- French
- Italian
- Dutch
- Danish
- Latvian
- German
- Norwegian
- Spanish (Spain)
- Spanish (Venezuela)
- Japanese (Katakana)
- Swedish
- Slovak
- Polish
- Portuguese (Brazil)
- Portuguese (Portugal)
- Russian
- Turkish

4.4 SYSTEM SETTINGS

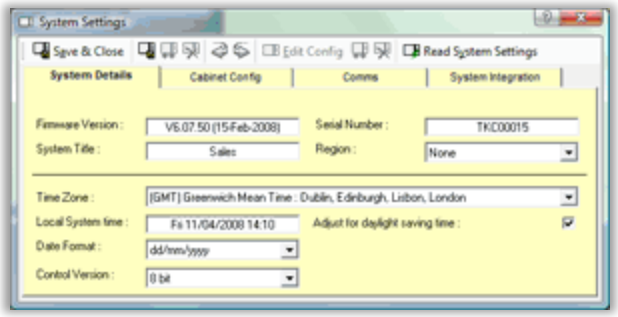
4.4.1 ADDING SYSTEMS

1. From the main screen click on **Tools**, **Configure Systems** and a list of the current systems will be shown.
2. From the system list click on the **Systems** menu followed by **Add New**.



NOTE: If you already have a system record open you can create a new record by simply clicking on the button.

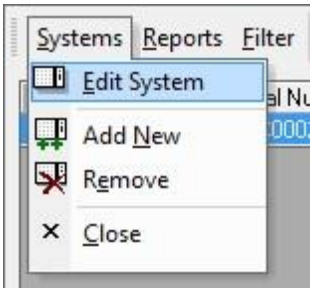
3. A new blank system record will be created.



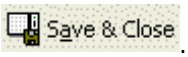
4. Edit the appropriate details, for more details refer to the System Settings section.
5. To **Save** your changes, simply click on or Save & Close.
6. To **Cancel** your changes, simply close the window and click **No** when asked if you wish to save your changes.

4.4.2 EDITING SYSTEMS

1. From the main screen click on **Tools**, **Configure Systems** and a list of the current systems will be shown.
2. From the system list simply **double click** on the system record you wish to edit or click on the **Systems** menu followed by **Edit System**.



NOTE: You can also edit a system's details from the System Viewer by right clicking over the picture of the selected system and clicking on Configure System.

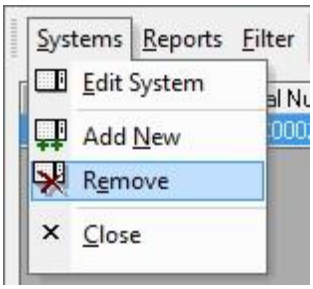
3. The selected system record will open.
4. Edit the appropriate details, for more details refer to the System Settings section.
5. To **Save** your changes, simply click on  or 

.
6. To **Cancel** your changes, simply close the window and click **No** when asked if you wish to save your changes.

4.4.3 DELETING SYSTEMS

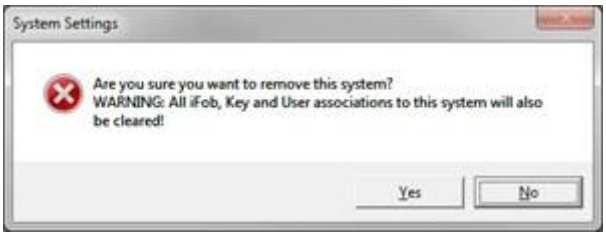
1. From the main screen click on **Tools**, **Configure Systems** and a list of the current systems will be shown.

2. From the system list simply **click** on the system record you wish to delete, click on the **Systems** menu followed by **Remove**.



NOTE: If you already have a system record open you can delete the record simply by clicking on the  **button.**

3. To delete the system simply click on **Yes**.

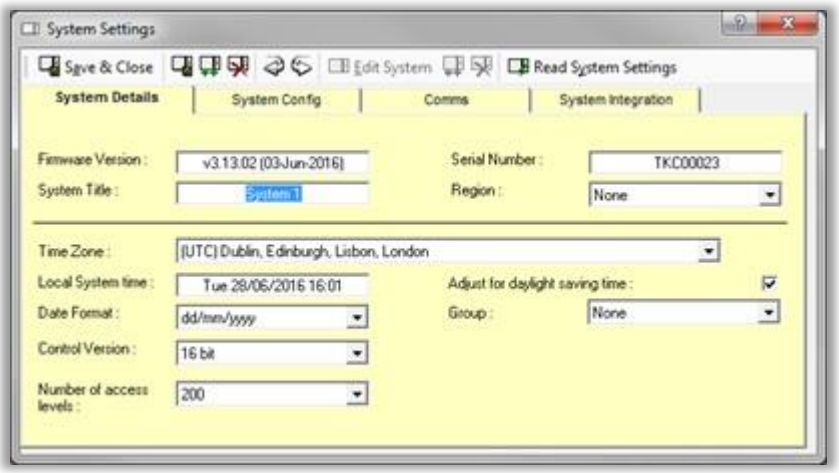


4. And **Yes** again.

4.4.4 SYSTEM SETTINGS

Right click the Pod and select Configure System to access the System Settings. The System Settings window allows you to add and edit the system details.

System Details



Firmware Version

This field shows the current firmware version of the system.

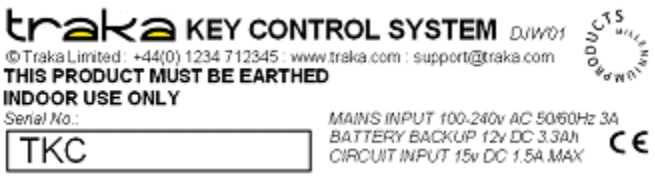
NOTE: This field will automatically be filled in when you communicate with the Traka System.

System Title

Enter a System Title to represent the system you are adding for example Reception or Basement.

Serial Number

Enter the Serial Number of the system for reference. This can be found on the inside of the Pod and starts TKC, for example TKC10123.



Region

If you are using Region access select the region the system falls in. If you are not using Region access, select None.

Time Zone

Select the Time Zone for where the Traka System is located.

Local System Time

This field shows the local time of the Traka System based upon the Time Zone, Daylight Saving and Date Format selected. This is only for reference to help confirm that the settings are correct.

NOTE: The date and time shown is calculated from the PC's date and time so if it appears wrong, please check your PC's date and time before adjusting the Traka32 settings.

Adjust for daylight saving time

Select this option if you want Traka32 to adjust the local time of the Traka System in accordance with the daylight saving rules for the selected time zone.

NOTE: This option is used only to calculate the local time of the Traka System. The Traka System will not automatically adjust its date and time for daylight saving unless the firmware is configured to do so. Please refer to the Configure Firmware section for more details.

Date Format

Select the date format of the Traka System.

- mm/dd/yyyy
- dd/mm/yyyy
- yyyy/mm/dd

Control Version

Select the Control Version that is fitted to the Traka System.

- 8bit
- 16bit
- THD iFob Transfer Unit

Group

Cabinets or Lockers can now be assigned to Groups, the first use for this feature was to group lockers into year groups for use with the Locker Allocation Wizard.

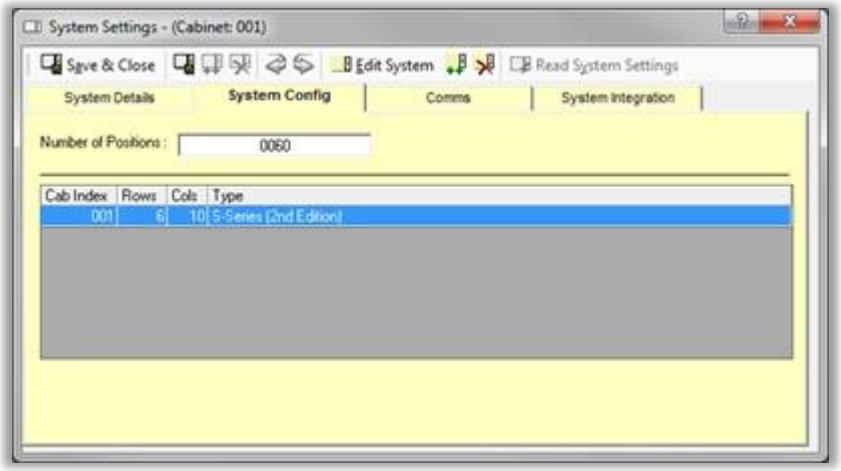
Number of Access Levels

Each system can now have the number of usable access levels defined. The default number of access levels is show below:

System Type	Number of Access Levels
16bit systems - Key Cabinets	2560
16bit systems - Locker Systems	200
8bit Key Cabinets and Locker Systems	200
8bit with Half Reduced User Security	8
8bit with Full Reduced User Security	8

You can select the number of access levels that you want to use (up to the maximum allowed for the cabinet configuration). The benefit of doing this is that it reduces the amount of time taken for all the calculations and the form load time anywhere the access levels are displayed. E.g. iFob Details, User Details, Access Grid etc.

System Config

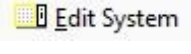


Number of Positions

This field shows this system's total number of iFob positions for a key cabinet, or number of locker doors for a locker system. The number is calculated from the total number of rows and columns defined in the Cabinet List below.

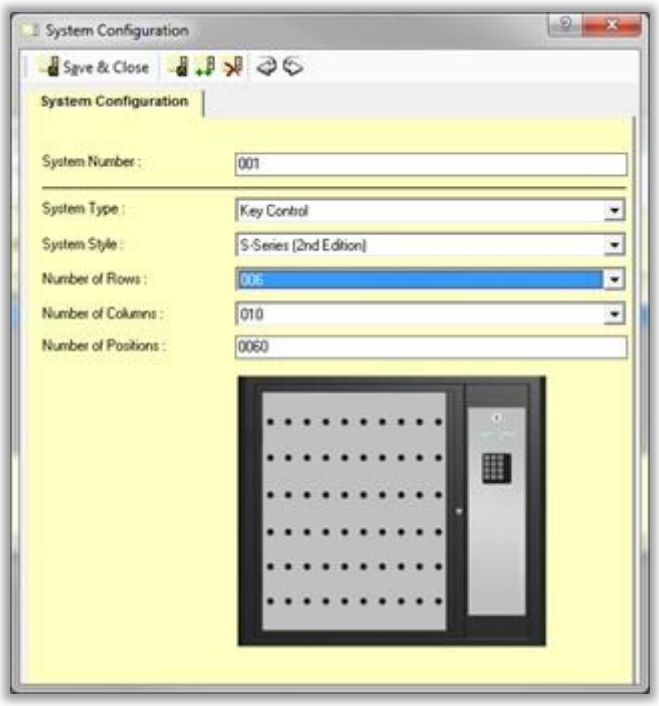
Cabinet List

You will see a list of cabinets that are attached to the system. A system comprises a control pod and one or more cabinets. By default there is one key cabinet that has 6 receptor strips or rows each comprising of 10 positions making a total of 60 positions. You must alter the cabinet configuration to match that of your physical system as follows.

To edit the default cabinet, either double click on the cabinet in the list or click on 

from the System Settings Menu.

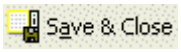
Choose your **System Type**, and then simply edit the **Number of Rows and Columns** if required to match that of the Cabinet in the System.



When you select the 'Cabinet Style' an image will be displayed at the bottom of the configuration window. This will show you what the system is going to look like, and makes it easier to identify the system.

To Add a Cabinet, click on  .

To Remove a Cabinet, click on  .

To save the changes, click on  or  .

Please refer to the System Configuration section for more details.

Comms

System ID Number

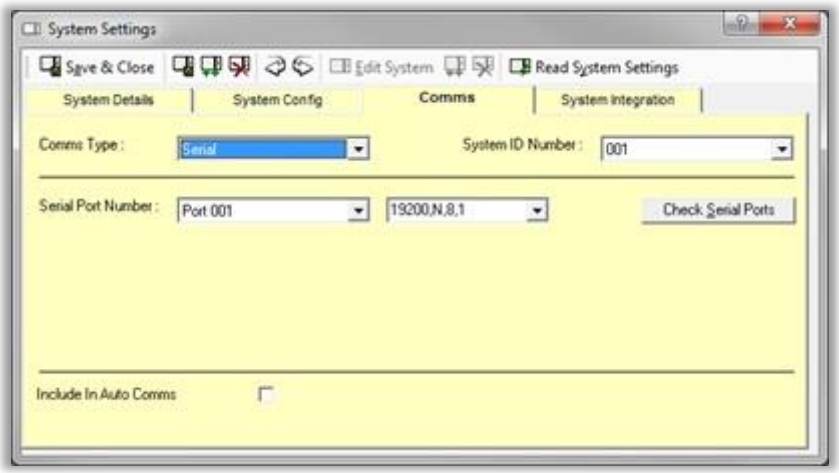
Select the System ID Number from the drop down menu. The System ID Number has to match that of the number programmed in the Traka System. For most systems this number will be 001. Please refer to the 8bit Configuration Menu or 16bit Configuration Menu section for details on setting the System ID.

Comms Type

Select the Comms Type from the drop down menu. From this you can select:

- Serial for RS232 or RS485.
- Modem.
- Network for Ethernet.

Serial



Serial Port Number

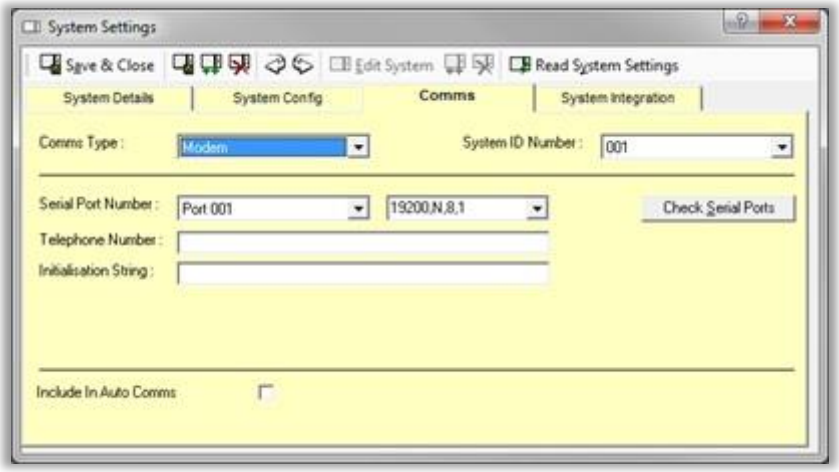
Select the Serial Port of the PC that you have connected the Traka system too.

Serial Port Settings

For an **8bit** system the setting depends upon the type of **crystal** your Traka system has been fitted with. Set **9600,N,8,1** if the 8bit Control PCB is fitted with a **3MHz** crystal or set **19200,N,8,1** if the 8bit Control PCB is fitted with a **7MHz** crystal. Please refer to the 8bit Control PCB Diagrams to locate crystal type.

For a **16bit** system the default setting is **38400,N,8,1.** The 16bit hardware can also be configured for 19200,N,8,1 or 9600,N,8,1 if required.

Modem



Serial Port Number

Select the Serial Port of the PC that you have connected the Traka System too.

Serial Port Settings

For an **8bit** system, the setting depends upon the type of **crystal** your Traka system Control hardware has been fitted with. Set **9600,N,8,1** if the 8bit Control PCB is fitted with a **3MHz** crystal or set **19200,N,8,1** if the 8bit Control PCB is fitted with a **7MHz** crystal. Please refer to the 8bit Control PCB Diagrams to locate crystal type.

For a **16bit** system the default setting is **38400,N,8,1.** The 16bit control hardware can also be configured for 19200,N,8,1 or 9600,N,8,1 if required.

Telephone Number

Enter the telephone number of the modem you wish to dial.

Initialisation String

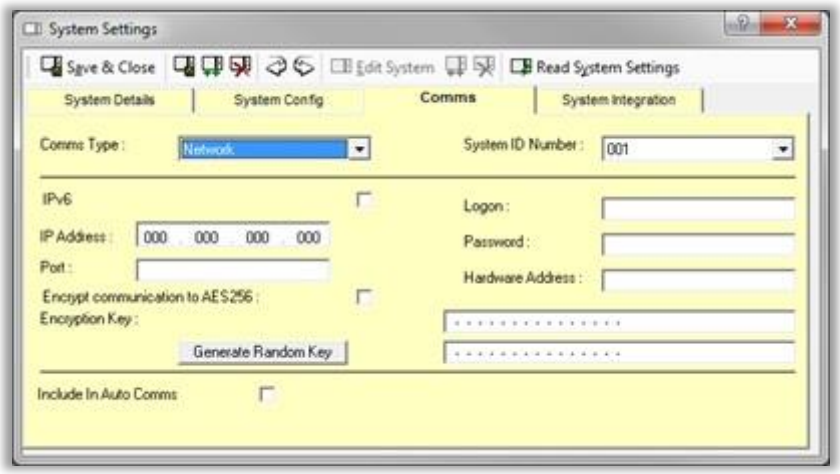
Please refer to your modem user guide to work out the appropriate initialization string. In v02.006.002 and prior the default dial initialisation string setting is **ATV0X4N1L1Q0&M0%C0&K0\N0**. From v02.006.002 the default dial is "" (blank).

All of the modem strings can now be edited from T32 Settings.ini and are as follows:

ModemDefaultInitialiseString ; Default = at&F0E0V0S2=43S12=45
ModemDefaultDialString; Default = atDT*
ModemDefaultEscapeString; Default = +++
ModemDefaultHangupString; Default = atH0

* string remains editable in the system settings window

Network



IP Address

Enter the IP Address of the Ethernet device, for example 10.0.0.215.

NOTE: Traka32 supports the input of IPv6 addresses. For this to work, IPv6 compatible Traka hardware must be present in the systems.

Port

Enter the Port number of the Ethernet device, this is usually **4001** for the Moxa device and **10001** for the XPort device.

Logon

This is not currently required for the commonly used Ethernet devices but is available if a different type of device is required.

Password

Again this is not currently required for the commonly used Ethernet devices but is available if a different type of device is required.

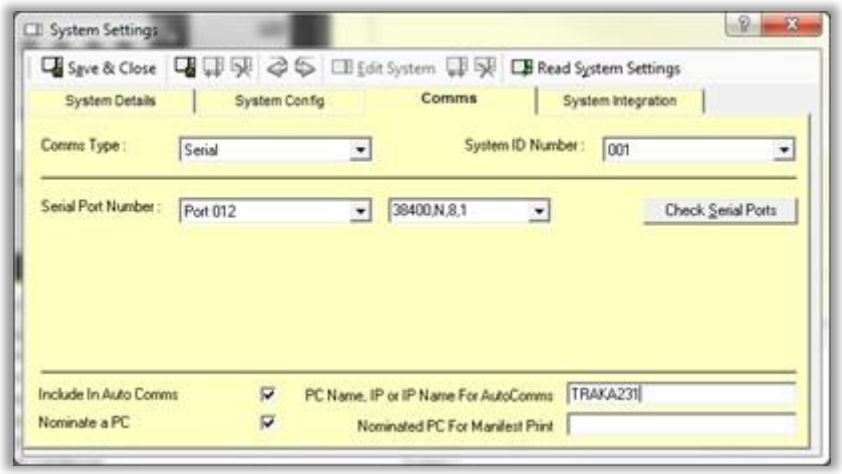
Hardware Address

This field is for reference only to help with the administration of the Ethernet devices. The Hardware Address is also known as the MAC Address, for example 00-90-E8-04-31-38.

AES-256 Encryption

AES-256 Encryption prevents data from being captured when travelling over the network between the Traka32 application and the customer database. This will prevent unauthorised access to personal information that could inherently provide unauthorised access to high security keys/items held in the Traka systems. For full details on setting up this feature please review the AES-256 Encryption topic.

Auto Communication



This allows the automatic communication between the Traka system and the supporting Traka32 software.

NOTE: For the Auto 'Communication' to operate you must set the Auto Communication drop down to either Interval, Specific Time of Day, Online or Remote Host in the Properties window.

Include In Auto Comms

Tick this option if you want to include the system in the 'Auto Communication' group.

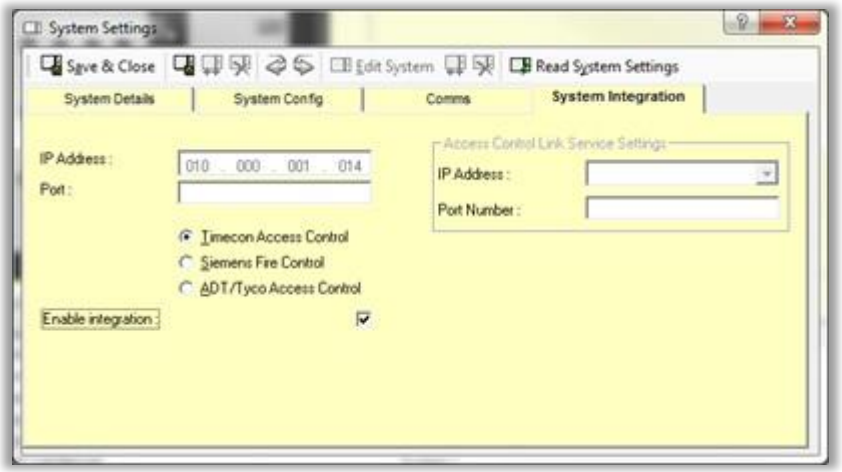
Nominate a PC

Tick this option to nominate a PC or Server to Auto Communicate with this system.

PC Name, IP or IP Name

Enter the PC Name, IP or IP Name of the nominated PC. Only the nominated PC will attempt to Auto Communicate with the selected System. If nominate a PC is left un-ticked, then any copy of Traka 32 set for auto-communications will attempt to communicate with the selected system.

System Integration



Timecon Access Control

Timecon Access control allows the potential of integration of access control systems to the Traka system.

A typical example is where an access control reader would be attached to the Traka System. The reader would be connected to an access control system. When a card is swiped at the reader, the card data would be sent directly to the access control system. The access control system would verify the user and record the fact that a card was swiped. If the card is valid, the access control system would send a packet of data containing details of the user via TCP/IP to the Traka32 software. Traka32 would decode the incoming packet, again verify the user details and if valid would send a command to the Traka System to open the door.

Please contact Traka for full details.

Siemens Fire Control

Siemens Fire control allows the potential of integration of fire control systems to the Traka system.

A typical example is where certain iFobs/items need to be released when a fire alarm is raised. In the event of a fire alarm, the fire control system would send a packet of data containing details of the alarm number and associated iFobs/items via TCP/IP to the Traka32 software. Traka32 would decode the incoming packet and if valid would send a command to the Traka System priming it to release the iFobs/items when the fire department accesses the Traka System.

Please contact Traka for full details.

ADT/Tyco Access Control

ADT/Tyco Access Control allows the potential to integrate an access control system to Traka32 so that the access control system can be kept informed if users have keys/items in their possession. If a user has keys/items and they try to leave the building, the access control system can be configured to prevent then from leaving the building.

Traka32 must be configured to be Remote Host to the Traka Systems. This means that every time an Event occurs at the Traka System (for example a key/item being taken or returned) the data is fed back automatically.

Traka32 will then make a check on each user every time a key/item is taken or returned.

If a user has one or more keys/items in their possession from any system, Traka32 will send a command via TCP/IP to the access control system to say the user 'xyz' has one or more keys/items in their possession.

Traka32 will know if it has sent a command to the Access Control System for a particular user so if that user takes subsequent keys/items further commands are not sent.

If a user has returned all the keys/items in their possession, Traka32 will again send a command via TCP/IP to the access control system to say the user 'xyz' has no keys/items in their possession.

Please contact Traka for full details.

IP Address

For Timecon Access Control and Siemens Fire Control, this field shows the IP Address of the workstation that the Traka32 software is installed on. This is to be used by the access / fire control system to make a connection to the Traka32 software.

For ADT/Tyco Access Control, enter the IP Address of the access control system that Traka32 will connect to.

Port

For Timecon Access Control and Siemens Fire Control, enter a Port number of the workstation that the access / fire control system will connect to.

For ADT/Tyco Access Control, enter the Port number of the access control system that Traka32 will connect to.

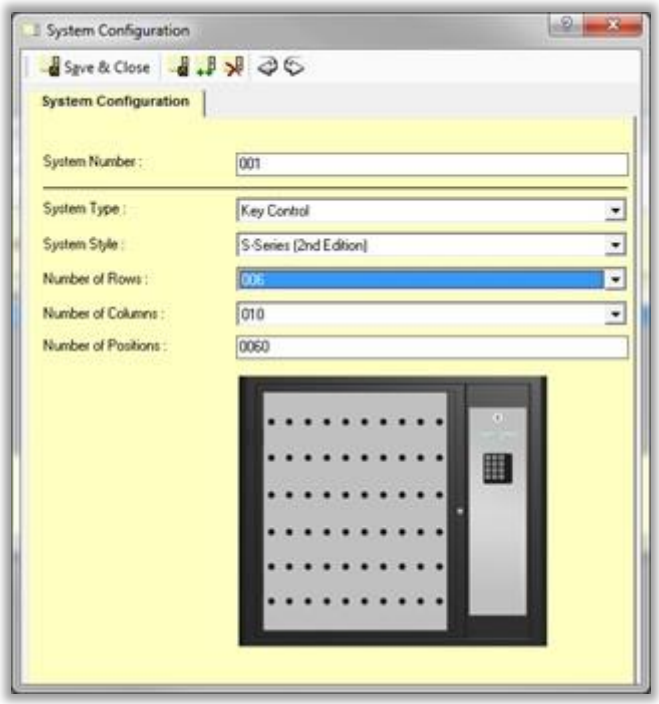
This can be any port number but as certain ports are reserved for certain applications; typically a port number of **1001** would be used with Traka32.

Enable Integration

Check the Enable Integration box to enable the Traka32 software to accept incoming data from the access / fire control system.

4.4.5 SYSTEM CONFIGURATION

The System Configuration window allows you to add and edit the cabinet details.



System Number

This is a reference number for the cabinet attached to the system. It is possible to have from 1 to 255 cabinets per system.

TIP: For key cabinets, if you have more than one cabinet, match the cabinet number to the door number.

System Type

Select your system type from the dropdown list. The options available are:

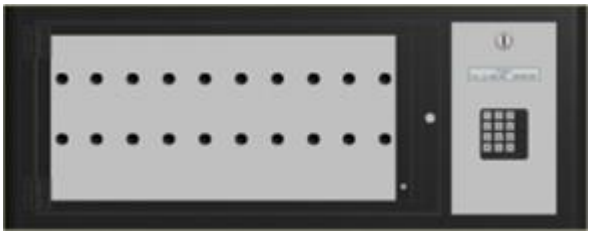
- Key Control
- Locker
- Other

System Style

Select the style of your system from the dropdown list. This list will change depending on which System Type has been selected. As you select the System Style a preview image is displayed below to enable you to match your system exactly. Some examples are shown below:

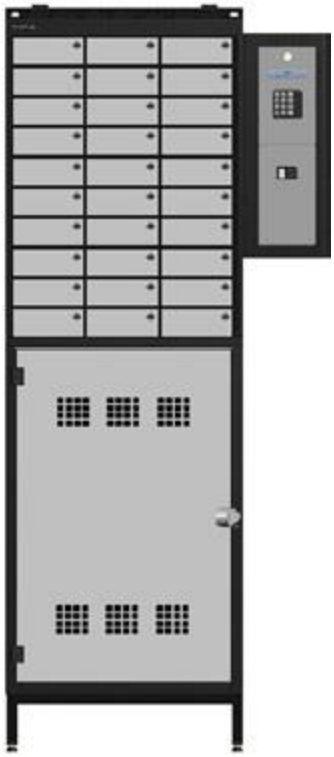
Key Control:

M-Series (3rd Edition)



Lockers:

Modular Lockers Group 4 (31 way)



Other:

Traka Handheld Device

Number of Rows

Select the number of rows within the cabinet. The number of rows selectable will depend on the System Style selected.

Number of Columns

Select the number of columns within the cabinet. The number of columns selectable will depend on the System Style selected.

Number of Positions

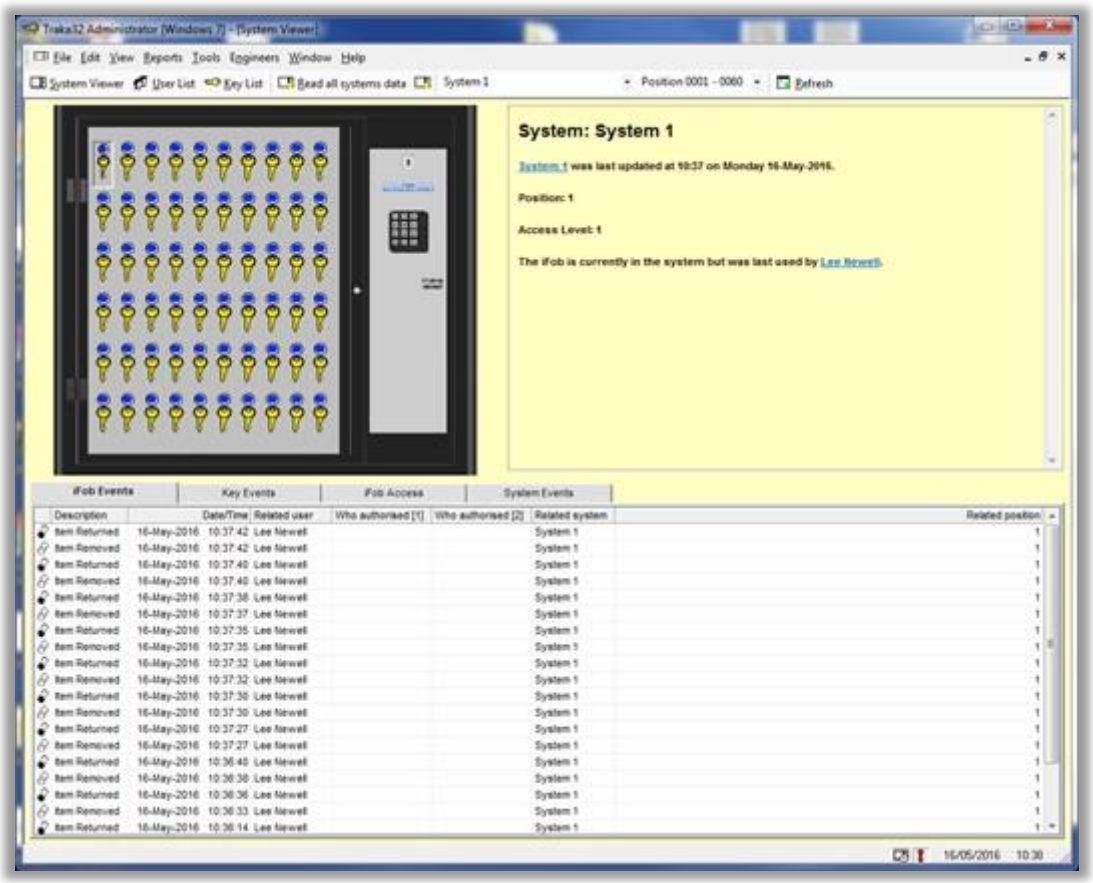
The total number of positions for the cabinet is calculated by multiplying the number of rows by the number of columns. For example:

- 4 Rows and 4 Columns = 16 positions.
- 6 Rows and 10 Columns = 60 positions.
- 18 Rows and 10 Columns = 180 positions.

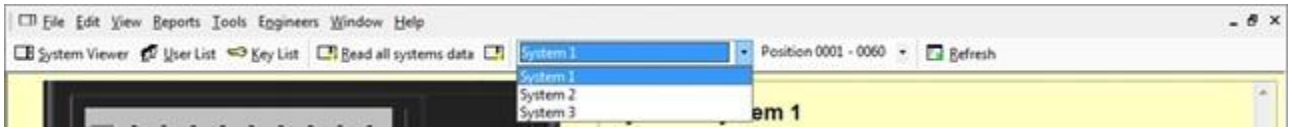
4.5 SYSTEM VIEWER

4.5.1 SYSTEM VIEWER OVERVIEW

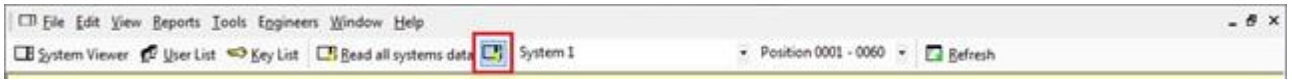
The System Viewer allows you to see a representation of the Traka System on your PC. It appears every time that you open the software. Only one system is shown at a time and can be selected from the system selection drop down menu on the main toolbar.



The system viewer is only as up to date as the last time the system data was read. To update the viewer and any other open windows, select the required system from the drop-down menu...



and then click on the 'Read Selected System' data button.



System Display

The colours of the iFob/Keys in the system viewer change colour depending on their current status...


No iFob defined


iFob currently in the system with no keys attached


iFob currently in the system with keys attached


or

iFob currently out of the system


iFob currently out of the system and under a curfew


iFob currently out of the system and is overdue


iFob currently in the system and has a fault logged against it


iFob currently in the system and has a repaired fault logged against it

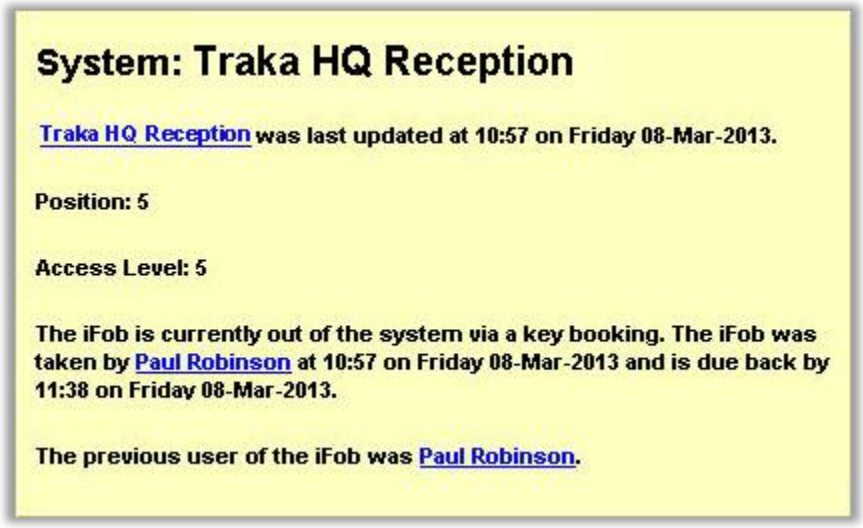

iFob in the wrong slot. The X shows where the iFob has been incorrectly located.


iFob in the wrong slot. The ✓ shows where the iFob should be correctly located.


No inforamtion available on the related iFob and/or key.

Information

The system viewer shows when the system was last updated with data from the Traka software. Always check to ensure you are looking at the latest information. By clicking over an iFob on the system viewer, the status of the iFob is clearly shown.



Certain information can be accessed such as System, User and Fault Details by simply clicking on the underlined links on the information panel.

Old Transactions

If you are running your Traka System with a firmware version of 6.07.30 or below the iFob and Key History will be recorded as transactions. A transaction is defined as an iFob being taken from and retuned to a Traka System. The iFob and Key Transaction history reports shows **Time Taken**, **Who took the iFob**, **Time Returned** and **Who returned the iFob** all in a single record along with any other relevant information such as Mileage, Fuel Level, Costs etc depending on what options are enabled in the firmware.

iFob History

The iFob history tab displays the last month's transactions for the selected iFob.

For more detailed reports and charts on the iFob history, click on **Reports**, **Transaction Reports**, **and iFobs** from the main menu.

Key History

The key history tab displays the details of the keys currently attached to the iFob and the last month's transactions of the keys currently attached to the selected iFob. To view the history of a particular key, highlight the key in the list and the history will be displayed beneath. To edit a key, simply double click on the key record.

For more detailed reports and charts on the key history, click on **Report**, **Transaction Reports**, **and Keys** from the main menu.

New Events

If you are running your Traka System with a firmware version of 6.07.31 or above the iFob and Key History will be recorded as events. An event can be any action performed on an iFob such as iFob Taken, iFob Returned, iFob

Overdue etc. This method gives much greater flexibility so that all the relevant history such as alarm and transaction information is shown together in one report making it much easier to see what is going on.

iFob Events

The iFob events tab displays the last month's events for the selected iFob.

For more detailed reports and charts on the iFob history, click on **Report**, **Crystal Reports**, **and iFobs** from the main menu.

Key Events

The key events tab displays the details of the keys currently attached to the iFob and the last month's events of the keys currently attached to the selected iFob. To view the events of a particular key, highlight the key in the list and the history will be displayed beneath. To edit a key, simply double click on the key record.

For more detailed reports and charts on the key history, click on **Report**, **Crystal Reports**, **and Keys** from the main menu.

System Events

The system events tab displays the last month's events for the selected System.

For more detailed reports and charts on the system events, click on **Report**, **Crystal Reports**, **and Events** from the main menu.

iFob Access

The iFob access tab displays all the users that are able to access the selected iFob. To edit a user, simply double click on the user record.

4.5.2 IFOB MENU

The iFob menu allows you to administer the selected iFob and attached Keys.

To access the System Menu, from the System Viewer, simply **click with the right mouse button over the picture of the iFob**.

Position

This field displays the position of the iFob you have clicked on.

Edit Key Details

Click on Edit Key Details to edit details of the keys that are attached to the iFob.

Please refer to the Key Details section for more details.

Edit iFob Details

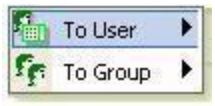
Click on Edit iFob Details to edit details of the select iFob.

Please refer to the iFob Details section for more details.

Security

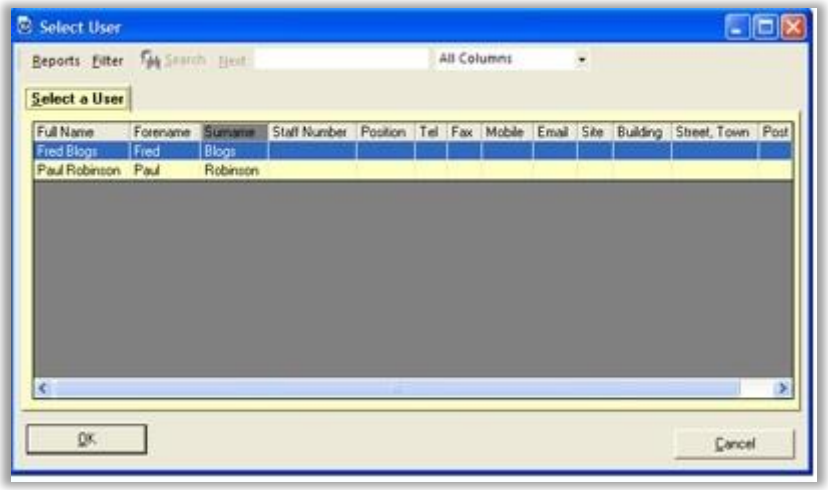
Grant Access

To User...



By selecting *Security* > *Grant Access* > *To User* , you are able to permit a user to have access to the selected iFob.

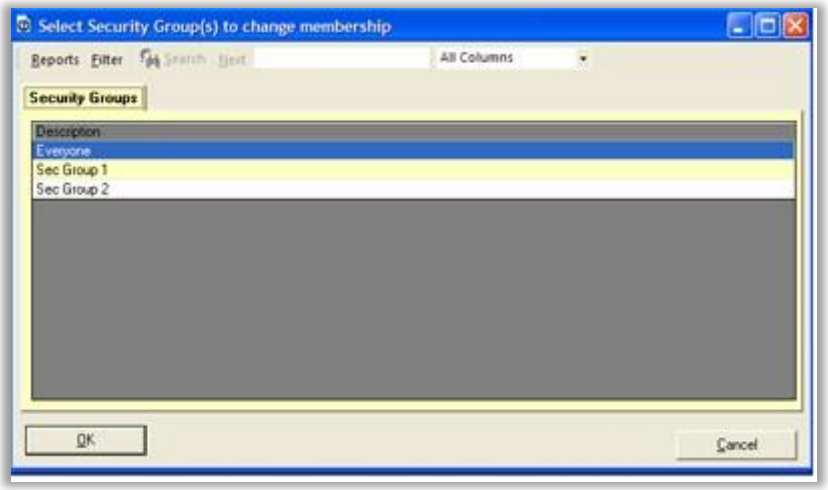
You will now be presented with a window that lets you search for the user that you require.



To Group...

Alliteratively if you select *Security* > *Grant Access* > *To Group* , you are able to permit a whole Group to have access to the selected iFob.

You will now be presented with a window that lets you search for the security group that you require.



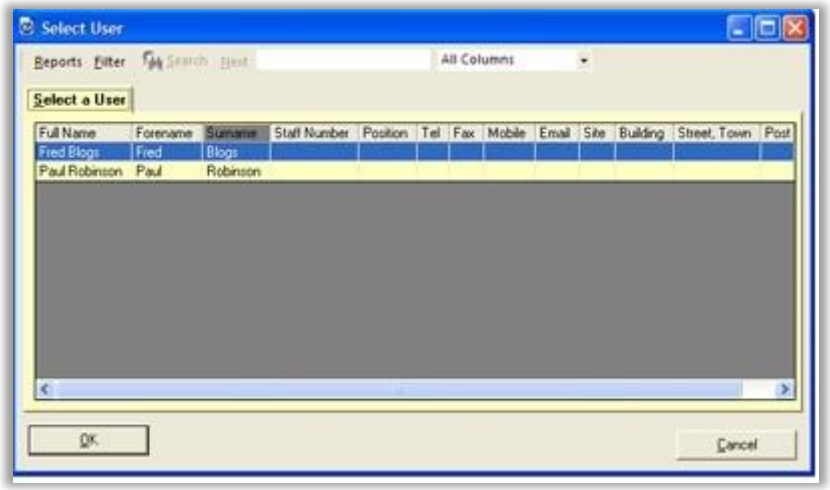
NOTE: If you allow a User or Group to have access to a particular iFob, you are effectively giving them the access level of the iFob without going into their User Details. This is particularly beneficial if you have many users in a Group and wish to assign them the same access level, this method is much quicker than editing their individual User Details.

Revoke Access

For User...

By Selecting *Security* > *Revoke Access* > *For User,* you are able to stop the user from having access to the selected iFob.

You will now be presented with a window that lets you search for the user that you require.



For Group...

Alliteratively if you select *Security* > *Revoke Access* > *For Group ,* you are able to stop whole Group from having access to the selected iFob.

You will now be presented with a window that lets you search for the security group that you require.

NOTE: If you revoke a User or Group from having access to a particular iFob, you are effectively taking the access level of the iFob away from them without going into their User Details. This is particularly beneficial if you have many users in a Group and wish to remove an access level that they all have, this method is much quicker than editing their individual User Details.

Immobilisor

iFob Programmer

Click on iFob Programmer to program either a Data32 or Data512 iFob.

Please refer to the iFob Programmer section for more details.

Set iFob Date & Time

Set the date and time of the selected Date Time iFob using the PC's current date and time.

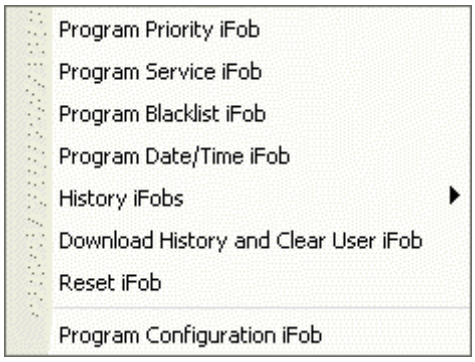
Read iFob Date & Time

Read the date and time from the selected Date Time iFob.

Download History and Clear User iFob

Download any user history in the iFob and clears the iFob ready for use.

Micro Traka iFobs



Program Priority iFob

Program Service iFob

Program Blacklist iFob

Program Data/Time iFob

Click on the type of iFob that is to be programmed for use with Micro Traka. Please refer to the Micro Traka Special iFobs section for more details.

History iFobs

Program

Program the selected iFob as a History iFob for use with Micro Traka.

Download

Download any history from the selected iFob.

Download History and Clear User iFob

Download any user history in the iFob and clears the iFob ready for use.

Reset iFob

Reset the memory in the iFob so that it can be reused by the next user.

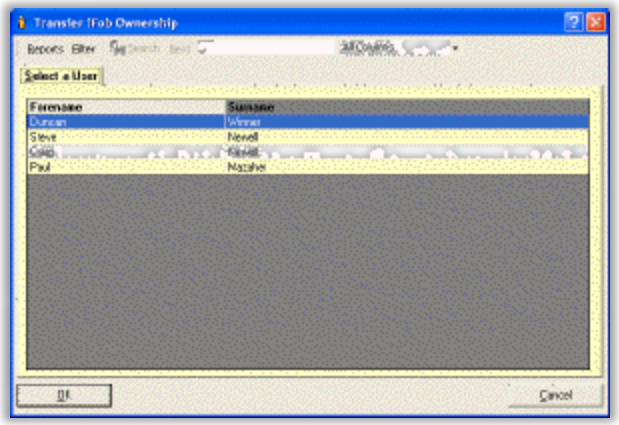
Program Configuration iFob

Program the selected iFob as a Configuration iFob. Please refer to the Micro Traka iFob Configuration section for more details.

Transfer iFob Ownership

This allows the software user (subject to their access permissions) to change the owner of an iFob.

For example the key associated with an iFob may be a vehicle key. If the vehicle breaks down, the key and iFob cannot be returned until the vehicle is repaired which may take some time. Therefore it is possible to change the ownership of the iFob from the person who withdrew the iFob to another user or department (say Motor Transport service).



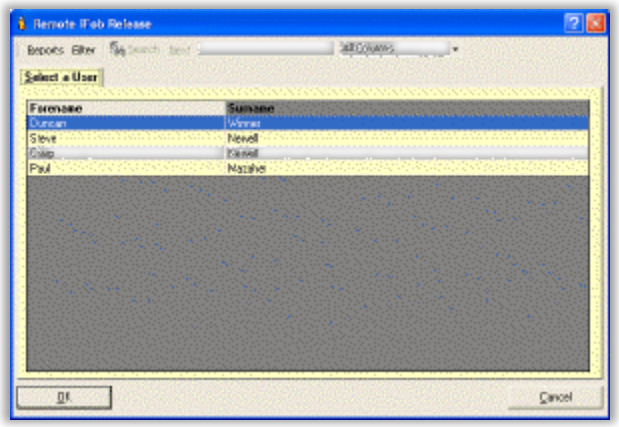
Simply select the name of a user of whom you wish to transfer the ownership to and click **OK**.

NOTE: You cannot transfer the ownership of an iFob if the iFob is currently in the system or if the user that you are transferring the iFob ownership to does not have the appropriate access.

NOTE: Transfer iFob Ownership is not available for systems with Random Return.

Remote iFob Release

This allows the software user to release a specific iFob to a selected user. The software records the name of the software user who released the iFob as well as the person to whom the iFob was released.



Simply select the name of a user of whom you wish to release the iFob to and click **OK**.

NOTE: You cannot release an iFob if the user that you are releasing the iFob to does not have the appropriate access.

NOTE: It is possible to hide this option within Traka32. If you require this feature to be hidden please contact Traka or your distributor.

Emergency Release

This opens the relevant cabinet door and releases the solenoid for the selected iFob for a maximum of 30 seconds. As soon as the iFob is removed, the user will be instructed to close the door and no further iFobs will be able to be removed. A remote key release is reported within the alarms report.

NOTE: It is possible to hide this option within Trak32. If you require this feature to be hidden please contact Traka or your distributor.

Engineers

NOTE: This menu can only be accessed if the current user of the software is logged in as an engineer.

iFob Memory Map

Click on iFob Memory Map to view the data currently stored in either a Data32 or Data512 iFob.

Reset iFob

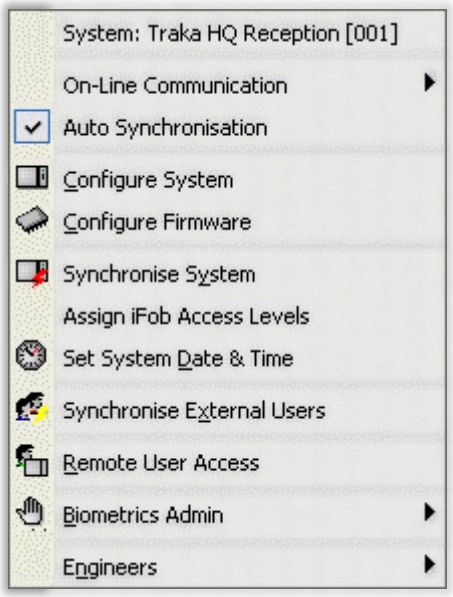
This option should be used with great caution! It deletes the information held within the selected Data iFob's memory.

NOTE: Traka will not be held responsible for the loss of data if you do not back up any data before resetting.

4.5.3 SYSTEM MENU

The system menu allows you to administer the selected system.

To access the System Menu, from the System Viewer, simply click with the right mouse button over the picture of the system.

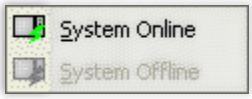


System

This field displays the name of the system you have clicked on.

Online Communication

Clicking on this menu will toggle the system between Online and Offline. When online a system will send real time data to the selected software.



Auto Synchronisation

Select this option to automatically keep the software and hardware synchronised whenever a change is made in the software to a User, iFob or Key details.

Clear this option if you wish to make changes to the database without synchronisation with the Traka system. This is useful if you have a large number of changes to make or if you are setting up a new database without the Traka System.

Clearing this option only lasts for the time the user is logged in to Traka32, once a user logs out and back in again the option will by default be enabled. There is an option 'Preserve the State of Auto-Comms Online Mode' that whilst enabled, will keep auto synchronisation disabled. For information on how to enable this option please view the Comms section of the Properties topic.

This option applies to only the selected System and is selected by default whenever Traka32 is loaded. If you want to set this option on all systems, this can be done from the Tools menu.

Configure System

Click on Configure System to edit details of the selected system.

Please refer to the System Settings section for more details.

Configure Firmware

This allows the cabinet firmware to be checked and configured as changes to the cabinet specification are made. Click on Configure Firmware to edit the firmware configuration of the selected system.

Please refer to the Configure Firmware section for more details.

Synchronise System

This communicates with the system to ensure that user and iFob details held in the system exactly match those held within the software. The synchronisation procedure will first prompt you to backup the system's memory. It will then reset the system's entire memory and synchronise the system with all the user, iFob and key booking details from the database as well as the date and time.

NOTE: Use with caution! Synchronising the system will reset the systems entire memory. As part of the synchronisation procedure it will request that you read the system data before the synchronising. To read the data first click on Yes. Once successfully read, you will be prompted to synchronise the system, to synchronise click on Yes.

NOTE: Traka will not be held responsible for the loss of data if you do not read the system data before synchronising.

Assign iFob Access Levels

This allows a user to (re)set all the iFob access levels within a system without having to edit each individual iFob record. Please refer to the Assign iFob Access Level section for more details.

Set System Date & Time

This lets you set the date and time of the selected system from the local PC date and time.

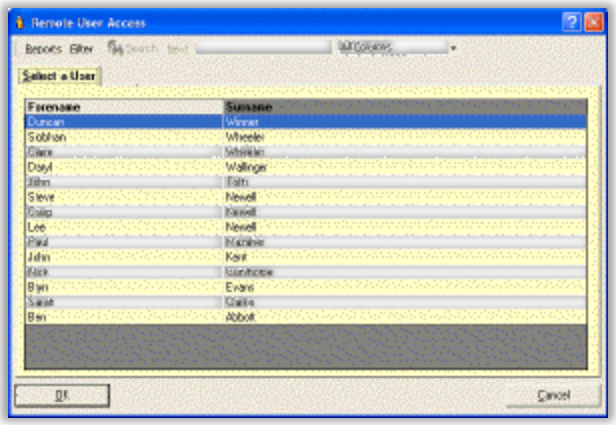
Please refer to the Set System Date & Time section for more details.

Synchronise External Users

This synchronises all the user records in the database that have been altered by the Traka.Net Pot-Box software with the selected system.

Remote User Access

This option allows the software operator to give system access to a user when perhaps the user had forgotten their ID card. The user will only be able to take keys if their access level allows.



Simply select the name of a user of whom you wish to give access to the system and click **OK**.

NOTE: You cannot give access if the user does not have the appropriate access.

Biometrics Admin

NOTE: This option will only show if the selected system has a Traka Biometrics Reader fitted.

Backup Templates

Click this option to backup all of the fingerprint templates to the database. This should be done on a regular basis to ensure no data is lost in the event of failure.

Restore Template

This synchronises all the user's fingerprint templates in the database with the selected biometrics reader.

Configure Biometrics

This allows the biometrics reader firmware to be checked and configured as changes to the reader specification are made. Click on Configure Biometrics to edit the firmware configuration of the selected reader.

Please refer to the Configure Biometrics section for more details.

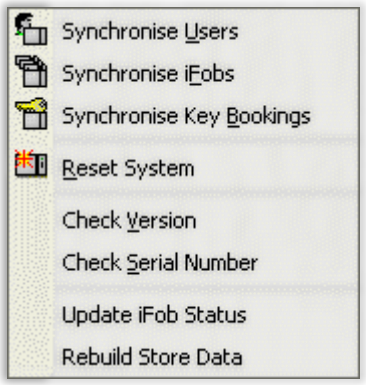
Reset Biometrics

This option should be used with great caution! It deletes the information held with the biometrics reader's memory. The reset procedure will first prompt you to backup the reader's memory. It will then reset the reader's entire memory.

NOTE: Use with caution! Resetting the biometrics reader will reset the reader's entire memory. As part of the reset procedure it will request that you backup the templates before the restoring. To backup the templates, first click on Yes. Once successfully backed up, you will be prompted to reset the templates, to reset click on Yes.

NOTE: Traka will not be held responsible for the loss of data if you do not backup the templates before resetting.

Engineers



NOTE: This menu can only be accessed if the current user of the software is logged in as an engineer.

Synchronise Users

This synchronises all the user records in the database with a specific system. If you want to synchronise all the user records in the database with all the systems, this can be done from the Tools menu.

Synchronise iFobs

This reads all the iFob serial numbers, creates new iFob records in the database for any unrecognised iFobs found and then synchronises all the iFob records in the database with the selected system.

Synchronise Key Bookings

This synchronises all the key bookings in the database with the selected system.

NOTE: This option will only show if the firmware of the selected system has Key Booking enabled.

Reset System

This option should be used with great caution! It deletes the information held with the system and resets the Traka system memory. The reset procedure will first prompt you to backup the systems memory. It will then reset the systems entire memory.

NOTE: Use with caution! Resetting the system will reset the systems entire memory. As part of the reset procedure it will request that you read the system data before the resetting. To read the data first click on Yes. Once successfully read, you will be prompted to reset the system, to reset click on Yes.

NOTE: Traka will not be held responsible for the loss of data if you do not read the system data before resetting.

Check Version

This communicates directly with the selected system to show the firmware version.

Check Serial Number

This communicates directly with the selected system to show the system serial number.

NOTE: This option is only available with a firmware version of 6.06.01 or above.

Update iFob Status

This option will examine the state of each iFob in the system and update state information about each iFob using transaction information.

This is the equivalent of reading the iFob Store in older versions of the firmware.

Before performing this operation, please ensure that '**Read All System Data**' has successfully completed.

NOTE: This option is only available with a firmware version of 6.07.00 or above.

Rebuild Store Data

This option will rebuild the iFob store data held internally for each iFob using the data that is currently held with each iFob.

This can be useful if the information displayed on the LCD is inaccurate.

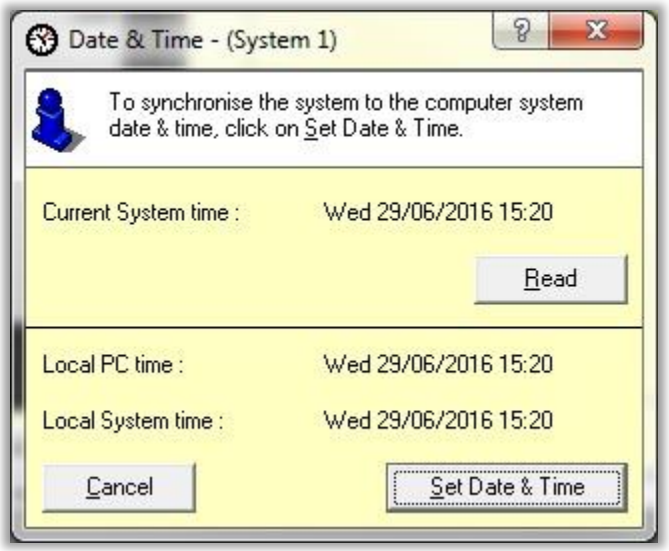
Before performing this operation, please ensure that '**Read All System Data**' has successfully completed.

NOTE: This option is only available with a firmware version of 6.07.00 or above.

4.5.3.1 SET SYSTEM DATE & TIME

To set a Traka System's Date and Time...

1. From the main screen select the required system from the dropdown and from the system viewer right click over the picture of the pod and click **Set System Date & Time**. Traka32 will read the current date and time from the system and display it along with the local PC's date and time.



2. Simply click on **Set Date & Time** to write the local PC's date and time to the Traka System.

NOTE: The Local System Time shows the local time of the Traka System based upon the Time Zone, Daylight Saving and Date Format selected. To alter this time, please refer to the System Settings section of the user guide.

NOTE: Make sure the date and time of your local PC is correct!

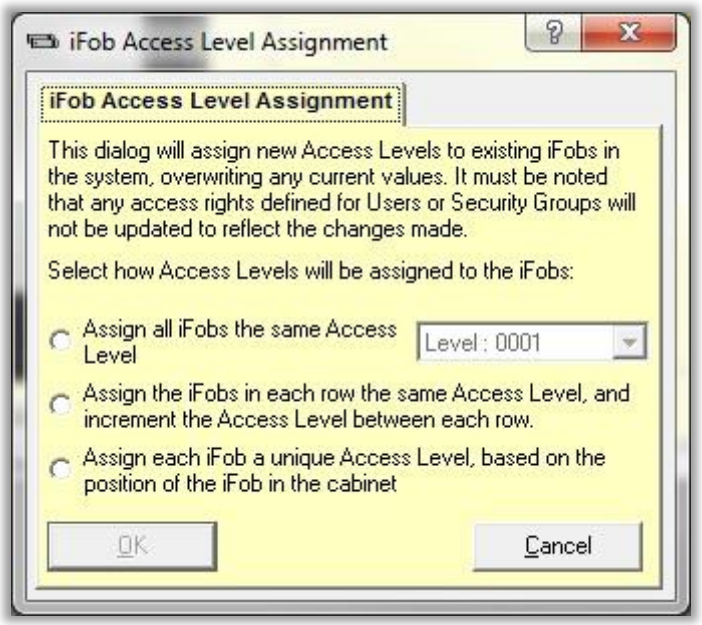
4.5.3.2 ASSIGN IFOB ACCESS LEVELS

This dialogue will assign new Access Levels to existing iFobs in the system, overwriting any current values.

NOTE: Any access rights defined for Users or Security Groups will not be updated to reflect the changes made.

To assign iFob access levels...

1. From the main screen select the required system from the dropdown and from the system viewer right click over the picture of the pod and click on **Assign iFob Access Levels**.



2. Select how you wish to assign the access levels to the iFobs from...

   - **Assign all iFobs the same Access Level.** Simply select the option and select the appropriate access level.

   - **Assign the iFobs in each row the same Access Level, and increment the Access Level between each row.** For example row 1 (slots 1 to 10) will have access level 1, row 2 (slots 11 to 20) will have access level 2 and so on.

   - **Assign each iFob a unique Access Level, based on the position of the iFob in the cabinet.**

3. Click on **OK** to assign or **Cancel** to quit.

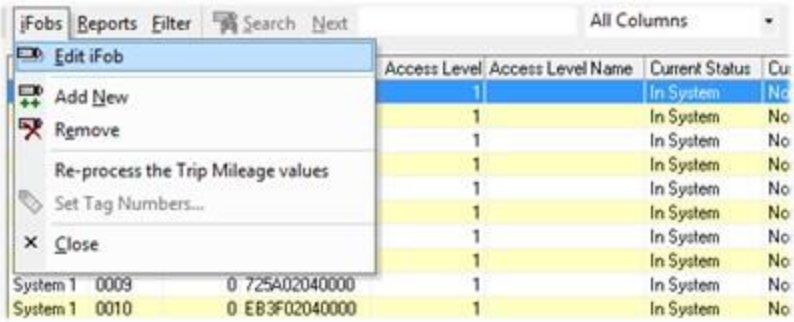
4.6 IFOB DETAILS

4.6.1 EDITING IFOBS

1. The quickest way to add a new iFob into a system is from the **System Viewer**.

2. From the main screen select the system from the drop down menu in the main toolbar, and from the system viewer right click over the picture of the relevant position and click on **Edit iFob Details**.

You can also access the iFob Details from the iFob List. Click on **View**, **iFob List** from the main menu and the iFob List will open. From the iFob list simply **double click** on the iFob record you wish to edit or click on the **iFobs** menu followed by **Edit iFob**.



3. The selected iFob record will open.

4. Edit the appropriate details. For more details refer to the iFob Details section.

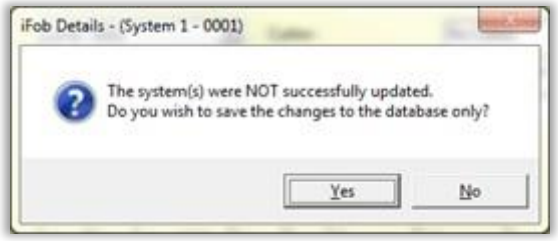
5. To **Save** your changes, simply click on  or 

.

6. To **Cancel** your changes, simply close the window and click **No** when asked if you want to save the changes.

7. If you save your changes, the software will automatically update the Traka System when you save any iFob details.

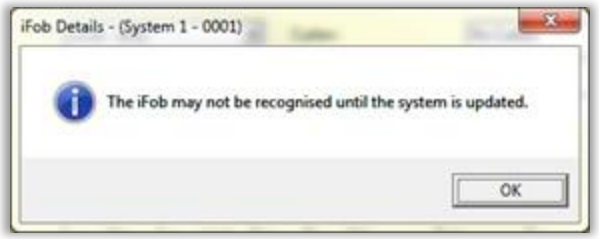
If the software was unable to update one or more of the systems the following message will be shown...



Click on **Yes** if you wish to save the changes to the database only. You can update the relevant systems at a later date using the Synchronise System option from the System Viewer.

Click on **No** if you wish to discard the changes.

If you clicked **Yes,** the following message will be shown...



4.6.2 ADDING / REPLACING IFOBS

NOTE: If your system is set up as Random Return to Multiple Systems, the process for replacing an iFob is different to the procedure shown here. Refer to the section Replacing iFobs in Random Return to Multiple Systems.

Most Traka Systems work on fixed iFob replacement basis which means the iFobs must be returned to the position from where they were taken. By default the system will not know where an iFob should go therefore the iFob serial number must be assigned to the position in the system and the Traka32 software.

1. Go to the system that you wish to assign the iFob to. If the system has one or more doors, access the system in the normal way.

   If you have a **No Door** system, do not access the system and proceed to the next step.

2. Insert the iFob into a vacant position.

3. If the system has a door the display should show...

   In which case, ignore the message and close the door.

   If the following message is shown...

   This means that the iFob you are using is already in use within the system. You must first deallocate or remove the iFob from Traka32 before reallocating it again. Please refer to the De-allocating iFobs or Removing iFobs section.

   NOTE: Ensure nobody accesses the system until the following steps are completed otherwise they will be asked to remove the unrecognised iFob and this may cause confusion.

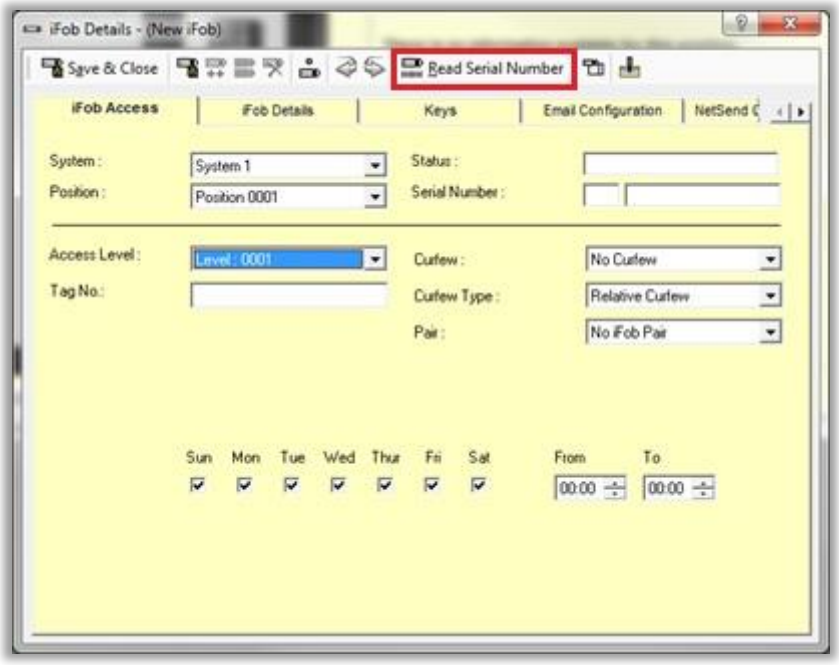
4. The quickest way to add a new iFob into a system is from the **System Viewer**.

5. From the main screen select the system from the drop down in the main toolbar, and from the system viewer right click over the picture of the relevant position and click on **Edit iFob Details**.

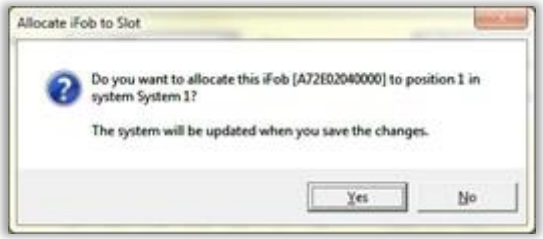
   

6. The selected iFob record will open.

7. Click on **Read Serial Number**. Traka32 will communicate to the selected system and read the iFobs serial number.



If the system successfully reads the serial number, click on **Yes** to allocate the serial number to the iFob Details record.



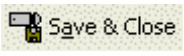
If the system could not detect an iFob...

Check that the iFob is in the correct slot, the iFob not recognised message is being displayed and that you are editing the correct details. If the iFob not recognised message is not being displayed on a system with a door then release the iFob using the Emergency release function from the System Viewer and try a different iFob. If after trying a new iFob you still cannot read the serial number there may be a problem with the slot, therefore contact your supplier.

If the system detects that the iFob is already in use...

You must first deallocate or remove this iFob from Traka32 before reallocating it again. Please refer to the De-allocating iFobs or Removing iFobs section.

8. Edit any of the other appropriate details. For more details refer to the iFob Details section.

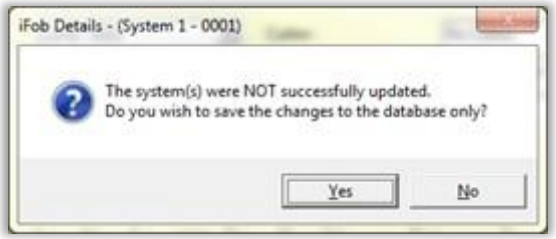
9. To **Save** your changes, simply click on  or 

.

10. To **Cancel** your changes, simply close the window and click **No** when asked if you want to save the changes.

11. If you save your changes, the software will automatically update the Traka System when you save any iFob details.

    If the software was unable to update one or more of the systems the following message will be shown...



    Click on **Yes** if you wish to save the changes to the database only. You can update the relevant systems at a later date using the Synchronise System option from the System Viewer.

    Click on **No** if you wish to discard the changes.

    If you clicked **Yes,** the following message will be shown...

4.6.3 ADDING / REPLACING IFOBS USING A DESKTOP PROGRAMMER

NOTE: If your system is set up as Random Return to Multiple Systems, the process for replacing an iFob is different to the procedure shown here. Refer to the section Replacing iFobs in Random Return to Multiple Systems.

Most Traka Systems work on fixed iFob replacement basis which means the iFobs must be returned to the position from where they were taken. By default the system will not know where an iFob should go therefore the iFob serial number must be assigned to the position in the system and the Traka32 software.

1. Insert the iFob into the desktop programmer.

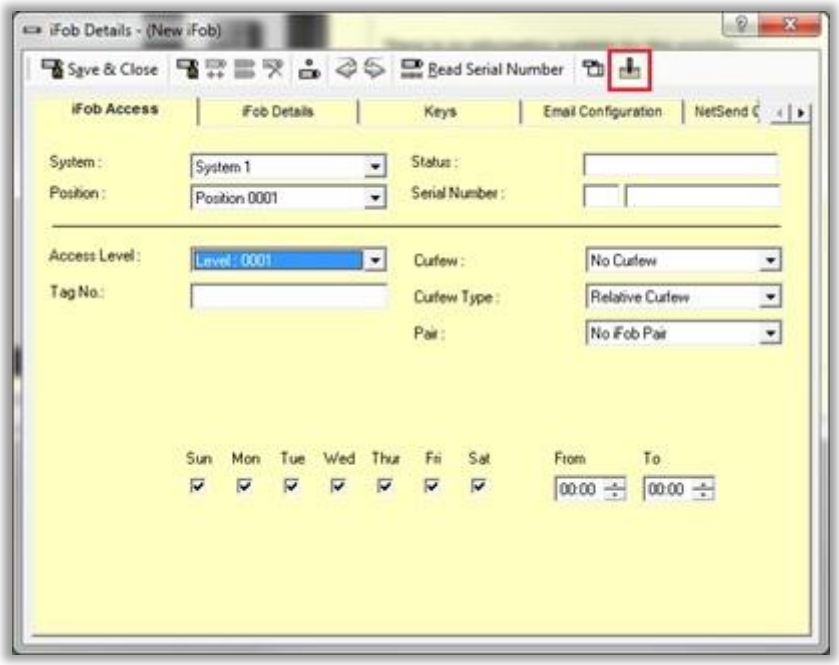
2. The quickest way to add a new iFob into a system is from the **System Viewer**.

3. From the main screen select the system from the drop down in the main toolbar, and from the system viewer right click over the picture of the relevant position and click on **Edit iFob Details**.

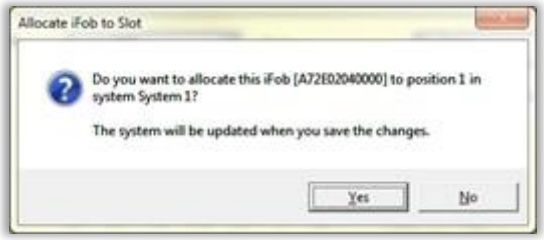
NOTE: It is very important to ensure that the correct System and Position is selected for the iFob you are about to assign using the desktop programmer.

4. The selected iFob record will open.

5. Click on the button highlighted below. Traka32 will communicate to the desktop programmer and read the iFobs serial number.



If the system successfully reads the serial number, click on **Yes** to allocate the serial number to the iFob Details record.



If the system could not detect an iFob...

Check that the iFob is inserted correctly into the desktop programmer. If after trying a new iFob you still cannot read the serial number there maybe a problem with the slot, therefore contact your supplier.

If the system detects that the iFob is already in use...

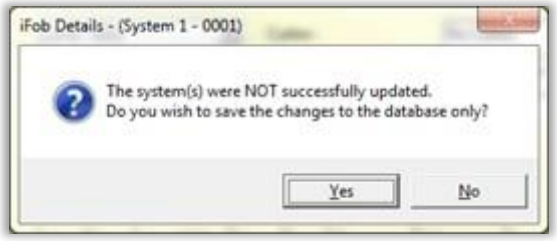
You must first deallocate or remove this iFob from Traka32 before reallocating it again. Please refer to the De-allocating iFobs or Removing iFobs section.

6. Edit any of the other appropriate details. For more details refer to the iFob Details section.
7. To **Save** your changes, simply click on  or 

.
8. To **Cancel** your changes, simply close the window and click **No** when asked if you want to save the changes.

9. If you save your changes, the software will automatically update the Traka System when you save any iFob details.

If the software was unable to update one or more of the systems the following message will be shown...



Click on **Yes** if you wish to save the changes to the database only. You can update the relevant systems at a later date using the Synchronise System option from the System Viewer.

Click on **No** if you wish to discard the changes.

If you clicked **Yes,** the following message will be shown...

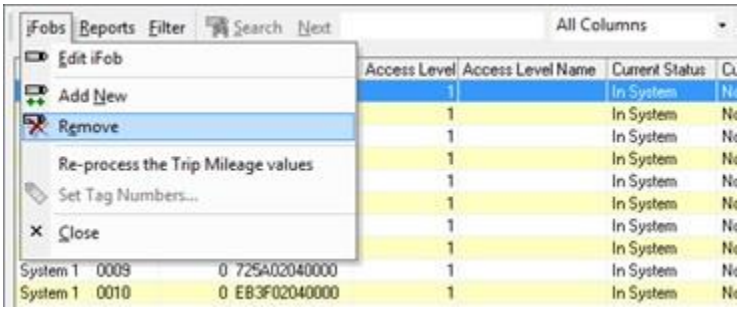
10. Finally, go and **place the iFob into the relevant Position** within the selected System and test.

4.6.4 REMOVING IFOBS

1. The quickest way to remove an iFob from a system is from the **System Viewer**.

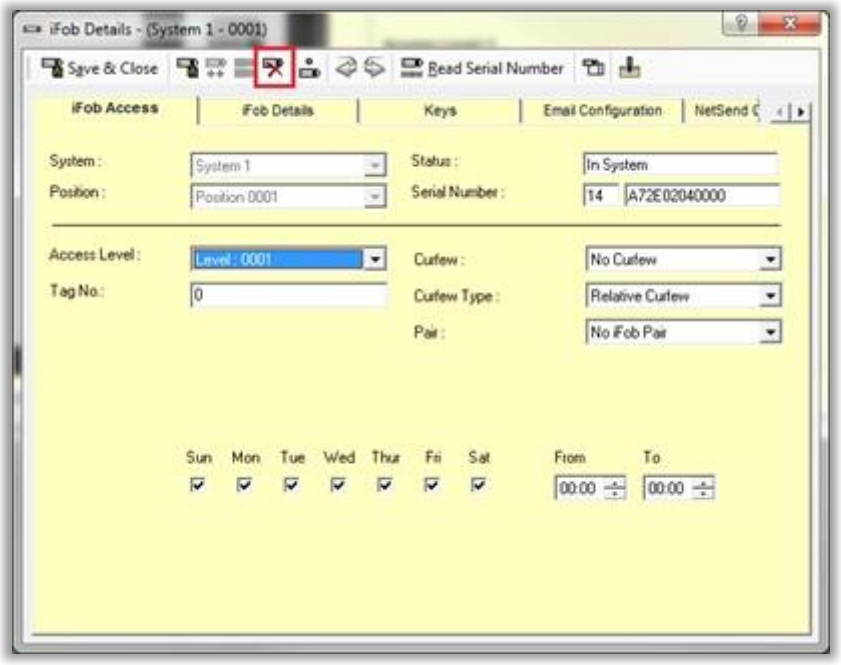
2. From the main screen select the system from the drop down in the main toolbar and from the system viewer right click over the picture of the relevant position and click on **Edit iFob Details**.

You can also remove an iFob from the iFob List. Click on **View**, **iFob List** from the main menu and the iFob List will open. From the iFob list simply **click** on the iFob record you wish to remove, click on the **iFobs** menu followed by **Remove**.



3. If you clicked Edit iFob Details from the system viewer, the selected iFob record will open.

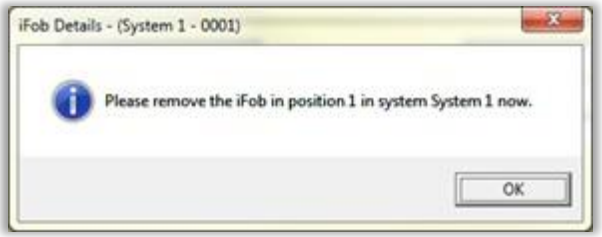
4. Click on the button highlighted below.



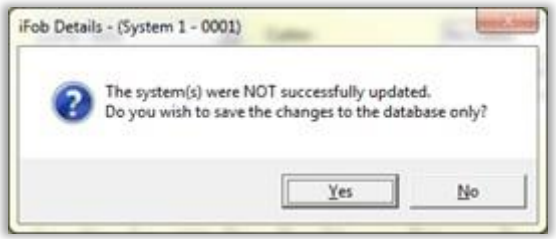
5. To remove the iFob click on **Yes**.

6. The software will automatically update the Traka System.

7. If successful you will be prompted to physically remove the iFob from the system.



If the software was unable to update the system the following message will be shown...



Click on **Yes** if you wish to save the changes to the database only. You can update the relevant system at a later date using the Synchronise System option from the System Viewer.

Click on **No** if you wish to discard the changes.

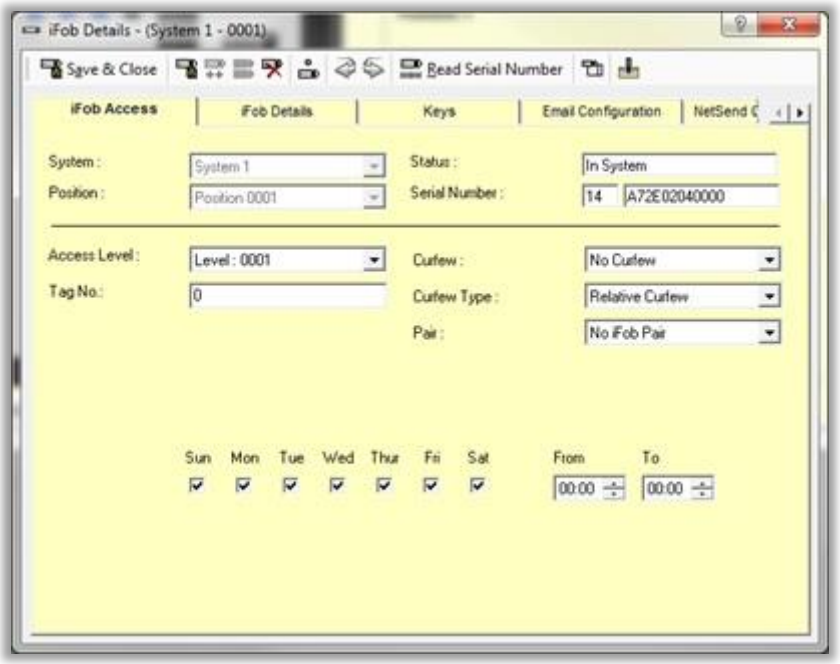
If you clicked **Yes,** the following message will be shown...

4.6.5 IFOB DETAILS

The iFob Details window allows you to add and edit the iFob details.

iFob Access

Here you define the accessibility of the iFobs.



System and Position

The System and Position fields show where the iFob is located. These are for reference only unless you are adding a new iFob in which case you will have to pick the system and position you want to allocate the iFob to.

Status

The status of the iFob simply shows whether the iFob is currently...

- In the system
- Out of the system
- Out of the system and under a curfew
- Out of the system and is overdue

Family Code

The family code fields show the family code of the iFob allocated to the selected position. The family codes can be interpreted as follows...

- 01 Traka iFob
- 14 Traka Data32 iFob
- 2D Traka Data128 iFob
- 23 Traka Data512 iFob
- 24 Traka Date & Time iFob

Serial Number

The serial number field shows serial number of the iFob allocated to the selected position.

To assign an iFob serial number, refer to the sections Adding/Replacing iFobs and Adding/Replacing iFobs using a Desktop Programmer.

Access Level

As supplied every iFob is given access level 001 and every user is given access to all iFobs with access level 001. Therefore every user will be able to take every iFob.

However, you will almost certainly wish to restrict certain users to certain iFobs and this is done by defining the access level for every iFob and subsequently by determining which access level each user may take.

If you wish you may give every iFob its own individual access level and by giving each user access to just that access level every user could be restricted to use only his iFob.

Up to 200 (8bit system) or 2560 (16bit system) Access Levels are available and users may have access to as many of these levels as is required.

A user may only take out an iFob if they have the same Access Level as the required iFob.

For more details please refer to the Access Levels section.

Tag No.

Here you can optionally define a Tag Number for the iFob. This tag number should match the number of the physical tag attached to the iFob (if used). Tags are most commonly used with the feature Random Return to Multiple Systems.

iFob Curfew

When using Curfews there are two different types that can be set depending on your control PCB. User iFob curfew can be used in conjunction with User Curfews.

NOTE: It is possible to change the curfew details for iFob's that are currently out of the system and not already under curfew. Once the details are changed, a message is shown warning that the new curfew will not take effect until the iFob is returned and removed again.

- **Relative Curfew**

  This curfew allows you to set a time limit for which the all the user's keys may be out of the cabinet. This time limit is set in multiples of 15 minutes to a maximum of 24 hours. Thus if you expect the key to be returned within 1 hour you should complete the key curfew accordingly. If the key is not returned within 1 hour, an alarm condition will be activated which will show as an alarm on the alarms report.

  NOTE: On a 8bit system if you have two curfews set (absolute user curfew and a relative iFob curfew) at the same time the iFob curfew takes priority.

  NOTE: On a 16bit PCB if there is a user and an iFob curfew set, the 16bit works out which one will expire first and uses that as priority.

- **Absolute Curfew**

  This curfew allows you to set a time for which the all the user's iFobs should be returned. For example, if you set the curfew to 17:30 all iFobs taken before this time will become overdue if not returned. This is a very powerful feature as it will highlight if keys are not returned at the end of a users shift.

Any keys out under curfew or overdue will be shown on the system viewer after you Read All System Data. You may also see a report on overdue iFobs or overdue keys from the Reports menu.

Pair

You may choose to relate one iFob to another. A related iFob must be replaced before the selected iFob can be removed.

To relate an iFob, simply complete the number in the Pair field. You may have one iFob related to another iFob but you do not have to have the second iFob related back to the first. If required you may have several iFobs related to a particular iFob. If you set up iFob pairs, the Traka display will clearly show which key must be replaced before the selected key can be removed.

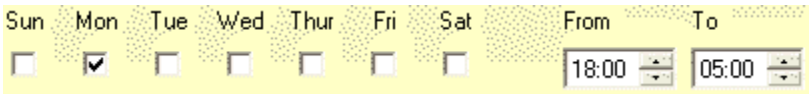
It is also possible to reverse pair an iFob by selecting **Reverse Pair**. If you reverse pair an iFob, the system will check the status of all other iFobs that are paired to the reversed iFob and will not allow access to the reversed iFob if one or more of the paired iFobs are out of the system.

NOTE: The Reverse Pair feature is only available in version 6.06.14 and above of the firmware.

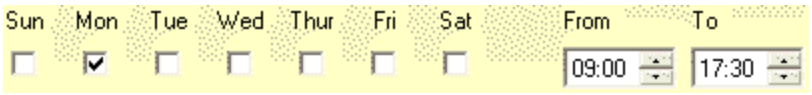
Access Times

You may control the hours the iFob is available. By default the iFob is always available (subject to the users access level) unless you select days with a start and end time.

The '**Days of the Week**' (Sun thru Sat) and the '**From**' time together defines the time at which the iFob will be available for access. The '**To**' time simply defines when the iFob will become unavailable for access. Here are some examples...



Here the iFob will be available from Monday 18:00 to Tuesday 05:00.

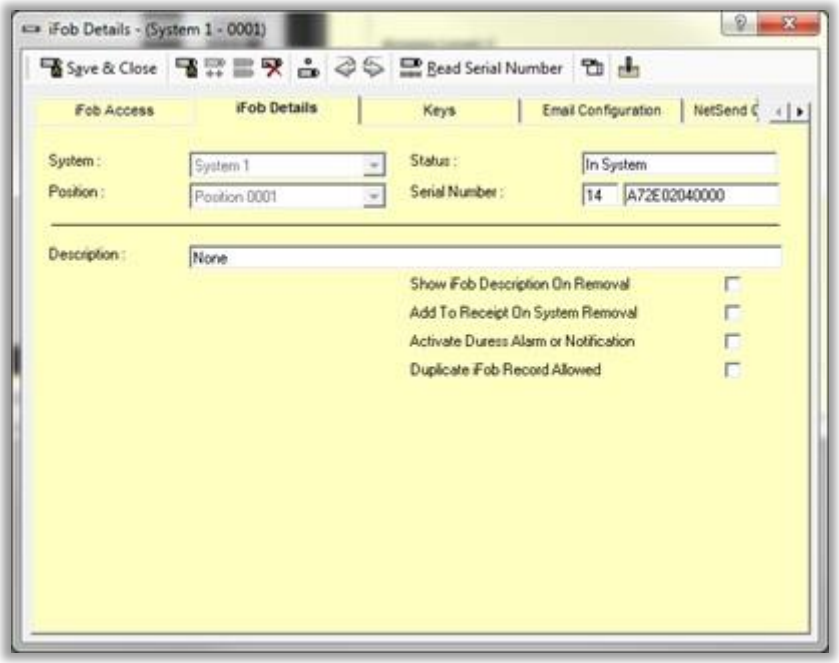


Here the iFob will be available from Monday 09:00 to Monday 17:30.

Tip: If you assign a user with an access level of **198** this will override the iFob Access Times allowing that user access 24 hours a day.

iFob Details

Here you can view and edit optional iFob details.



Description

This field shows the current key description associated to the iFob. A description of up to 70 characters can be used.

NOTE: When using the 'Random Return to Multiple Systems' option, the description field can only have up to 10 characters.

The description field can either be entered manually here, or alternatively can be populated automatically with the description given in one of the Key Details fields of the key(s) assigned to that iFob.

To configure the required key details, please refer to the Properties section. By selecting the 'Use as iFob Description' option against the required field, then all keys attached to the iFob will be used to auto-fill the description.

Show iFob Description on Removal

With this option enabled the description of the iFob will be displayed on the LCD when it is removed.

Add To Receipt On System Removal

Activate Duress Alarm or Notification

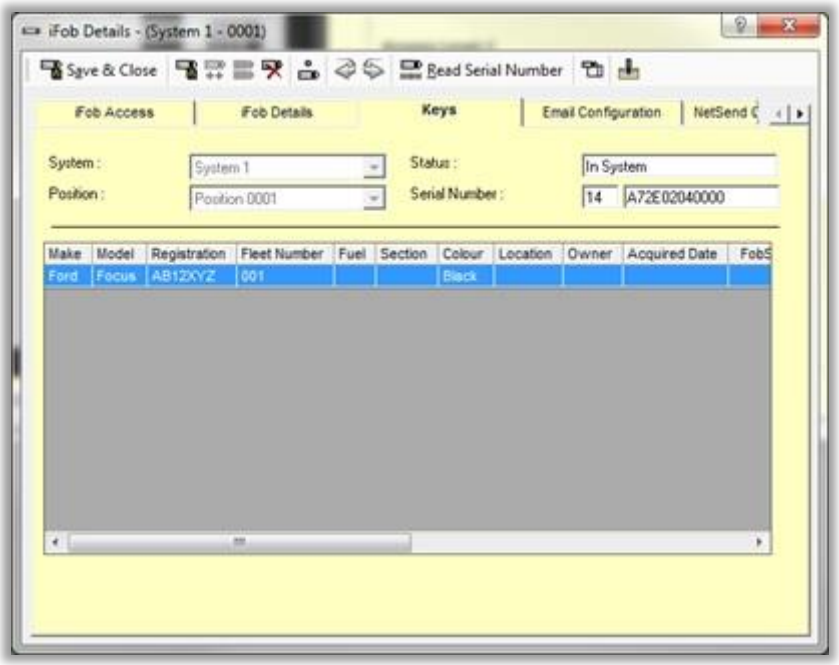
Select this option to activate a Duress alarm whenever the selected iFob is removed from the system, or alternatively you can set this option within the User details.

Duplicate iFob Record Allowed

Select this option to enable the iFob to be used in Fixed Return to Multiple Systems. For more information on Duplicate iFob Record, refer to the section Fixed Return to Multiple Systems.

Keys

Here you can view the details of any keys attached to the iFob.



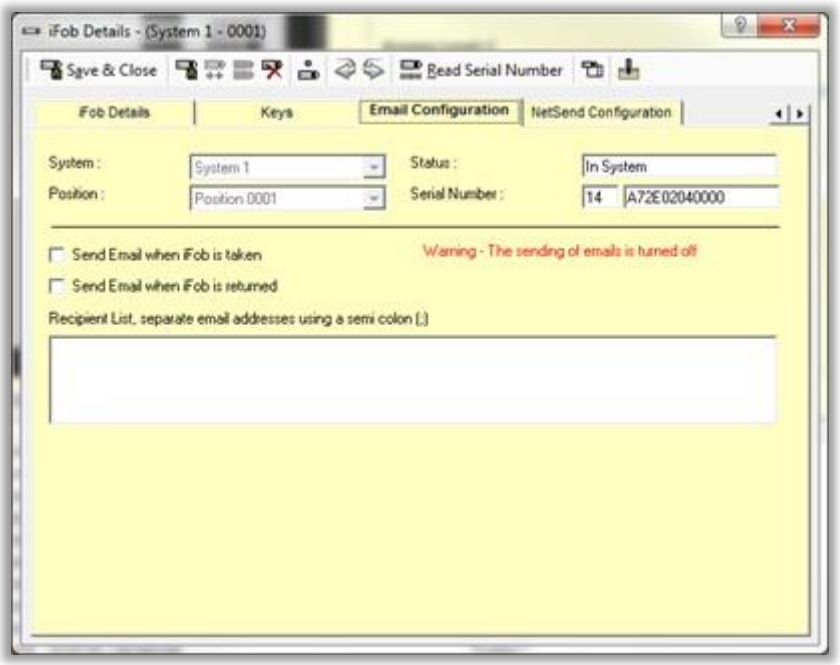
Editing Keys

To edit any of the keys attached to the iFob simply double click on the key in the list.

Email Configuration

Here you can configure emails to be sent automatically whenever certain events occur for the selected iFob.

NOTE: This basic messaging system has now been superseded by the comprehensive Message Notification System from Traka32 Version 02.006.002.



Send Email when iFob is taken

Select this option to enable Traka32 to send an email each time the selected iFob is taken. The email will be sent to each address listed in the recipient list below.

Send Email when iFob is returned

Select this option to enable Traka32 to send an email each time the selected iFob is returned. The email will be sent to each address listed in the recipient list below.

Recipient List

Enter a list of email addresses that Traka32 will automatically email each time the selected iFob is taken and/or returned. To enter more than one email address, separate each email address with a semi colon ';' for example, djw@traka.com; support@traka.com; license@traka.com

NOTE: For this feature to work, the feature must be enabled in the Properties window and a valid SMTP Server defined.

NOTE: On certain SMTP servers such as Microsoft Exchange, relaying may have to be enabled in order allow Traka32 to send e-mails to the outside world. For a guide on how to safely configure Microsoft Exchange for relaying, please refer to the Relaying on Microsoft Exchange section.

Example Emails

Duncan Winner has taken an iFob

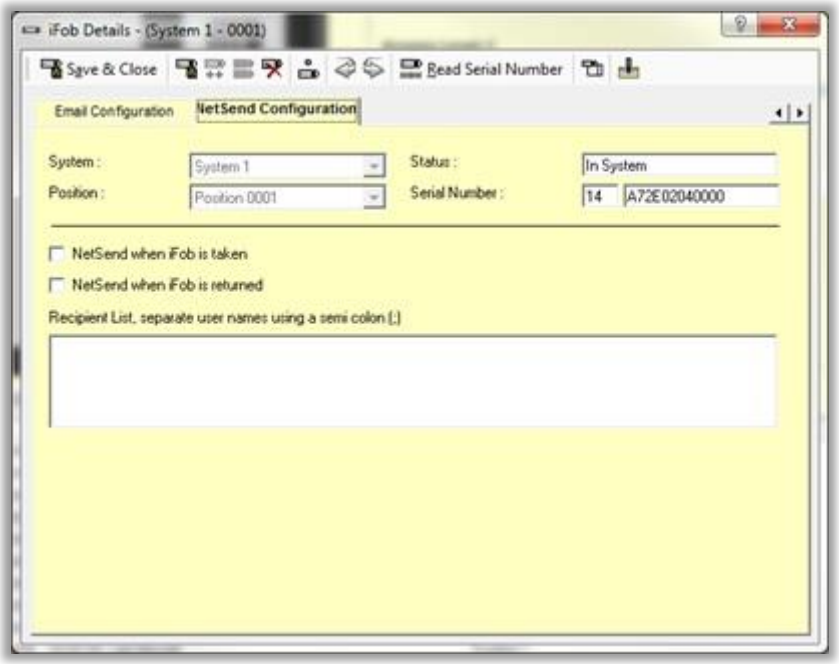
```
Duncan Winner has taken an iFob from position 1 (key description: 'Porsche') in system
'System 1 [001]' at 09-May-2005 10:55:00.
```

Duncan Winner has returned an iFob

```
Duncan Winner has returned an iFob to Position 1 (key description: 'Porsche') in system
'System 1 [001]' at 09-May-2005 10:55:00.
```

NetSend Configuration

Here you can configure messages to be sent automatically using NetSend whenever certain events occur for the selected iFob.



NetSend when iFob is taken

Select this option to enable Traka32 to send a message each time the selected iFob is taken. The message will be sent to each user listed in the recipient list below.

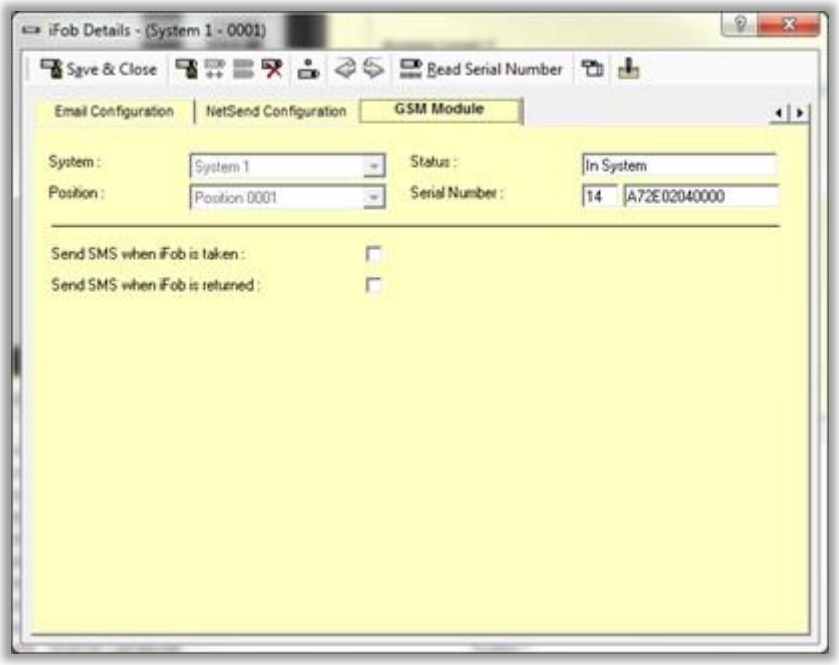
NetSend when iFob is returned

Select this option to enable Traka32 to send a message each time the selected iFob is returned. The message will be sent to each user listed in the recipient list below.

NOTE: For this feature to work, the Windows Messenger Service must be running. For a guide on how to enable the Microsoft Messenger Service, please refer to Messenger on Microsoft Windows section.

GSM Module

NOTE: This tab will only show if the firmware of the selected system has the GSM Module Interface enabled.



Send SMS when iFob is taken

Select the Send SMS when iFob is taken option to allow the Traka Cabinet to send a SMS each time the selected iFob is taken from the Cabinet.

Send SMS when iFob is returned

Select the Send SMS when iFob is returned option to allow the Traka Cabinet to send a SMS each time the selected iFob is returned to the Cabinet.

4.6.6 DE-ALLOCATING IFOBS

iFobs can be de-allocated from a System without being deleted. De-allocated iFob can then be re-allocated again in the future. This is very useful if you want to transfer an iFob from one slot to another or one cabinet to another.

To De-Allocate an iFob

1. Edit the record of the iFob that your require to de-allocate.
2. Click on the **De-allocate iFob** toolbar button: 
3. This will change the **System** field to 'No System Selected' and **Position** field to 'No iFobs Available'.
4. Click on **Save & Close**.
5. The iFob will then appear in the iFob List as a de-allocated iFob.

To Re-Allocate an iFob

1. Edit the record of the iFob that you wish to re-allocate.
2. Set the **System** and **Position** to the new location for the iFob.
3. Click on **Save & Close**.

4.7 KEY DETAILS

4.7.1 KEY LIST

The Traka system allows you to define as many keys as you wish to attach to each iFob. You may also define keys that are not currently attached to any iFob. However, as soon as the key is attached to an iFob, the Traka system will monitor the activity of the key, recording every usage, even if the key is moved from one iFob to another.

Where the Traka Immobilisor is installed and the iFob is being used as the key then describe the iFob in this section.

The key list can be filtered to show Allocated Keys, Non-allocated Keys or both by clicking on **Filter** and selecting the appropriate filter from the drop down menu.

Keys that are used long term by an organisation...

Most organisations will hold each key or bunch of keys for a long period of time. For example the keys to the Stock room are probably never likely to change and the history of the iFob and the key(s) will probably be the same. However, if one of the keys from a bunch should be removed or moved to a different iFob then the iFob history will start to differ from the Key history.

Keys that are used short term by an organisation...

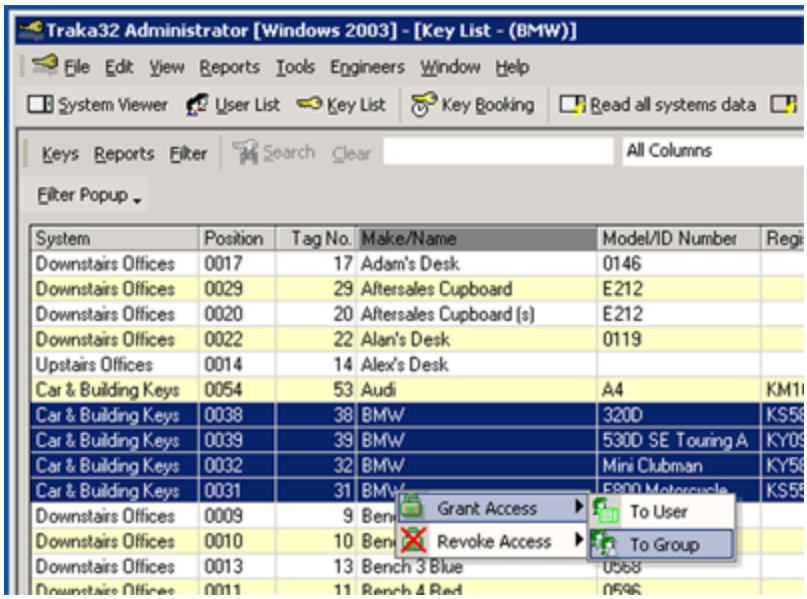
Organisations that hold keys for short terms such as motor dealers may wish to create an intermittent history. Every new key is added as described before and allocated to a free iFob. Once the key (for the car) has been sold or serviced, it should be deallocated and any further activity will automatically stop. If the vehicle should be returned at a later date, use the search facility to find the vehicle and then reallocate the vehicle again as described before. Now the activity history will continue. By deallocating and reallocating a key, a complete broken history can be cumulated.

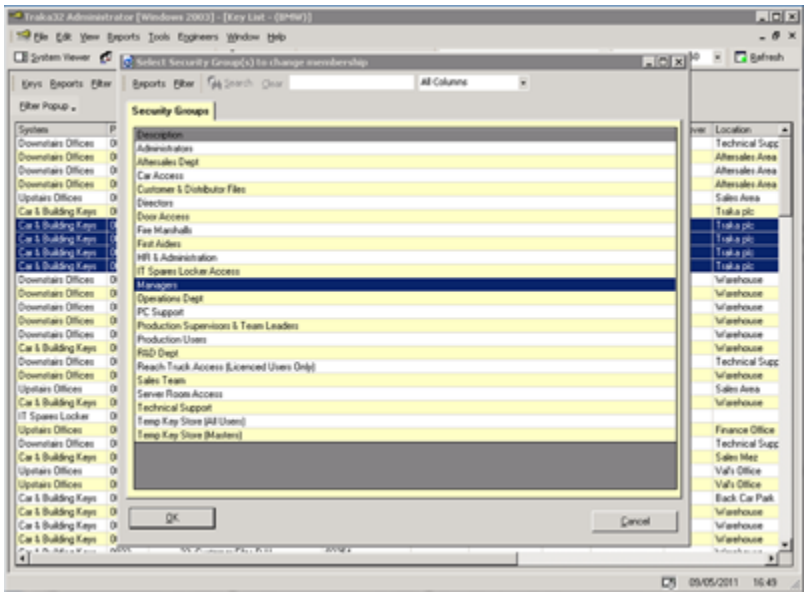
Assigning Access levels to Users and Security Groups from the Key List

You can now assign access levels to users and security groups from the Key List. This is achieved by right clicking on one or more Keys in the key List and selecting either the user or security group.

Below is a screen shot showing a user being assigned to a selection of keys:

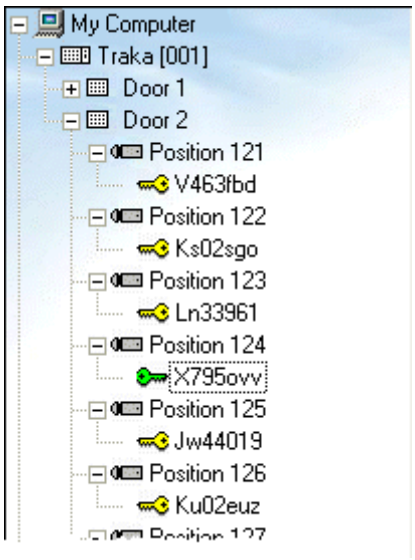
Below is a screen shot showing a security group being assigned to a selection of keys:





4.7.2 KEY TREE

The Key List comprises of a list of all the keys and a tree view of how the keys have been attached to the iFobs.



Keys can be moved from iFob to iFob or placed in the Non-Allocated Keys Bin at the bottom of the tree. From the key tree, click on the required key, press and hold down the **Shift** key and then drag the key to the required iFob.

When a key is attached to an iFob, every time that the iFob is taken from the cabinet, each key will have its own individual history of activity.

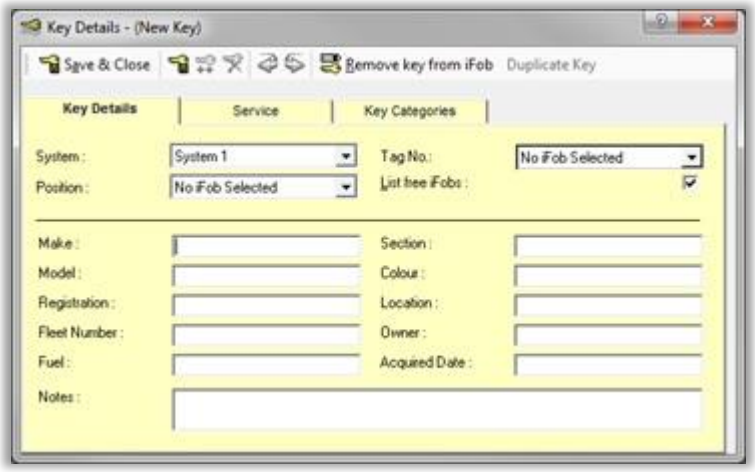
The Key Tree can be toggled on and off by clicking on **Filter**, **Hide Key Tree** or **Show Key Tree**.

4.7.3 ADDING KEYS

1. From the main screen click on **Key List** and a list of the current keys will be shown.
2. From the key list click on the **Keys** menu followed by **Add New**.

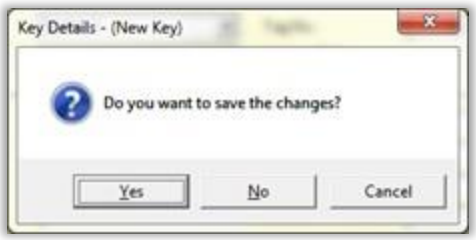
If you already have a key record open you can create a new record by simply clicking on the  button.

3. A new blank key record will be created.



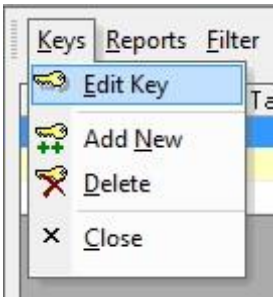
4. Edit the appropriate details. For more details refer to the Key Details section.
5. To **Save** your changes, simply click on  or 

.
6. To **Cancel** your changes, simply close the window and click **No** when asked if you want to save the changes.

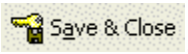


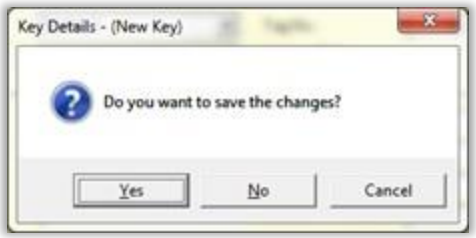
4.7.4 EDITING KEYS

1. From the main screen click on **Key List** and a list of the current keys will be shown.
2. From the key list simply **double click** on the key record you wish to edit or click on the **Keys** menu followed by **Edit Key**.



You can also edit key details from the **System Viewer**, simply right click over the position that the keys are associated with and click on **Edit Key Details**.

3. The selected key record will open.
4. Edit the appropriate details. For more details refer to the Key Details section.
5. To **Save** your changes, simply click on  or  .
6. To **Cancel** your changes, simply close the window and click on **No** when asked if you want to save the changes.

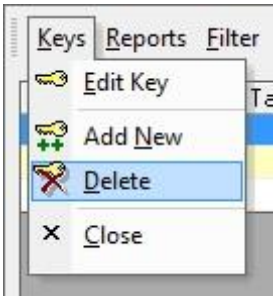


4.7.5 DELETING / REMOVING KEYS

There is a fundamental difference between deleting a key record and removing the key from a system. Traka32 has the ability to store the records of keys even if they are not attached or assigned to an iFob in a Traka system.

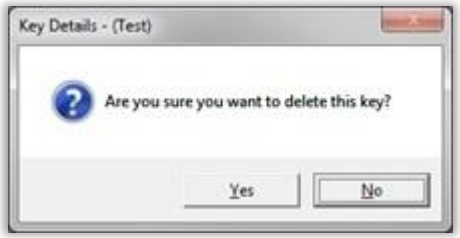
To delete a key...

1. From the main screen click on **Key List** and a list of the current keys will be shown.
2. From the key list simply click on the key record you wish to delete, click on the **Keys** menu followed by **Delete**.



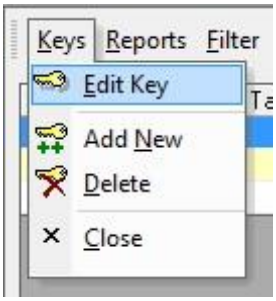
If you already have a key record open you can delete the record simply by clicking on the  button.

3. To delete the key simply click on **Yes**.



To remove a key from an iFob...

1. From the main screen click on **Key List** and a list of the current keys will be shown.
2. From the key list simply **double click** on the key record you wish to edit or click on the **Keys** menu followed by **Edit Key**.

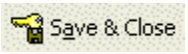


You can also edit key details from the **System Viewer**, simply right click over the position that the keys are associated with and click on **Edit Key Details**.

3. The selected key record will open.

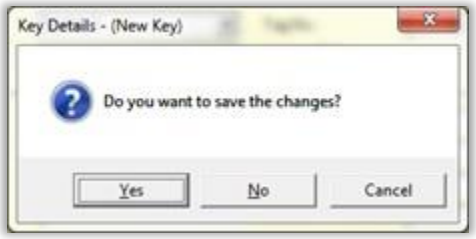
4. To remove a key from an iFob simply click on the 

button.

5. To **Save** your changes, simply click on  or 

.

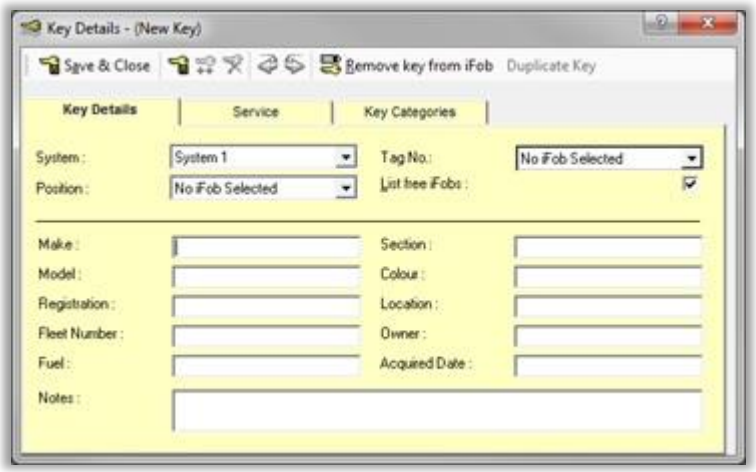
6. To **Cancel** your changes, simply close the window and click **No** when asked if you want to save the changes.



4.7.6 KEY DETAILS

The Key Details window allows you to add and edit the key details.

- You may input all the key details without allocating them to any system or position. This could be completed at a later date.
- You may also use the system as an inventory of your keys, even keys that are not monitored by the Traka system.
- Traka allows unlimited numbers of key records to be created. Keys may be allocated to iFobs as required and then de-allocated if they are no longer to be monitored. However the history is maintained and extended every time the key is re-allocated to an iFob even if it is to a different iFob.



System and Position

Select the system and iFob position to which you wish to attach the key.

List Free iFob

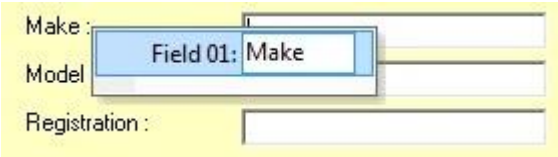
- Check this box if you wish to list only the iFobs in the **Position** drop down list that currently do not have any keys attached to them.
- Uncheck this box if you wish to list all the iFobs in the **Position** drop down list.

Tag No

This section allows a user to assign specific tag numbers against particular keys in the system, once the iFobs have had tag numbers distributed to them via the iFob list. For example position 1 in the cabinet can have a tag number 10 to reference something specific to the customer if desired.

Key Details

On the Key Details tab there are ten user definable fields and one notes field available to store details about the key. These fields are only used within the Traka32 software for reporting on keys. The heading for the user definable fields can altered from the properties window or by clicking with the right mouse button on the field heading, editing the information and pressing Enter.



Mandatory Key Details

Certain information about keys is critical to any audit trail. If it is a requirement that certain information is filled in about a key then the Key Details window can be configured with mandatory fields which show with a red background.

The mandatory key details can be enabled from the properties window.

When adding or editing a key record and provided one or more mandatory fields have been enabled, if one or more of the mandatory fields have not had any information entered then the following message will appear...

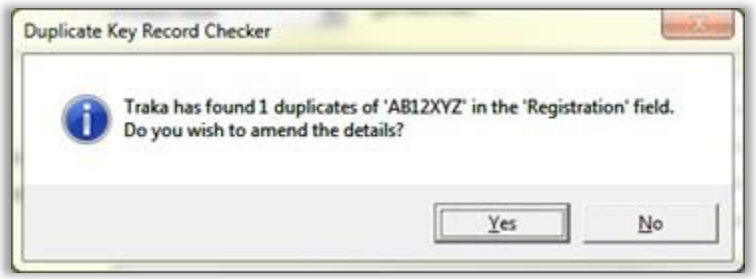
Simply click on OK and complete the required information.

Duplicate Key Record Checker

In applications where there is a large turnover of key records such as the motor trade, it may be important to check if there is already a record for that key. Traka32 can automatically check the individual fields of all the key records against the one you are adding or editing to check for duplications.

The duplication checker can be enabled from the properties window.

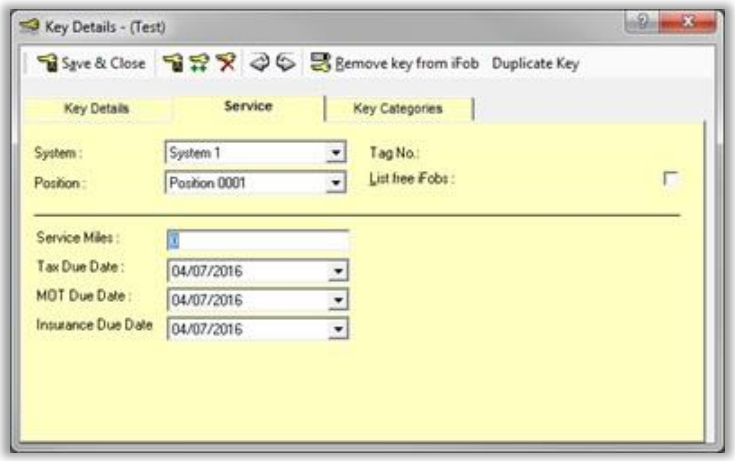
When adding or editing a key record and provided the duplication checker is enabled, if duplication is found the following message will appear...



Simply click on Yes to amend your entry or click on No to ignore the checker and continue.

Service

This tab is called 'Service' by default, however it can be renamed along with the 4 fields to suit customer requirements. To rename this tab and the fields refer to the Service section of the Key Details in the Properties window.



The following fields are defined by default:

Service Miles

This allows a user to enter how many miles the vehicle needs to travel until its next service.

Tax Due Date

Allows the user to select a date for the next time the vehicles Tax is due.

MOT Due Date

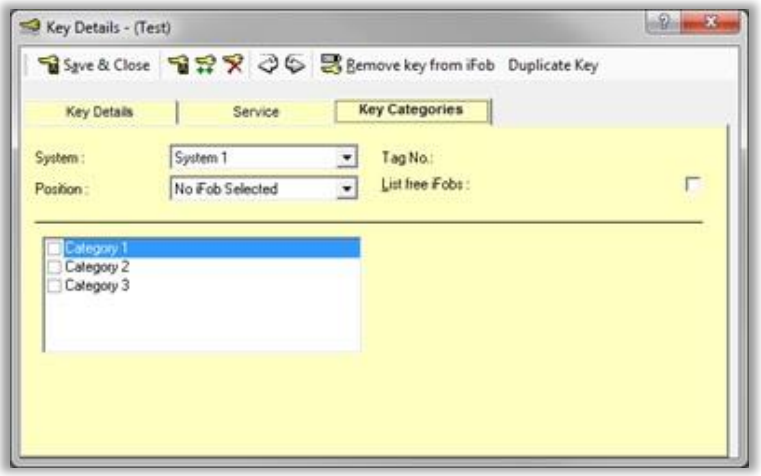
Allows the user to select a date for the next time the vehicle MOT is due.

Insurance Due Date

Allows the user to select a date for the next time the vehicles insurance is due.

Key Categories

The Key Categories tab is for use in conjunction with the option Key Booking Web Portal. Here you can select a category or multiple categories that a key belongs to from a user definable list. This allows multiple keys to be grouped together to narrow down searches. The categories can be defined in **File>Options>Key Categories**.



4.8 USER DETAILS

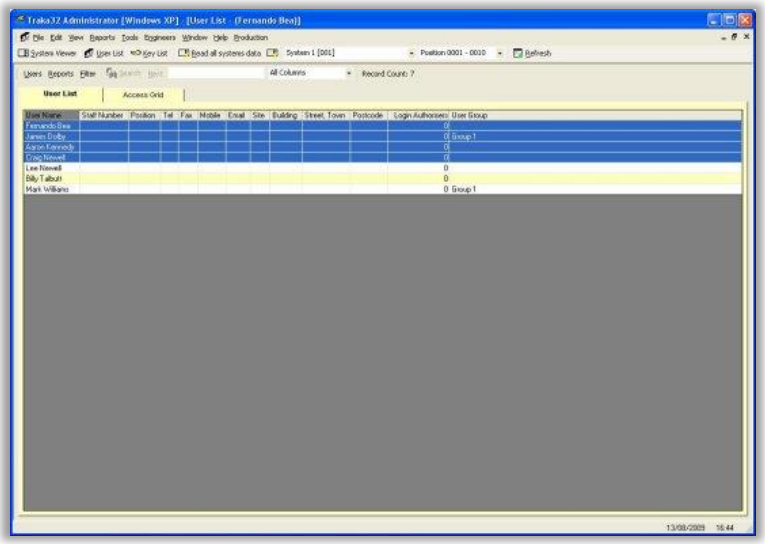
4.8.1 USER LIST

User List

The user list shows a list of all the users in the Traka32 database. By double clicking on a user or right clicking a user you can edit their individual user details.

Additionally you can highlight multiple users and edit them at the same time. To do this simply click on a user and with the left mouse still pressed drag and highlight all the desired users then release the mouse. Alternatively click the individual desired users whilst holding the 'Ctrl' key.

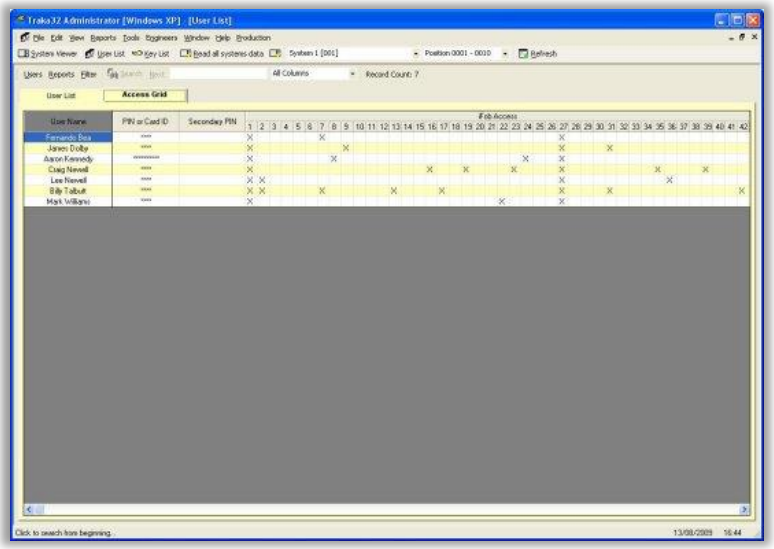
With multiple users selected you can right click and edit options such as Regions, Security Groups and make the user 'Active' or 'Inactive' with the system. You can also set multiple user expiry dates.



User Access Grid

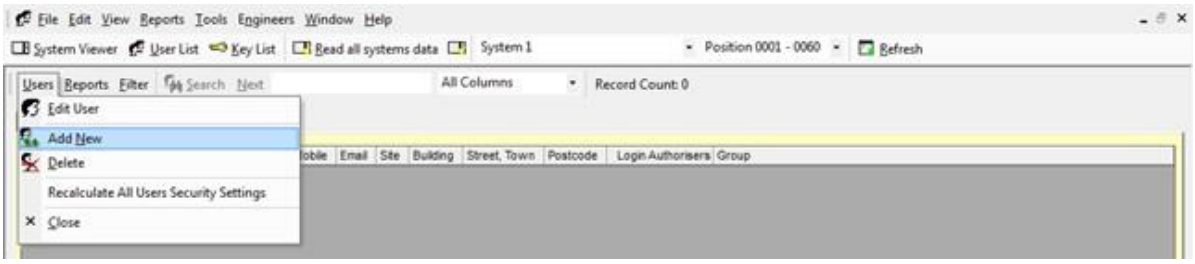
By selecting the Access Grid tab, the user list shows a grid of all the user and access levels and places an X in the grid for every access level assigned. Please refer to the User Access Grid section for more details.

NOTE: The Access Grid can take a while to load if there are a large number of users. User details cannot be edited from the Access Grid.



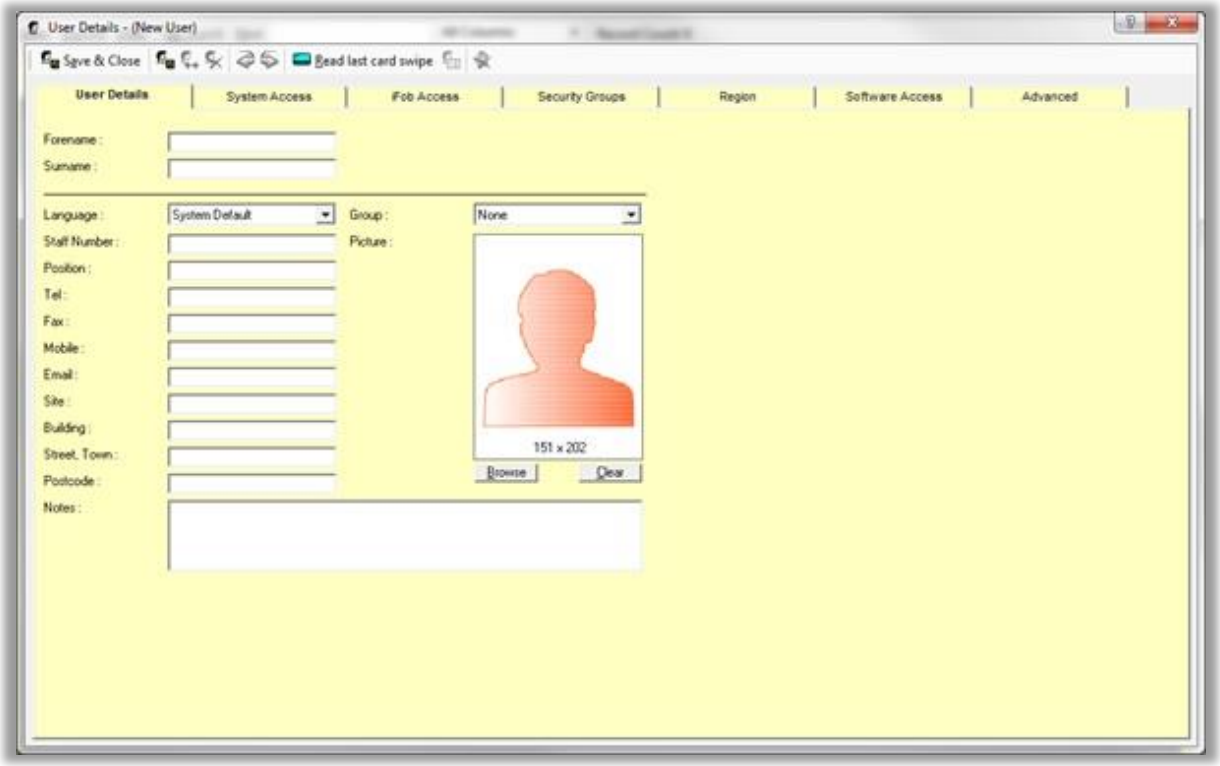
4.8.2 ADDING USERS

1. From the main screen click on **User List** and a list of the current users will be shown.
2. From the user list click on the **Users** menu followed by **Add New**.



NOTE: If you already have a user record open you can create a new record by simply clicking on the button.

3. A new blank user record will be created.



4. Edit the appropriate details, for more details refer to the User Details section.
5. To **Save** your changes, simply click on or Save & Close.
6. To **Cancel** your changes, simply close the window and click **No** when asked if you want to save the changes.
7. If you save your changes, the software will automatically update the Traka System when you save any user details.

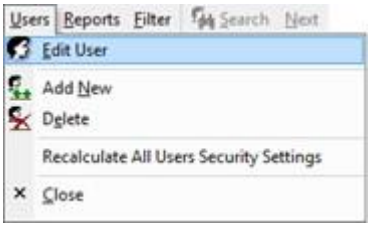
If the software was unable to update one or more of the systems the following message will be shown…

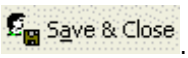
Click on **OK** and the following message will be shown…

Click **OK**.

4.8.3 EDITING USERS

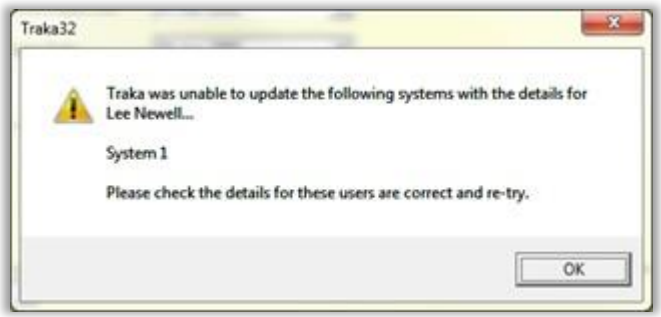
1. From the main screen click on **User List** and a list of the current users will be shown.
2. From the user list simply **double click** on the user record you wish to edit or select the record and click on the **Users** menu followed by **Edit User**.



3. The selected user record will open.
4. Edit the appropriate details, for more details refer to the User Details section.
5. To **Save** your changes, simply click on  or 

.
6. To **Cancel** your changes, simply close the window and click **No** when asked if you want to save the changes.
7. If you save your changes, the software will automatically update the Traka System when you save any user details.

   If the software was unable to update one or more of the systems the following message will be shown…



   Click on **OK** and the following message will be shown…

   Click **OK**.

4.8.4 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:

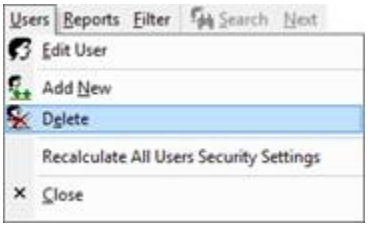
- **Define the user as in-active so that the user cannot use the Traka system(s) any more**
- **Replace the User 'Forename' & 'Surname' with non-specific details such as 'Former employee#1'**

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).

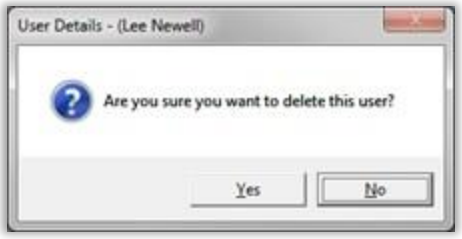
4.8.5 DELETING USERS

1. From the main screen click on **User List** and a list of the current users will be shown.
2. From the user list simply **click** on the user record you wish to delete, click on the **Users** menu followed by **Delete**.



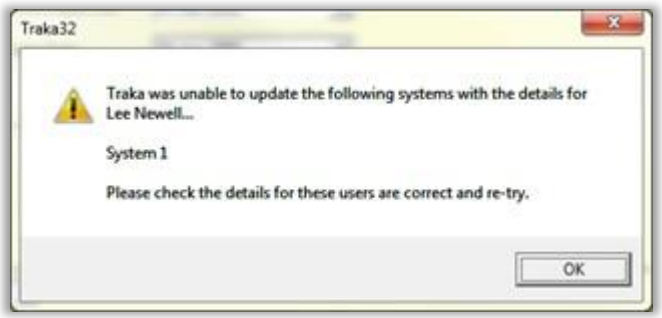
NOTE: If you already have a user record open you can delete the record simply by clicking on the  **button.**

3. To delete the user simply click on **Yes**.

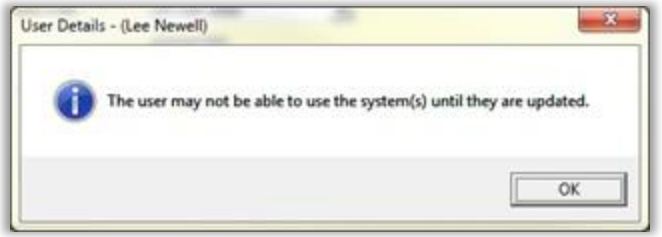


4. If you delete the user, the software will automatically remove the user from Traka System.

   If the software was unable to update one or more of the systems the following message will be shown…



   Click on **OK** and the following message will be shown…



   Click **OK**.

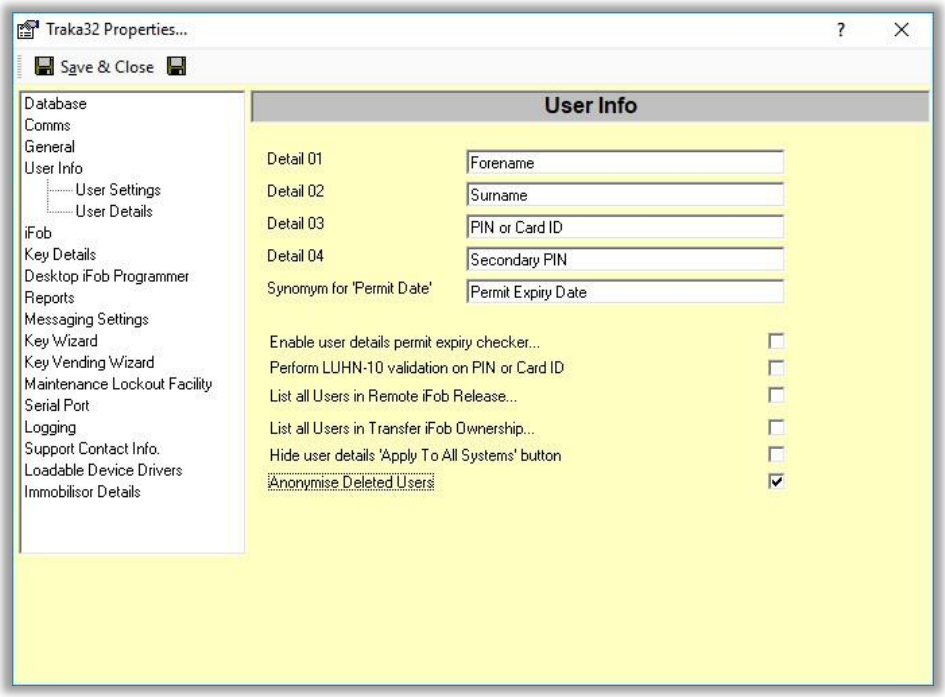
4.8.6 ANONYMISE DELETED USER RECORDS – GDPR

In addition to the GDPR statement regarding Users, this section covers the 'Anonymising' of deleted Users in relation to GDPR compliancy. Within the Traka32 Properties/User Info screen, an additional checkbox can now be located for 'Anonymise Deleted Users'.

1. Within Traka32, click on 'File' and then 'Properties'.

2. Once the 'Properties' window has opened, select 'User Info' from the left side panel.

3. In the 'User Info' section, place a tick in the checkbox next to 'Anonymise Deleted Users' to enable the option as shown below.

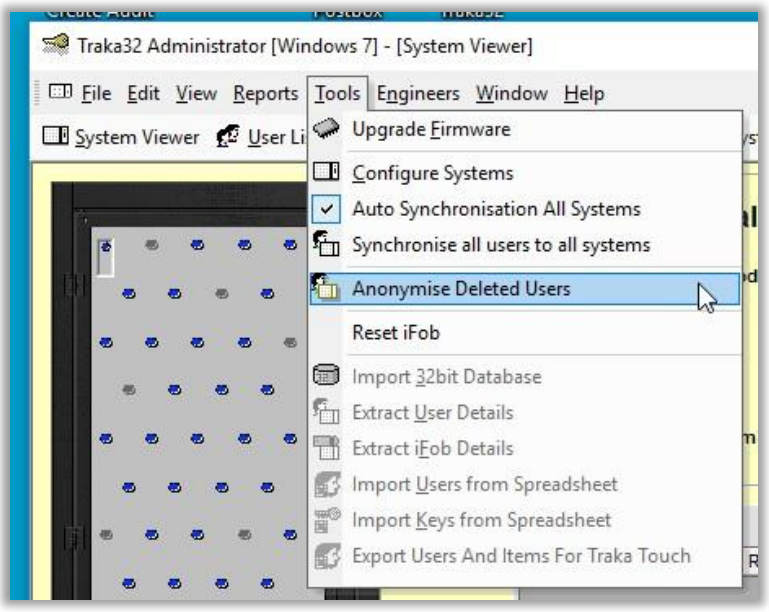


4. Once completed, close the window.

With this option enabled, all future user deletions will have their data anonymised.

From the tools menu, an option is available to anonymise all past deleted users.

5. At the main Traka32 Administration screen, select 'Tools' and then locate 'Anonymise Deleted Users' from the drop-down menu.



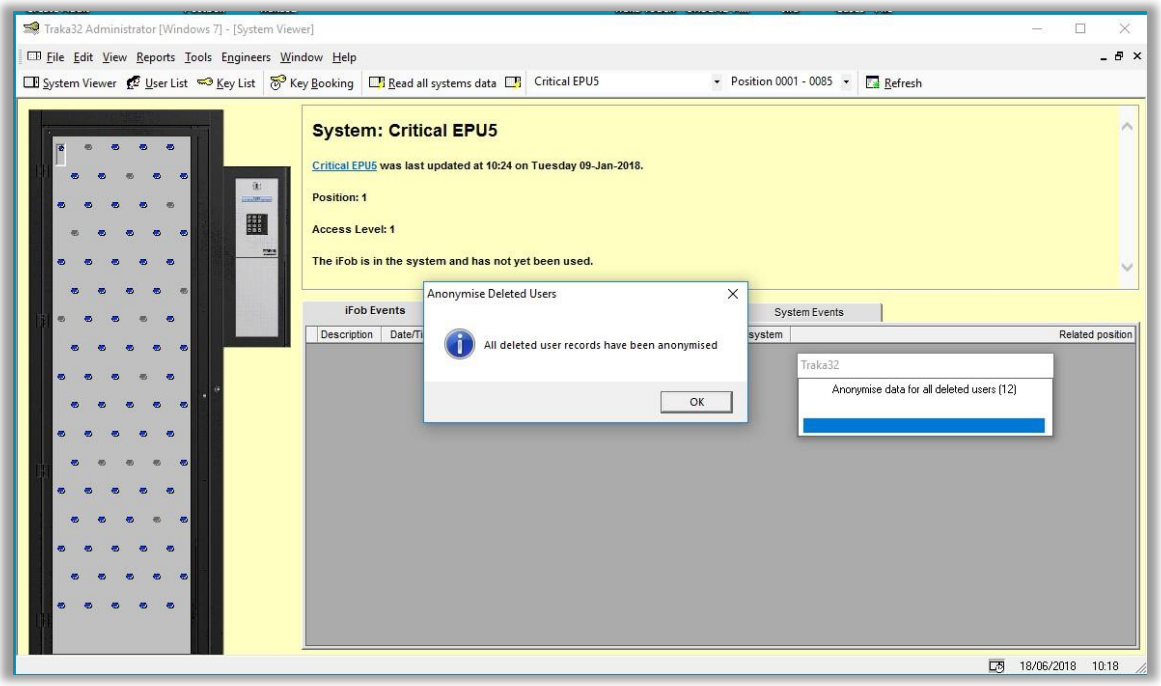
A window will appear asking for confirmation that you wish to Anonymise all deleted User Records.

NOTE: This option can be used independently to having the Anonymising Deleted Users checkbox enabled.

6. Click on the 'Yes' button to proceed.

A progress bar will be displayed during the process. Once completed, a window will appear confirming that all the deleted Users have been Anonymised.

7. Click on the OK button to complete the process.

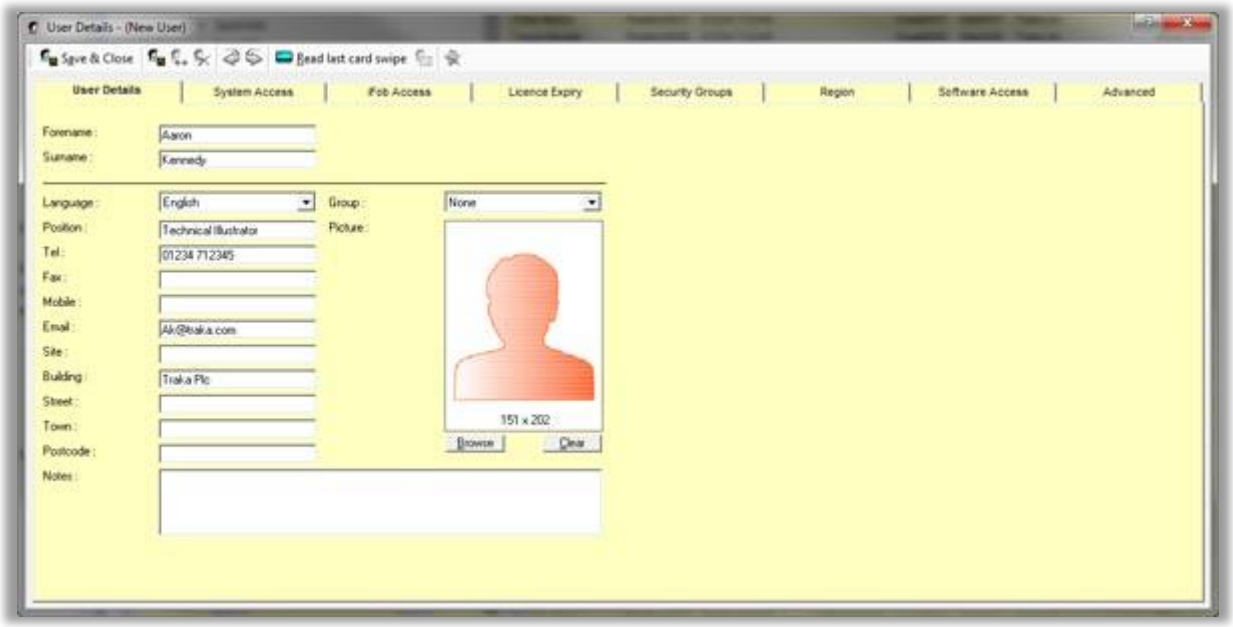


4.8.7 USER DETAILS

The user details window allows you to add and edit user details. The window is re-sizeable allowing it to be dragged to the width and height desired. To do this, hover the mouse cursor over the vertical or horizontal edges until the cursor changes to ⇔ , hold down the left mouse button and drag to the desired size.

User Details

This screen allows you to input details about the users. You must complete the first two fields but the others are optional.



Forename & Surname

Enter the name of the user. It is essential that these fields are completed.

Tip: You may include a telephone extension number or bleeper reference within the Surname field. This will show whenever the user name is presented on the LCD screen.

Language

On 16bit Traka Systems, it is possible to select a language for each individual user. When a user identifies themselves to a Traka System, the instructions on the LCD will show in the selected language. If the default language is selected, then the default language of the Traka System will be displayed. Please refer to the Languages topic for currently supported languages.

User Group

Select a user group that the user belongs to.

User Picture

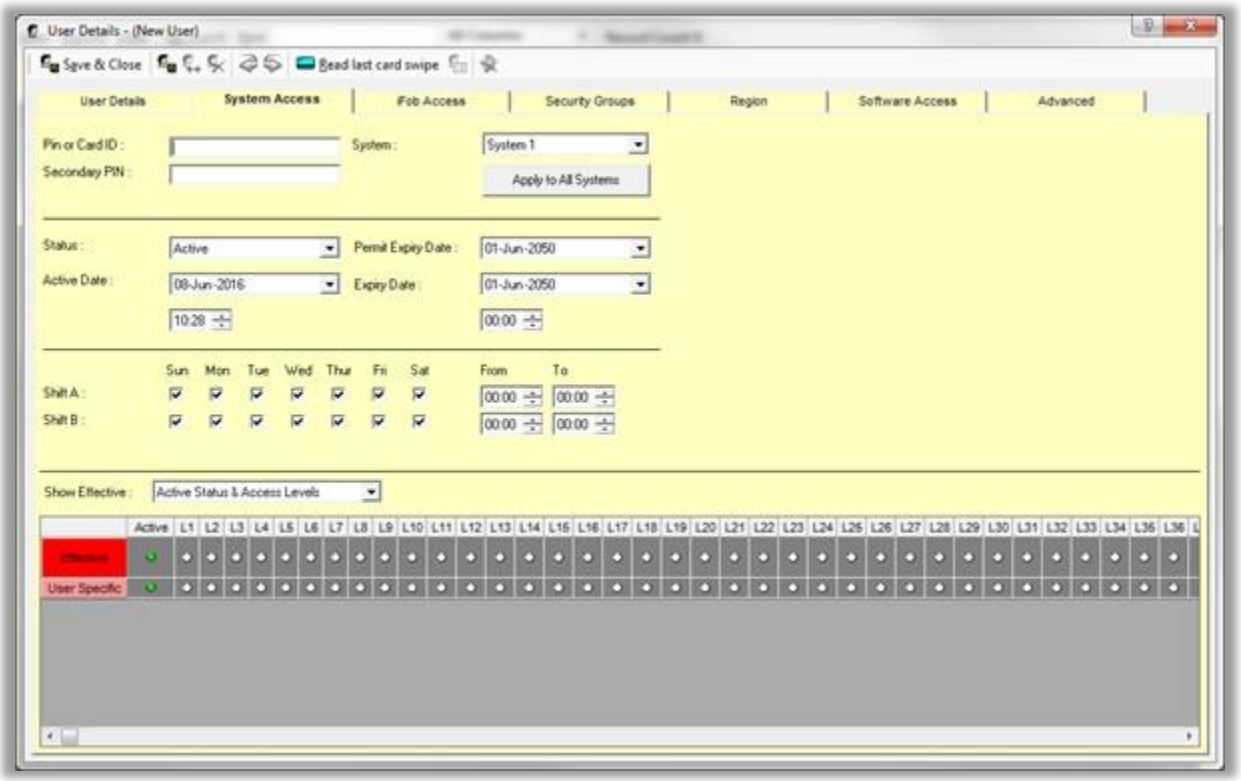
This feature allows you to attach an image of the user..

User Details

There are ten user definable fields and one notes field available to store details about the user. These fields are only used within the Traka32 software for reporting on users. The heading for the user definable fields can be altered from the Properties window or by clicking with the right mouse button on the field heading, editing the information and pressing Enter.

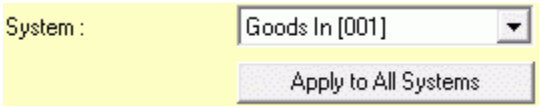
System Access

Here you define the access code the user must use, the period of validity and the times of access.



System / Apply to All Systems

When configuring the **System Access** and **iFob Access**, it is possible to configure the access individually for each Traka System.



If the access settings are the same for each system, then click the **Apply to All Systems** button to copy the access settings for the current system in view to all Traka systems.

If the access settings are different for each Traka System, then do **not** click the **Apply to All Systems** button. Simply select the Traka System from the drop down menu to configure the access settings for that system.

NOTE: The Forename, Surname, PIN or Card ID and Secondary PIN are always applied to all Traka Systems.

PIN or Card ID

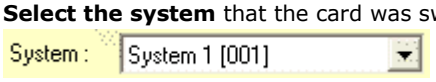
- For a Keypad entry Traka System, enter the primary Personal Identification Number (PIN).

  NOTE: Different Users can have the same PIN (primary and secondary) as long as they are in different regions.

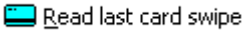
- For a Card Reader entry Traka System, enter the Card ID. If you do not know the Card ID:-

  a. **Swipe the card** through the reader fitted to one of the Traka systems. The Traka system should beep and display **ID Not Recognised** on the LCD.

  NOTE: Make sure no other user swipes their card until you have read the Card ID!

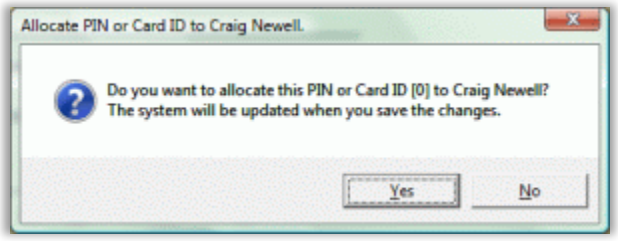
  b. **Select the system** that the card was swiped on from the 

  drop down menu.

  c. **Read the last card swipe** by clicking on the 

  button.

  d. If successful, the Card Number will be displayed…



  e. Click on **Yes** to allocate the Card Number to the user and you will see a series of **** in the PIN or Card ID field.

Secondary PIN

It is also possible to allocate a 4 digit Secondary PIN to a user if required. If a 4-digit Secondary PIN is allocated, after the user has entered their primary PIN or swiped their card, they will be asked to enter their secondary PIN. If no secondary PIN is allocated, the user will not be asked for the secondary PIN.

NOTE: Different Users can have the same PIN (primary and secondary) as long as they are in different regions.

User requires Card and PIN to Access Cabinet

NOTE: This option will only be available if the firmware of the selected system has the Card And/Or PIN option enabled.

If this option is available, there are four different ways a user can access a system depending on how you configure the users:-

Card ID	Secondary Pin	Tick Box	Function
Yes	No	No Tick	The user can only access the system with their Card
No	Yes	No Tick	The user can only access the system with their Secondary PIN
Yes	Yes	No Tick	The user can either access the system with their Card and Secondary PIN **or** just by their Secondary PIN
Yes	Yes	Ticked	The user can only access the system with their Card **and** Secondary PIN

Status

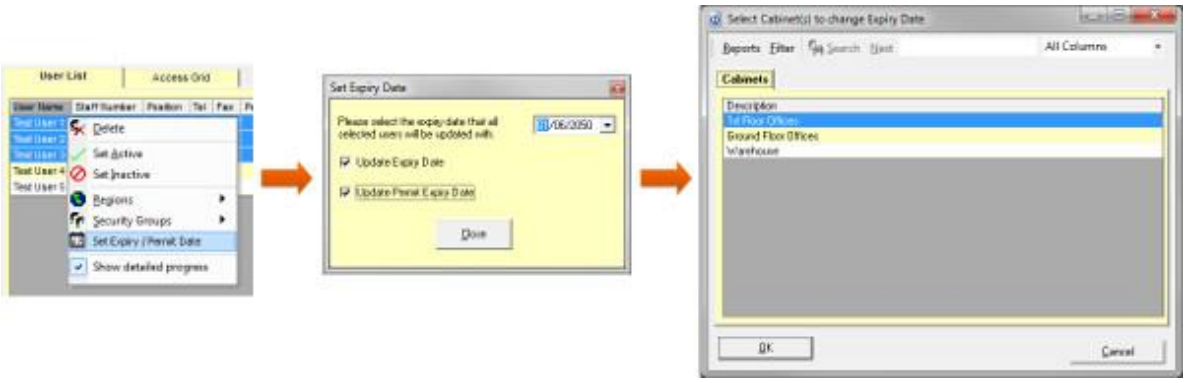
The Active / Inactive Status allows or denies a user access to one or all Traka Systems. Setting the user's status to Active allows access to the relevant Traka System whilst setting to Inactive will deny access.

Active / Expiry Dates

The Active and Expiry Dates allow the user access to one or all Traka Systems between the two dates. Access is denied outside of these dates.

This information is held in the Traka System allowing the creation of a user with a start or joining date and time as well as an expiry date and time. This is especially useful for contract staff.

You can also set expiry dates for multiple users from the User List. Simply highlight all the desired users, right click and select **Set Expiry/Permit Date**. You can then specify a date, whether or not you want to also apply it to Permit Expiry, followed by which system(s) you wish the expiry date to apply to as shown below. Once confirmed a summary of changes will also be displayed.



Permit Expiry Date

Active and Expiry dates may be further enhanced with a permit expiry date. This option allows the definition of a date beyond which the user cannot work until the Permit date is extended.

For example a contract worker may have a work permit or licence that expires on the 22nd August 2002. He is required to carry out contract work on a monthly basis. However, the software will not allow him to work beyond the expiry date of his Permit.

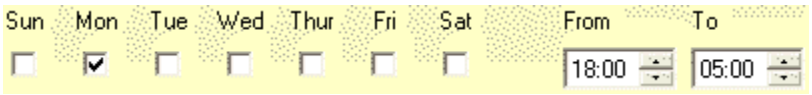
To activate the Permit date, select **File, Properties, General, Enable user details permit expiry checker.**

You can also set Permit Expiry dates for multiple users from the User List. See above in the Active / Expiry Dates section.

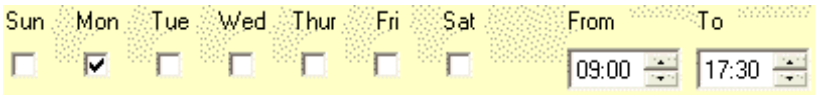
Shift A and B

The System Access Times allow or deny the user access to one or all systems on specific days and between specific times. The system effectively allows two shift patterns giving access at different times on different days of the week.

The '**Days of the Week**' (Sun through Sat) and the '**From**' time together defines the time at which the user will be allowed access. The '**To**' time simply defines when the user will be denied access. Here are some examples:-



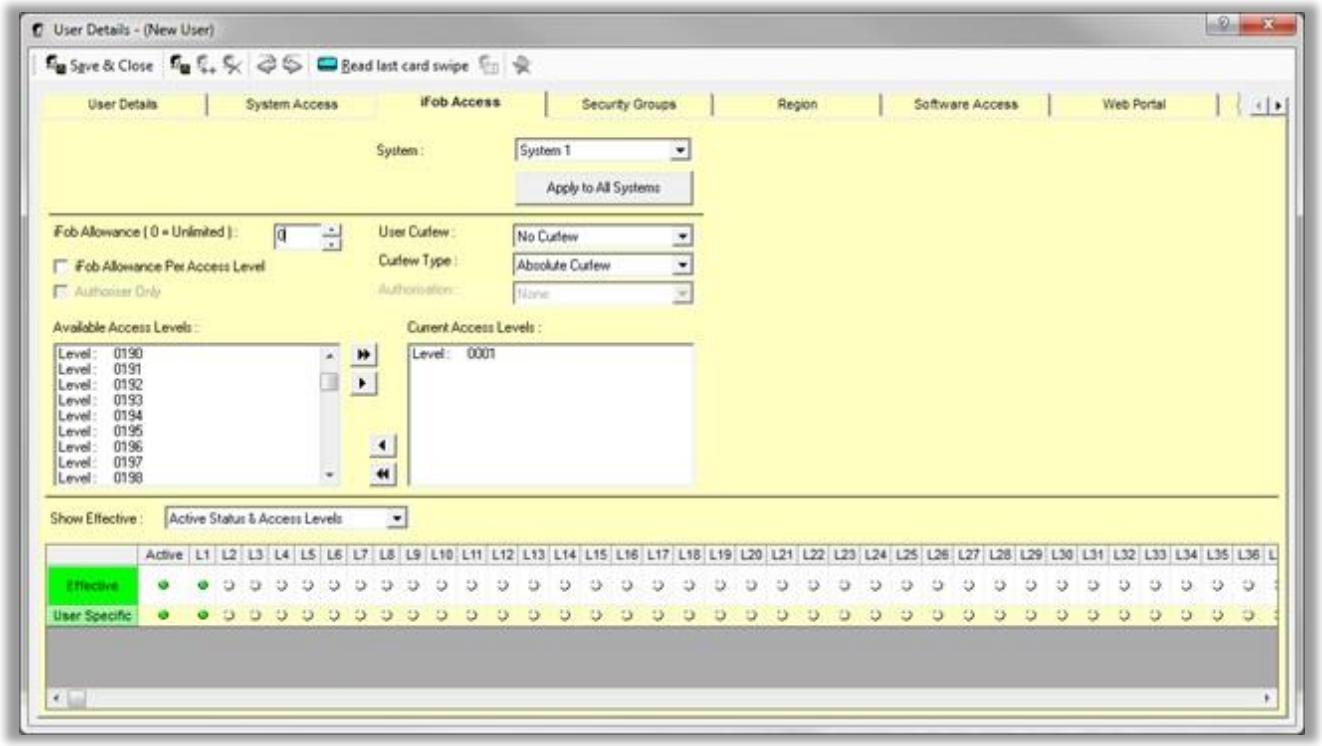
Here the user is allowed access from Monday 18:00 to Tuesday 05:00.



Here the user is allowed access from Monday 09:00 to Monday 17:30.

iFob Access

Here you define the access the user has to the iFobs.



iFob Allowance

The iFob Allowance can restrict how many iFobs a user can take out at any one time. If set to 0 the user can take an unlimited number of iFobs that they have access to.

When checking a user's iFob allowance across multiple systems there are two options to do this:

a. Use hard wired CAN Gateway systems

b. Use the Real Time Update Service (TACLS)

When using CAN Gateway and the communication is down the default behaviour is to not release the iFob. However, when using TACLS and the server is unavailable the default behaviour is to release the iFob. Because the default behaviour between these two systems was different, a tick box has been added into the Product Wizard and Traka32 to set whether the iFob allowance should be ignored if either options didn't reply in time.

This will be set before the system arrives on site but can be altered once the system is installed.

iFob Allowance per Access Level

iFob allowance per access level when enabled, will allow a user to remove a certain amount of iFobs for each access level they have.iFob Allowance per Access Level is only compatible with the 16bit Board, Firmware Version v2.00.20 and Software Version v02.08.0008 and above.

Example:

In the user details window above the iFob allowance per Access Level option is ticked and is set to 2, and the user has access levels 1 & 2, therefore the user can take any two iFobs which have an access of level 1 and any two iFobs that have an access level of 2. The iFob allowance is customisable to whatever number is desired, the maximum allowance is 255 iFobs per access level. If you set the iFob Allowance to 0 then this provides unlimited iFob access.

Authoriser Only

This option will only be enabled if the firmware of the selected system has X System Authorisers enabled. Refer to the X System Authorisers section for more details.

User curfews

When using Curfews there are two different types that can be set depending on your control PCB. User curfews can be used in conjunction with iFob Curfews.

Absolute Curfew

This curfew allows you to set a time for which the all the user's iFobs should be returned to the system. For example, if you set the curfew to 17:30 all iFobs taken before this time will become overdue if not returned. This is a very powerful feature as it will highlight if keys are not returned at the end of a users shift.

Any keys out under curfew or overdue will be shown on the system viewer whenever you click on the  button. You may also see a report on overdue iFobs or overdue keys from the Reports menu.

Relative Curfew

This curfew allows you to set a time limit for which the all the user's keys may be out of the cabinet. This time limit is set in multiples of 15 minutes to a maximum of 24 hours. Thus if you expect the key to be returned within 1 hour you should complete the key curfew accordingly. If the key is not returned within 1 hour, an alarm condition will be activated which will show as an alarm on the alarms report.

Any keys out under curfew or overdue will be shown on the system viewer whenever you click on the  button. You may also see a report on overdue iFobs or overdue keys from the Reports menu.

NOTE: On an 8bit system if you have two curfews set (absolute user curfew and a relative iFob curfew) at the same time the iFob curfew takes priority.

NOTE: On a 16bit system if there is a user and an iFob curfew set, the system works out which one will expire first and uses that as the priority curfew.

Authorisation

This option will only be enabled if the firmware of the selected system has X System Authorisers enabled. Refer to the X System Authorisers section for more details.

Available / Current Access Levels

Each iFob in a system has an Access Level assigned to it. For a user to be able to take an iFob, the user must have that access in their Current Access Levels list. For example, if an iFob has access level 021, and the user needs access to this iFob, they must have access level 021 in their Current Access Level list. If not, the user will not be able to take the iFob.

For more details please refer to the Access Levels section.

To **Add All** access levels to the Current List, click on 

To **Add Selected** access levels, select the appropriate levels from the Available List and click on 

To **Remove Selected** access levels, select the levels from the Current List and click on 

To **Remove All** access levels from the Current List, click on 

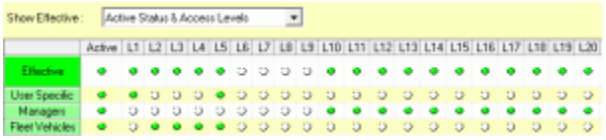
To select a group of access levels, click on the first access level, hold down the **Shift** key and click on the last access level in the group.

To select several individual access levels hold down the **Ctrl** key and click on the access levels in the group.

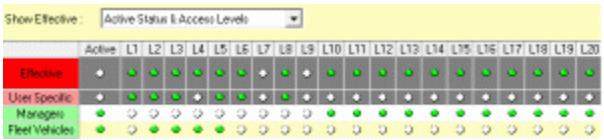
Show Effective Security

This grid provides a graphical representation of the user's effective system and iFob access taking into account their user specific security settings and the security groups to which they belong.

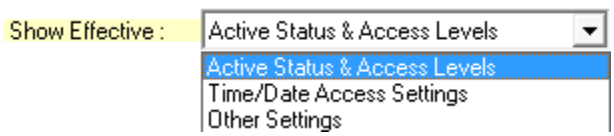
If the effective box is **green**, then the user has access to the currently selected system.



If the effective box is **red**, then the user does not have access to the currently selected system.



It is possible to display the effective security different access credentials. Select from the Show Effective drop down list:-



Active Status and Access Levels

When selected from the drop down list, the access levels that apply to the specific user and the security groups to which a user belongs are displayed.

Time / Date Access Settings

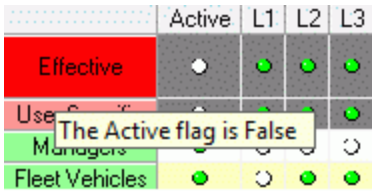
When selected from the drop down list, the time/date access settings for the user and the security groups to which a user belongs are displayed.

Other Settings

When selected from the drop down list, the curfew and authorisation settings that apply to the specific user and the security groups to which they belong are displayed.

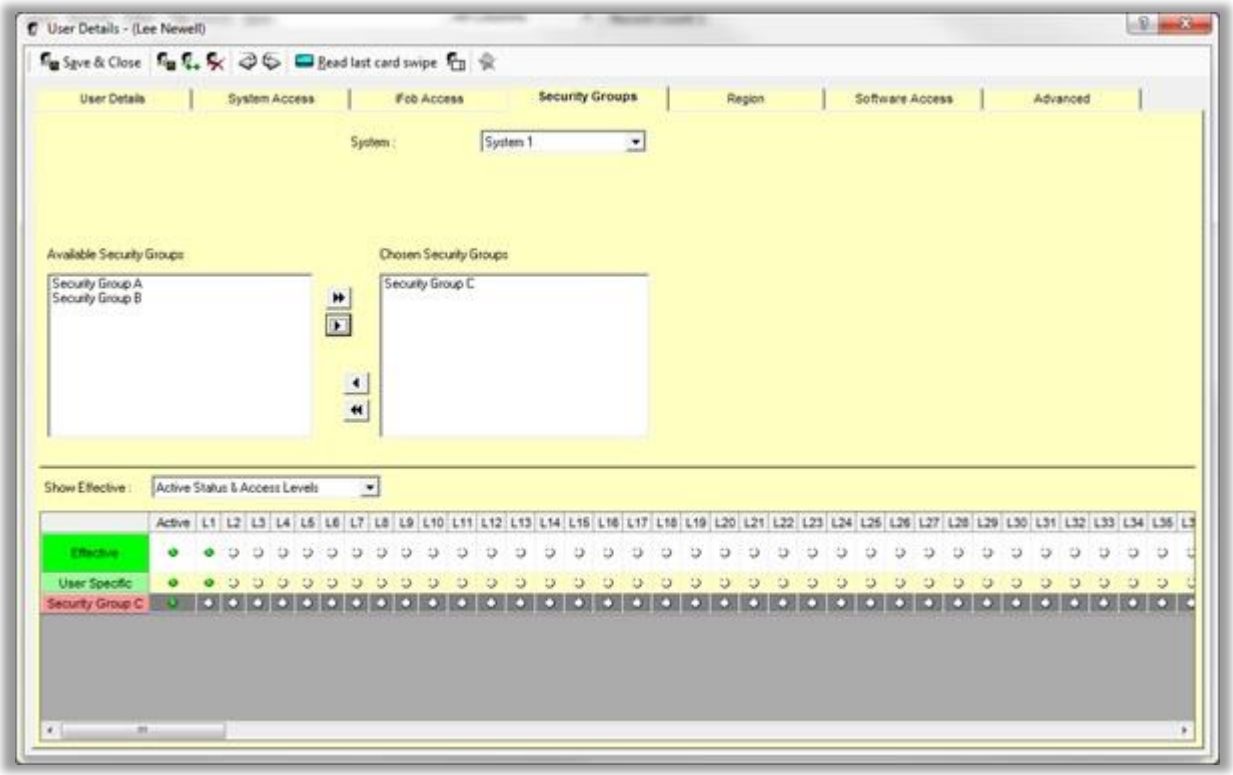
Tip: The show effective graphic provides an easy way to see how a users security settings are made up from their user specific security settings and the security groups to which they belong. However if the effective security box is red (meaning the user does not have access to the selected system), then hover the mouse over the box to display a reason as to why the user does not have access. Also the user specific box or security group denying the user access will also be displayed in red.

Below is an example of where the user does not have access to the system because the Active Flag is false for their user specific security settings.



Security Groups

Here you can define which Security Groups the user belongs to. Click here to read an overview of Security Groups.



Available / Chosen Security Groups

To **Add All** available Security Groups to the Current List, click on 

To **Add Selected** Security Groups, select the appropriate levels from the Available List and click on 

To **Remove Selected** Security Groups, select the security groups from the Current List and click on 

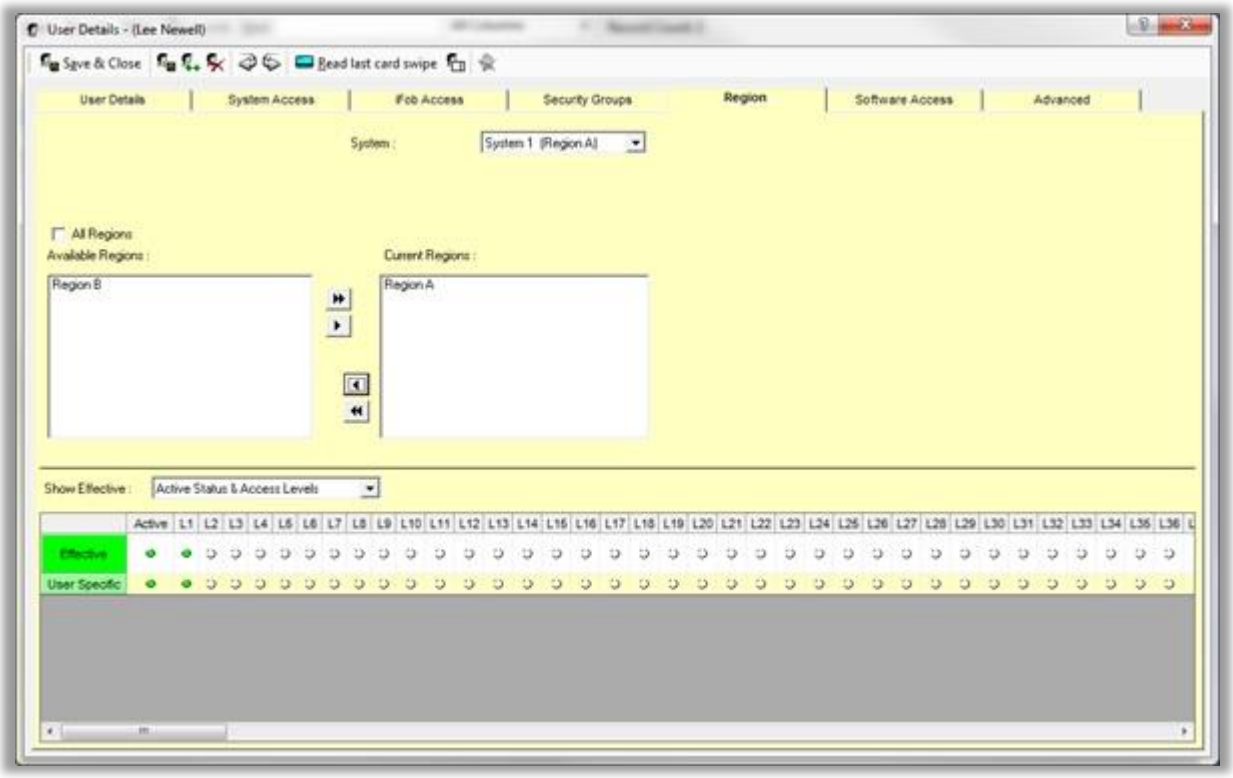
To **Remove All** security groups from the Current List, click on 

Tips:

- To select a group of security groups, click on the first security group, hold down the **Shift** key and click on the last access level in the group.
- To select several individual regions hold down the **Ctrl** key and click on the access levels in the group.
- To select a group of security groups, click on the first security group, hold down the **Shift** key and click on the last access level in the group.

Region

Here you define which Region(s) the user belongs to.



All Regions

Select if the User is to have access to All Regions. Note this tick box is only available to edit if the logged in User is an All Regions Administrator.

Available / Current Regions

Each User can belong to one or more Regions or No Regions. Note that only the Regions matching that of the logged in Traka32 Administrator will be displayed.

To **Add All** available regions to the Current List, click on 

To **Add Selected** regions, select the appropriate levels from the Available List and click on 

To **Remove Selected** regions, select the regions from the Current List and click on 

To **Remove All** regions from the Current List, click on 

Tips:

- To select a group of regions, click on the first region, hold down the **Shift** key and click on the last region in the list.
- To select several individual regions hold down the **Ctrl** key and click on the regions in the list.

Software Access

Here you define the access the user has to the Traka32 software. The software access tab will alter depending upon which database type you are using.

Allow Software Access

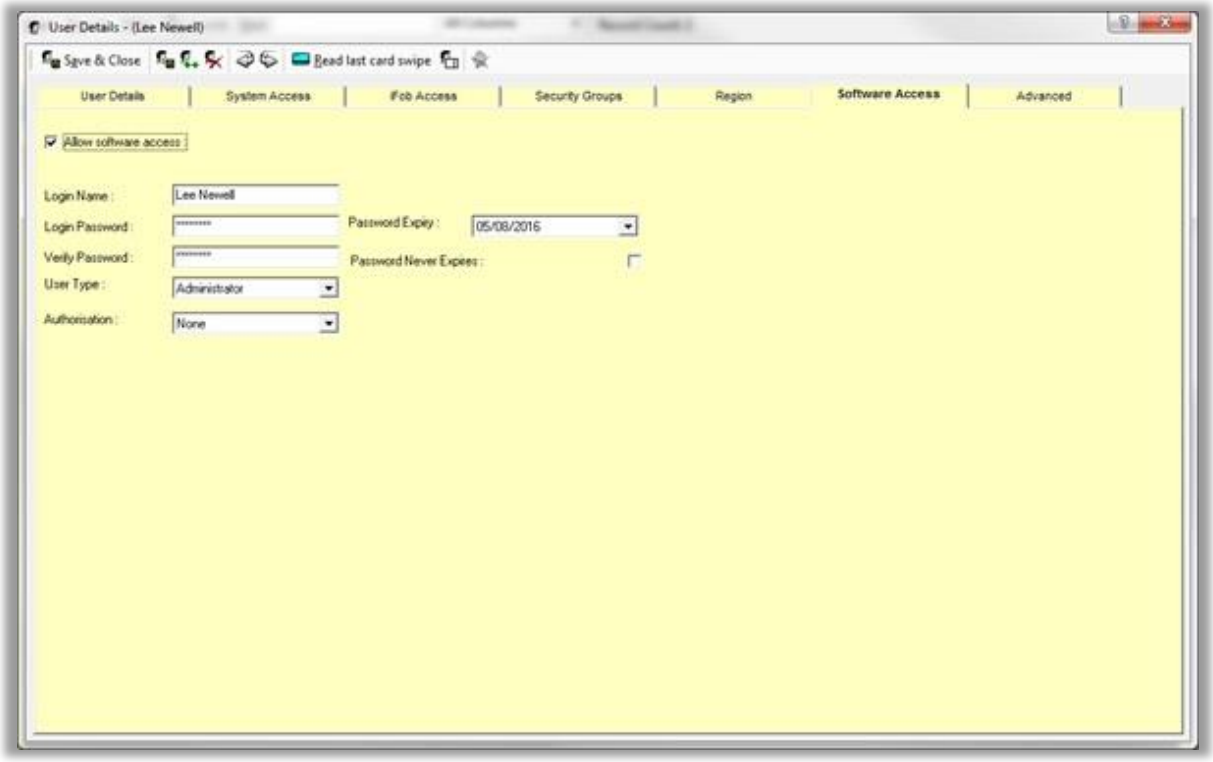
If the user needs access to the Traka32 Software, click on the Allow Software Access check box. If the box is un-checked, the user will not be able to access the software.

NOTE: If no users are given software access, the software will not request a login and allow entry for any use.

User Type

The User Type can restrict the user access in the Traka32 Software. The user types can be customised as required. To customise the user types, please refer to the **File, Options, Software Access** section.

Microsoft Access Database



Login Name

The Login Name uniquely identifies the user so when the Traka32 Software is loaded, the user will be asked for their login name and password.

Login / Verify Password

The Login Password is required in order for the user to log into the Traka32 Software. If the Login Password is hidden by ***** then the password will have to be re-typed into the Verify Password field.

Password Expiry

Enter a date for when the Login Password will expire. Once expired Traka32 will prompt the user for a new password when they next login to Traka32.

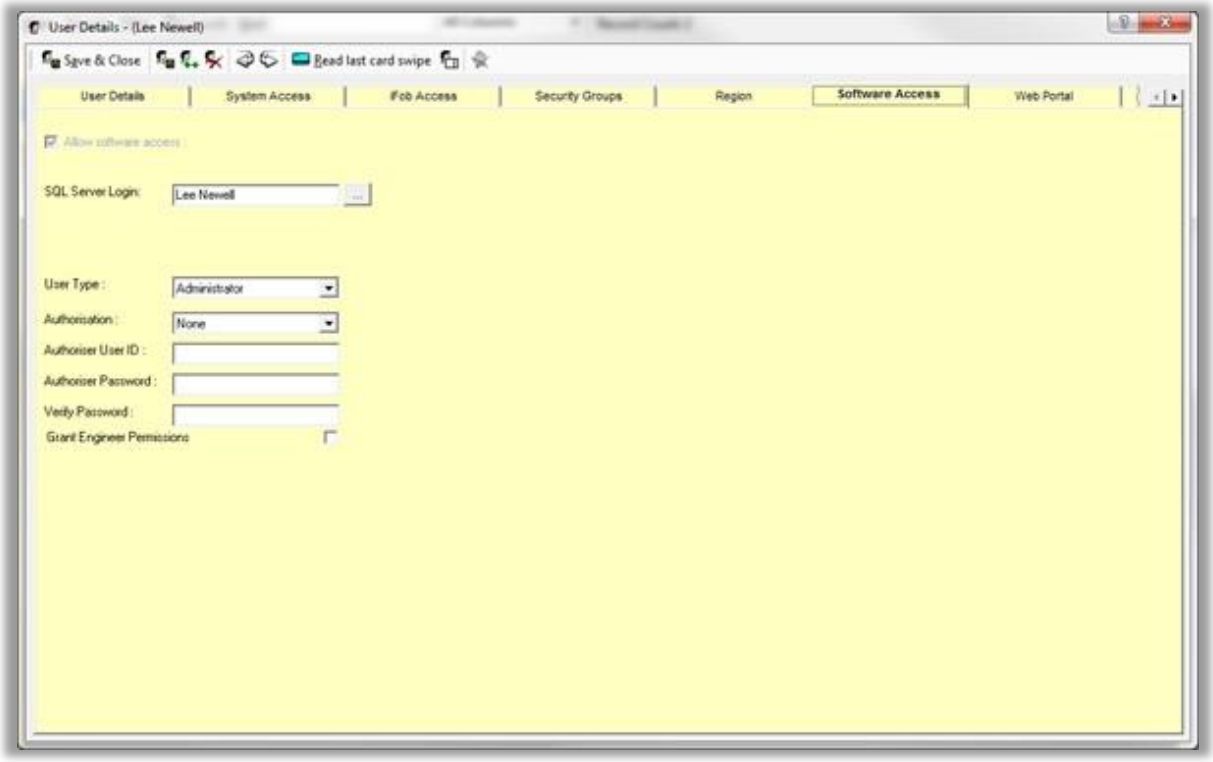
Password Never Expires

Optionally select this option so that the Login Password never expires.

Authorisation

If the User has been allowed software access, they can be configured to require authorisation from none, 1 or 2 Authorisers before they are granted access to Traka 32. Select none, 1 or 2 from the Authorisation drop down box. For an Access database, the Authoriser uses their normal Traka 32 login details to authorise the login.

Microsoft SQL Database



To grant user's access to Traka, you must first create a user record in the Traka database and then associate a SQL Login to that user.

NOTE: The user in Traka does not need to be granted access to any cabinets.

SQL Server Login

Enter the appropriate SQL Login used to access the database.

Click on the ... button to search for the users. The list that appears will depend on whether Integrated Security has been enabled from the Properties window.

- If integrated security has been enabled then a list of Domain Users will appear.
- If integrated security has not been enabled, then a list of SQL Server Users will appear.

Authorisation

If the User has been allowed software access, they can be configured to require authorisation from none, 1 or 2 Authorisers before they are granted access to Traka 32. Select none, 1 or 2 from the Authorisation drop down box.

Authoriser User ID

When configuring the User as an Authoriser, this field must be completed with a User ID. The Authoriser User ID can be the same or different to the Users normal login ID.

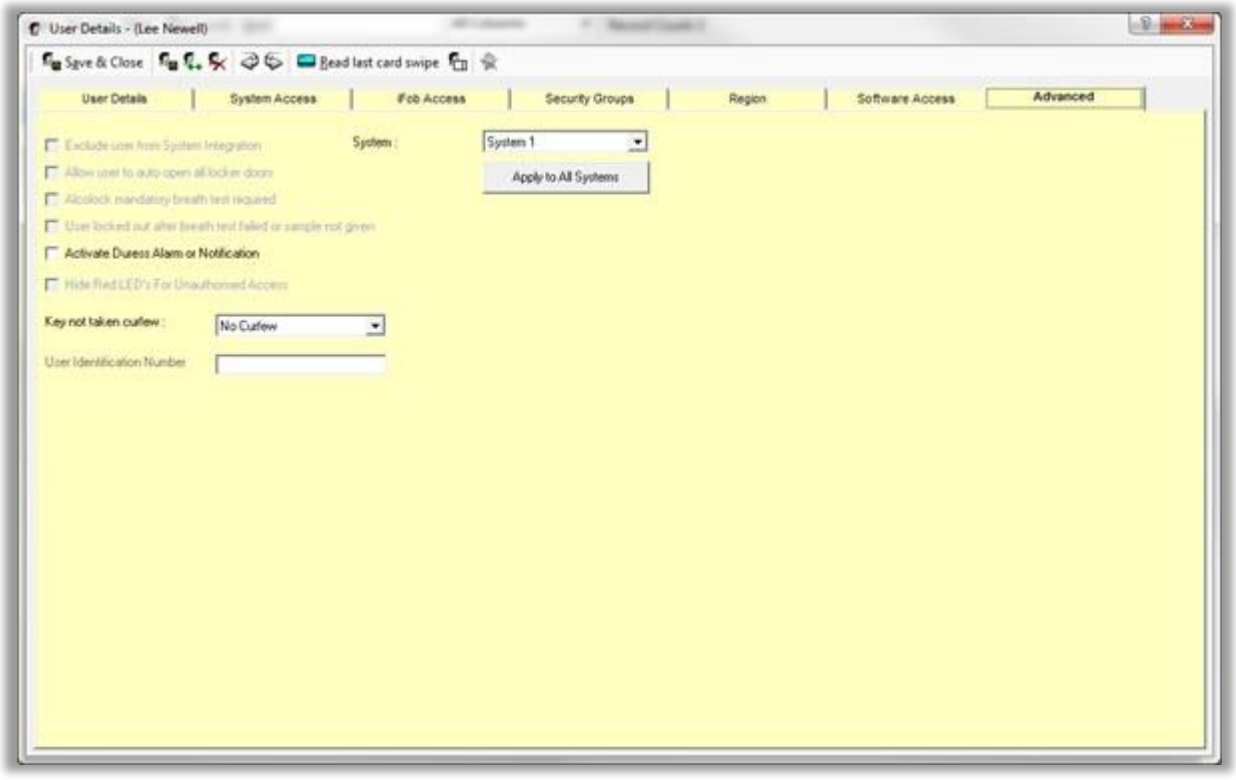
Authoriser Password

When configuring the User as an Authoriser, this field must be completed with an Authoriser Password. The Authoriser Password can be the same or different to the User's normal login Password.

Grant Engineering Permissions

Check this option to grant engineering capabilities which will allow the user access to the Engineers menus.

Advanced



Exclude user from System Integration

Select this option to exclude a user from the System Integration utility. This is useful if you want to exclude users from access control rules such as preventing users from leaving a site with keys in their possession.

Allow user to auto open all locker doors

Select this option to open all locker doors the User has access to. For example if a user has access to lockers 1-10 only, upon authorising themselves to the system (e.g swiping their ID card) lockers 1-10 will all open in turn.

Alcolock mandatory breath test required

Select this option to force the user to take a mandatory breath test when selecting an iFob with Prompt for Breath Test enabled. This is applicable to Traka systems with Alcolock Integration.

User locked out after breath test failed or sample not given

Select this option to automatically lock-out a user from the system(s). This will prevent the user from being able to remove any iFob with Prompt for Breath Test enabled. This is applicable to systems with Alcolock integration. This tickbox will also be checked when a User has failed the breath test or failed to supply a sample. To unlock the User the tick box is simply unchecked.

Activate Duress Alarm or Notification

Select this option to activate a Duress alarm whenever a specific user accesses the system, or alternatively you can set this option within the iFob details.

Hide Red LED's For Unauthorised Access

With this box ticked, Red LED's will not be displayed against unauthorised iFobs for this specific user. This feature is only available when using the firmware option Hide Red LED's for Unauthorised Access.

Key not taken curfew

Select a curfew time from the drop down box by which a key should have been taken by the User. If a key has not been taken by this time, then a 'key not taken' event is recorded against the user.

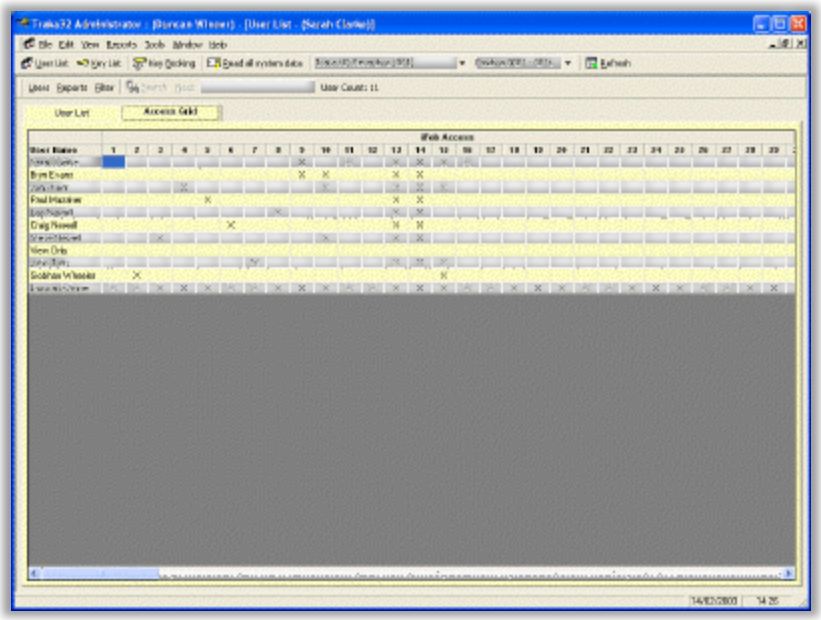
User Identification Number

The User Identification Number was developed to allow a user to securely assign themselves a PIN at the system. For more details on how to set his up and how it works please refer to the User Identification Number Section.

4.8.8 USER ACCESS GRID

4.8.8.1 USER ACCESS GRID OVERVIEW

The user access grid can be used to edit a user's access levels. By selecting the **Access Grid** tab, the user list shows a grid of all the user and access levels and places an X in the grid for every access level assigned.



To view the User Access Grid, click **View**, **User List** which will open the User List. Then click on the **Access Grid** tab to view the Access Grid.

NOTE: The Access Grid can take a while to load if there are a large number of users. User details cannot be edited from the Access Grid.

4.8.8.2 USER ACCESS GRID FILTERING

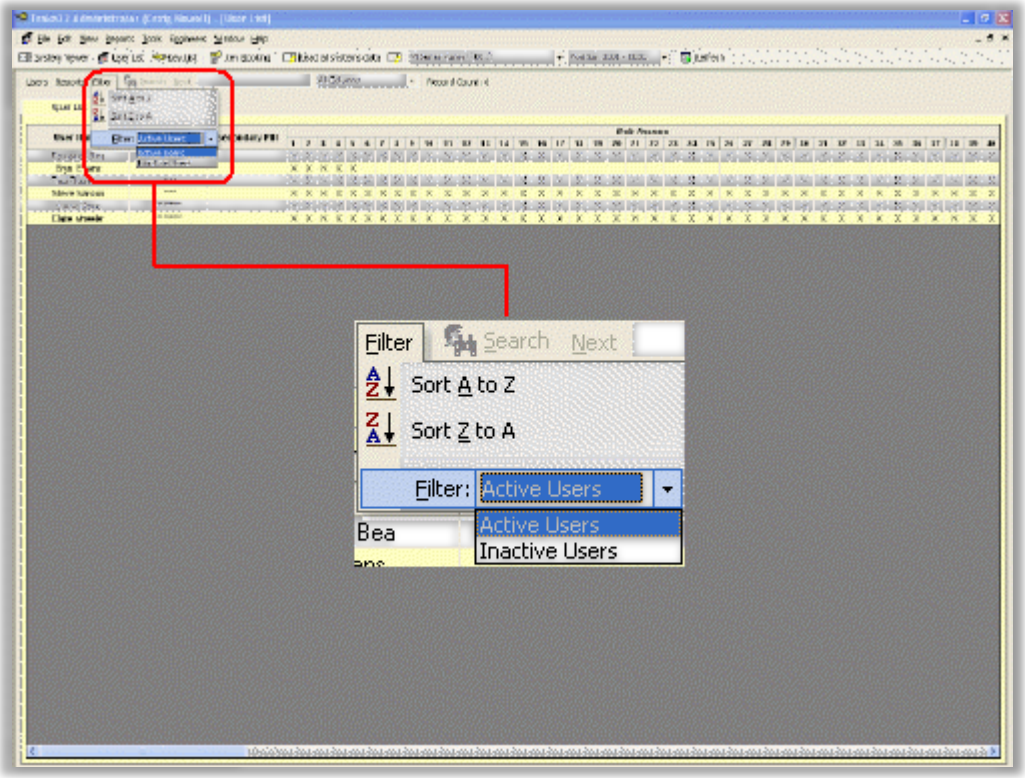
Prior to v02.006.002 the User Access Grid lists only the users who have access to the system currently selected from the system selection drop down menu in the main toolbar.

From v02.006.002 the Users can be filtered to show who is **Active** and who is **Inactive** on the currently selected system:

1. Click on **Filter** and select either:

    a. **Active Users** to display all Users who have access to the selected system.

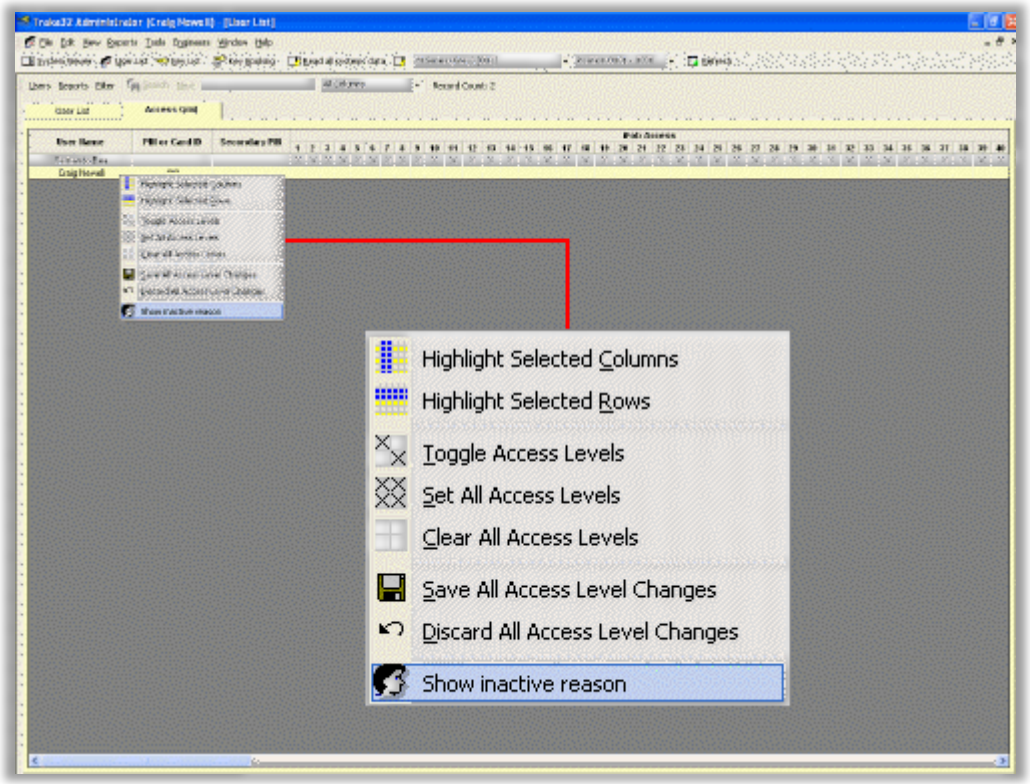
    b. **InactiveUsers**to display all Users who do NOT have access to the selected system.



2. It is possible to query why a User does not have access to the selected system:

   a. Filter the list for **Inactive** Users.

   b. Right click over a User and click on **Show Inactive Reason.**



3. The Inactive Reason(s) are displayed.

For a user to have access to a cabinet they must have the following...

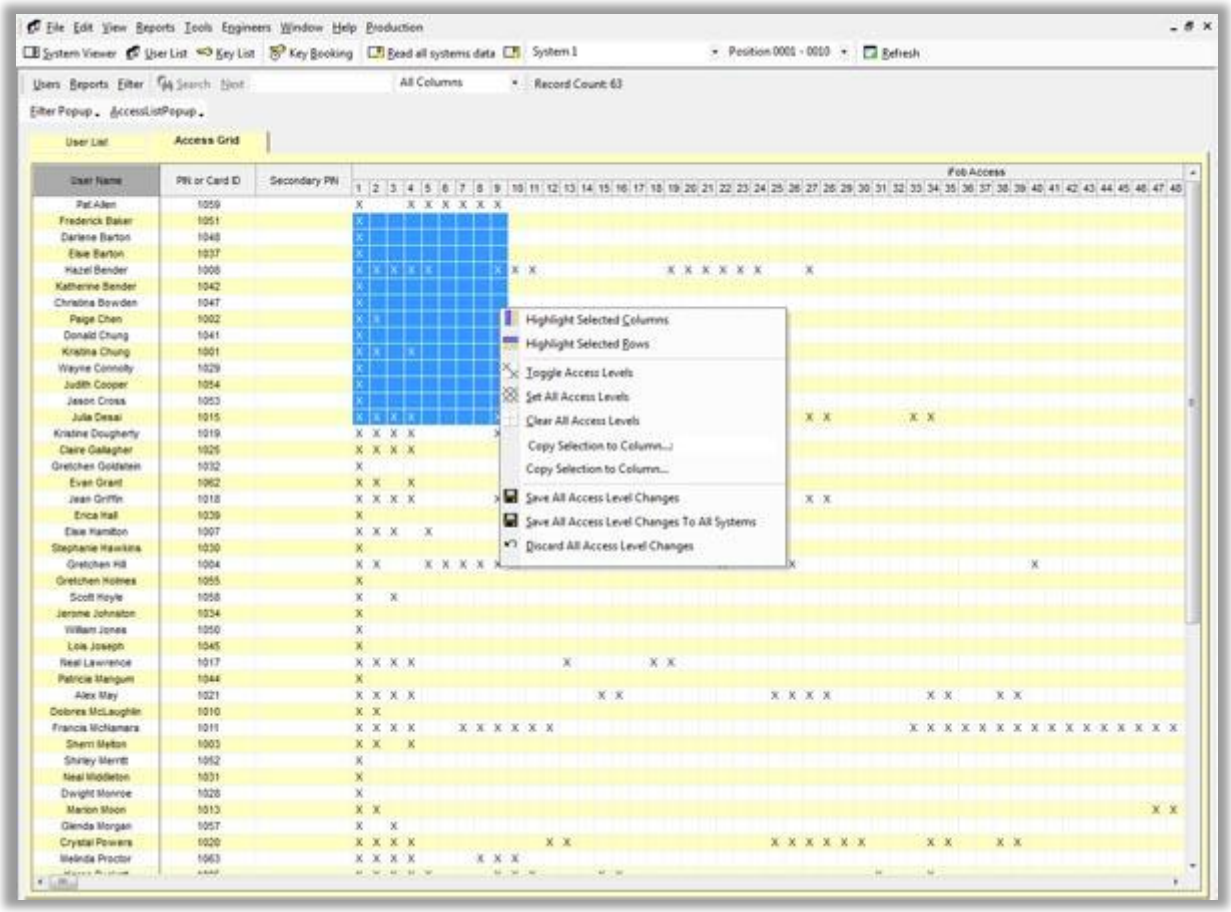
- At least 1 access level (from 1 - 200 for 8bit systems, 1-2560 for 16bit systems)
- Access to the cabinet at least 1 day a week (shift A or shift B)
- Have their active status set to active
- Have a valid primary ID (card and/or PIN)
- The user must not have expired
- Be in the same region of the cabinet

If the user does not meet all of these requirements they will not have access to the selected system and will not appear in the Access grid when filtered for Active Users.

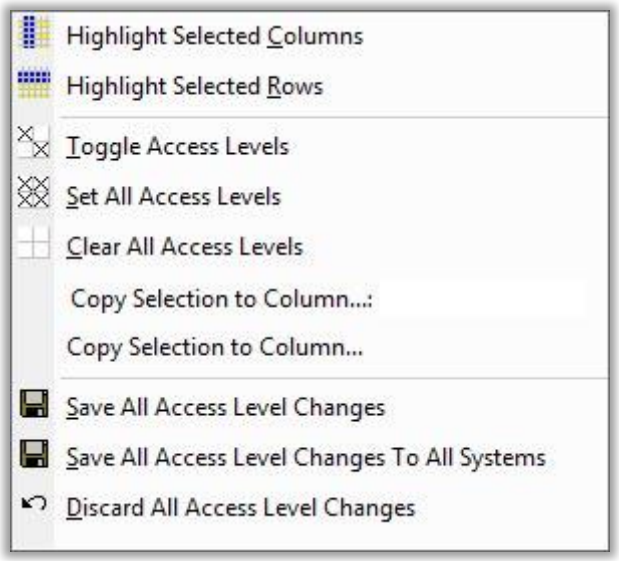
To make a user Active on the selected system, go back to the User List, search for the user and edit their record ensuring they meet all of the criteria listed above.

4.8.8.3 EDITING ACCESS LEVELS FROM THE ACCESS GRID

It is possible to edit a user's access levels from the grid.



A pop-up menu is available on the Access Grid by right clicking over the grid.



The pop-up menu can be used to highlight rows and columns on the grid, toggle access level statuses for the highlighted rows and columns and also save and discard any changes.

Edit an Individual Access Level

The simplest way to edit a single access level is to double click on the relevant box. This will toggle the status of the access level. Then simply save the changes.

Add / Remove an Access Level to / from Every User

This simplest way to add / remove an access level to / from every user, is to

1. Highlight any cell under the relevant access level
2. Right click and click on **Highlight Selected Column**. This will highlight all the cells for the selected column.
3. Right click again and click on either:
    a. **Set All Access Levels** to add an access level to every user or
    b. **Clear All Access Levels** to remove an access level from every user
4. Right click again and click on **Save All Access Level Changes**.

Add / Remove an All Access Levels to / from a Single User

This simplest way to add / remove all access levels to / from a single user, is to

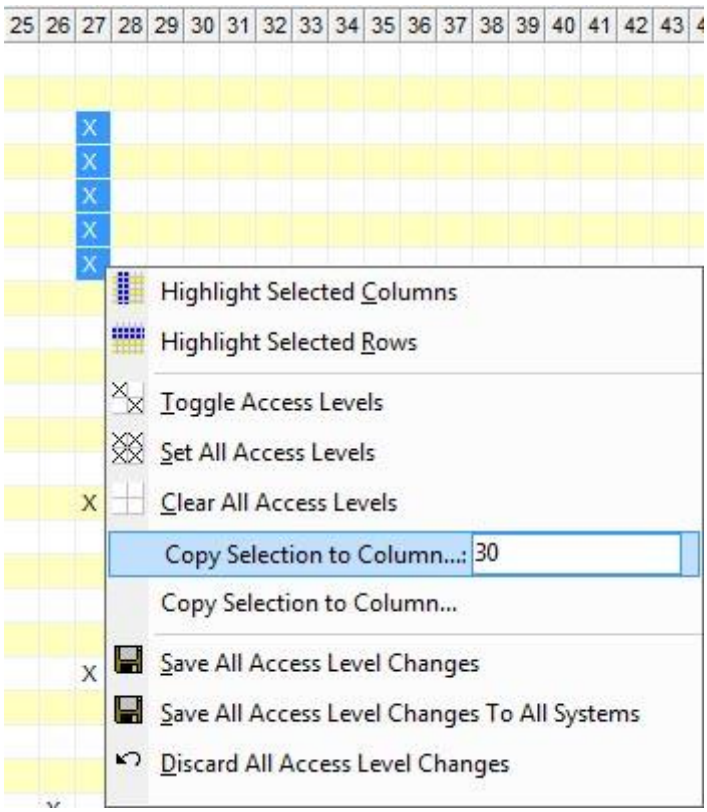
1. Highlight any cell along side the relevant user
2. Right click and click on **Highlight Selected Row**. This will highlight all the cells for the selected row.
3. Right click again and click on either:
    a. **Set All Access Levels** to add all access levels to the user or
    b. **Clear All Access Levels** to remove all access level from the user
4. Right click again and click on **Save All Access Level Changes**.

Copy Selection to Column

In Traka32 version 02.10.0013 and above, it is possible to copy a selection of access levels from one column and/or row to another. This works across multiple users and is a very efficient way of assigning access levels.

Example:-

1. Highlight all the desired access levels, whether its a row, column or both.
2. Right click the highlighted access levels and enter the column number you wish to copy the access levels to into the 'Copy Selection to Columns' field.



3. Select the 'Copy Selection to Columns' button underneath the Copy Selection field to apply the changes.
4. You will now see that the access levels have 'mirrored' into the selected column.

Multiple Changes

It is possible to make multiple changes to the Access grid before saving. Every user record that has been edited will be highlighted in **Green**.

Users Security Groups

It is NOT possible to edit access levels for users that are allocated to user security groups. If an attempt is made to edit a use record that is allocated to a user security group, the user record will be highlighted in **Red**, a message box will show and no changes will be made to that user record.

Saving Changes

When changes are saved to the database, Traka32 will automatically communicate the changes to the Traka System.

Discard All Access Level Changes

At any point it is possible to undo any unsaved changes made to the grid. Simply right click and click on **Discard All Access Level Changes**, and click on **Yes** when prompted.

4.9 FILE

4.9.1 PROPERTIES

The properties window allows you to configure various settings within the software.

Notes:

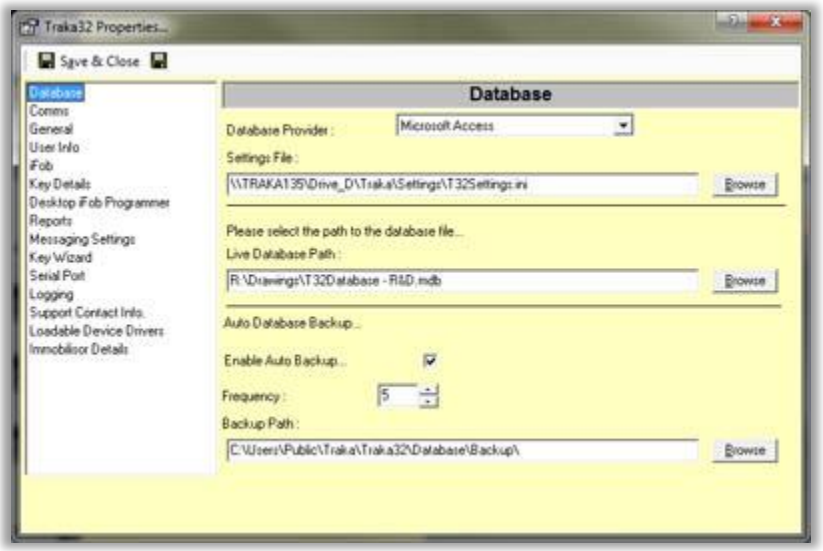
- Workstation specific settings are stored in the T32Settings.ini file, which is saved during installation on the local workstation. The default location for this file is C:\Users\Public\Traka\Traka32\Settings.
- User specific settings are stored in the registry at HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Traka32. If a setting does not exist in the registry it will be extracted from the T32Settings.ini file and if there is no entry in the T32Settings.ini file a default entry is selected.
- Centralised settings such as field headings are stored within the database and will affect all users of Traka32 connecting to the same database.

Database

Database Provider

Select the type of database you wish to connect to.

Microsoft Access Database



Settings File

This section allows you select the path for the T32Settings.ini file. The Settings File is Customisable and allows certain applications to be active or inactive within Traka32.

Live Database Path

The live database path contains the path to the live database. To search for the database simply click on the **Browse** button. Please refer to the Database Installation section for more information.

Check the integrity of the database each time the application starts

Select this option to enable the Database Integrity Checker to check the state of the database each time the database is opened. Please refer to the Check Database Integrity section for more details.

Auto Database Backup

This automatically prompts the backup of the database to a chosen location (we advise a backup directory on your local hard drive or server). You may select the number of uses of the software before the backup takes place.

Enable Auto Backup

Select this option to enable the auto backup facility. Clear this selection if you want to disable the auto backup facility.

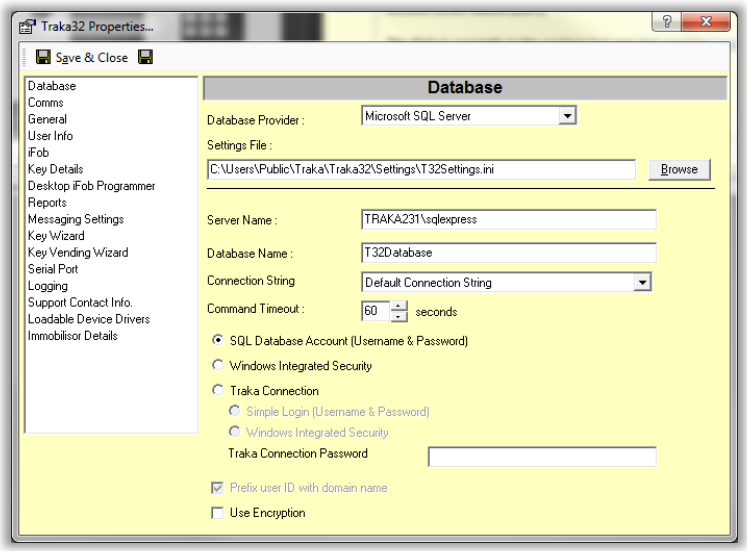
Frequency

Enter the number of times the software has to be closed before the auto backup utility will prompt you to back up the database.

Backup Path

Select the path to where you wish the database backup file to be located. To search for a backup path simply click on the lower **Browse** button. When the backup prompt is displayed, you will be offered the chance to alter the path if required.

Microsoft SQL Database



Settings File

This section allows you select the path for the T32Settings.ini file. The Settings File is Customisable and allows certain applications to be active or inactive within Traka32.

Server Name

Enter the name of the SQL Server that will host the database.

Database Name

Select the name of the SQL Database.

Connection String

Set to 'Default Connection String' unless you are connecting to a server that has TLS 1.0 disabled, in which case select 'Support for non TLS 1.0 enabled servers'.

NOTE: The client machine must have Windows 7 or higher in order for the 'Support for non TLS 1.0 enabled servers' option to work.

Command Time-out

Adjust the command time-out value in seconds accordingly. The default command time-out value is 60 seconds. If you experience **Command Time-out Error** messages then increase the command time-out values in increments of 10 until the errors no longer appear.

NOTE: It is not recommended that you enter a command time-out value below 30 seconds.

Use Integrated Security

Select this option to allow integrated security.

Match user via database

When using integrated security, select this option so that Traka32 matches the SQL Server Login entered into the user details window to the user name returned by the SQL Server. If the user logging is has administrative rights to the SQL Server (direct or inherited) then they will be given full unrestricted access to the Traka32 software.

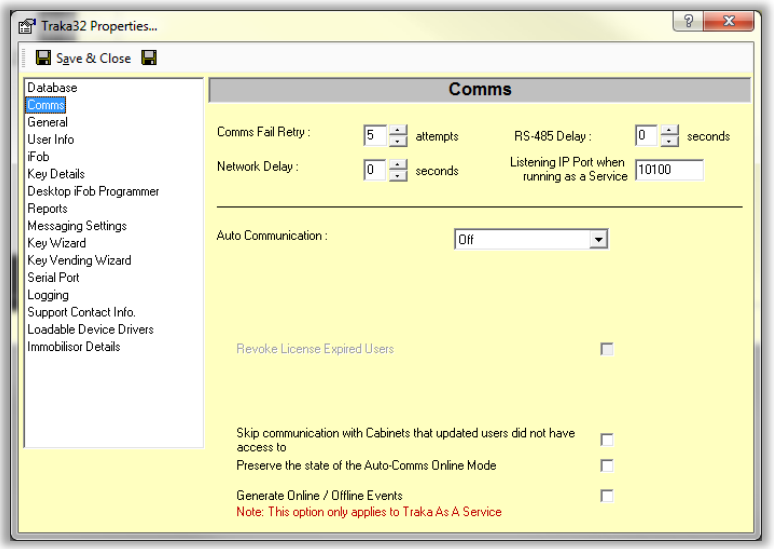
Match user via environment

When using integrated security, select this option so that Traka32 matches the SQL Server Login entered into the user details window to the user name returned by the Windows. This is useful if the user logging is has administrative rights to the SQL Server but you want to identify them as a standard user within Traka32.

Prefix with domain name

When using the match user via environment option, set this option if it's a requirement to prefix the SQL Server Login name with the Domain name. For example <DOMAIN NAME\USER NAME>. If this option is not set only the user name will be matched upon.

Comms



Comms Fail Retry

Enter the number of time the software will attempt to wake a system in order to communicate before the software gives up. If a system is being used or the door has been left open, the software will not be able to communicate.

Network Delay

If you have a very busy Ethernet network, there may be a delay in the response times during the communications. If you are finding that the software is timing out, increase the delay accordingly.

RS485 Delay

If you have a very busy RS485 network, there may be a delay in the response times during the communications. If you are finding that the software is timing out, increase the delay accordingly.

Listening IP Port When Running as a Service

If you are running T.A.S (Traka as a service) you match this IP Port number to the IP Port number within the T.A.S application to make a communication.

Auto Communication

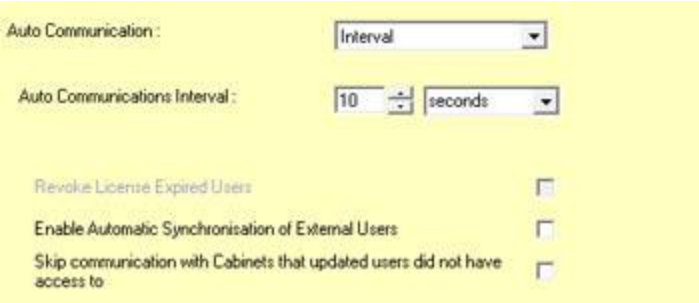
This allows the automatic communication between the Traka system and the supporting Traka32 software. By automatically communicating you ensure that the transactions recorded by the Traka system are always backed up to the PC.

For automatic communication it is of course essential that the Traka32 software is running.

In most applications only one PC should setup as online and should be on a PC that is not commonly used or switched off.

- **Off**
  The default is **Off**, which means that all communications must be manually completed using the  button.

- **Interval**
  By selecting interval you may specify how frequently, in seconds, that Traka32 should communicate with the systems.

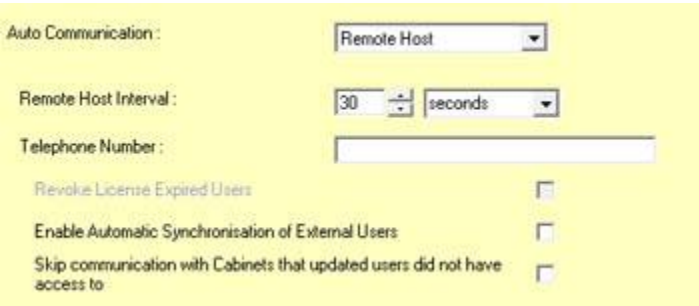


- **Specific Time of Day**
  By selecting specific time of the day you may specify exact times of each day that Traka32 should communicate with the systems.

  To add a time, enter the required time and click on **Add**. The time will appear in the list opposite. To remove a time, select the time to remove from the list and click on **Remove**.

- **Online**
  By selecting online each selected system will automatically switch online when the Traka32 software is loaded.

- **Remote Host**
  By selecting remote host, Traka32 will add a host entry into each Traka System and will then listen for remote connections from the Traka System every time an event occurs. For further information, please refer to the XPort Remote Host section.



  The **Remote Host Interval** can be set to specify how frequently, in seconds, that Traka32 should communicate with the systems. This is in addition to the Remote Host communications but can be disabled by setting to 0.

  The **Telephone Number** field is available for using the remote host option with a Modem but this option is not yet available.

IMPORTANT:

Once Auto Comms has been activated, you can select which systems are to be included in Auto Comms on an individual basis. To include a system, tick **Include In Auto Comms** in the System Details window. Here you can also **Nominate a PC** to auto communicate **only** with the selected system.

Nominating a PC can help to prevent the potential problem of more than one copy of Traka32 trying to communicate with the same system at the same time in which case one of them could fail with an error. If **Nominate a PC** is left **not ticked**, then **all** copies of Traka32 will auto communicate with the system.

Enable Automatic Synchronisation of External Users

Checking this option will automatically upload any user records that have been altered via the Traka.Net Post-Box software to the relevant systems.

Skip Communication with Cabinets that Updated Users Did Not Have Access to

Normally, when a User's security is changed by the 3rd Party Link Stored Procedures, Traka32 will communicate with ALL cabinets to make sure that the user does not exist in any cabinets to which they don't have access (regardless of whether they had access or not). Switching this option on suppresses this behaviour and results in much faster cabinet updates where there are many cabinets and users generally only have access to one or two cabinets.

Preserve the State of Auto-Comms Online Mode

Selecting this option will allow you un-select the default 'Auto Synchronisation' & 'Auto Synchronisation All Systems' options, close Traka32 and have them remain un-selected when you re-open Traka32.

Generate Online / Offline Events

Selecting this option when using Traka As A Service (TAAS) will enable the system to generate 'Online' and 'Offline' events. If this feature is enabled, when TAAS starts up events are generated showing that all systems are offline and as each system has a successful communication an event is generated showing that it is now online. If in the future a system fails to communicate successfully then the offline event will be generated again.

User Upload Limit

When user records are being added or updated by any of the 3rd party links all the updated users get sent to all the required cabinets the next time that the auto-comms fires. If there are hundreds of users that need syncing to lots of systems this can take a very long time, therefore an option is available to limit the number of users that get updated each time the auto-comms runs.

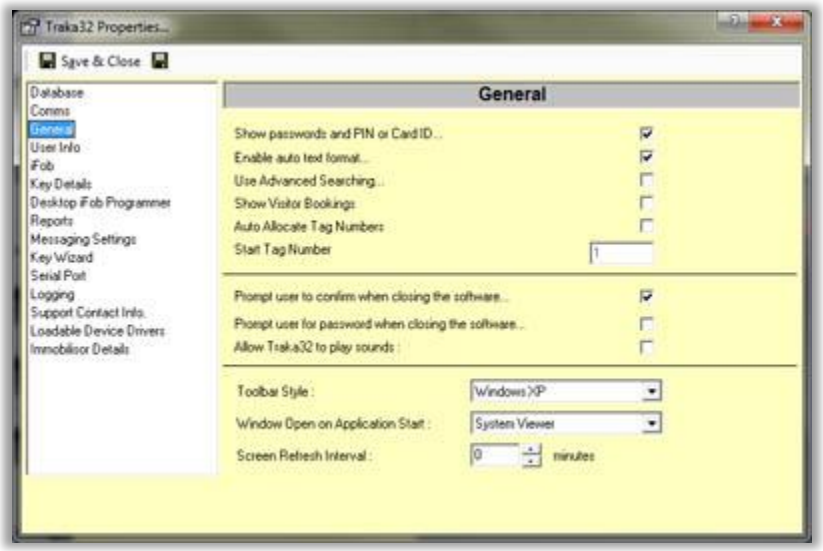
This limit is configured by adding a line into the [AutoComms] section of the T32Settings.ini file as follows:

```
[AutoComms]

SyncExternalUserLimit=100
```

The example above is configured to upload 100 users each time but this value can be changed to suit the customers' needs.

General



Show password and PIN or Card ID

Select this option to make all passwords, personal identification numbers and card ID's visible. Clear this option to hide.

Enable auto text format

Checking this option forces the entry fields to automatically capitalise the first letter and to force the remaining letters in the same word to lower case.

Use Advanced Searching

Select this option to enable the Advanced Search option. Clear this option to use the Standard Search option. The Advanced Search option allows you to search on one or more criterion and allows you to filter out records from a list whereas the Standard Search option only allows you to search on only one criterion and highlights the matches.

Show Visitor Bookings

To enable the Visitor Booking wizard in Traka32, select Show Visitor Bookings.

Auto Allocate Tag Numbers

This feature when enabled automatically adds a tag number to iFobs that are newly synchronised to the system. Also if an iFob is deleted and another takes it pace it will automatically be given the previous iFobs tag number.

Prompt user to confirm when closing the software

Select this option to prompt for confirmation every time the software is closed.

Prompt user for password when closing the software

If you are using the user login to the software you can prompt the user to enter their password in order to close the software. This is useful if you want to leave the software running in Auto Comms or Online modes as this will discourage users from closing the software.

Allow Traka32 to play sounds

Select this option to allow Traka32 to play sounds upon certain events.

Toolbar Style

The look and behaviour of the toolbars within Traka32 can be altered to match those of your operating system. Simply select from Office 97, Windows 2000 or XP styles.

Window Open on Application Start

Select the Window you require to open when the Traka32 software is loaded. This will depend on the roll of the workstation the software is installed upon or the application of the Traka32 software. For example motor dealers often use the Key List for day to day administrations or a Fork Truck engineer may use the Fault List to administer day to day truck faults.

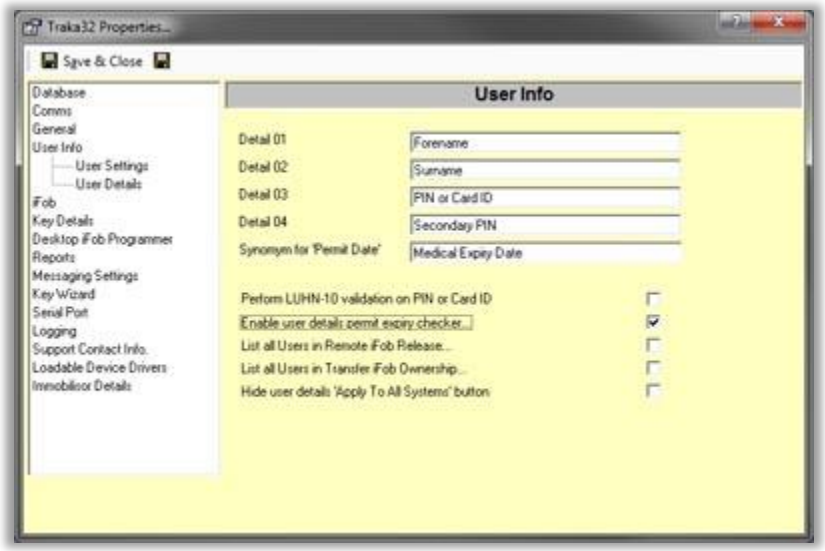
Screen Refresh Interval

This option when enabled will automatically refresh any of the windows you have open in Traka32 to ensure they are visually up to date with the database. You can define how often the refresh happens in increments of one minute.

This is extremely useful if you have many copies of Traka32 connecting to the same database and you wish to automatically refresh any open windows in Traka32 with the changes made by other users and auto communications.

NOTE: If Auto Communications are enabled, this option is automatically disabled as the auto communications inherently refresh any open windows.

User Info



Detail

This allows change to the field descriptions of the essential information on the user details and system access screens. For most systems this should not be changed.

Synonym for 'Permit Date'

The text entered here will be used wherever the original 'Permit Dates' was used in Traka32.

Perform LUHN-10 validation on

Checking this option will force a check on the Primary ID field of the User Details each time a user record is saved. If the check fails an error message will be shown. This check is primarily used for validating Credit Card numbers and is useful if Credit Cards are used for accessing Traka Systems. If Credit Cards are not used as the Primary ID then do **NOT** select this option.

Enable user details permit expiry checker

Checking this field activates an additional field on the user details, system access screen to allow the definition of a Permit expiry date.

List all Users in Remote iFob Release

Select this option to show all users who have access and who do NOT have access to the selected iFob when using the Remote iFob Release function. Clear this option to only show users who have access to the selected iFob when using the Remote iFob Release function.

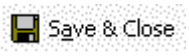
Hide User Details 'Apply to all Systems' Button

The User Info section to allow you to hide the "Apply to All Systems" button in the User Details screen. This prevents users from pressing this button and applying changes to all Systems by mistake when making changes.

User Settings

Force all users to use common security settings

Checking this option will force the **Apply to all systems** check box on the User Details window to always be checked. If this option has not previously been selected, the **Apply settings from this system** drop down menu will become active, allowing the selection of the system that the security settings will be copied from for each user.

NOTE: If you select this option along with a system, when you click 

all the user records will be updated, overwriting the previous security settings.

Set Default Expiry Dates

Checking this option will enable the automatic completion of the User Expiry Date depending on the selection below. If the option is cleared the default expiry date of 01-June-2050 is used.

- Specified Date and Time
- Calculated Date from Activation Date

Updating existing users expiry date when editing their record

Select this option if you wish to the software to automatically adjust the User Expiry Date according to the rules above every time the User Details are edited.

Minimum Password Length

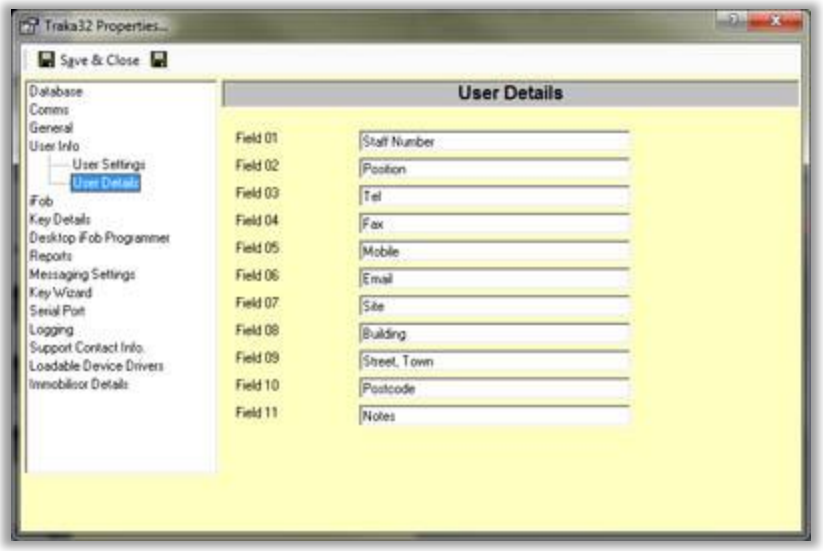
Set the minimum path for the User Login Password. This only applies when used with a Microsoft Access Database.

Password Expiry Period

Set the number of Days / Weeks / Months / Years before the User Login Password expires. This only applies when used with a Microsoft Access Database only.

When a user goes to login to Traka32 and their password has expired, the user will be prompted to enter a new password and their password expiry date will be reset as per the password expiry period.

User Details



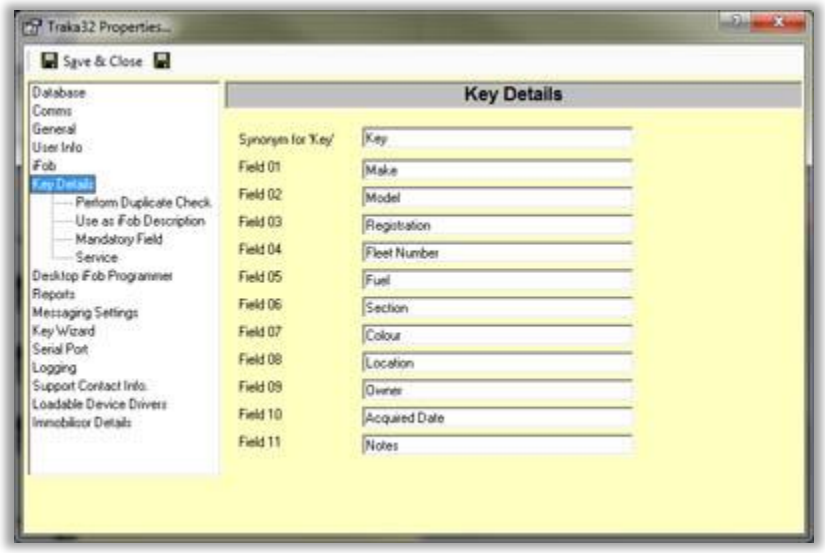
Field

This allows change to the field descriptions of the non essential information on the user details screen.

iFob

The iFob page allows you to assign text that would normally represent the iFob Per Truck labels. The iFob Per Truck labels are used in applications such as reports. This is particularly useful if you have a locker system.

Key Details



Field

This allows change to the field descriptions of the screen describing the keys. Note that these field descriptions also apply to all reports.

Perform Duplicate Check

In applications where there is a large turnover of key records such as the motor trade, it may be important to check if there is already a record for that key. Traka32 can automatically check the individual fields of all the key records against the one you are adding or editing to check for duplications.

To activate the duplication checker, simply check the box against the field or fields you wish to check.

Use as iFob Description

It is possible to allow users to search for keys at the cabinet using a description search facility via the alphanumeric keypad. For example, details such as vehicle registrations or chassis numbers could be searched upon to locate the keys within the cabinet.

As there are 10 fields for each key record, to simplify the searching only 1 field can be searched upon. Select one of the Key Detail description fields to be written to the Traka systems for searching.

Two Key fields can be chosen as the description of the iFob. These should be selected in priority order. Field 1 will be used if that field has any data; if not field 2 will be used.

Mandatory Field

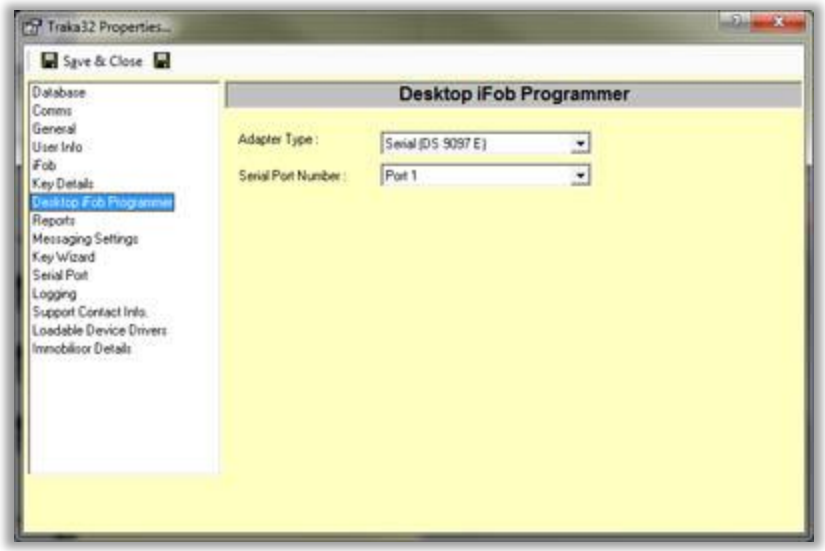
Certain information about keys is critical to any audit trail. If it is a requirement that certain information is filled in about a key then the Key Details window can be configured with mandatory fields which show with a red background.

To enable a mandatory field, simply check the box against the field or fields you wish to make mandatory.

Service

This section allows you to customise what field descriptions you have in the Service section within the Key Details screen.

Desktop iFob Programmer



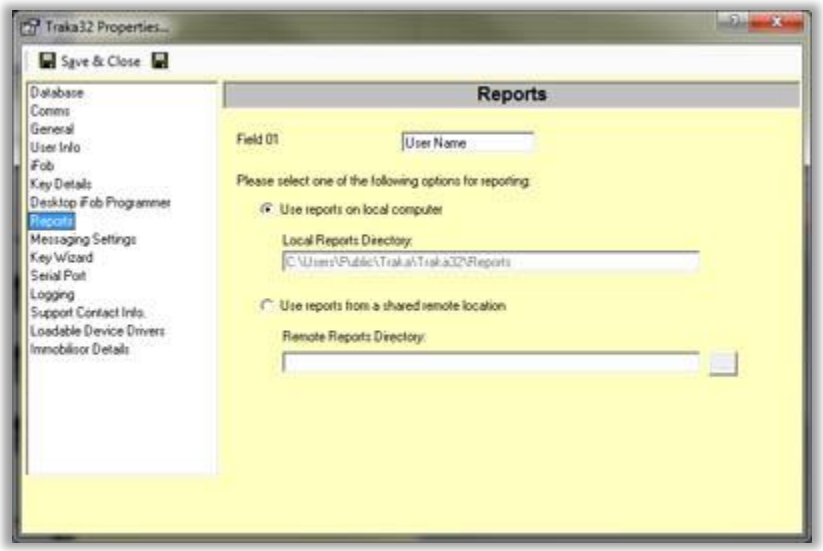
Adaptor Type

Select the Adaptor Type accordingly. There are 3 adaptor types, two serial and one USB. The adaptor type is printed on the serial port connector of the Desktop iFob Programmer, if you require USB type the port number is Unnecessary.

Serial Port Number

Select the relevant Serial Port Number according to which serial port you have connected the Desktop iFob Programmer to.

Reports



Field

This allows the specific change to the title of the User Name field on the reports.

Crystal Report Options

Select one of the following options:

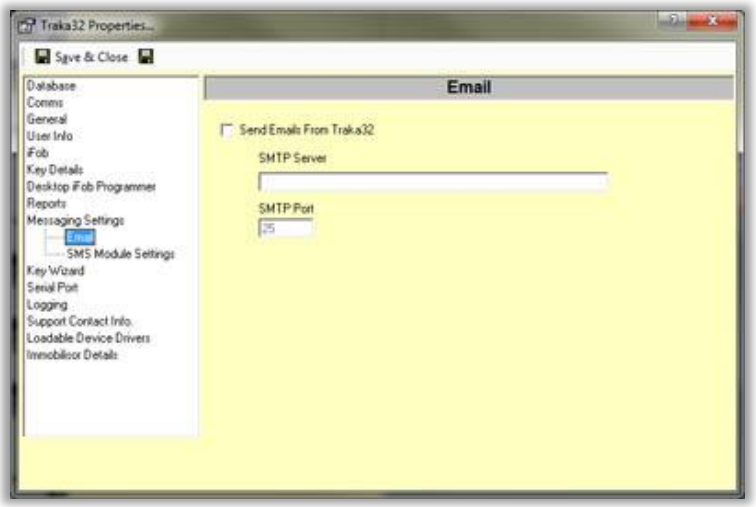
- **User reports on local computer** - this will use the Crystal Report (*.rpt) files that are installed on the local computer in the Reports directory of Traka32. C:\Program files\Traka Limited\Traka32\Reports
- **Use reports from a shared remote location** - this will use the Crystal Report (*.rpt) files that are installed in a remote location.

Hide Transaction Reports

When the old Transaction style reports are no longer required the Transaction Reports menu can be hidden by selecting this option.

Messaging Settings

Email



Send Emails From Traka32

Checking this option will allow Traka32 to send e-mails automatically whenever certain events occur. Please refer to Notification Message System for more information.

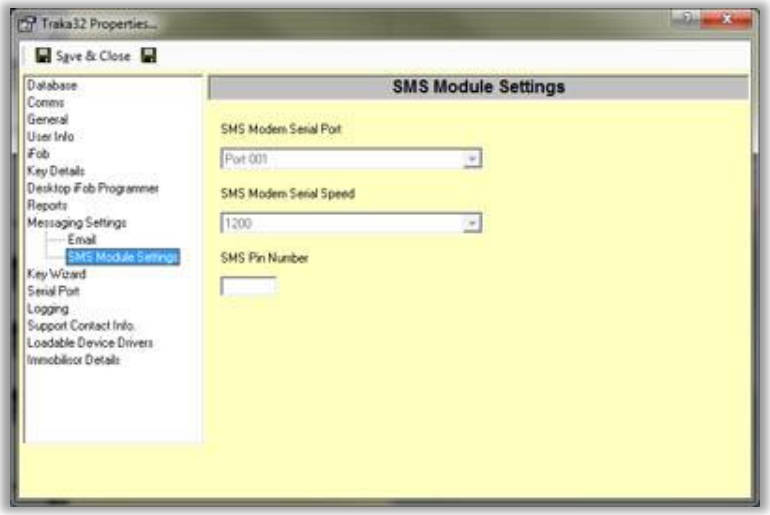
SMTP Sever

Enter the Name or IP Address of the SMTP Sever that Traka32 will use to send e-mails.

SMTP Port

Enter the Port Number of the SMTP Sever that Traka32 will use to send e-mails. The standard default port number used by most SMTP Servers is **25**.

SMS Module Settings



SMS Modem Serial Port

Select the modem serial port number which Traka32 will use to send SMS messages.

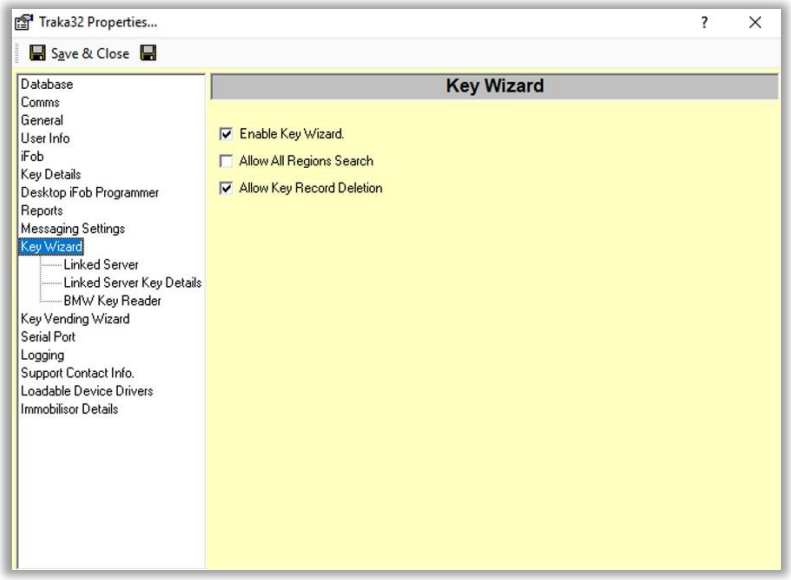
SMS Modem Serial Speed

Select the appropriate speed you require for the modem you will be using.

SMS Pin Number

This field requires you enter the pin number from the SIM card that you will be using to send SMS messages.

Key Wizard



Enable Key Wizard

To enable the Key Wizard in Traka32, select Enable Key Wizard.

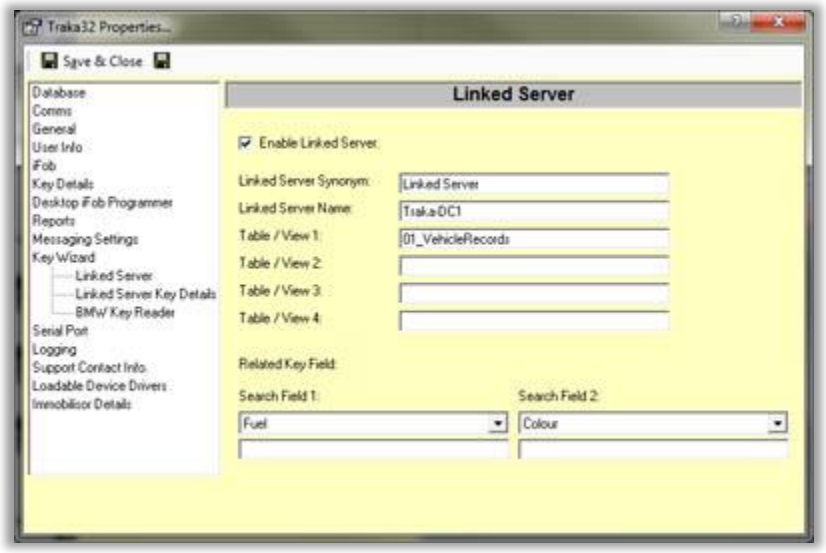
Allow All Regions Search

When selected, this option will allow the Key Wizard to search across all Regions regardless of the region of the logged in user. This is useful in Random Return to Multiple Systems where an iFob that is out of a system and is not in any region and therefore cannot be seen by any user that is not in 'All Regions'.

Allow Key Record Deletion

With the release of Traka32 version 02.40.0000, a tickbox has been added to the properties form. Once enabled, the Key Wizard will ask if the logged-in user wants to delete unmatched key records when importing data from Kerridge. If the option is not enabled, the user will not have the option to delete unmatched keys. By default, the option will be enabled.

Linked Server



Linked Server Synonym

Enter an alternative word or phrase for 'Linked Server'.

Linked Server Name

This field allows you to assign you linked server a name.

Enable linked Server

To allow the importing of data from a linked server, select Enable linked server.

Table/View 1-4

Enter the Table names for Traka32 to search within Kerridge. Up to 4 tables can be searched.

For example: MK_01_VehcleRecords

Search Field 1

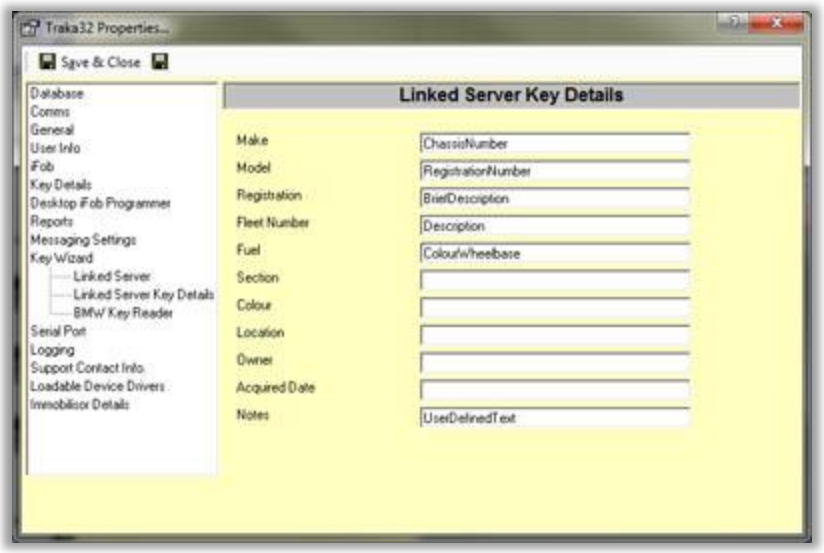
Enter the Chassis Search Field name that Traka32 will search within the selected tables for the vehicle Chassis Number. Also select the **Related Key Field** that Traka32 will use to compare the chassis number against.

Search Field 2

Enter the Reg Search Field name that Traka32 will search within the selected tables for the vehicle Registration Number. Also select the **Related Key Field** that Traka32 will use to compare the registration number against.

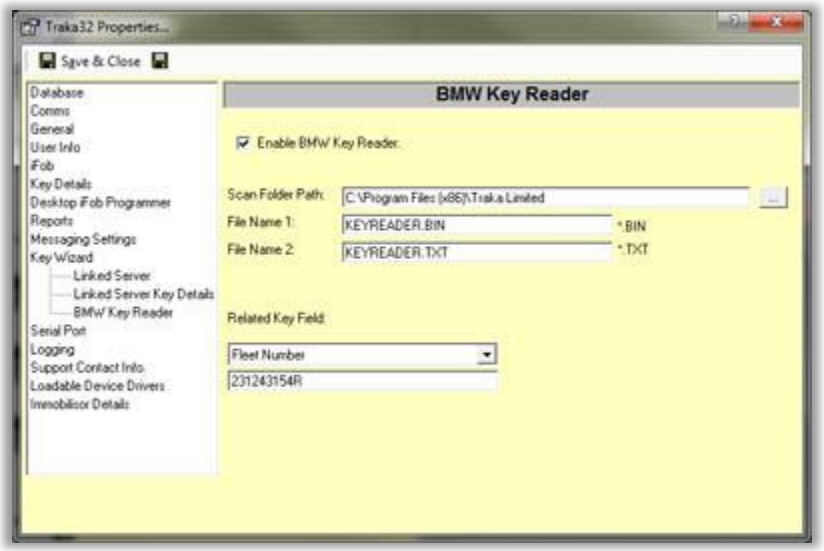
Linked Server Key Details

Enter the linked server keys detail **Field** names for Traka32 to import the data from. If a field is not required for importing, leave the field blank. For example:



ChassisNumber
RegistrationNumber
BriefDescription
Description_
ColourWheelbase
-
-
-
-
-
UserDefinedText

BMW Key Reader



Enable BMW Key Reader

To allow the use of the BMW Key Reader, select Enable BMW Key Reader.

Scan Folder Path

Enter the Scan Folder Path to where the BMW Key Reader dumps the KEYREADER.BIN and KEYREADER.TXT files.

NOTE: Please configure the BMW Key Reader to output BOTH the KEYREADER.BIN and KEYREADER.TXT files.

File Name 1

Set the File Name 1 to KEYREADER.BIN

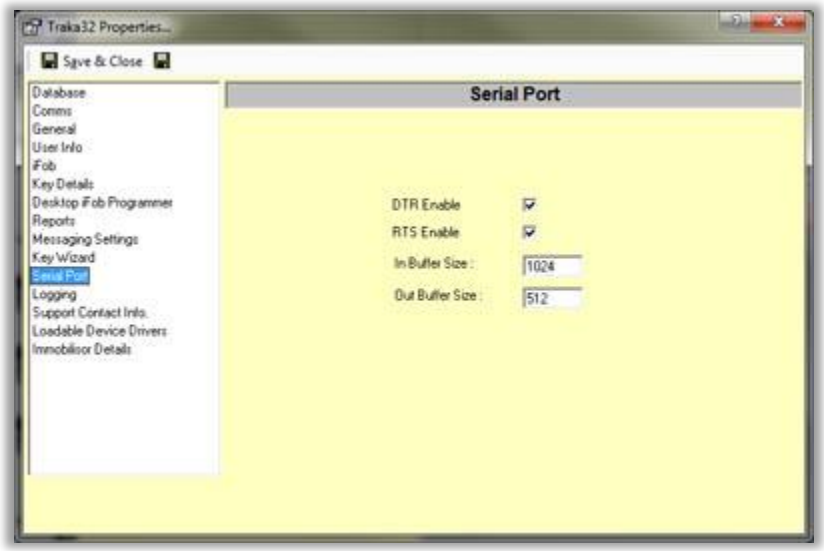
File Name 2

Set the File Name 2 to KEYREADER.TXT

Related Key Field

Select the Related Key Field that Traka32 will use to compare the chassis number against.

Serial Port

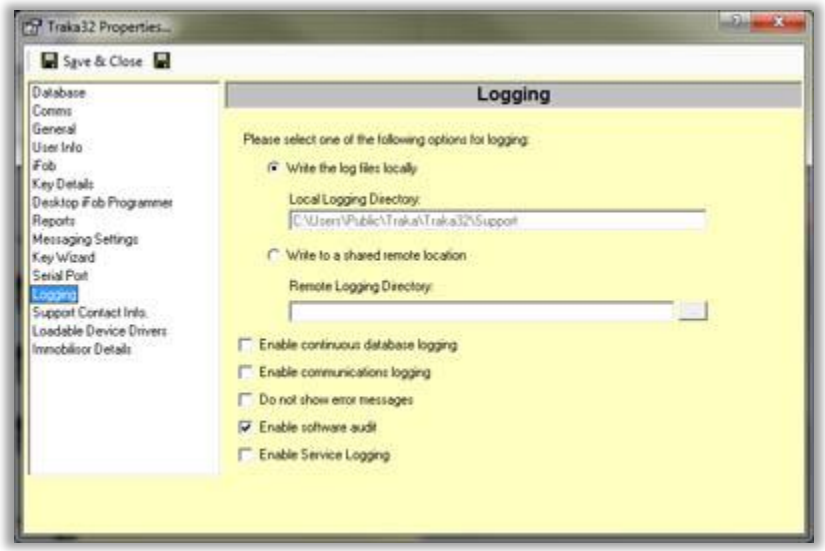


Various Settings

When experiencing difficulties communicating to Traka Systems using the Serial Port it is possible to adjust some of the more advanced settings of the Serial Port from here.

Logging

The Logging tab can only be accessed if the current user of the software is logged in as an engineer.



Write the log files locally

Select this option to record any internal software errors to log files on the local computer.

Write to a shared remote location

Select this option to record any internal software errors to log files located at the selected path.

Enable continuous database logging

Select this option to keep a continuous log of database activity. This option will help track potential problems with database corruption.

Enable communications logging

Select this option to log communication activity between the software and the cabinet(s). This option will help track potential problems with the cabinet(s).

Do not show error messages

Select this option to disable the software from displaying the Internal Traka Error dialogs in the unlikely event of an error. If an error does occur whilst this option is selected the error will be logged and the  symbol will appear in the status bar. To view the error log, double click on the  symbol.

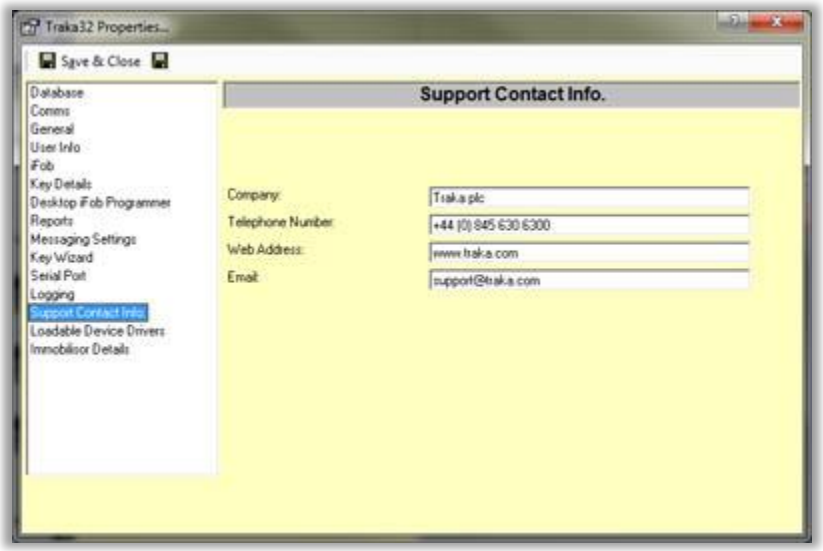
Enable software audit

Select this option to keep a continuous log of every change that is made in the software along with the name of the user who made the change, when the change was made and what the change was. If this option is cleared, a log will be recorded of who cleared the option.

Enable Service Logging

This option works in conjunction with T.A.S (Traka As a Service) and writes all the event data from T.A.S to a text document in the support folder which is stored on your hard drive in a location of your choice when installing Traka32.

Support Contact Info.



The information entered into this section of the Traka32 Properties will be visible to all users of Traka32 when they click on **Help**, **Technical Support**. Customers and Distributors can amend these details as required.

Company

Enter the company name of the technical support contact.

Telephone number

Enter the telephone number of the technical support contact.

Web Address

Enter the web address of the technical support contact.

Email

Enter the email address of the technical support contact.

Loadable Device Drivers

Choose one of These Installed Tablet Types

Use this drop down box to select the appropriate Tablet type driver you require to use your Tablet.

Choose one of These Installed Fingerprint Readers

Use this drop down box to select the appropriate Fingerprint reader driver you require to use your Fingerprint hardware.

Choose one of These Installed SMS Drivers

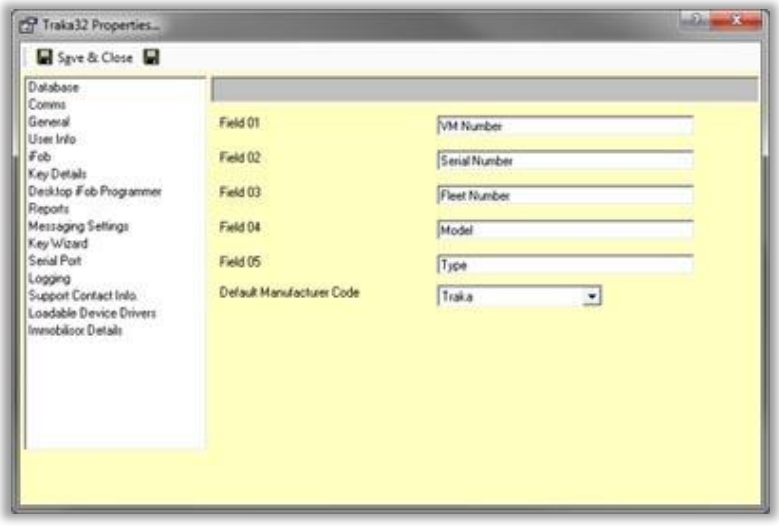
Use this drop down box to select the appropriate driver you require to send and receive SMS messages.

Immobilisor Details

To cater for the long descriptions given to Immobilisor Trucks, five extra user definable fields have been added to the Immobilisor Details window. The headings for these description fields can be defined in the Properties window.

Default Manufacturer Code

This drop down selection box allows you to set a default manufacturer code across the database. This will allow you to open the Immobilisor Details form and not need to change the manufactures code for each individual Immobilisor that needs programming.



4.9.2 OPTIONS

4.9.2.1 SOFTWARE ACCESS

4.9.2.1.1 SOFTWARE ACCESS OVERVIEW

It is possible to set up various user login types, each with their own restrictions so that when users log into the Traka32 software they can only access the parts of the software defined in the login type.

The default user type is Administrator. Administrators must of course have all of these permissions and it is therefore not possible to change the Administrator options. However, you may wish to create a user type that only allows a user to have access to record changes or perhaps to only allow communication.

By checking the relevant boxes, it is possible to allow the amendment to the records, to allow communication and to allow configuration etc.

Once one or more Software Login Groups have been created, each user can be assigned with their individual login and group. Please refer to the User Details Software Access section on how to assign the login types to the individual users.

When one or more users have been assigned with a login name and password, the next time the software is loaded the user will be prompted to login.

To login the user simply has to enter their username and password. Once logged in the software will record certain tasks the user performs.

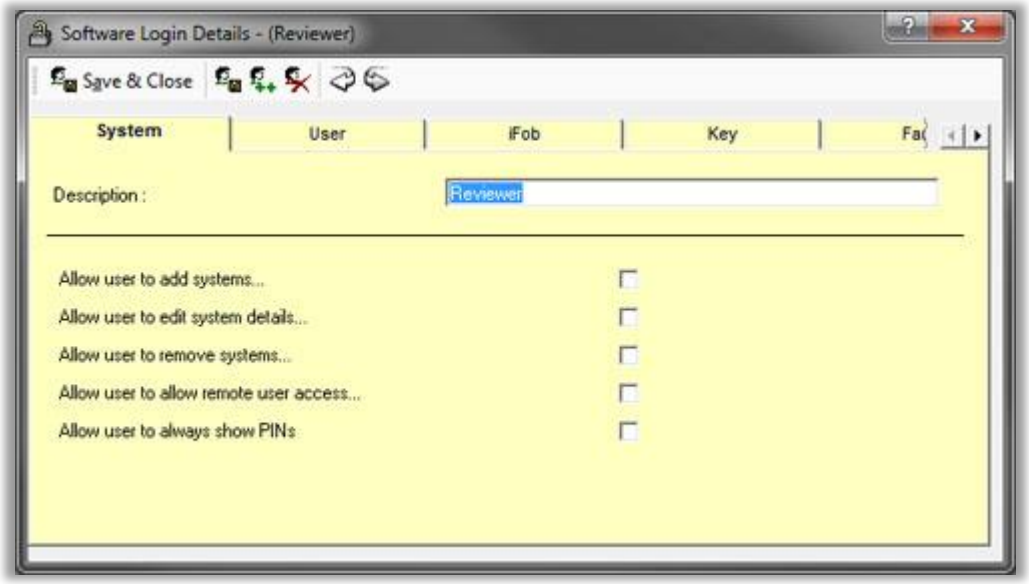
4.9.2.1.2 SOFTWARE LOGIN DETAILS

The Software Login Details window allows you to add and edit the login details. Please refer to the User Details Software Access section on how to assign the login types to the individual users.

Description

Enter a description for the login type. This description will appear in the User Details Software Access drop down list.

System



Allow user to add systems

Check this box to allow the logged in user to be able to add system records. Checking this box will automatically check the edit systems box. This option should only be available to administrators.

Allow user to edit systems

Check this box to allow the logged in user to be able to edit system records. This option should only be available to administrators.

Allow user to remove system

Check this box to allow the logged in user to be able to delete system records. This option should only be available to administrators.

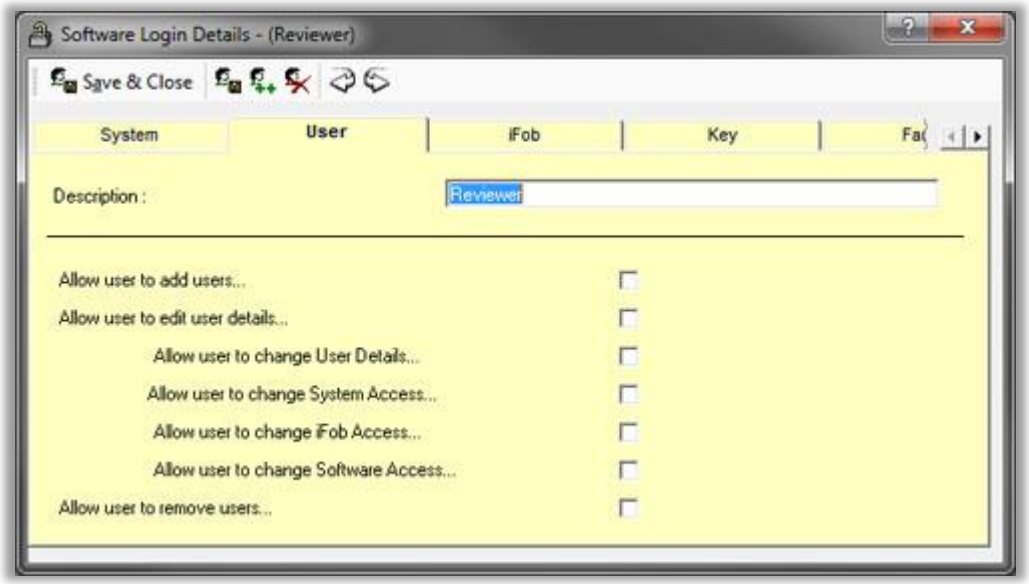
Allow user to allow remote user access

Check this box to allow the logged in user to be able to give another user remote access to a selected system. This option is useful for supervisors as it can be used if a user has forgotten their ID Card, the user will be given access as if they have swiped their card and will be able to take authorised iFobs / keys as normal.

Allow user to always show PINs

There option allows members of a group to keep the status of the 'Show PINs' option. e.g. If the logged in user has turned on the option to show users PIN numbers in the User Details or Properties screen, the PIN numbers will only show until the user logs out of Traka32. If this new tick box is ticked and the logged in user is a member of the correct Software Login group then when they log back into Traka32 the user PIN numbers will still be shown.

User



Allow user to add users

Check this box to allow the logged in user to be able to add user records. Checking this box will automatically check the edit user's box.

Allow user to edit user details

Check this box to allow the logged in user to be able to edit user records.

Allow user to change User Details

Check this box to allow the logged in user to be able to edit a user's details.

Allow user to change System Access

Check this box to allow the logged in user to be able to edit user's system access.

Allow user to change iFob Access

Check this box to allow the logged in user to be able to edit user's iFob access.

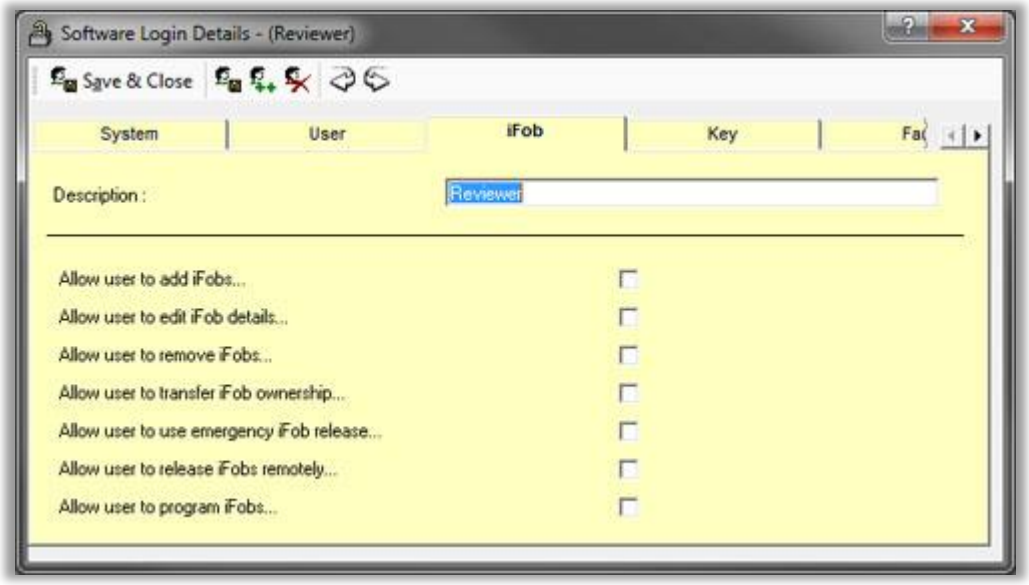
Allow user to change Software Access

Check this box to allow the logged in user to be able to edit user's software access.

Allow user to remove users

Check this box to allow the logged in user to be able to delete user records.

iFob



Allow user to add iFobs

Check this box to allow the logged in user to be able to add iFob records. Checking this box will automatically check the edit iFobs box.

Allow user to edit iFob details

Check this box to allow the logged in user to be able to edit iFob records.

Allow user to remove iFobs

Check this box to allow the logged in user to be able to delete iFob records.

Allow user to transfer iFob ownership

Check this box to allow the logged in user to be able to transfer the ownership of an iFob that is currently out of the system to another user. This option is useful for supervisors as it can be used if an iFob / key has been passed to another user, for example a vehicle maintenance department, without the iFob / key being returned to the system.

Allow user to use emergency iFob release

Check this box to allow the logged in user to be able remotely release an iFob in an emergency. This option is useful for supervisors in case of problems or emergency situations.

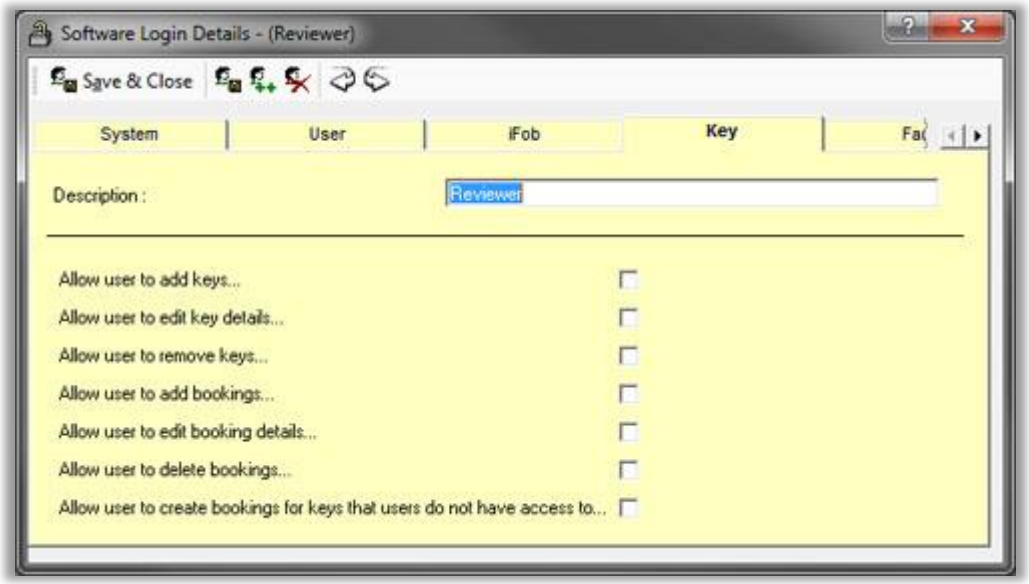
Allow user to release iFobs remotely

Check this box to allow the logged in user to be able to give another user remote access to a selected iFob. This option is useful for supervisors as it can be used if a user has forgotten their ID Card, the user will be given access as if they have swiped their card and will be able to take only the selected iFob / key as normal.

Allow User to Program iFobs

Check this box to allow the logged in user to Program iFobs using the Traka iFob Programmer.

Key



Allow user to add keys

Check this box to allow the logged in user to be able to add key records. Checking this box will automatically check the edit keys box.

Allow user to edit key details

Check this box to allow the logged in user to be able to edit key records.

Allow user to remove keys

Check this box to allow the logged in user to be able to delete key records.

Allow user to add bookings

Check this box to allow the logged in user to be able to add key booking records. Checking this box will automatically check the edit key booking box.

Allow user to edit booking details

Check this box to allow the logged in user to be able to edit key booking records.

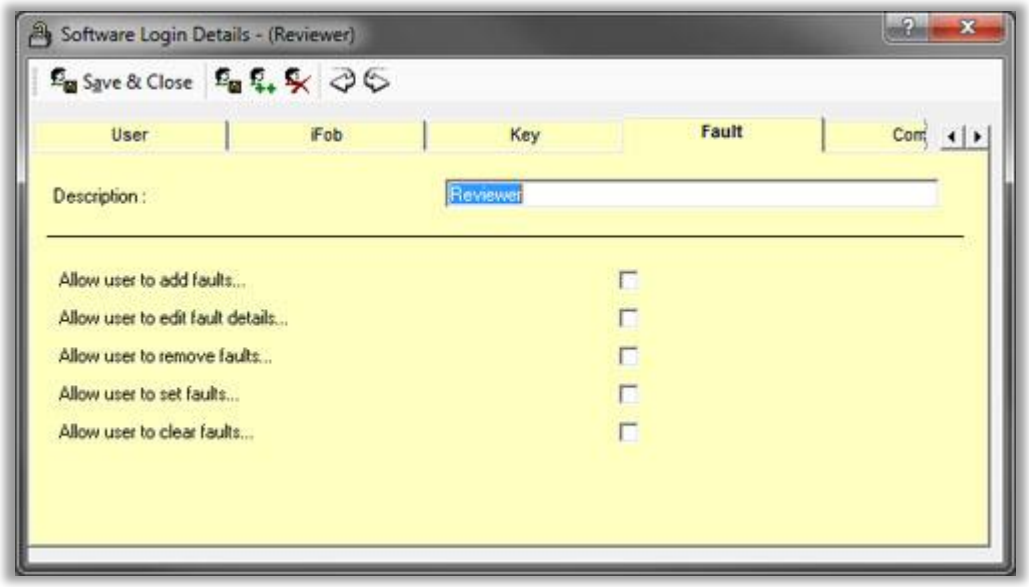
Allow user to delete bookings

Check this box to allow the logged in user to be able to delete key booking records.

Allow user to create bookings for keys that users do not have access to

Check this box to allow the logged in user to create bookings for keys the users (associated to the booking) do not have access to.

Fault



Allow user to add faults

Check this box to allow the logged in user to be able to add fault records. Checking this box will automatically check the edit faults box.

Allow user to edit faults

Check this box to allow the logged in user to be able to edit fault records.

Allow user to remove faults

Check this box to allow the logged in user to be able to delete fault records.

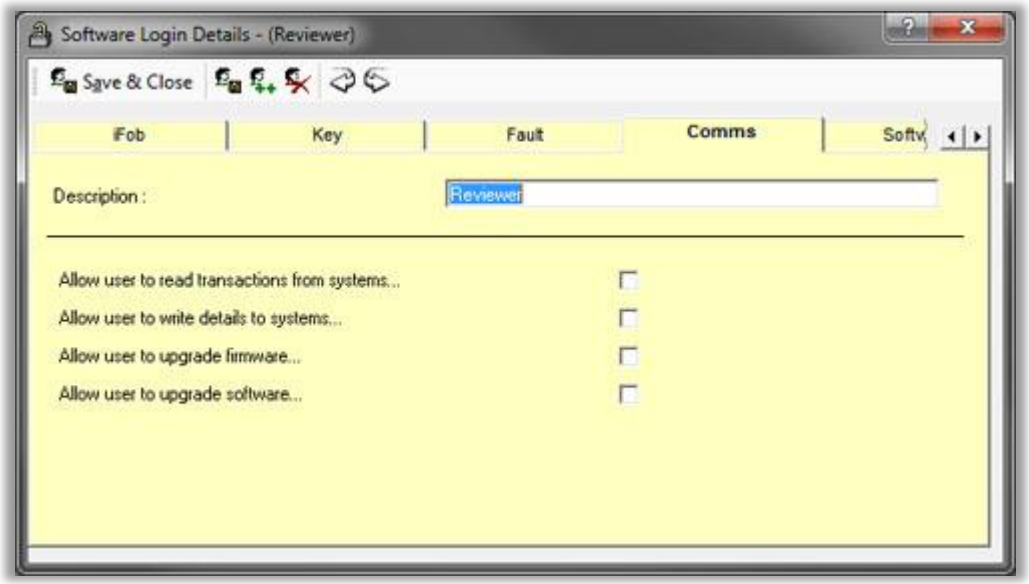
Allow user to set faults

Check this box to allow the logged in user to log new faults against an iFob. This option is useful for engineers who wish to record faults and prevent users from taking iFobs / keys with faults logged against them.

Allow user to clear faults

Check this box to allow the logged in user to clear logged faults from an iFob. This option is useful for engineers who wish to record faults and prevent users from taking iFobs / keys with faults logged against them.

Comms



Allow user to read transactions from system

Check this box to allow the logged in user to be able to read all the transactions and alarm data from the Traka Systems. This option should be made available to all users.

Allow user to write details to system

Check this box to allow the logged in user to be able to write data such as user records, iFob records, the date & time etc. to the Traka Systems. This option should only be available to administrators.

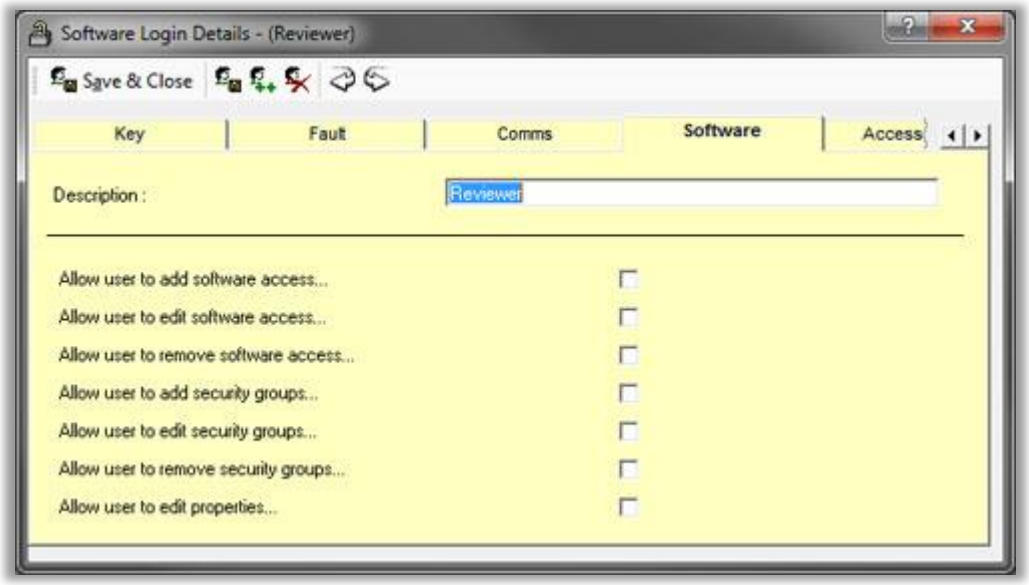
Allow user to upgrade firmware

Check this box to allow the logged in user to be able to upgrade the firmware of the Traka Systems. This option should only be available to administrators.

Allow user to upgrade software

Check this box to allow the logged in user to be able to upgrade the Traka32 software. This option should only be available to administrators.

Software



Allow user to add software access

Check this box to allow the logged in user to be able to add software access records. Checking this box will automatically check the edit software access box. This option should only be available to administrators.

Allow user to edit software access

Check this box to allow the logged in user to be able to edit software access records. This option should only be available to administrators.

Allow user to remove software access

Check this box to allow the logged in user to be able to delete software access records. This option should only be available to administrators.

Allow user to add security groups

Check this box to allow the logged in user to be able to add security group records. Checking this box will automatically check the edit security group box.

Allow user to edit security groups

Check this box to allow the logged in user to be able to edit security group records.

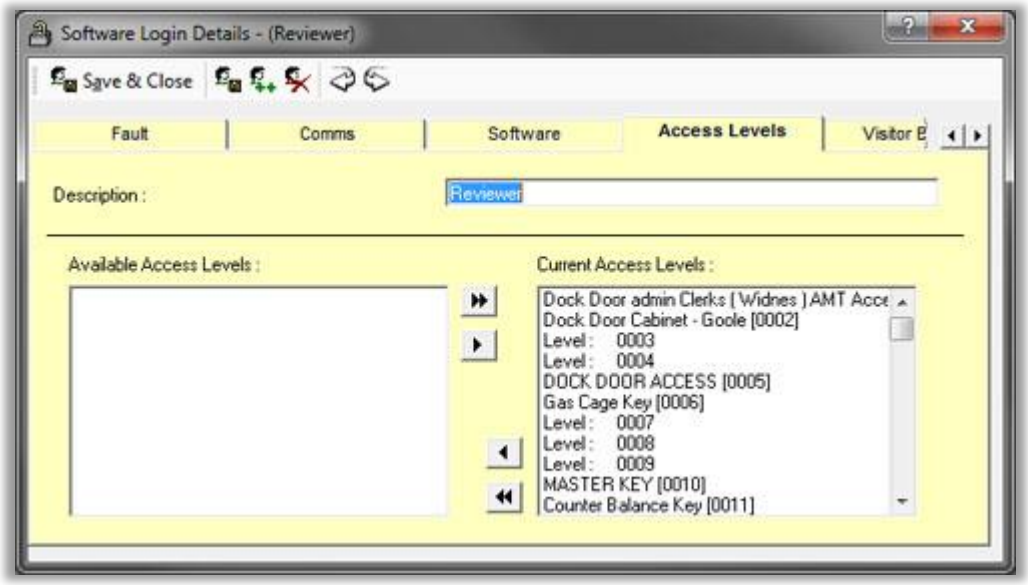
Allow user to remove security groups

Check this box to allow the logged in user to be able to delete security group records.

Allow user to edit properties

Check this box to allow the logged in user to be able to edit the Traka32 properties. This option should only be available to administrators.

Access Levels



Available / Current Access Levels

Select the Access Levels that the logged in user will be able to administer. This will allow the logged in user to administer iFobs that have one of the Current Access Levels. This will also only allow the logged in user to administer Keys attached to iFobs that have one of the Current Access Levels. Also when administering User Details, the logged in user will only be able to allocate users with the access levels listed in the Current Access Levels list.

To **Add All** access levels to the Current List, click on 

To **Add Selected** access levels, select the appropriate levels from the Available List and click on 

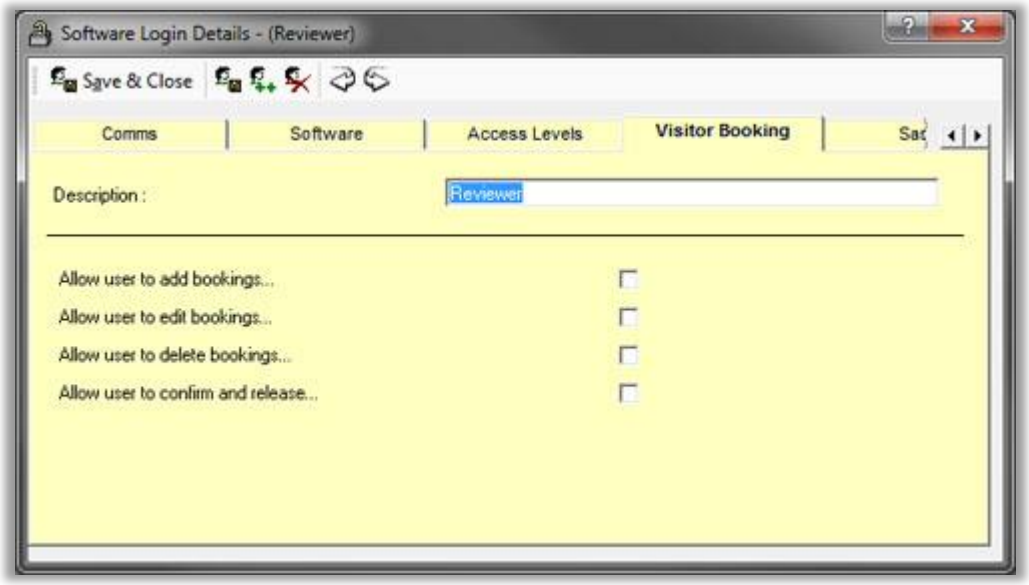
To **Remove Selected** access levels, select the levels from the Current List and click on 

To **Remove All** access levels from the Current List, click on 

Tips:

- To select a group of access levels, click on the first access level, hold down the Shift key and click on the last access level in the group.
- To select several individual access levels hold down the **Ctrl** key and clock on the access levels in the group.

Visitor Booking



Allow user to add bookings

Check this box to allow the logged in user to be able to add visitor booking records. Checking this box will automatically check the edit visitor booking box.

Allow user to edit booking details

Check this box to allow the logged in user to be able to edit visitor booking records.

Allow user to delete bookings

Check this box to allow the logged in user to be able to delete visitor booking records.

Allow user to confirm and release

Check this box to allow the logged in user to be able to confirm the identity of a visitor and release the associated key for the visitor booking.

Sasol

Allow user to assign Sasol Administrator role

Check this box to allow the logged in user to be able to assign Sasol Administrator roles.

Allow user to assign plant states rights

Check this box to allow the logged in user to be able to assign plant states rights.

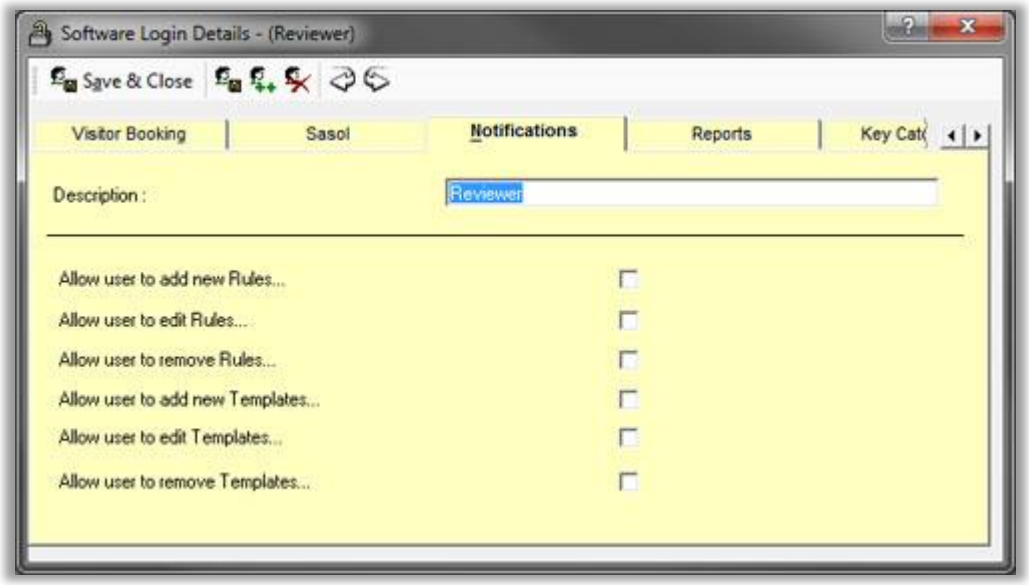
Allow user to assign Sasol restricted access

Check this box to allow the logged in user to be able to assign Sasol restricted access.

Allow user to assign Emergency Release rights rights...

Check this box to allow the logged in user to be able to assign Emergency release rights rights.

Notifications



Allow user to add new Rules

Check this box to allow the logged in user to add new Rules for the Message Notification system.

Allow user to edit Rules

Check this box to allow the logged in user to edit Rules for the Message Notification system.

Allow user to Remove Rules

Check this box to allow the logged in user to edit Rules for the Message Notification System.

Allow user to add new Templates

Check this box to allow the logged in user to add new Templates for the Message Notification System.

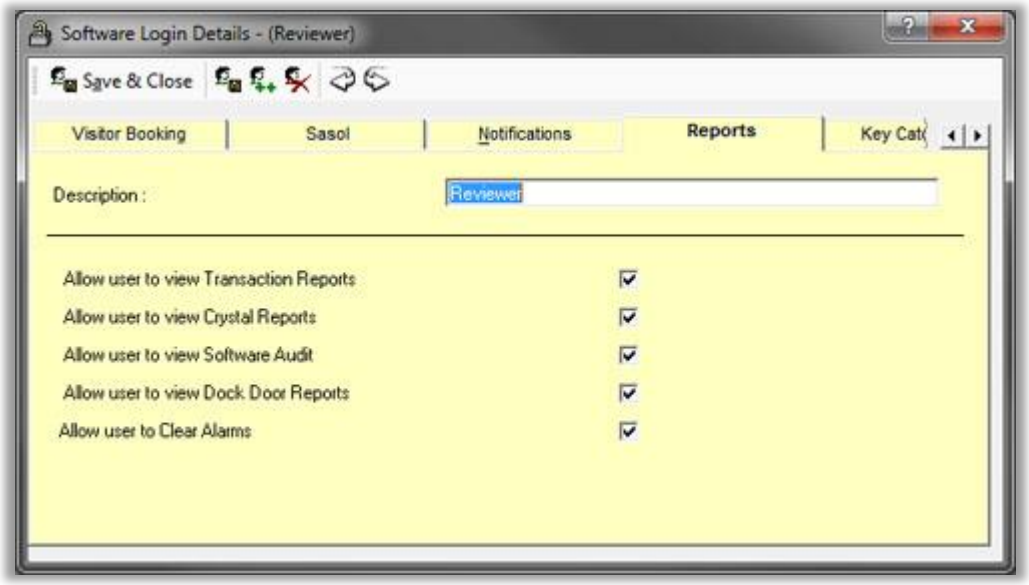
Allow user to edit Templates

Check this box to allow the logged in user to edit Templates for the Message Notification system.

Allow user to remove Templates

Check this box to allow the logged in user to remove Templates for the Message Notification system.

Reports



Allow user to view Transaction Reports

Check this box to allow the logged in user to be able to view Transaction Reports.

Allow user to view Crystal Reports

Check this box to allow the logged in user to be able to view Crystal Reports. These reports generate various types of information on the iFobs/Keys/Items you have in the system.

Allow user to view Software Audit

Check this box to allow the logged in user to view the Software Audit Feature. Please click the hyperlink to learn more about the Alarm Notifications.

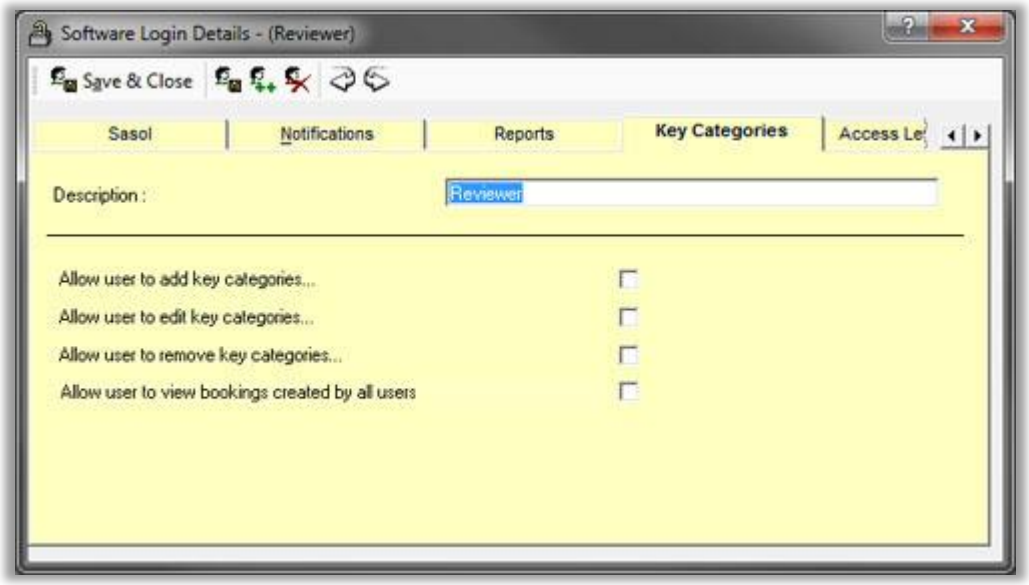
Allow user to view Dock Door Reports

Check this box to allow the logged in user to view Dock Door KPI & Training Reports. Please click the hyperlink to learn more about Dock Door Reports.

Allow user to Clear Alarms

Check this box to allow the logged in user to the ability to Clear the Alarms notifications in Traka32. Please click the hyperlink to learn more about the Alarm Notifications.

Key Categories



Allow user to Add Key Categories

Check this box to allow the logged in user to the ability to add Key Categories.

Allow user to Edit Key Categories

Check this box to allow the logged in user to the ability to edit Key Categories.

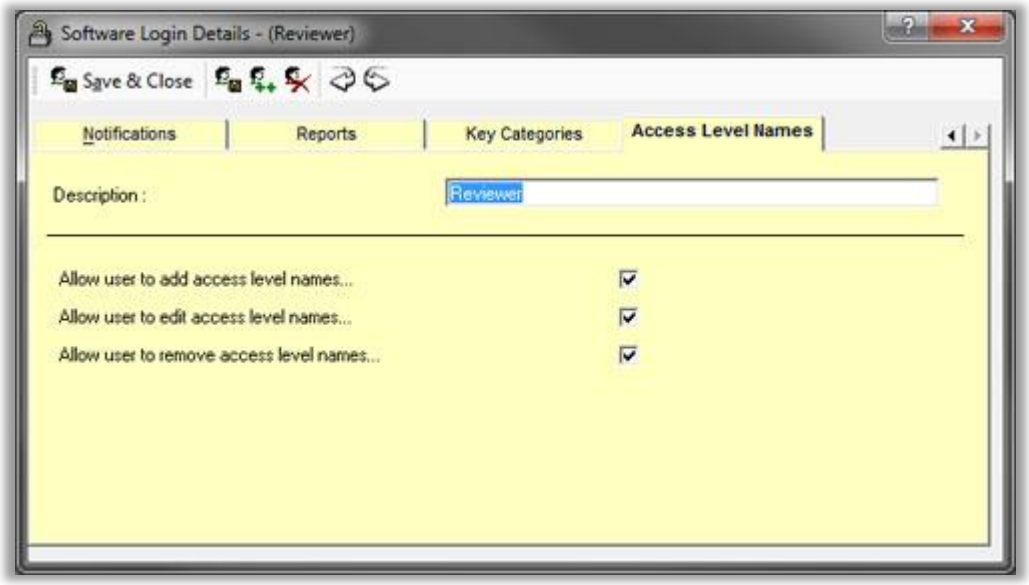
Allow user to Remove Key Categories

Check this box to allow the logged in user to the ability to remove Key Categories.

Allow user to View Bookings Created by all Users

Check this box to allow the logged in user view Key Bookings that have been created by all users in Traka32.

Access Levels Names



Allow user to Add Access Level Names

Check this box to allow the logged in user to Add Access Level Names.

Allow user to Edit Access Level Names

Check this box to allow the logged in user to Edit Access Level Names.

Allow user to Remove Access Level Names

Check this box to allow the logged in user to Remove Access Level Names.

4.9.2.2 SECURITY GROUPS

4.9.2.2.1 SECURITY GROUP OVERVIEW

A Security Group defines a set of common system and iFob access credentials that can be applied to multiple users. For example all Line Managers within an organisation may each require access to the same group of keys. A Security Group called Line Managers could be created with only the iFob access levels (the keys) the Line Managers are allowed to take. All Line Managers would be placed into the Line Managers Security Group.

If you add a new key to your system that all Line Managers require access to, you simply add the access level for the key into the Line Managers Security Group. The opposite could apply also, if you need to restrict this group to a particular access level, you simply remove the access level from the group. This saves lots of time because you do not have to edit the access levels for each individual Line Manager.

Users may belong to Multiple Security Groups, for example you may have a Facilities Manager who is a Line Manager but who also needs access to the fleet vehicle keys. In this case all the fleet vehicle keys could belong to a Security Group called Fleet Vehicles. The Facilities Manager would therefore belong to the Line Managers *and* Fleet Vehicles Security Groups. In addition Users can still be provided with their individual access levels.

Using Security Groups in this way allows for much simpler administration of your Traka system, particularly where you have many users to maintain whom have common system and iFob access requirements. Coupled with the Multiple Regions facility, this makes for ultimate flexibility over your Traka system administration.

View Security Group Details for how to configure Security Groups.

View User Details > Security Groups for how to apply Security Groups to users.

4.9.2.2.2 SECURITY GROUP DETAILS

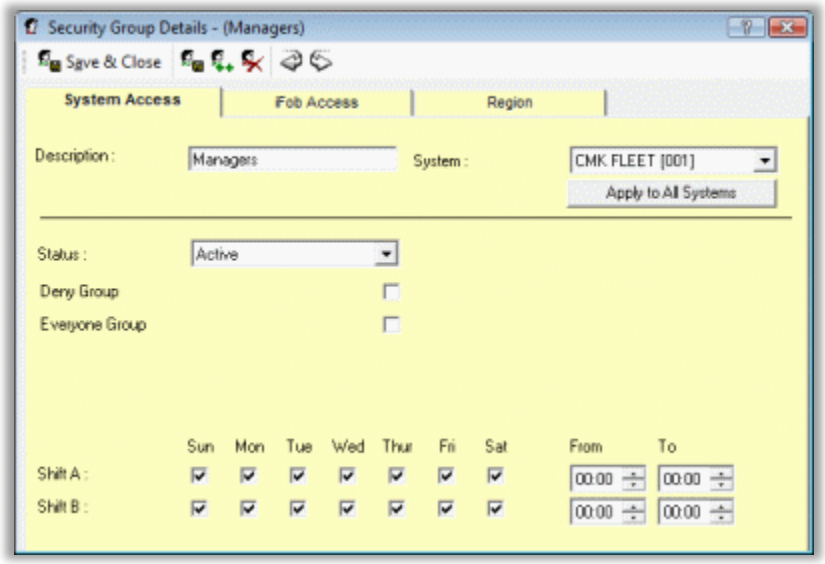
The security group details window allows you to add and edit security group details.

Please refer to the User Details Security Group section on how to assign the security groups to the individual users.

Description

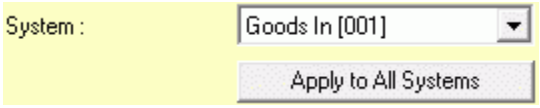
Enter a description for the security group. This description will appear in the User Details Security Group drop down list.

System Access



System / Apply to all systems

When configuring the **System Access** and **iFob Access**, it is possible to configure the access individually for each Traka System.



If the access settings are required to be the same for each system, then configure the access settings for the selected system and then click the **Apply to All Systems** button to copy the access settings to all other systems in the drop down list.

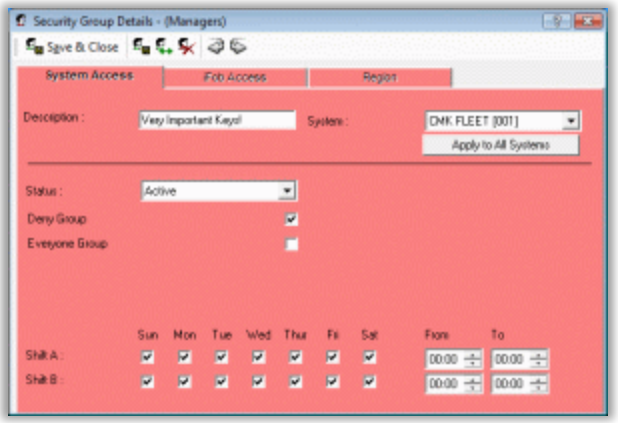
If the access settings are required to be different for each Traka System, then do **not** click the Apply to All Systems button. Simply configure the system and iFob access for each Traka System in the drop down list.

Status

The Active / Inactive Status allow or deny a user within a security group access to one or all Traka Systems. Setting the group's status to Active allows access to the relevant Traka System whilst setting to Inactive will deny access.

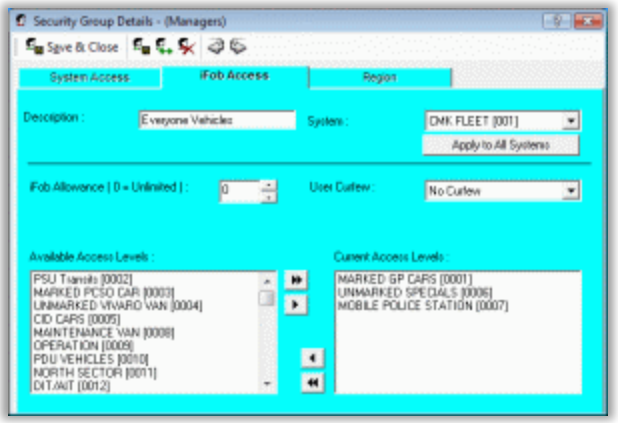
Deny Group

Tick to make the selected Security Group a Deny Group. Upon selecting Deny Group the form will turn red. A Deny Group **denies** access to all system and iFob credentials defined by the group. For example if access levels 1 to 20 belong to the group and you make it a deny group, then any member of the group will be denied access to access levels 1 to 20 regardless of the other security groups to which they belong or their individual access settings.



Everyone Group

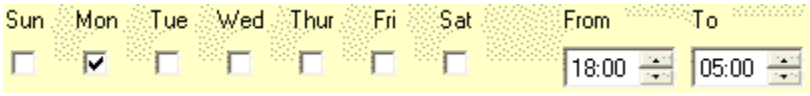
Tick to make the selected Security Group an Everyone Group. Upon selecting Everyone Group the form will turn green. An Everyone Group means that every user (belonging to the regions defined by the group) will be automatically placed into the group. For example this is useful if you have a bunch of keys that all existing and new users require access to. Any new users that are added will automatically be placed into the Everyone group and therefore have access to the system and iFob access credentials defined.



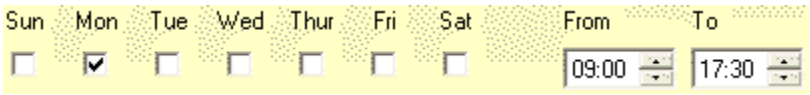
Shift A and B

The System Access Times allow or deny users within the security group access to one or all systems on specific days and between specific times. The system effectively allows two shift patterns giving access at different times on different days of the week.

The '**Days of the Week**' (Sun thru Sat) and the '**From**' time together defines the time at which the security group will be allowed access. The '**To**' time simply defines when the security group will be denied access. Here are some examples:-

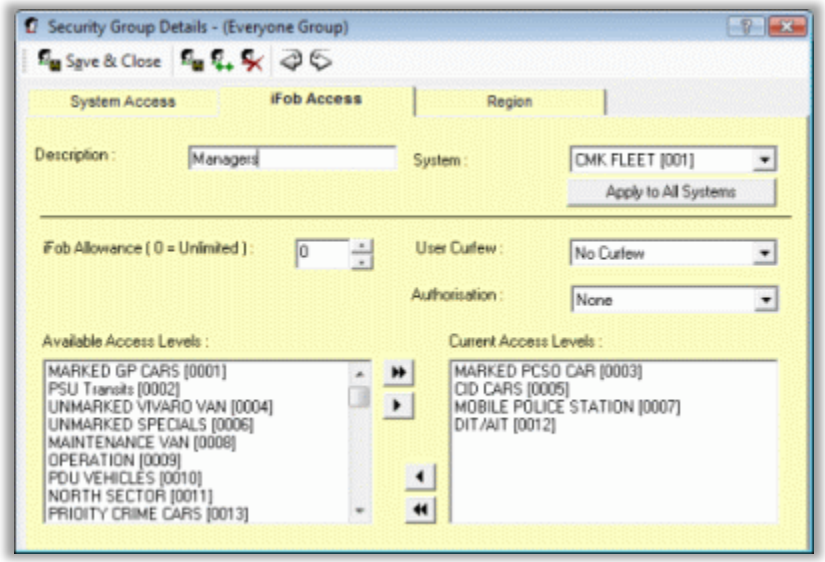


Here the group is allowed access from Monday 18:00 to Tuesday 05:00.



Here the group is allowed access from Monday 09:00 to Monday 17:30.

iFob Access



iFob Allowance

The iFob Allowance can restrict how many iFobs a user within the security group can take out at any one time. If set to 0 the user can take an unlimited number of iFobs that they have access to.

User curfew

The user curfew allows you to set a time for which the all the user's iFobs should be returned provided the iFob does not already have an iFob curfew set. For example, if you set the curfew to 17:30 all iFobs taken before this time will become overdue if not returned. This is a very powerful feature as it will highlight if keys are not returned at the end of a users shift.

Authorisation

Select **None**, to allow normal access to the system without the need for additional users to authorise.

Select either **1 Authoriser** or **2 Authorisers** to force either one or two users to authorise the access to the system.

For more details please refer to the System Authorisers section.

NOTE: This option will only show if the firmware of the selected system has X System Authorisers enabled.

Available / Current Access Levels

Each iFob in a system has an Access Level assigned to it. For a user to be able to take an iFob, the user must have that access in their Current Access Levels list.

For example, if an iFob has access level 021, and the user needs access to this iFob, they must have access level 021 in their Current Access Level list. If not, the user will not be able to take the iFob.

For more details please refer to the Access Levels section.

To **Add All** access levels to the Current List, click on 

To **Add Selected** access levels, select the appropriate levels from the Available List and click on 

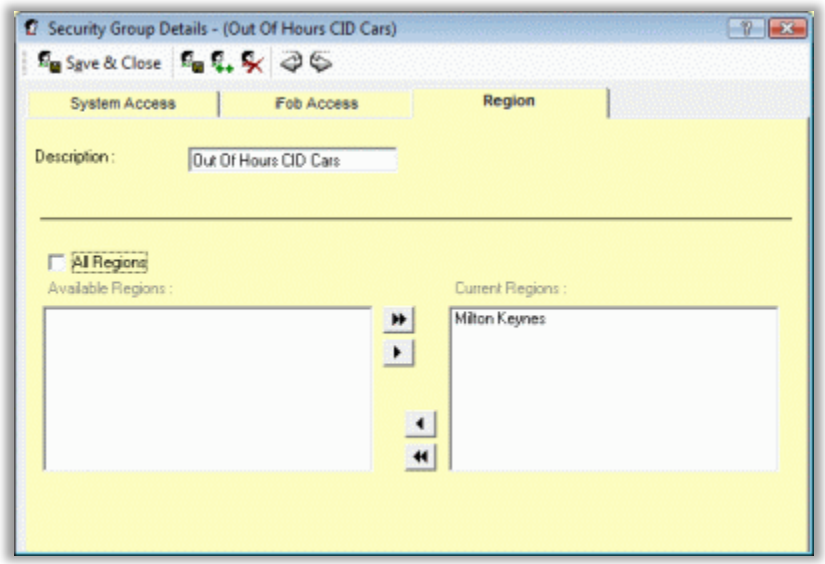
To **Remove Selected** access levels, select the levels from the Current List and click on 

To **Remove All** access levels from the Current List, click on 

Tips:

- To select a group of access levels, click on the first access level, hold down the Shift key and click on the last access level in the group.
- To select several individual access levels hold down the **Ctrl** key and clock on the access levels in the group.

Region



All Regions

Select if the Users within the security group are to have access to All Regions. Note this tick box is only available to edit if the logged in User is an All Regions Administrator.

Available / Current Regions

Each security group can belong to one or more Regions or No Regions. Note that only the Regions matching that of the logged in Traka32 Administrator will be displayed.

To **Add All** available regions to the Current List, click on 

To **Add Selected** regions, select the appropriate levels from the Available List and click on 

To **Remove Selected** regions, select the regions from the Current List and click on 

To **Remove All** regions from the Current List, click on 

Tips:

- To select a group of regions, click on the first region, hold down the Shift key and click on the last access level in the group.
- To select several individual regions hold down the **Ctrl** key and click on the access levels in the group.

4.9.2.3 ACCESS LEVEL NAMES

4.9.2.3.1 ACCESS LEVEL NAME OVERVIEW

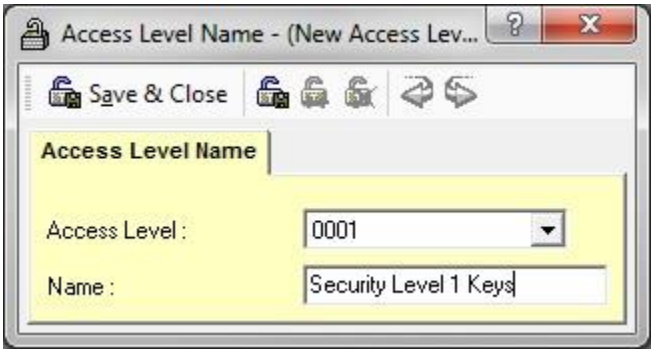
To make it easier to identify how the iFob Access Levels are assigned, it is possible to add a meaningful description against each access level.

These names are then used throughout the software wherever an Access Level needs to be selected or displayed, such as in the User Details and iFob Details.

Refer to the section Assigning an Access Level Name to learn how to assign, edit and delete Access Level names.

4.9.2.3.2 ASSIGNING AN ACCESS LEVEL NAME

1. To assign an Access Level with a name go to **File>Options>Access Level Names**.
2. Select **Options>Add New**.
3. Select the access level number that you wish to assign the name to.
4. Enter the name or description of the access level.



5. Click Save & Close.

To edit or delete an Access Level Name, simply highlight the Access level Name from the list and then select **Options**, followed by **Edit** or **Delete**.

4.9.2.4 REGIONS

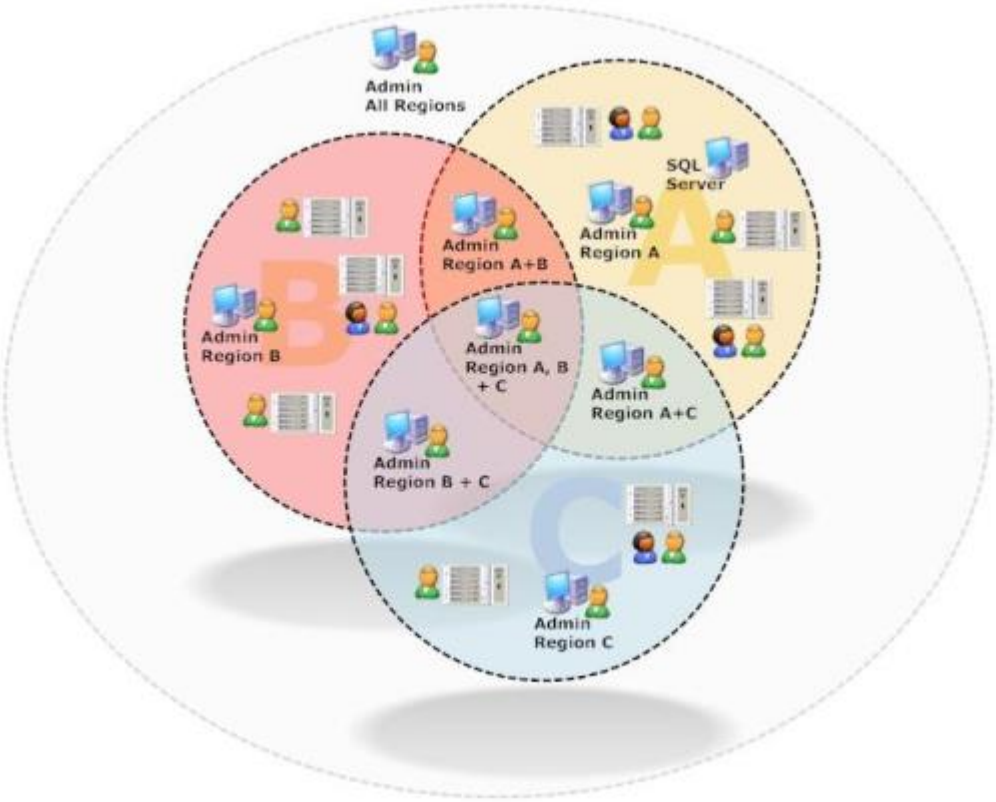
4.9.2.4.1 REGION OVERVIEW

Regions allows for Traka32 Administrators to see and access only the information from Systems, iFobs, Keys and Users within their specified region(s). In addition it allows Traka system cabinet users to only access the cabinets within their specified region(s).

From Traka32 Version 02.07.0001, Region functionality has been significantly improved to allow users to belong to **Multiple Regions**. Prior to Traka32 Version 02.07.0001, a user could only belong to a single region. Click here for a graphic of single regions operation.

Multiple Regions provides much increased flexibility for customers with more complex software and system access requirements. An example of where Multiple Regions maybe necessary, is where an organisation has many Traka systems spread geographically and each region has one or more Traka32 Administrators that are only responsible for maintaining their own Region(s). The Traka systems could be spread over a county, country, a continent or even all over the world using a Wide Area Network (WAN). In addition some organisations may choose to regionalise by department i.e. Sales, Finance, Engineering, where each department has a Traka32 Administrator who can only see Traka Systems and Users within their department(s).

Following is a graphic representing how a Multiple Region system may be defined.



It is important to note the following...

- A Traka system can only belong to a single Region. It has a fixed location.
- A Traka user may belong to Multiple Regions. Users are not fixed and may move around from region to region.

Coupled with the Multiple Security Groups (that can belong to Regions) facility, it makes for ultimate flexibility over your Traka system administration.

Defining Regions

Regions are defined within the Region Details tab of the Options window. Once the regions have been defined, each Traka system can be placed into a single region from the System Details window. When you allocate a system to a region, inherently all the iFobs and Keys within that system will also be allocated to that region.

Placing Users in Regions

When setting up users from the User Details window, the user can be placed into one or more regions. This inherently gives the user access to the Systems and users within their specified regions and automatically denies access to systems and users outside of their specified regions.

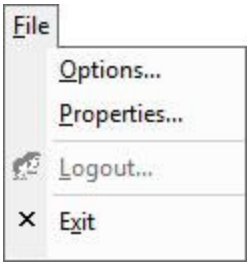
For overall administration of all regions, users can be setup with All Region access. Traka32 users with All Region access can administer systems in any region including systems with no defined region.

When a user logs into the Traka32 software, if they have been placed into one or more regions, the software will only show details of System, iFob, Keys, User and Reports for regions to which they belong.

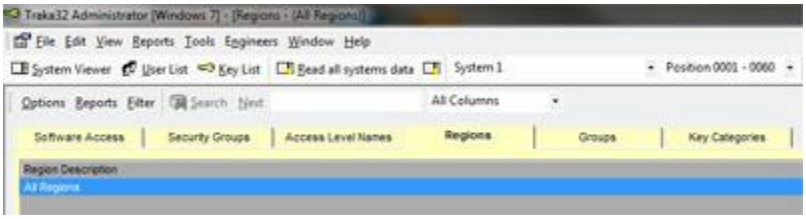
4.9.2.4.2 REGION DETAILS

The Region Details window allows you to add, edit and delete the Regions.

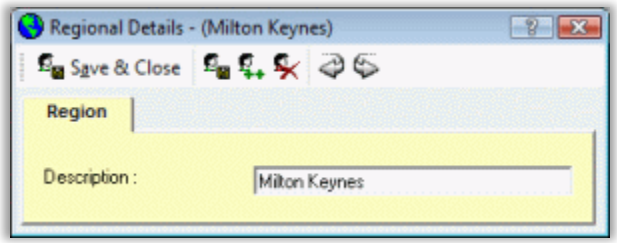
1. To create a new region click **File>Options**.



2. Select the Regions tab.



3. Click **Options>Add New** and the Region Details window will appear.



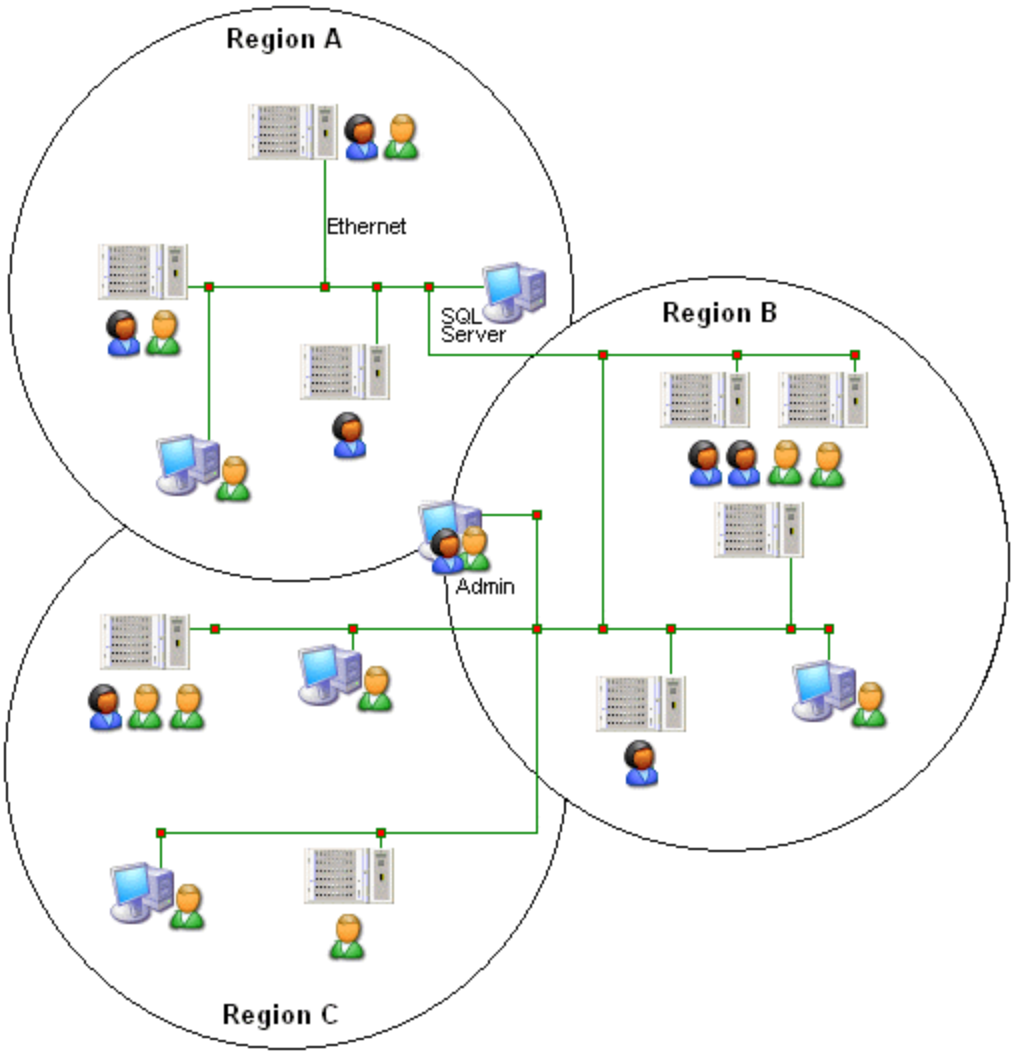
Description

Enter the name or description of the region.

4. Click Save & Close.

4.9.2.4.3 SINGLE REGIONS (TRAKA32 VERSION 02 .07.0000 AND PRIOR)

For customers using version 02.07.0000, the graphic below indicates how systems and users could only belong to a single Region.



4.9.2.5 USER GROUPS

4.9.2.5.1 USER GROUPS OVERVIEW

User Groups by their definition allow users to be separated into different groups. At present, a single user cannot belong to multiple groups. User Groups can simply be used for administration purposes to report on users in a specific groups.

When using the X iFob Authorisers or X System Authorisers option with the Force Authoriser from Different Group option enabled, this forces each Authoriser to be from a different User Group.

4.10 EDIT

4.10.1 CUT

Cut is used to Copy and 'remove' information from Traka32 and put it in the clipboard. This information can then be retrieved using the Paste option.

Cut works very similarly to delete with the exception that cut object(s) are placed in the clipboard and can be pasted elsewhere into Traka32 as normal OR into other Windows based applications like Word and Excel etc. If the object is a graphic, such as a graph, it will be pasted as a graphic. If it is a text string it will be pasted as text.

4.10.2 COPY

Copy is used to 'copy' information from Traka32 and put it in the clipboard. This information can then be retrieved using the Paste option.

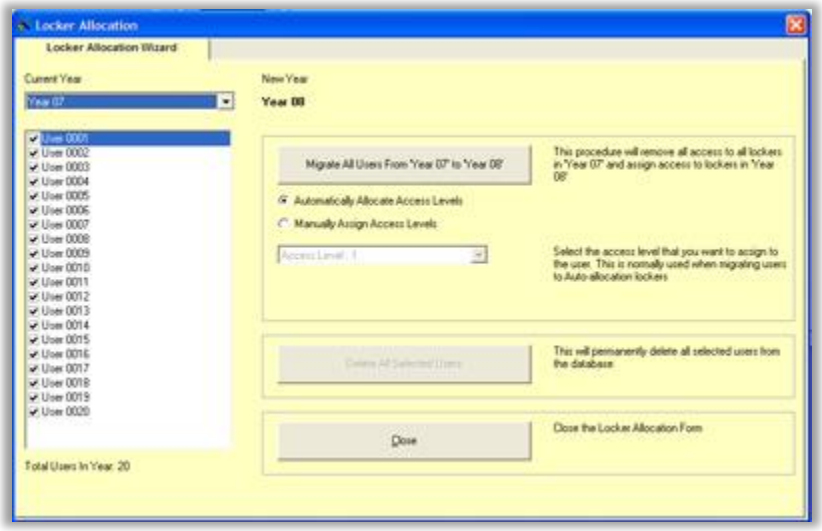
4.10.3 PASTE

Paste is used to 'paste' information which has been previously saved to the clipboard using the Cut or Copy options, or Text which has been saved to the clipboard from another application.

4.11 VIEW

4.11.1 LOCKER ALLOCATION WIZARD

A Locker Allocation Wizard has been written to help customers (primarily schools and academies) migrate all the students from one year to another. When the Migrate button is pressed all the selected users will have their access revoked in all lockers in their current year and then assigned to new lockers in the next year.

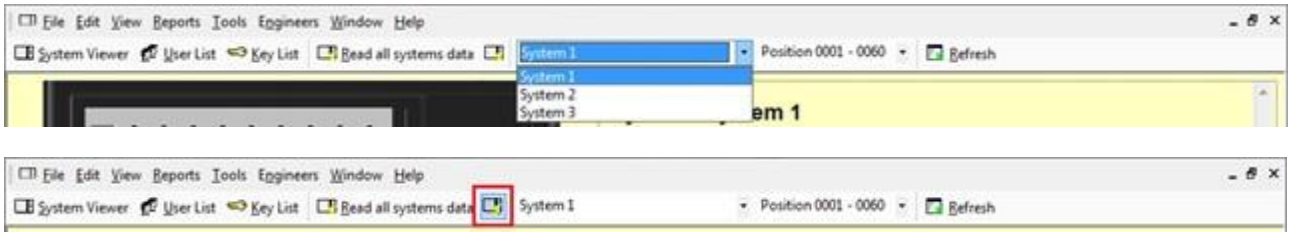


4.12 REPORTS

4.12.1 REPORTS OVERVIEW

A range of reports are available from the main **Reports** menu.

NOTE: To ensure the reports are up-to-date for a system, select a system from the drop down menu and then click on the 'Read Selected Systems Data' button.



Crystal Reports

If you are running your Traka System with a firmware version of 6.07.31 or above, the iFob and Key History will be recorded as events. An event can be any action performed on an iFob such as iFob Taken, iFob Returned, iFob Overdue etc. This method gives much greater flexibility so that all the relevant history such as alarm and transaction information is shown together in one report making it much easier to see what is going on.

Dock Door Reports

If you are using the Traka Dock Door hardware you can run reports that show information such as how many times the dock door has been opened while on override, how long the dock door was open for, events where the door has been raised using an iFob etc.

Transaction Reports

If you are running your Traka System with a firmware version of 6.07.30 or below the iFob and Key History will be recorded as transactions. A transaction is defined as an iFob being taken from and retuned to a Traka System. The iFob and Key Transaction history reports shows **Time Taken**, **Who took the iFob**, **Time Returned** and **Who returned the iFob** all in a single record along with any other relevant information such as Mileage, Fuel Level, Costs etc depending on what options are enabled in the firmware.

All the transaction reports can be filtered between user specified dates and also between systems. Please refer to the Filtering section for more details.

Key Access Report

The Key Access report can show all the keys and which users have access to them or all the users and which keys they can take.

Software Audit

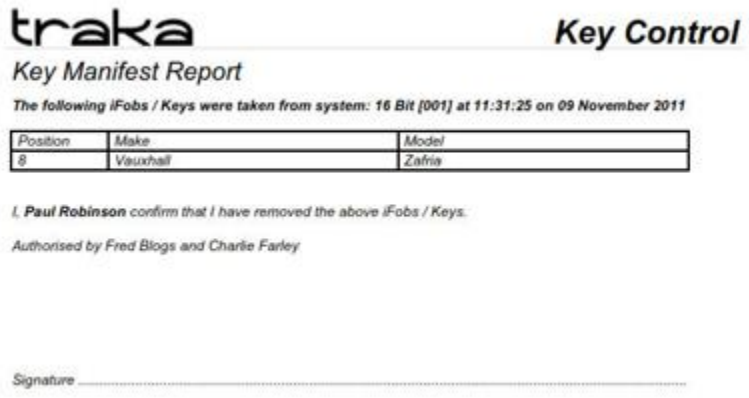
This report lists all the changes that have been made in the Traka32 software.

Advanced Software Audit

This report allows you to select various filters and parameters before listing all the changes that have been made in the Traka32 software.

Key Manifest Report

A new facility has been written to automatically print a report whenever a user logs out of a system, the report will show all the iFob's that have been removed with the first two Key detail fields. To enable this report you must have 'Auto Comms' and 'Nominate a PC' enabled on the desired system.



traka **Key Control**

Key Manifest Report

The following iFobs / Keys were taken from system: 16 Bit [001] at 11:31:25 on 09 November 2011

Position	Make	Model
8	Vauxhall	Zafira

*I, **Paul Robinson** confirm that I have removed the above iFobs / Keys.*

Authorised by Fred Blogs and Charlie Farley

Signature .....

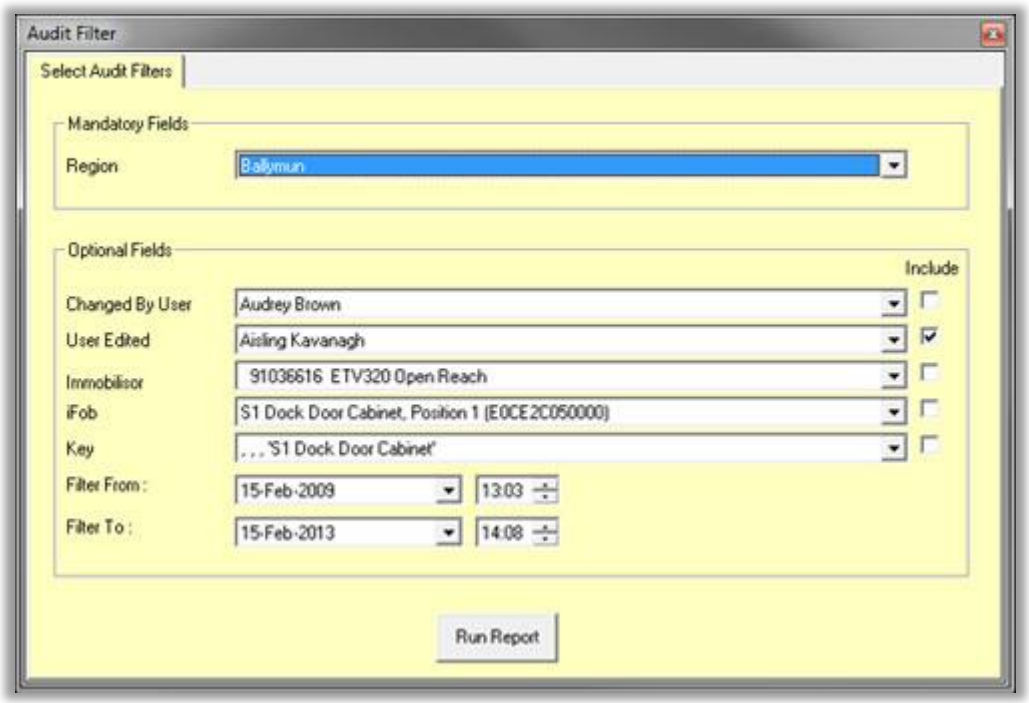
4.12.2 SOFTWARE AUDIT

This report lists all the changes that have been made in the Traka32 software.

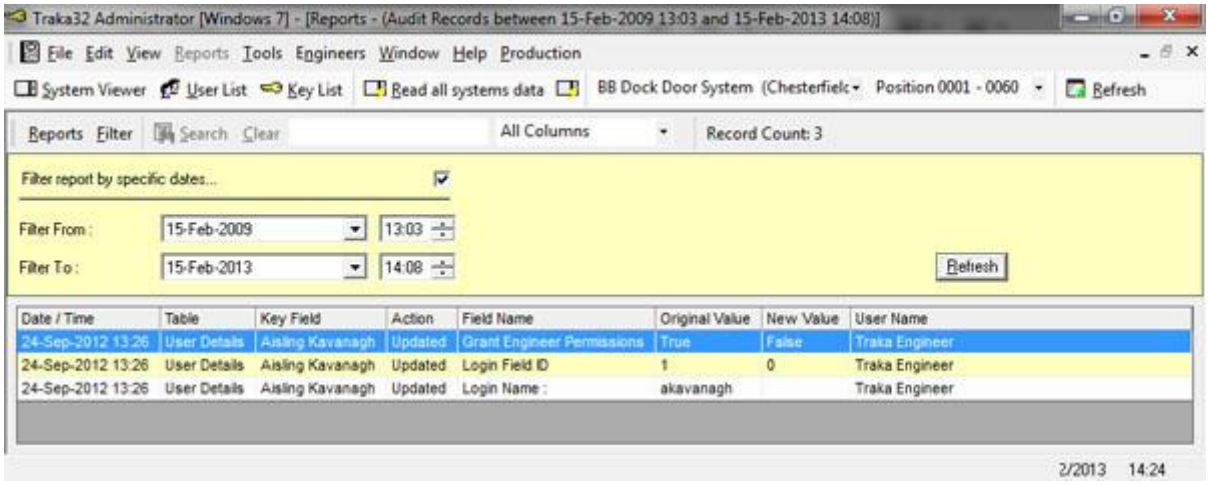
4.12.3 ADVANCED SOFTWARE AUDIT

This report, like the regular Software Audit, lists all the changes that have been made in the Traka32 software, however, the Advanced Audit allows you to select various filters and parameters to better define the results.

The Region field is a mandatory field that must have a region selected before continuing. The search can be filtered via optional fields such as iFob, Key, Immobilisor, a user whose details have been edited and a user who has edited another user's details.



Report results after filtering...



4.12.4 KEY ACCESS REPORT

Using Traka32 you can now generate a report that shows all the keys in the system/s and which user/s have access to them, or alliteratively you can view all the users and which keys they are authorised to take. When you run the report you can choose to run it on all systems or you can select an individual system. Also when you run the key report you can view the report on all keys or an individual key and the same you can view all users or an individual user.

You can view this report by selecting **Reports > Key Access Report**.

You will then be confronted by the 'Key Access Report' window, here you can select the details of the report System/s, User/s, Key/s etc.

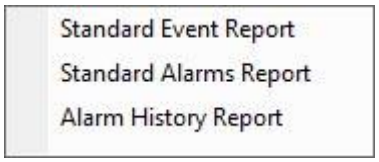
4.12.5 CRYSTAL REPORTS

4.12.5.1 CRYSTAL REPORTS

The new event reports in Traka32 designed and implemented using a package called Crystal Reports. Crystal Reports allows Traka and Customers to design new reports for Traka32 quickly and efficiently.

If you would like to design your own reports for Traka32, please contact us and we can supply details on the Crystal Reports packages available.

4.12.5.2 CRYSTAL REPORTS - EVENTS



Standard Event Report

This report lists all the events for every System and iFob.

Standard Alarm Report

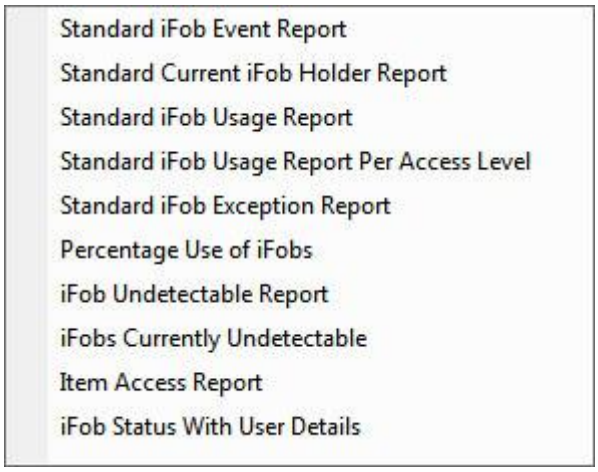
This report lists all the events filtered by alarm type for every System and iFob.

For a full list of Alarm and Event types please refer to the Alarm & Event Types section.

Alarm History Report

This report will display the alarms that have been cleared at Traka32 along with any notes that have been logged against them. If no notes are logged against an alarm the heading 'Notes not Entered' will be above the current alarms.

4.12.5.3 CRYSTAL REPORTS - IFOBS



Standard iFob Event Report

This report lists all the events for every iFob.

Standard Current iFob Holder Report

This report lists all the current holders of any iFobs that are currently out of a system.

This report also shows any iFobs that are out under a curfew, what time they are due back and if they are overdue.

NOTE: The curfew status has been added to the Current iFob Holder Report so you can filter the reports to only show iFobs that are currently under or past their curfew.

Standard iFob Usage Reports

This report and chart details the number of days, hours or minutes the iFobs have been out of the system.

Standard iFob Usage Reports Per Access Level

This report and chart details the number of days, hours or minutes the iFobs with a specific access level have been out of the system.

Standard iFob Exception Report

This report lists events where the following exceptions have occurred.

1. The user who took the iFob is not the same as the user who put it back.

Percentage Use of iFobs

The report and chart details the percentage of iFob that were out of the system on the hour every hour over a specified period.

iFob Undetectable report

This Crystal Report has been written to summarise the iFob Undetectable events. A date range can be selected and the report can be run for all cabinets or a selected cabinet.

iFobs Currently Undetectable

The iFob Currently Undetectable Report can show what iFobs are undetectable at the time the report is run.

Item Access Report

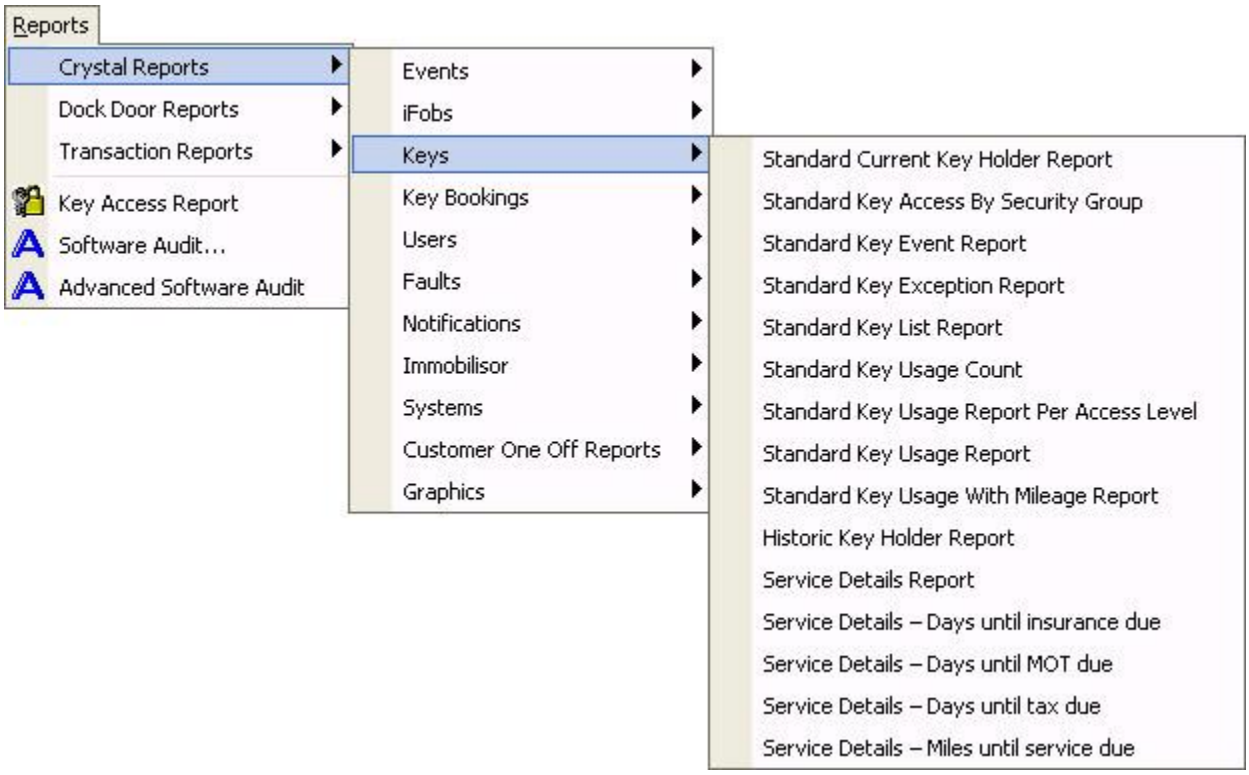
This report displays all the iFob or locker positions in the system and who can access them.

iFob Status with User Details

This report will list all the iFobs along with their status and various user details for the current and previous owner.

For a full list of Alarm and Event types please refer to the Alarm & Event Types section.

4.12.5.4 CRYSTAL REPORTS - KEYS



Standard Current Key Holder Report

This report lists all the current holders of any Keys that are currently out of a system.

This report also shows any Keys that are out under a curfew, what time they are due back and if they are overdue.

NOTE: The curfew status has been added to the Current Key Holder Report so you can filter the reports to only show keys that are currently under or past their curfew.

Standard Key Access By Security Group

This report will display all the iFobs and keys that a user would be granted access to if they were assigned to the security group.

Standard Key Event Report

This report lists all the events for every Key.

Standard Key Exception Report

This report lists events where the following exceptions have occurred...

1. The user who took the key is not the same as the user who put it back.

This report and chart details the number of days, hours or minutes the keys have been out of the system.

Standard Key List Report

This report generates a list of the current Keys in the system and their information such as Make, Model etc

Standard Key Usage Count

This report will list the number of times that a key has been removed and returned to a system.

Standard Key Usage Report Per Access Level

This report and chart details the number of days, hours or minutes the keys with a specific iFob access level have been out of the system.

Standard Key Usage with Mileage Report

This report and chart details the number of days, hours or minutes the keys have been out of the system and the Mileage associated with each key.

For a full list of Alarm and Event types please refer to the Alarm & Event Types section.

Service Details Report

This report combines all of the reports below to provide service details on the selected keys.

Service Details - Insurance Date

This report informs you when the insurance on the selected key is due to run out.

Service Details - MOT Due Date

This report informs you when the MOT on the selected key is due to run out.

Service Details - Tax Due Date

This report informs you when the Tax on the selected key is due to run out.

Service Details - Miles Until Service

This report informs you how many miles you have left before the vehicle is due for service.

4.12.5.5 CRYSTAL REPORTS - KEY BOOKINGS

Two new reports have been added to Traka32, one is for normal fixed return Key Booking and the other if for Key Booking By Reference.

NOTE: In software version 02.10.0006 these reports are only visible for SQL Server and Access databases.

Key Booking By Reference

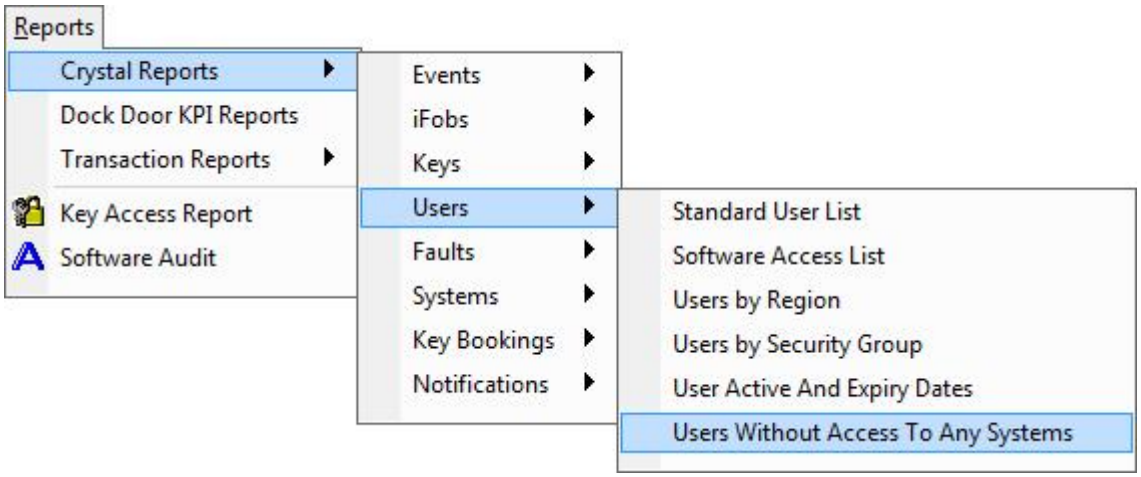
This report lists all the events for every Key that has been booked using the optional feature 'Key Booking by Reference'.

NOTE: This report can only be used if your system has the optional feature 'Key Booking by Reference'.

Key Booking History

This report lists the history of every completed booking.

4.12.5.6 CRYSTAL REPORTS - USERS



Standard User List

This report lists all of the users in the Traka database along with their User details i.e Staff Number, Position, Tel, Email etc.

Software Access List

This report lists all of the users that have access to the Traka 32 software along with their User details i.e Staff Number, Position, Tel, Email etc.

User by Region

This report lists all of the users and what regions they belong too along with their User details i.e Staff Number, Position, Tel, Email etc.

User by Security Group

This report lists all of the users and what security groups they belong too along with their User details i.e Staff Number, Position, Tel, Email etc.

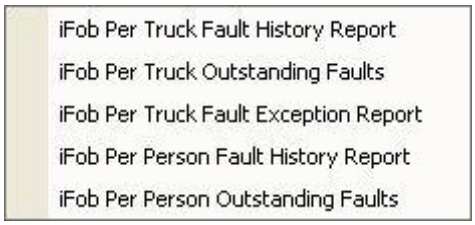
User Active And Expiry Dates

This report listall of the users that are currently active and shows when their profile expires, along with their User details i.e Staff Number, Position, Tel, Email etc.

User Without Access To Any System

This report has been written to list all users that do not have access to any system in your database.

4.12.5.7 CRYSTAL REPORTS - FAULTS



iFob Per Truck Fault History Report

This report lists all the recorded faults, when they occurred, who logged the fault, when the fault was cleared and who cleared the fault.

iFob Per Truck Outstanding Faults

This report lists all the current faults that are outstanding on any of the iFobs.

iFob Per Truck Fault Exception Report

This report lists fault history where the following exceptions have occurred...

1. The user who returned the iFob did not Accept the vehicle and did not record a Fault against the vehicle.

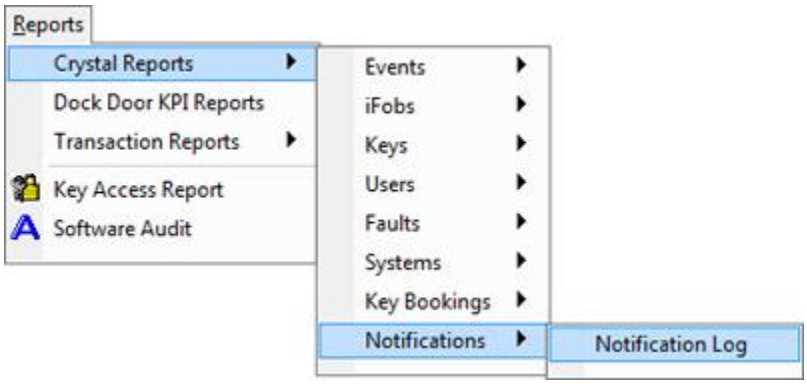
iFob Per Person Fault History Report

This report gives provides you with a history of faults that have been cleared.

iFob Per Person Outstanding Faults

This report gives provides you with a list of faults that have been logged but haven't been cleared.

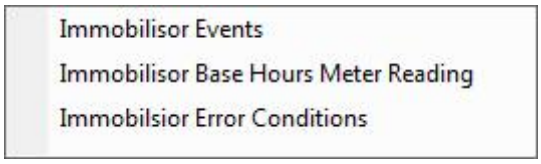
4.12.5.8 CRYSTAL REPORTS - NOTIFICATIONS



Notification Log

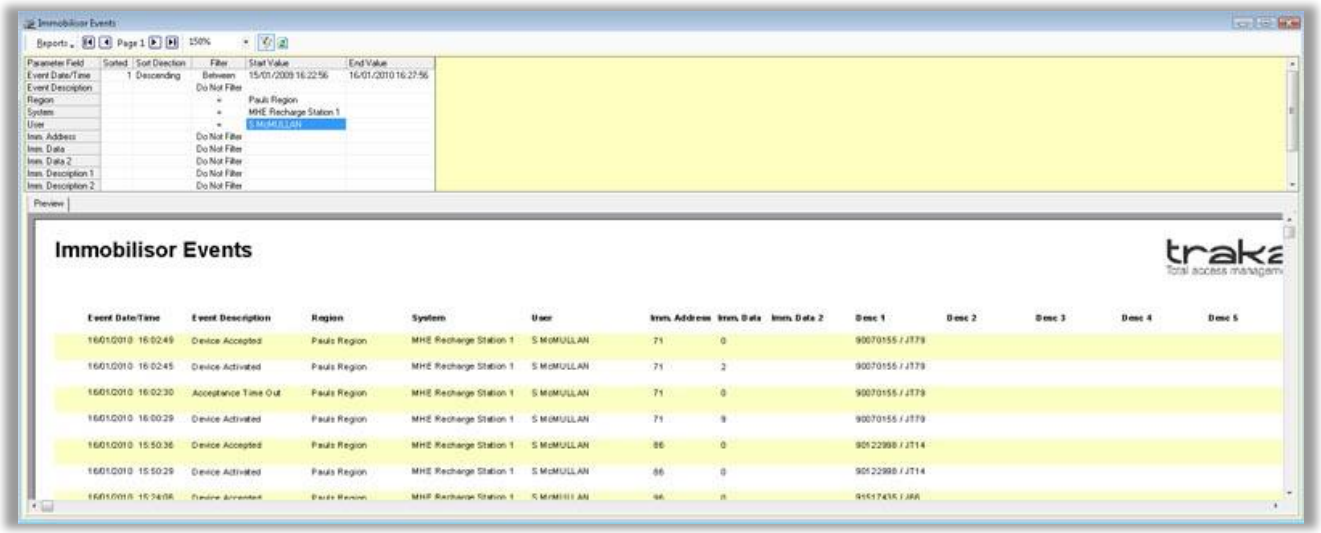
This report shows which Email Notifications were sent when the events were downloaded. The report shows details of the Notification Template, the Notification Rule and a status showing whether or not the email was sent successfully.

4.12.5.9 CRYSTAL REPORTS - IMMOBILISOR



Immobilisor Events

A Crystal Report is now available which shows all events generated by the Immobilisor, e.g. Device Activated, Device Accepted etc. You can filter this report by Region, System, or User.



Immobilisor Base Hours Meter Reader

This report shows the Immobilisor Base hour's usage for trucks.

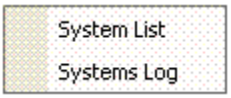
Immobilisor Error Conditions

This report shows lists all of the error conditions each Immobilisor in the database has currently acquired.

Immobilisor User Exception Report

This report will display truck users that have driven more than one truck in a 24 hour period.

4.12.5.10 CRYSTAL REPORTS - SYSTEMS



System List

This report lists all of the systems in the Traka database along with their System Details i.e System Title, Serial No., Firmware Version, Region etc.

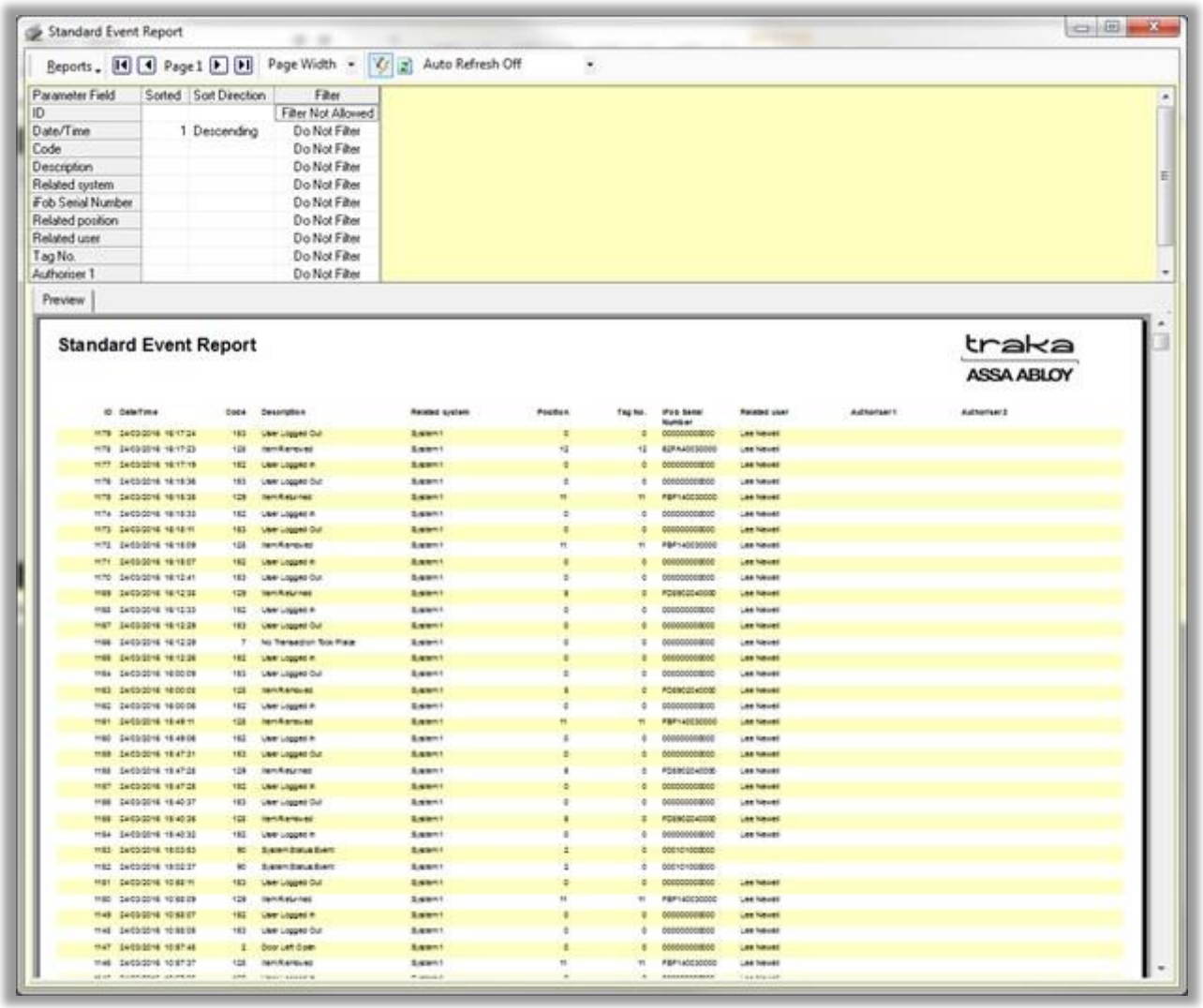
System Log

This report lists the details of which users have logged into Traka32.

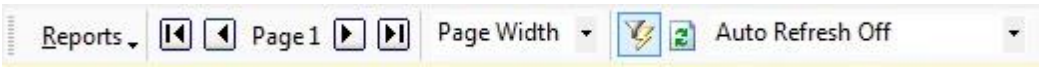
Systems Log

Date/Time	Workstation	User Name	Event Description
16 March 2010 10:51:22	VM-PR-WINXP	Fernando	Traka32 Logged On As Traka Engineer
16 March 2010 10:50:57	VM-PR-WINXP	Fernando	Traka32 Logged Off By Traka Engineer
16 March 2010 10:35:36	VM-PR-WINXP	Fernando	Traka32 Logged On As Traka Engineer

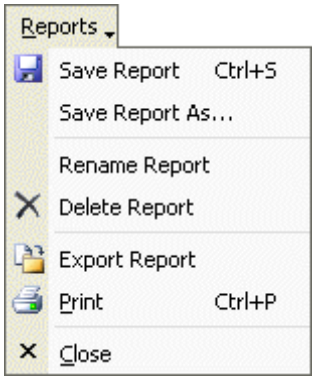
4.12.5.11 EVENT REPORT VIEWER



Toolbar



Reports Menu



Save Report

When a report has been filtered and sorted it can be saved as a custom report. Simple give the report a name and it will appear in the main Reports menu. All the filter parameters will be saved with the report along with the name.

Save Report As

A saved report can be customised further and can be saved under a different name.

Reme Report

A saved report can be renamed.

Delete Report

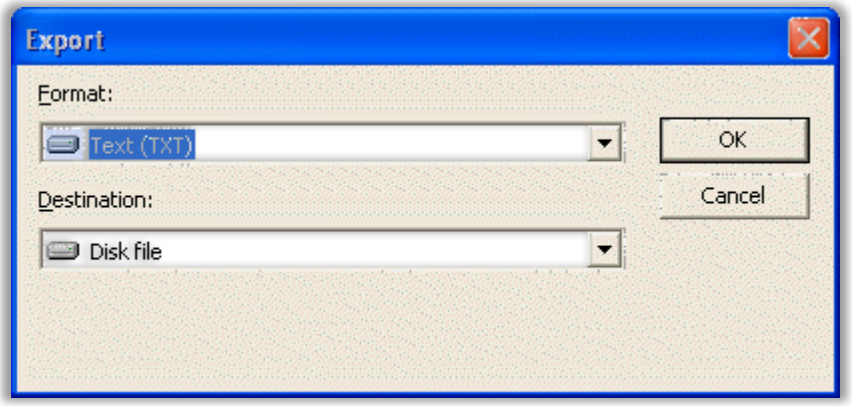
A saved report can be deleted.

Export Report

Any report can be exported to other applications including...

- Adobe Acrobat (PDF)
- Crystal reports (RPT)
- HTML 3.2 & 4.0
- Microsoft Excel
- Microsoft Word
- Rich text Format (RTF)
- Tab Separated Text (TTX)
- Text (TXT)

Simply pick the application, pick whether to save it as a file or load directly into the application and click on OK.



Print

Any report any be printed. The main Preview is shown at all times.

Close

Close the report viewer.

Page Navigator

Click the relevant arrow to move from page to page on the report.

Zoom

Click to zoom in or out of a page.

Show / Hide Filter

The filter at the top of the screen can be hidden so that he Preview is easier to see. Click the filter button again to show the filter.

Refresh

Whenever a parameter is changed, click the Refresh button to refresh the report with the new parameters.

Auto Refresh

Some reports can be set to Auto Refresh. The options available in the dropdown allow you to specify an Auto Refresh every 5 seconds, or every minute. Upon each refresh, the Event Reports will automatically adjust the 'End Value' so that the latest events will always be included.

Parameters Table

The data within the report can be filtered as required.

Parameter Field	Sorted	Sort Direction	Filter	Start Value	End Value
ID			Filter Not Allowed		
Date/time			Between	19/12/2005 12:00 AM	19/12/2005 11:59 PM
Code			=		
Description			Do Not Filter		
Related system	1	Ascending	=	Traka HQ Reception	
iFob Serial Number			Do Not Filter		
Related position	2	Ascending	Do Not Filter		
Related user			Do Not Filter		

Sorted

A report can be sorted on one or more fields. Select a field to sort on and set the Sorted order. Repeat this for each field to sort on.

Sort Direction

For each field that has been selected to sort on, select the direction of the sort.

Filter

Each field can be filtered. This allows reports to be narrowed down to the exact requirements. For each field the following filter can be applied...

Do Not Filter	Not filter is applied to the field.
=	Equals to a specific value. Select a **Start Value** for the filter.
<	Less than a specific value. Select a **Start Value** for the filter.
>	Greater than a specific value. Select a **Start Value** for the filter.
Between	Between two specific values. Select a **Start Value** and an **End Value** for the filter.
<>	Outside a specific value. Select a **Start Value** and an **End Value** for the filter.

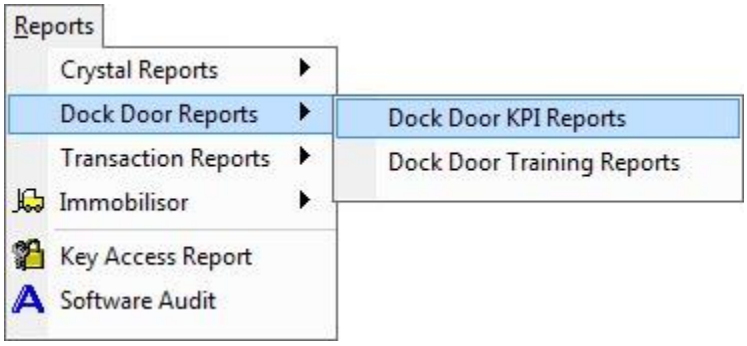
Refresh

When the sort and filter parameters have been selected, click the Refresh button to apply the filter to the report. 

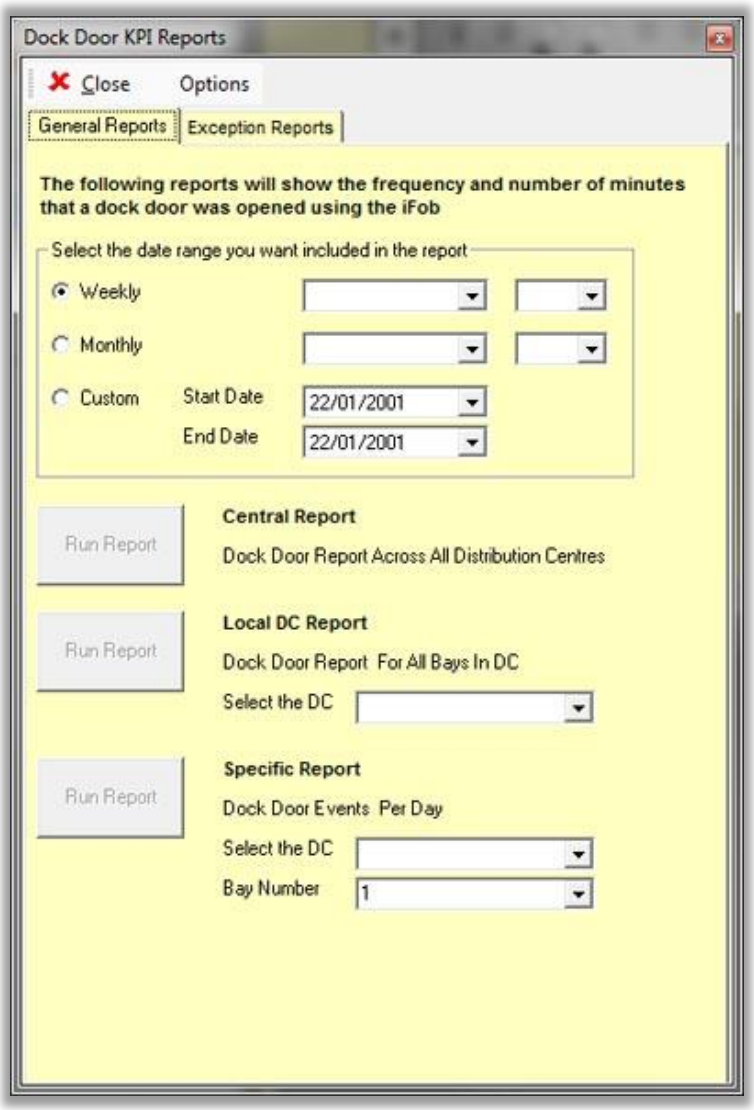
4.12.6 DOCK DOOR REPORTS

4.12.6.1 DOCK DOOR KPI REPORTS

The Dock Door report can show normal events where the door has been raised using an iFob as well as events when the 'Override' mode has been used, this will show how long the doors have been up for in minutes. You can also see how many times and for how long the dock door has been opened while on override.

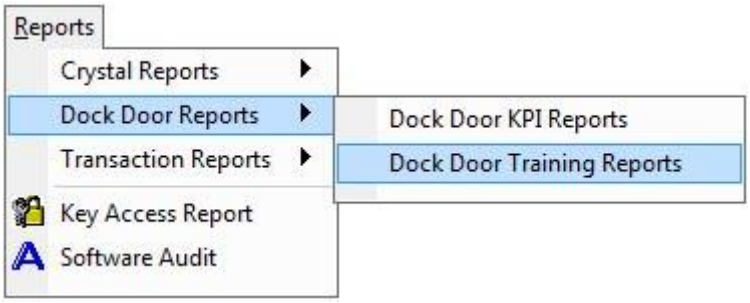


The user can filter the results by picking a week number, month and year or specific date ranges and then clicking 'Run Report'.

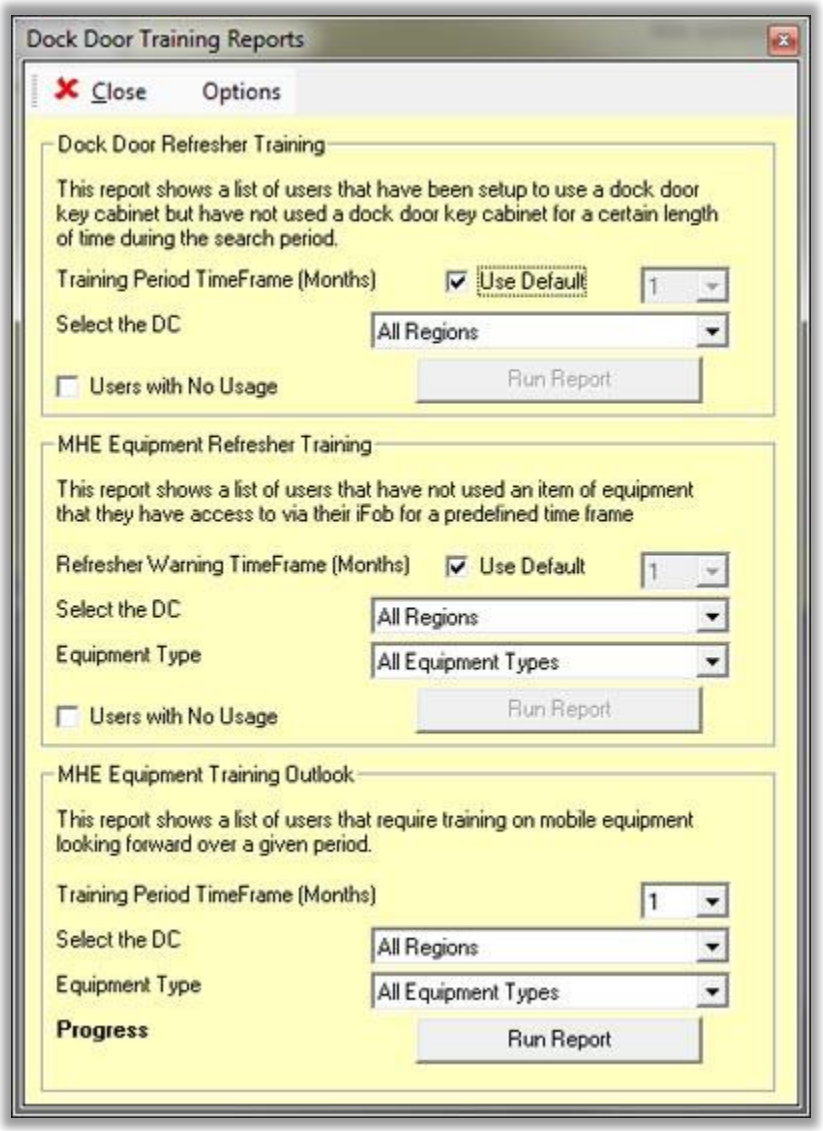


4.12.6.2 DOCK DOOR TRAINING REPORTS

This report allows you to view different users and their level of use/access regarding the Dock Door.

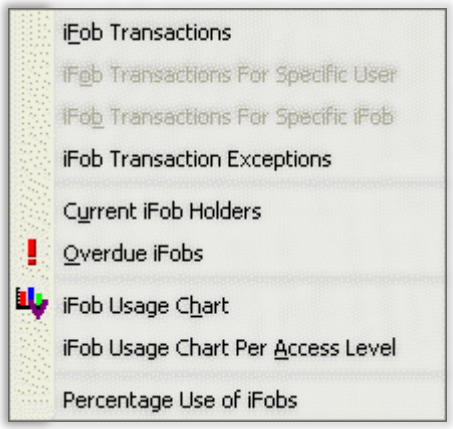


Please see below for descriptions of each report.



4.12.7 TRANSACTION REPORTS

4.12.7.1 TRANSACTION REPORTS - IFOBS



iFob Transactions

This report lists all the transactions of every iFob.

iFob Transaction for Specific User

This report is the same as the iFob transactions report but can be filtered down to a specific user.

To highlight this option, open the User List by clicking on 

, select the user in question from the list and click on Reports, iFobs, iFob Transactions For 'xxxx'.

iFob Transactions for Specific iFob

This report is the same as the iFob transactions report but can be filtered down to a specific iFob.

To highlight this option, open the iFob List by clicking on **View**, **iFob List**, select the iFob in question from the list and click on Reports, iFobs, iFob Transactions For 'xxxx'.

iFob Transaction Exceptions

This report lists transactions where the following exceptions have occurred...

1. The user who took the iFob is not the same as the user who put it back.

Current iFob Holders

This report lists all the current holders of any iFobs that are currently out of the system.

Overdue iFobs

This report lists any iFobs that are out of the system, are under a curfew and a overdue for return.

iFob Usage Chart

This report and chart details the number of days, hours or minutes the iFobs have been out of the system.

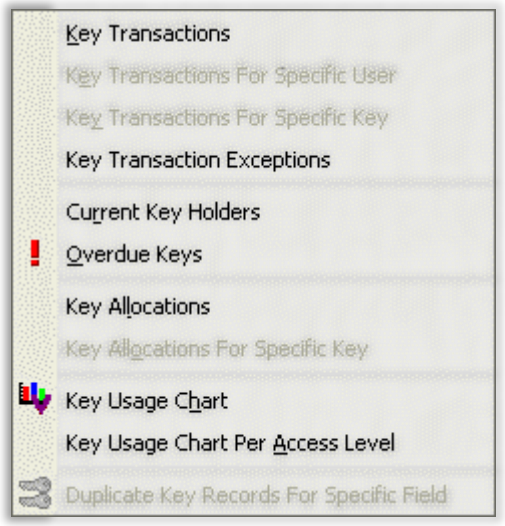
iFob Usage Chart per Access Level

This report and chart details the number of days, hours or minutes the iFobs with a specific access level have been out of the system.

Percentage Use of iFobs

The report and chart details the percentage of iFob that were out of the system on the hour every hour over a specified period.

4.12.7.2 TRANSACTION REPORTS - KEYS



Key Transactions

This report lists all the transactions of every key.

Key Transaction for Specific User

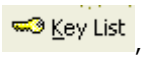
This report is the same as the key transactions report but can be filtered down to a specific user.

To highlight this option, open the User List by clicking on 

, select the user in question from the list and click on Reports, Keys, and Key Transactions For 'xxxx'.

Key Transactions for Specific Key

This report is the same as the key transactions report but can be filtered down to a specific key.

To highlight this option, open the Key List by clicking on 

, select the key in question from the list and click on Reports, Keys, and Key Transactions For 'xxxx'.

Key Transaction Exceptions

This report lists transactions where the following exceptions have occurred...

1. The user who took the key is not the same as the user who put it back.

Current Key Holders

This report lists all the current holders of any keys that are currently out of the system.

Overdue Keys

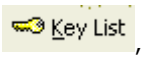
This report lists any keys that are out of the system, are under a curfew and are overdue for return.

Key Allocations

This report lists all the allocations of a key such as when the key was added to the system, when it was edited or moved from iFob to iFob and when it was removed from an iFob and who by.

Key Allocations for Specific Key

This report is the same as the key allocations report but can be filtered down to a specific key.

To highlight this option, open the Key List by clicking on 

, select the key in question from the list and click on Reports, Keys, and Key Allocations For 'xxxx'.

Key Usage Chart

This report and chart details the number of days, hours or minutes the keys have been out of the system.

TIP: The headings along the x axis of the chart can be altered by selecting the one of the key detail columns in the report.

Key Usage Chart per Access Level

This report and chart details the number of days, hours or minutes the keys with a specific iFob access level have been out of the system.

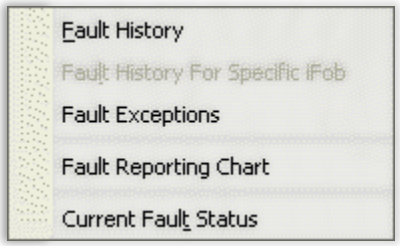
Duplicate Key Records for Specific Key

This report will list all the duplications within the key records for a specific field.

To highlight this option, open the Key List by clicking on 

; select the field heading in question from the list and click on Reports, Keys, Duplicate Key Records For 'xxxx' Field.

4.12.7.3 TRANSACTION REPORTS - FAULTS



Fault History

This report lists all the recorded faults, when they occurred, who logged the fault, when the fault was cleared and who cleared the fault.

Fault History for Specific iFob

This report is the same as the fault history report but can be filtered down to a specific iFob.

To highlight this option, open the iFob List by clicking on **View**, **iFob List**, select the iFob in question from the list and click on Reports, iFobs, Fault History For 'xxxx'.

Fault Exceptions

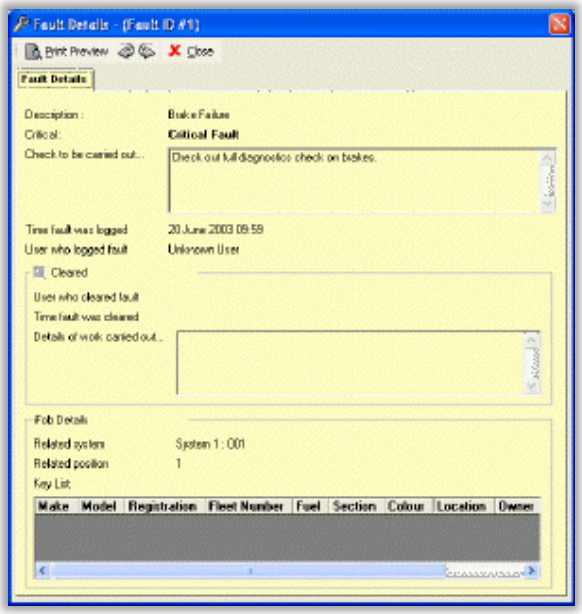
This report lists fault history where the following exceptions have occurred...

1. The user who returned the iFob did not Accept the vehicle and did not record a Fault against the vehicle.

Current Fault Status

This report lists all the current faults that are outstanding on any of the iFobs.

When viewing any Fault report, it is possible to expand the information recorded about the fault simply by double clicking on the fault in question.



4.12.7.4 TRANSACTION REPORTS - IMMOBILISOR

Immobilisor Events

This report lists all the events for each Immobilisor.

Immobilisor Events for Specific User

This report is the same as Immobilisor Events report but can be filtered down to a specific user.

To highlight this option, open the User List by clicking on 

, select the user in question from the list and click on Reports, Immobilisor, and Immobilisor Events for 'xxxx'.

Immobilisor Events for Specific Immobilisor

This report is the same as Immobilisor Events report but can be filtered down to a specific Immobilisor.

To highlight this option, open the Immobilisor List by clicking on **View**, **Immobilisor List**, select the Immobilisor in question from the list and click on Reports, Immobilisor, and Immobilisor Events for 'xxxx'.

Immobilisor Usage Chart

This report and chart details the number of days, hours or minutes the Immobilisors have been activated.

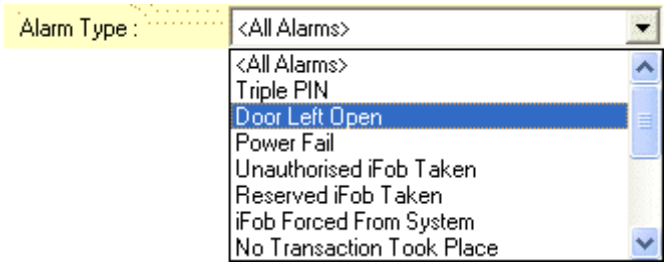
4.12.7.5 MICRO TRAKA

User History

This report lists all the activities performed at each Micro Traka system.

4.12.7.6TRANSACTION REPORTS - ALARMS

This report lists all of the alarms that have occurred. An alarm is recorded if the system is used incorrectly or if something untoward has happened. The alarm report may be filtered by alarm type by selecting the appropriate alarm from the filter list.



For a full list of Alarm types please refer to the Alarm & Event Types section.

4.13 TOOLS

4.13.1 FIRMWARE UPGRADE

The firmware of the Traka Systems can be updated very easily using the Firmware Upgrade Wizard in conjunction with an upgrade file supplied by Traka. Upgrading the firmware will allow users to benefit from all the latest features available without changing any hardware.

The firmware upgrades for the 8bit and 16bit Traka Systems are very similar however there are some slight differences. Please refer to the relevant 8bit Firmware Upgrade or 16bit Firmware Upgrade sections for assistance with upgrading.

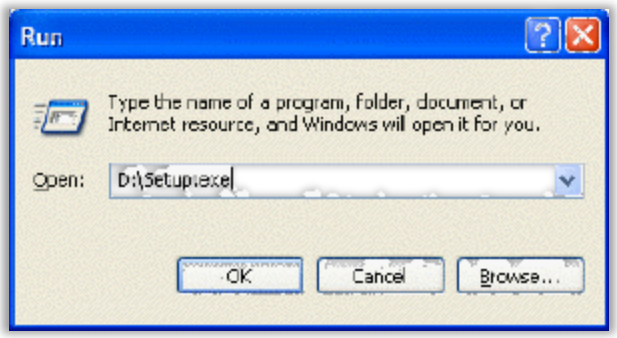
4.13.2 SOFTWARE UPGRADE

NOTE: This utility is still under development.

To obtain an upgrade of the Traka32 software, please contact your supplier or visit our web site www.traka.com and click on the **support** link. To upgrade the software follow the instructions below.

1. Insert the Traka32 CD into the CD-ROM drive.
2. After a few seconds the set-up wizard should run automatically.

   If not, click on Start > Run and type D:\Setup.exe followed by Enter
   (replacing the D with the appropriate CD-ROM letter)



3. The set-up wizard will guide you through the installation.

4.13.3 CONFIGURE SYSTEMS

Please refer to the System Settings section.

4.13.4 AUTO SYNCHRONISATION ALL SYSTEMS

Select this option to automatically keep the software and hardware synchronised whenever a change is made in the software to User, iFob or Key details.

Clear this option if you wish to make changes to the database without synchronisation with the Traka system. This is useful if you have a large number of changes to make or if you are setting up a new database without the Traka System.

This option applies to All Systems and is selected by default whenever Traka32 is loaded. If you want to set this option on specific systems only, this can be done from the System Viewer's, System menu.

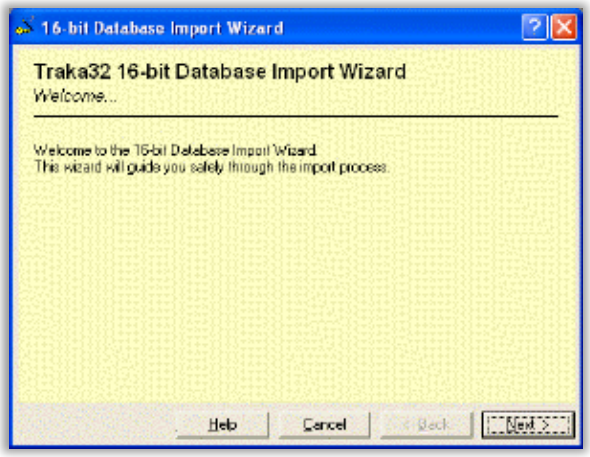
Clearing this option only lasts for the time the user is logged in to Traka32, once a user logs out and back in again the option will by default be enabled. There is an option 'Preserve the State of Auto-Comms Online Mode' that whilst enabled, will keep auto synchronisation disabled. For information on how to enable this option please view the Comms section of the Properties topic.

4.13.5 SYNCHRONISE ALL USERS TO ALL SYSTEMS

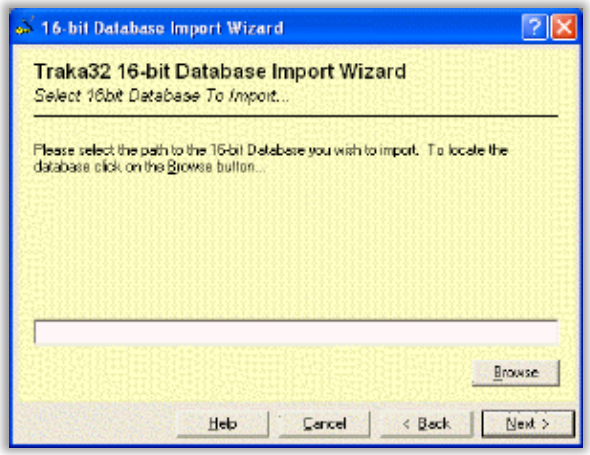
This synchronises all the user records in the database with the all the systems. If you want to synchronise all the user records in the database with a specific system, this can be done from the System Viewer's, System menu.

4.13.6 IMPORT 16BIT DATABASE

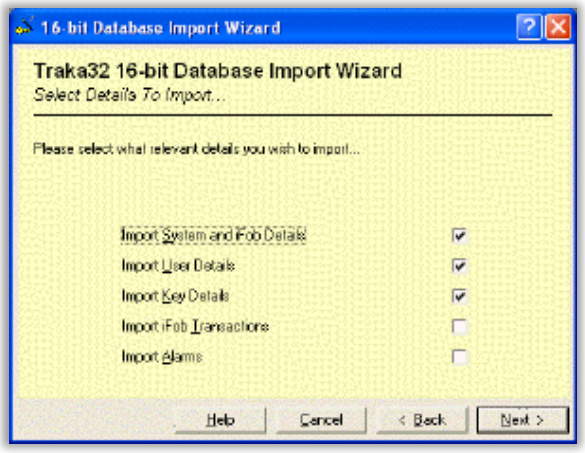
1. To enable this option, close any open windows within the software so you have a grey screen.
2. Click on **Tools** followed by **Import 16bit Database** from the main menu.



3. Click on **Next**



4. Select the path to the 16bit database that you wish to import. To search for the database file simply click on the **Browse** button.
5. When you have selected the path, click on **Next**



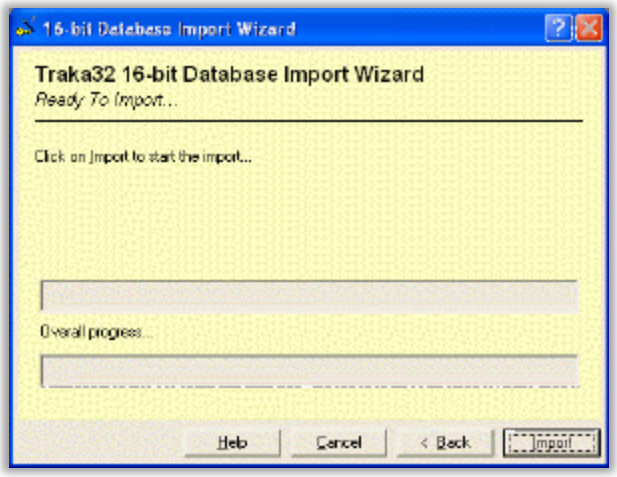
6. Select the information that you wish to import from the database.

    - Import System and iFob Details
    - Import User Details
    - Import Key Details
    - Import iFob Transactions
    - Import Alarms

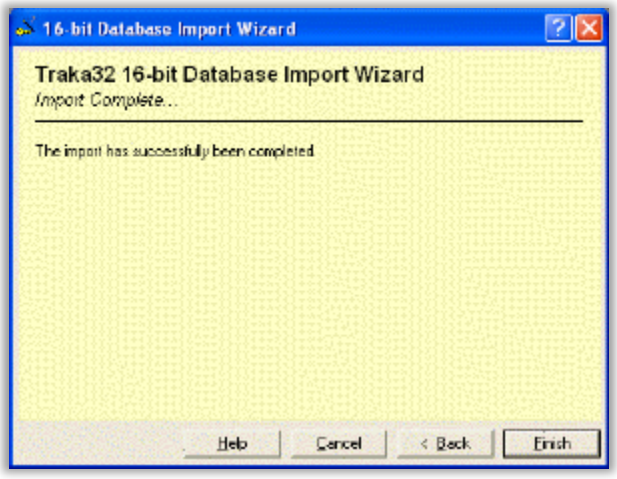
NOTE: Importing the iFob Transactions and/or Alarms will take a long time depending on how many transactions and alarms there are to import. On a slow PC this could take at least an hour to import.

7. When you have selected the information to import, click on **Next**

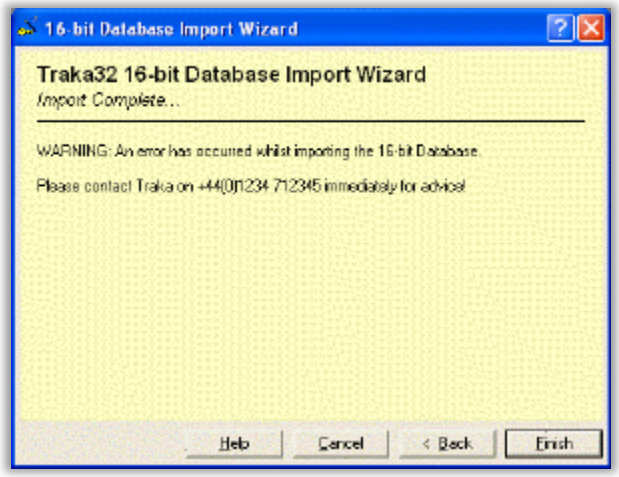
8. When you are happy click on **Import**



9. Provided the import completed successfully, click on **Finish**



What if the upgrade goes wrong?



- It is possible that the database is corrupt. Open the database using the old **Traka16** software, **Enable the Admin** menu from the File menu, and click on the **Admin** menu followed by **Tools, Database Tools, and Repair Database**. Once repaired try the import again.

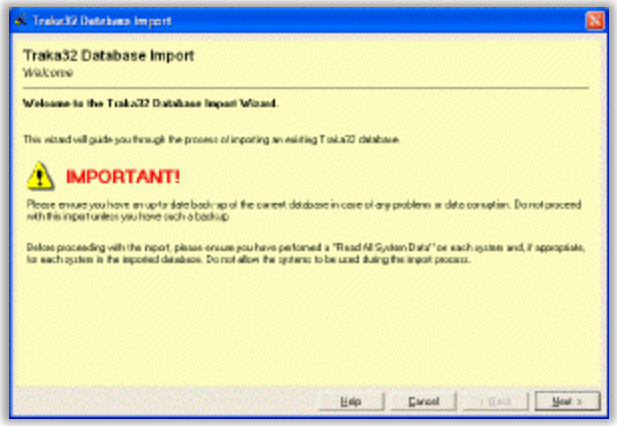
- If an error has occurred during the upgrade that is not covered, please contact one of our engineers on + 44 (0) 1234 712345 immediately for advice.

4.13.7 IMPORT 32BIT DATABASE

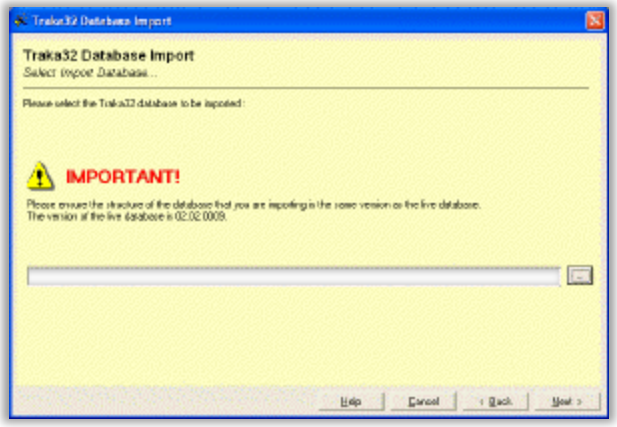
Before You Start

The version of the Traka32 software that is used with the database you wish to import MUST be the exact same version as that being used with the current database. If the versions are different, upgrade the Traka32 software that is used with the database you wish to import to the same version as going to be used with the current database. You must also run the Traka32 software so the database checks are made. This is to ensure the database structures are the same.

1. To enable this option, close any open windows within the software so you have a grey screen.
2. Click on **Tools** followed by **Import 32bit Database** from the main menu.



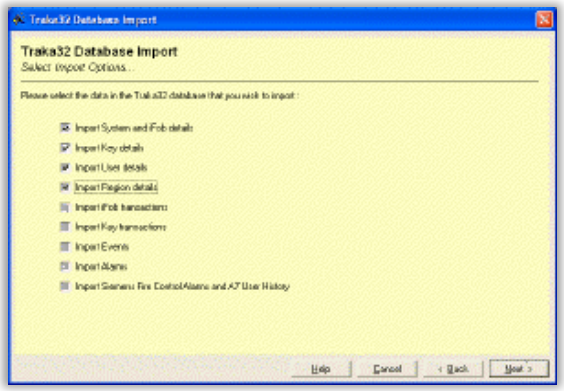
3. Click on **Next**.



4. Select the path to the 32bit database that you wish to import. To search for the database simply click on the **...** button.

   NOTE: Please ensure the Traka32 software version that is used with the database you are importing matches the Traka32 version you are currently running (see note above).

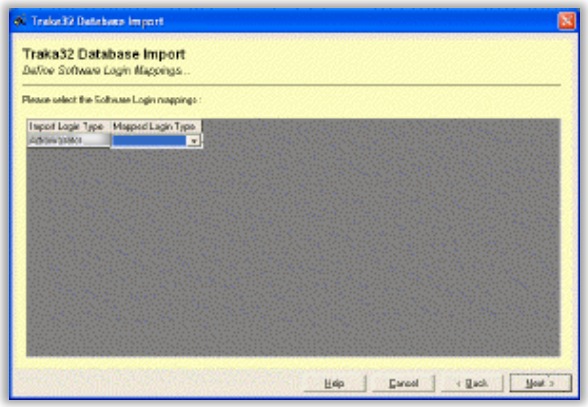
5. Click on **Next**



6. Select the data that you wish to import.

   If you want to assign all the Systems, iFobs, Keys and Users within the import database into a specific region, uncheck the **Import Region details** check box and select the desired region. You can also specify None as the region in which case no regions will be assigned.

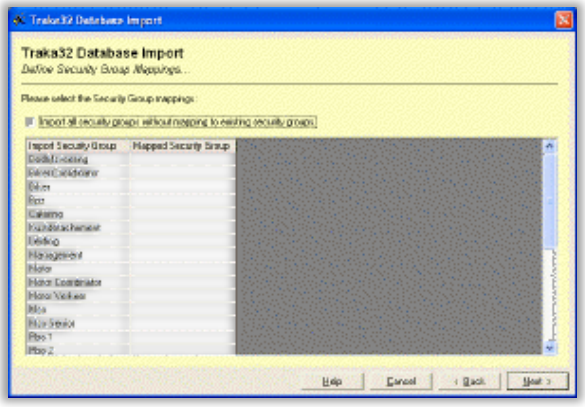
7. Click on **Next**



8. Select the appropriate mapping for the software logins.

   If you do not want to map logins from the import database to those in the live database but simply import, check the **Import all logins without mapping to existing logins** checkbox.

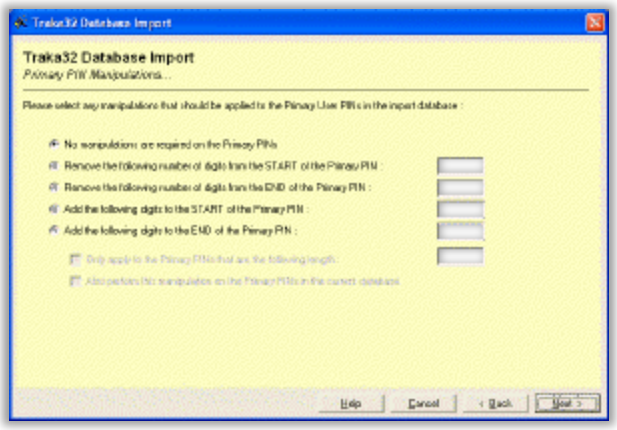
9. Click on **Next**



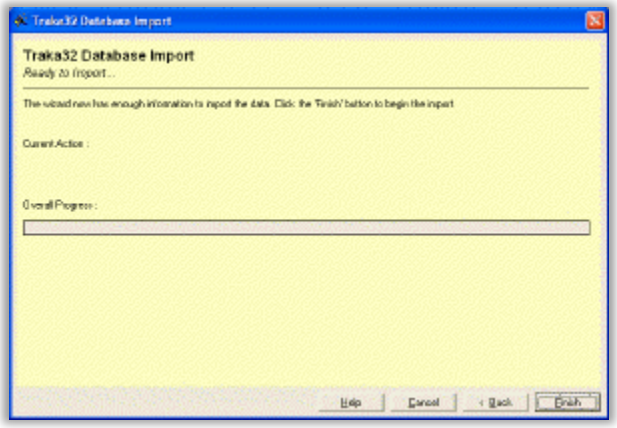
10. Select the appropriate mapping for the security groups.

    If you do not want to map security groups from the import database to those in the live database but simply import, check the **Import all security groups without mapping to existing security groups'** checkbox.

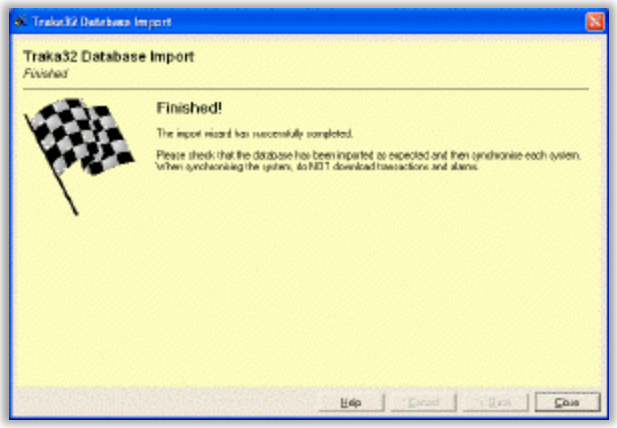
11. Click on **Next**



12. Select the appropriate Primary PIN manipulations and click on **Next**



13. When you are happy click on **Finish**



14. Provided the import completed successfully, click on **Close.**

4.13.8 EXTRACT USER DETAILS

The Extract User Details facility has been introduced to the Traka32 software to enable users that have lost their database or the database has become corrupted to be able to extract the user records currently stored in the Traka System into a new database.

To enable this option, close any open windows within the software so you have a grey screen.

NOTE: If you have lost your database or the database appear to be corrupt, please contact your supplier for who may be able to retrieve the data for you.

NOTE: This utility should only be used on a database that has no user records, otherwise duplicate user records may occur. If you require a blank database, please contact your supplier.

4.13.9 EXTRACT IFOB DETAILS

This utility is still under development.

The Extract iFob Details facility will be introduced to the Traka32 software to enable users that have lost their database or the database has become corrupted to be able to extract the iFob records currently stored in the Traka System into a new database.

To enable this option, close any open windows within the software so you have a grey screen.

NOTE: If you have lost your database or the database appear to be corrupt, please contact your supplier for who may be able to retrieve the data for you.

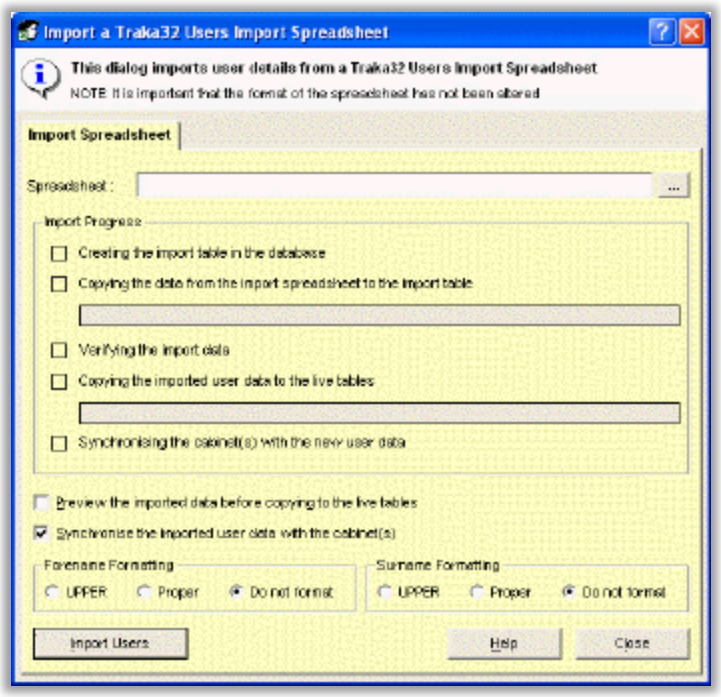
NOTE: This utility should only be used on a database that has no iFob records for the affected system, otherwise duplicate user records may occur. If you require a blank database, please contact your supplier.

4.13.10 IMPORT USERS FROM A SPREADSHEET

Import User Spreadsheet

This utility allows user data to be imported from an Excel Spreadsheet into the Traka32 database. The Excel Spreadsheet must be in a pre-defined format. Blank spreadsheets are available from the root of the Traka32 installation, for example 'C:\Users\Public\Traka\Traka32\Import\Traka32 User Import.xls'.

1. To enable this option, close any open windows within the software so you have a grey screen.
2. Click on **Tools** followed by **Import Users from Spreadsheet** from the main menu.

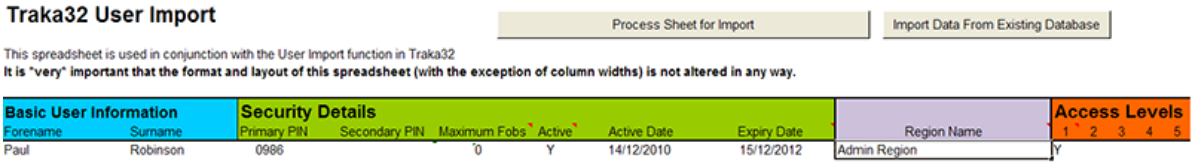


3. Select the path to the spreadsheet that you wish to import. To search for the spreadsheet file simply click on the **...** button.
4. To preview the data before the data is imported, select the **Preview the imported data before copying to the live tables'** checkbox.
5. To automatically upload the data to the relevant Traka Systems, select the **Synchronise the imported user data with the cabinet(s)** checkbox.
6. Select the appropriate formatting for the Forenames and Surnames.
7. When you are happy with your selections, simply click on **Import Users**.

Importing Users into Regions

It is possible to import users from a spreadsheet into specific regions in Traka32. Doing this is beneficial as it will save time manually inputting users into regions.

1. First you will need to create your desired regions within Traka32.
2. Enter the appropriate information along with the desired region into the provided fields in the Traka32 User Import excel spreadsheet.



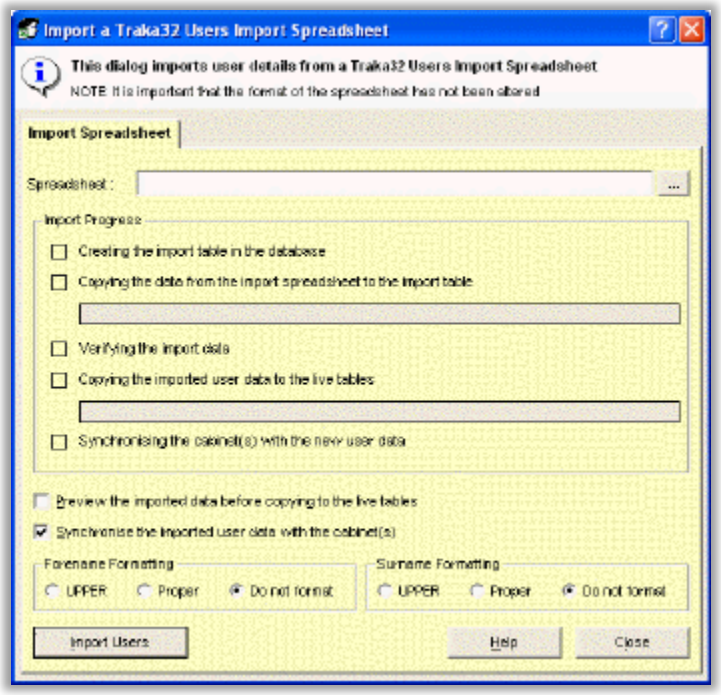
NOTE: You can put a user into more than one region by placing a comma in between each region name. E.g. *Admin Region,User Region.*

NOTE: If the Region field is left blank then 'All Regions' is assumed.

The Excel Spreadsheet must be in a pre-defined format. Blank spreadsheets are available from the root of the Traka32 installation, for example 'C:\Program Files\Traka Limited\Traka32\Import\Traka32 User Import.xls'.

3. Close any open windows within Traka32 so you have a grey screen.

4. Click on **Tools** followed by **Import Users from Spreadsheet** from the main menu.



5. Select the path to the spreadsheet that you wish to import. To search for the spreadsheet file simply click on the **...** button.

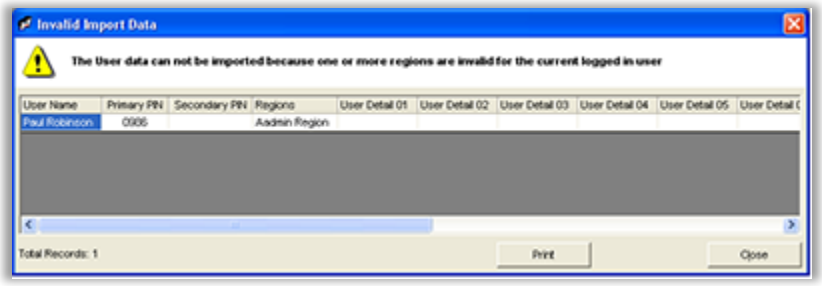
6. To preview the data before the data is imported, select the **Preview the imported data before copying to the live tables'** checkbox.

7. To automatically upload the data to the relevant Traka Systems, select the **Synchronise the imported user data with the cabinet(s)** checkbox.

8. Select the appropriate formatting for the Forenames and Surnames.

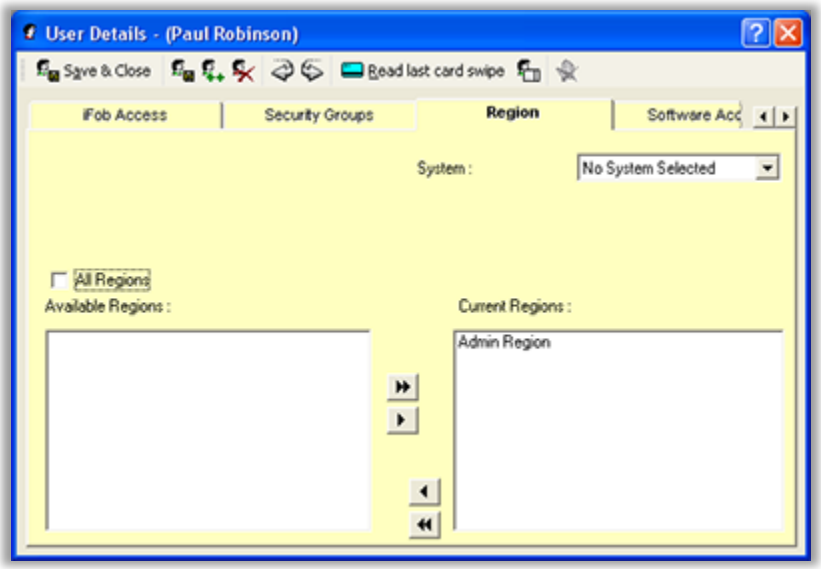
9. When you are happy with your selections, simply click on **Import Users**.

NOTE: If the region name inside the spreadsheet is non-existent or is spelled incorrectly then an error message will appear telling you the import could not continue. You will need to correct the spreadsheet and begin again.



10. A message will appear informing you the import was a success.

11. Navigate to any user you imported via the spreadsheet. Click the regions tab, you will notice the user now belongs to the region you have specified in the spreadsheet.



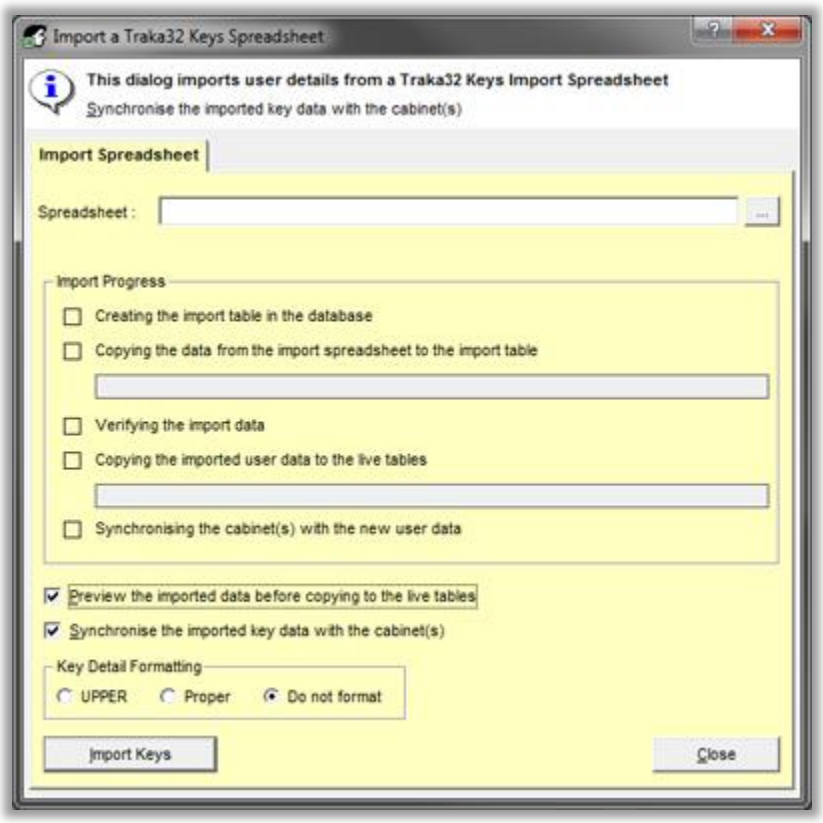
NOTE: You can only import users into regions that the logged in user can administer. E.g. If the logged in user is only in Region A then they will only be allowed to import users into Region A, if the logged in user is an 'All Regions' administrator then they can import users into any region or 'All Regions'.

4.13.11 IMPORT KEYS FROM A SPREADSHEET

This utility allows key data to be imported from an Excel Spreadsheet into the Traka32 database. The Excel Spreadsheet must be in a pre-defined format. Blank spreadsheets are available from the root of the Traka32 installation, for example 'C:\Users\Public\Traka\Traka32\Import\Traka32 Key Import.xls'.

The Key Import Spread sheet is used to allow users to import key records and assign them to a system and position or import them as de-allocated keys. Fill out the spreadsheet accordingly and click the 'Process Sheet For Import' Button.

1. To import a spreadsheet ensure all windows currently open in Traka32 are closed so you have a grey screen.
2. Click on **Tools** followed by **Import Keys from Spreadsheet** from the main menu.



3. Select the path to the spreadsheet that you wish to import. To search for the spreadsheet file simply click on the browse button (**...**) button.
4. To preview the data before the data is imported, select the **Preview the imported data before copying to the live tables'** checkbox.
5. To automatically upload the data to the relevant Traka Systems, select the **Synchronise the imported key data with the cabinet(s)** checkbox.
6. Select the appropriate formatting for Uppercase, Proper or not at all.
7. When you are happy with your selections, simply click on **Import Keys**.

4.13.12 EXTRACT USERS AND ITEMS FOR TRAKA TOUCH

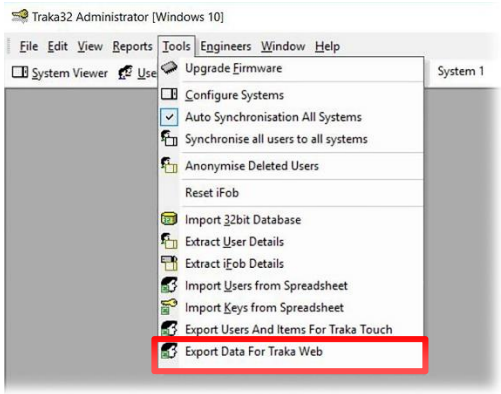
This utility allows User and Item details to be exported from the Traka32 database directly into a Traka Touch import spreadsheet format. This allows a simple process for transferring the users from a 16bit system to a Traka Touch system. The following information will be exported:

- User Forename and Surname
- Pin or Card ID
- Secondary Pin
- Active/Expiry Dates
- iFob/Item Access
- iFob/Item Description

NOTE: This feature is available for 16bit key cabinets and lockers only.

4.13.13 EXPORT DATA FOR TRAKAWEB

The Export Data for TrakaWEB comprises of a Data Export Wizard. This will enable you to export data into a TrakaWEB Data Import spreadsheet file, allowing the migration of data from Traka32 into TrakaWEB. This file is compatible with TrakaWEB version 3.9 or later.



For more information on the TrakaWEB Data Import procedure, refer to **TD0155 – Traka32 Data Export & TrakaWEB Data Import Procedure.**

4.13.13.1 REPAIR & COMPACT DATABASE

NOTE: This option is only available to Microsoft Access Database users.

The Repair & Compact utility has been provided to allow users to compact the size of the database to its absolute minimum. This utility also checks the database for any errors and will correct them automatically.

To enable this option, close any open windows within the software so you have a grey screen

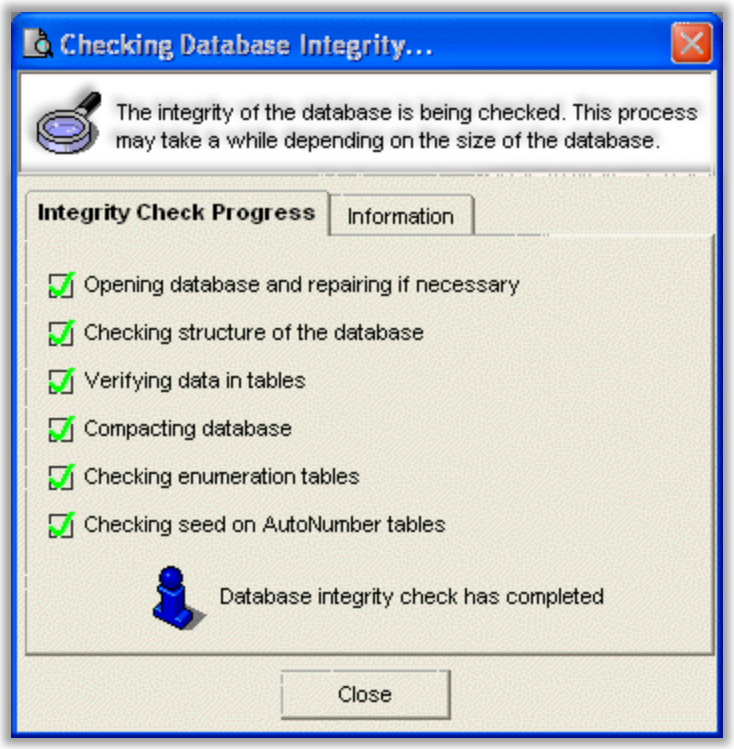
NOTE: Every time a backup of the database is made of the database the database will be compacted automatically.

4.13.14 CHECK DATABASE INTEGRITY

NOTE: This option is only available to Microsoft Access Database users.

As the Traka32 software is developed with new features, extra tables and fields are required within the database. The Check Database Integrity utility will check the current version of the Traka32 software and ensure that all the appropriate tables and fields are present and correct within the database. In addition to checking the structure, the integrity checker also checks the status of the database to ensure there is no corruption.

To enable this option, close any open windows within the software so you have a grey screen.



NOTE: If a manual upgrade is performed the database integrity check must be invoked by holding down the F10 key the first time you run the software after the upgrade.

NOTE: Every time the Traka32 software is upgraded using the installation CD, the database integrity will be automatically checked.

4.13.15 BACKUP DATABASE

NOTE: This option is only available to Microsoft Access Database users.

Backing up the database is an important part of day to day administration of the Traka32 software as with any database application. To manually backup the database...

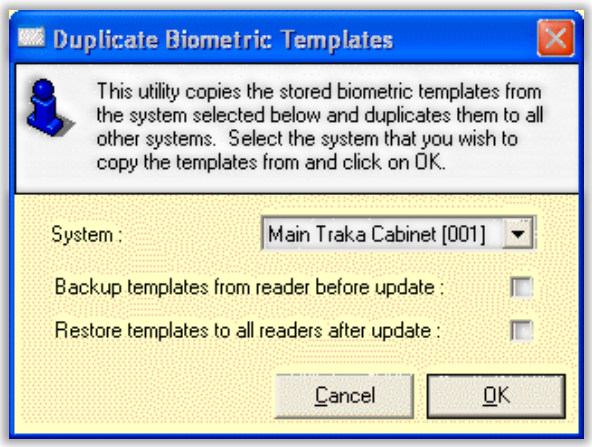
1. To enable this option, close any open windows within the software so you have a grey screen.
2. Click on **Tools**, **Backup Database**.
3. Select a **Path** and **Filename** for the backup.
4. Click on **Save**.

TIP: An auto backup utility is available with the Traka32 software to prompt the user to backup the database at intervals whenever the software is closed. Please refer to the Properties section for more details.

4.13.16 DUPLICATE BIOMETRIC TEMPLATES

When enrolling several users on a Traka System fitted with a Traka Biometrics Reader, it now possible to backup the biometric templates of the enrolled users and replicate them to other Traka Systems also fitted with a Traka Biometrics Reader. This will save the users from having to enrol of every Traka System fitted with a Traka Biometrics Reader.

1. Enroll all the users onto any one Traka System fitted with a Traka Biometrics Reader.
2. Click on **Tools**, **Duplicate Biometric Templates**.



3. Select the **System** that users have been enrolled onto.
4. Select the **Backup templates from reader before update**. This forces the utility to backup the templates from the selected system to the Traka32 Database.
5. Select the **Restore templates to all readers after update**. This forces the utility to replicate the templates out to all the Traka System fitted with a Traka Biometrics Reader.
6. Click on **OK**.

4.14 ENGINEERS

4.14.1 ENGINEERS MENU OVERVIEW

The engineers menu has been added to Traka32 so that problems that may occur on site can be diagnosed quickly without the loss of any data. The engineers menu should only be used by trained engineers or with guidance from an engineer over the phone.

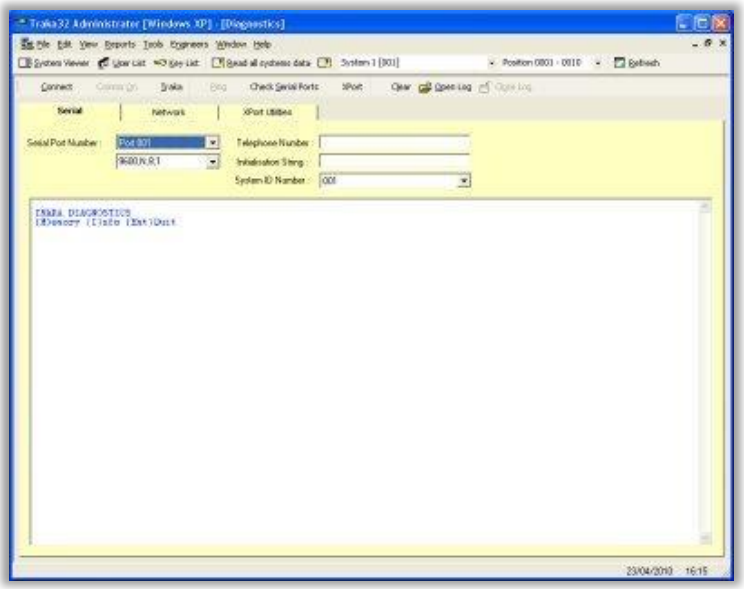
If you are experiencing problems with your Traka system please contact your vendor for advice and assistance before using the engineers menu.

The engineers menu can only be accessed if the current user of the software is logged in as an engineer. If there are no user login defined then when the software loads the engineers menu will be made available.

To login as the engineer please contact your supplier for the **username** and **password**.

4.14.2 DIAGNOSTICS

To load the diagnostics window, click on the **Engineers** menu from the system viewer, followed by **Diagnostics**.



To enter a systems diagnostic mode...

1. Select the system you wish to diagnose from **System Selection** menu.

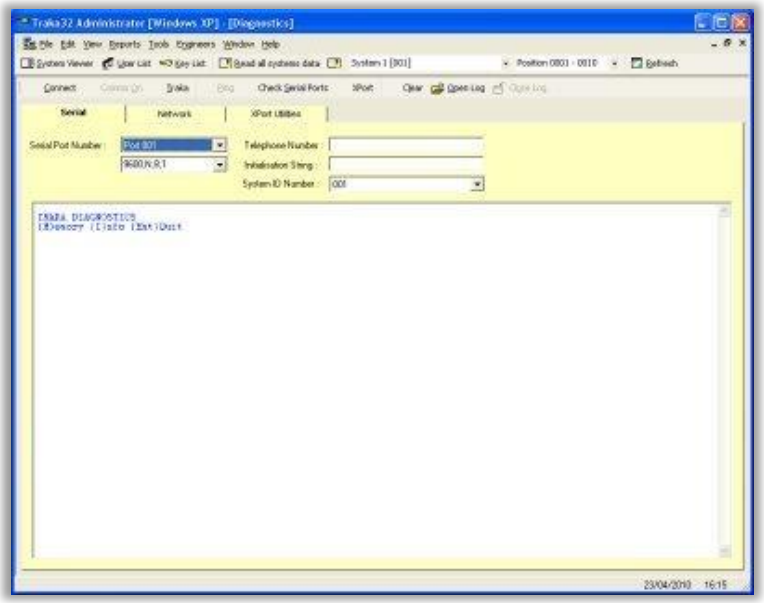
   

2. Click on the **Connect** button, this will open the serial or network port.

   (Note that if successful the Connect button changes to Disconnect)

3. Click on the **Comms On** button, this will wake and enter the system into diagnostic mode.



NOTE: that if successful the Comms On button changes to Comms Off.

4. Once in diagnostic mode you can use the keyboard to navigate through the various menus presented to you by the Traka System.

Using the Traka Diagnostics Menus...

The Traka Diagnostic Menus are driven by the keyboard of your PC. To use the menus, please ensure your cursor is in the diagnostics window.

Each available option will be shown in the menu presented to you. To select a menu option press the corresponding letter on the keyboard that is shown in brackets on the menu, for example...

TRAKA DIAGNOSTICS

(M)emory (I)nfo (Ent)Quit

To select the **(I)nfo** menu, press the '**I**' key on the keyboard and so on...

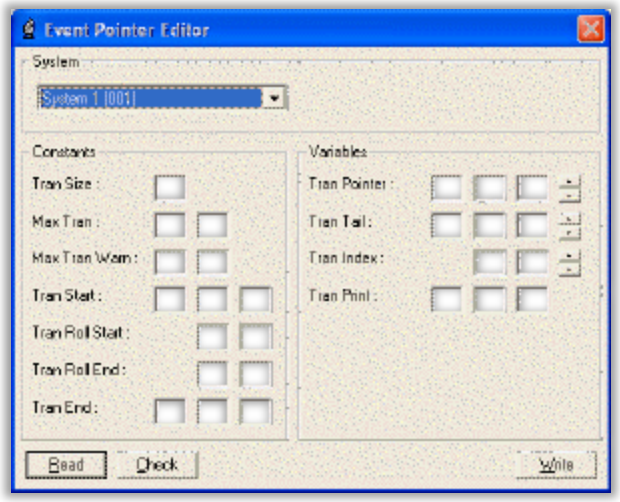
To exit a system from diagnostics mode...

1. Click on the **Comms Off** button, this will take the system out of diagnostics mode.
   (Note that the Comms Off button will only be available if the system is still in diagnostics mode. If no keyboard presses have been made for 30 seconds or the (Ent)Quit option is selected the Traka system will exit diagnostics mode automatically.)

2. Click on the **Disconnect** button, this will close the serial or network port.
   (Note that closing the Diagnostics window will automatically close the serial or network port automatically.)

4.14.3 EVENT POINTER EDITOR

The event pointer editor has been added to Traka32 so that problems that may occur on site can be diagnosed quickly without the loss of any data. The event pointer editor should only be used by trained engineers or with guidance from an engineer over the phone.



4.14.4 DESKTOP IFOB PROGRAMMER

The Traka Desktop iFob Programmer is single iFob receptor incorporated into a desktop programmer device. The desktop programmer connects to a computer running Traka32 via a spare serial or USB port.

NOTE: This menu can only be accessed if the current user of the software is logged in as an engineer.

iFob Memory Map

Click on iFob Memory Map to view the data currently stored in either a Data32 or Data512 iFob.

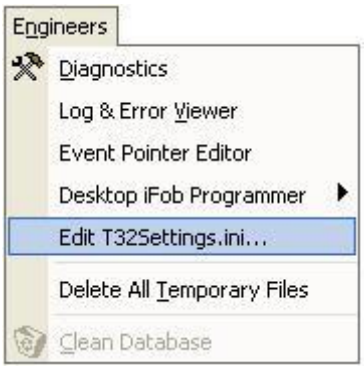
Reset iFob

This option should be used with great caution! It deletes the information held within the selected Data iFob's memory.

NOTE: Traka will not be held responsible for the loss of data if you do not back up any data before resetting.

4.14.5 EDIT T32SETTINGS.INI

When selected this opens the active T32Settings.ini file in notepad. This is useful for when the T32Settings.ini file is not stored in the default location.



4.14.6 DELETE ALL TEMPORARY FILES

This feature allows you to delete all the temporarily download files (*.trn) created by Traka32 when communicating with Traka Systems.

4.14.7 CLEAN DATABASE

This feature allows you to permanently destroy all previously deleted System, iFob, Key and User details and any associated transaction and alarms from the database.

4.14.8 TRAKA DIAGNOSTICS MENU

4.14.8.1 POINTERS

The Traka Pointers are used to index the various transaction and alarms that are currently stored in the memory of Traka. This only applies to firmware versions 6.07.23 and below. For firmware versions 6.07.24 and above, please refer to the Event pointer Editor section.

1. First enter the system into diagnostics mode.

   TRAKA DIAGNOSTICS
   (M)emory (I)nfo (Ent)Quit

2. From the Traka Diagnostics Menu, Press '**I**' for **(I)nfo**

   (P)ointers (V)ersion (Ent)Backup

3. Press '**P**' for (P)ointers

   Alarm Pointer $0760CA
   Alarm Tail $0760CA
   Alarm Index $ 0000

   Tran Pointer $057055
   Tran Tail $057055
   Tran Index $ 0000

   (P)ointers (V)ersion (Ent)Backup

4. The data in step 3 can be used by a Traka Engineer to analyse any problems that may have occurred.

5. Press '**Enter**' on your keyboard **twice** to exit the system from diagnostics mode.

   Traka Diagnostics
   (M)emory (I)nfo (Ent)Quit

   Communication Off

6. Finally click on the **Disconnect** button, this will close the serial or network port. If successful the Disconnect button changes to Connect.

4.14.8.2 RESETTING ALARMS

Various sections of the memory within a Traka System can be reset if there is a problem.

NOTE: By resetting the alarms, any alarm data will be lost permanently. This procedure should only be followed in the event of a problem and should only be carried out on the instruction of a Traka Engineer.

1. First enter the system into diagnostics mode.

   TRAKA DIAGNOSTICS
   (M)emory (I)nfo (Ent)Quit

2. From the Traka Diagnostics Menu, Press '**M**' for **(M)emory**

   Info: (P)age Dump (E)dit Loc (Q)uit (Ent)Backup
   Reset: (U)sers (F)obs (T)rans (A)larms (S)tack (I)Title

3. Press '**A**' to reset the **(A)larms**

   RESETTING - Please Wait
   Info: (P)age Dump (E)dit Loc (Q)uit (Ent)Backup
   Reset: (U)sers (F)obs (T)rans (A)larms (S)tack (I)Title

4. Press '**Enter**' on your keyboard **twice** to exit the system from diagnostics mode.

   Traka Diagnostics
   (M)emory (I)nfo (Ent)Quit

   Communication Off

5. Finally click on the **Disconnect** button, this will close the serial or network port. If successful the Disconnect button changes to Connect.

4.15 WINDOW

4.15.1 CASCADE

Overlays open windows diagonally across the screen.

4.15.2 TILE HORIZONTAL

Tiles open windows in a vertical column. Horizontal breaks.

4.15.3 TILE VERTICAL

Tiles open windows in horizontal row. Vertical breaks.

4.15.4 ARRANGE ICONS

Arranges the icons of open, but minimised windows.

4.15.5 REFRESH

Refresh, refreshed the content of all open windows. This is useful in a multi-user environment where changes are made at multiple workstations.

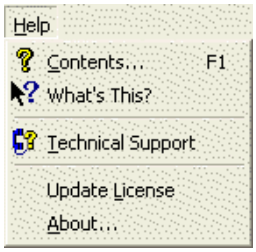
4.15.6 SHOW STATUS BAR

Show or hide the Status bar.

4.16 HELP

4.16.1 CONTENTS

For help with the Traka32 software simply click on Help followed by Contents from the main menu or simply press F1 to view the online user guide.



4.16.2 WHAT'S THIS?

Traka32 also incorporates a 'What's this help?' facility. Each details window has a  button in the top right hand corner. Click on the  and the cursor will change to  , click on the control you want to know more about and a pop up window will appear with details on that control.

4.16.3 TECHNICAL SUPPORT

The technical support window shows the contact information for technical support:

4.16.4 EXPLORE DATA FILES FOLDER

When selected this opens up Explorer in the folder which contains download and support folders. This is useful for when the data files are not stored in the default location.

4.16.5 UPDATE LICENSE

NOTE: When you run the Traka32 software for the first time you will be asked for a software registration code, please refer to the Traka32 Registration section for more details.

When you have registered the Traka32 software you can update your license at any time to either increase the number of concurrent users or to extend the period of the license.

To update the license please contact Traka by telephoning +44 (0)1234 712345 between the hours of 08:30 and 17:30 GMT/BST or by email to support@traka.com quoting the following...

- Application
- Customer Code
- Software Code

You will be given a 20 digit unlock code, enter the unlock code and click on **Register** to complete the registration process.

4.16.6 EASY HELP

Traka easy HELP is a quick way to access the most commonly used sections of the Traka32 User Guide. If you would like the easy HELP menu to be customized to suit your business needs, please contact you supplier with details and we will help you create a new menu.

4.17 SOFTWARE ACCESS

4.17.1 SOFTWARE ACCESS

Software Access is a fundamental part of the Traka32 software which allows restrictions to be applied against user logins preventing users from accessing certain areas of the software. The Software Access also forms part of the Software Audit report where every user action is logged.

This section assumes that the database has been successfully installed and initialised. For further details on initialising a database, please refer to the following sections:

- Microsoft Access Installation
- Microsoft SQL Installation

4.17.2 SOFTWARE ACCESS USING A MICROSOFT ACCESS DATABASE

This section assumes that the database has been successfully installed and initialised.

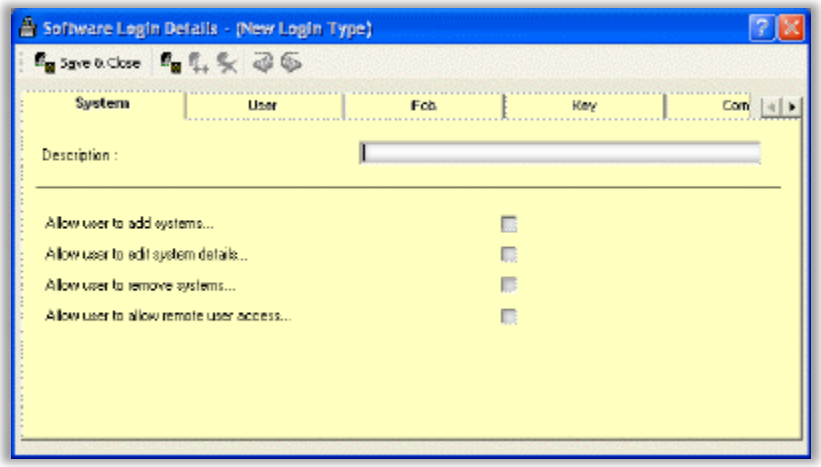
When using a Microsoft Access Database, if there are no users defined in the Traka32 software, for example when first setting up a database, or if there are no user records that have the **Allow Software Access** option enabled then there is no Software Access in place at all and so when the Traka32 software is open, no user login will be prompted for and all areas of the software will be accessible.

As soon as one or more user records have the Allow Software Access option enabled, Software Access will be enabled and so when the Traka32 software is open, a user login will be prompted for:

Setting up Software Access

The first step is to create Software Access Groups.

1. Click on **File**, **Options**.
2. The Options screen will open and you will see the **Software Access** tab is already selected. You will also notice that there is a predefined Login called **Administrator**. This login record cannot be edited or deleted and allows access to all areas of the Traka32 software except for the Engineer sections.
3. To add a new Login, click on **Options**, **Add New**.



4. Enter a **Description**.

5. Tick the relevant boxes to allow members of the Software Access Group access to the relevant areas of the software. The options are categorised, simply click on the tabs to view each category:

    - System
    - User
    - iFob
    - Key
    - Comms
    - Software

      For more details of the categories and options, please refer to the Software Access section.

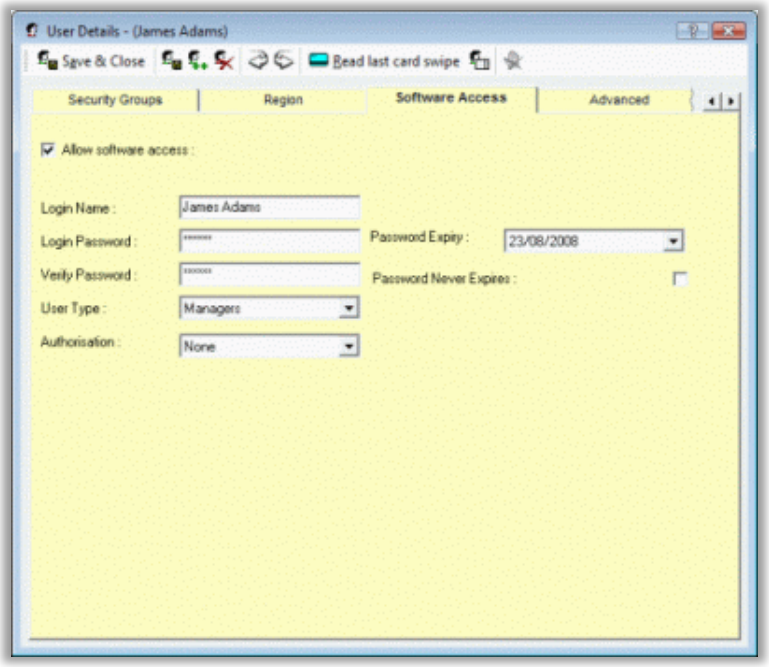
6. There is one final tab called **Access Levels**. Select the Access Levels that the members of the Software Access Group will be able to administer. This will allow the members to administer iFobs that have one of the Current Access Levels. This will also only allow the logged in user to administer Keys attached to iFobs that has one of the Current Access Levels. Also when administering User Details, the members will only be able to allocate users with the access levels listed in the Current Access Levels list.

7. Click on **Save & Close**.

Associate User Records to the Software Access Groups

Once the Software Access Groups have been the next step is to associate the users to the software access group.

1. Click on **View**, **User List**.
2. Click on Users, **Edit User** or **Add New** as required.
3. The User Details screen will open and you will see the **User Details** tab is already selected.
4. Enter a **Forename** and **Surname**.
5. Click on the **Software Access** tab.
6. Tick the **Allow Software Access** tick-box.



7. Enter a **Login Name**.
8. Enter a **Login Password**.
9. Re-type the password into the **Verify Password** field.
10. Select the **User Type**. This is the Software Access Group that was defined above.
11. Enter a **Password Expiry** date or select the **Password Never Expires** option.
12. Click on **Save and Close**.

Logging into Traka32

When one or more user records have been setup with Software Access, the Traka32 software will prompt for a user login when open:

Password Expiry

When a user logs into Traka32 and if their password has expired, Traka32 will prompt for a new password. Simply enter a new password and re-type the password into the Verify Password field:

4.17.3 SOFTWARE ACCESS USING A MICROSOFT SQL SERVER DATABASE

This section assumes that the database has been successfully installed and initialised.

When using a Microsoft SQL Server Database, some form of login will always be required.

Although Traka32 only requires one login, there are two levels of authentication that occurs before allowing access to Traka32. The first level is the SQL Server Authentication. This is where the SQL Server must authenticate the user connecting to the database. This can either be done with Integrated Security or SQL Server Authentication. The second level is matching up the Login Name to that of a user record in the Traka32 Database itself.

When logging into Traka32 for the first time with a new database you will need to use the SQL Server's own SA account Login Name and Password. This will be available from the SQL Server administrator. The SA login will allow access to all areas of the Traka32 software including the Engineer sections.

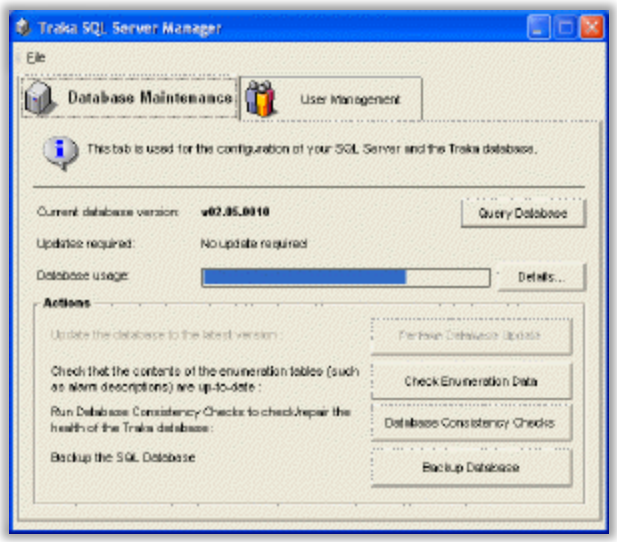
For more details on Integrated Security and SQL Server Authentication please refer to the Integrated Security section.

Setting up SQL Server User Accounts (SQL Server Authentication Only)

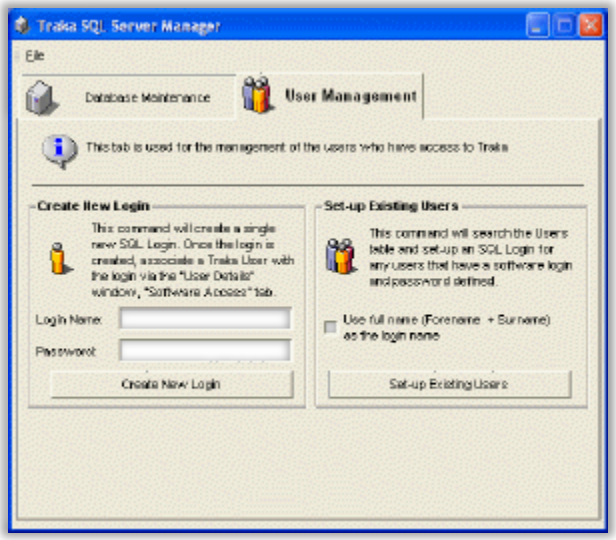
This does not apply if you are using Integrated Security.

The first step is to create SQL Server User Accounts using the Traka SQL Server Manager.

1. Load the Traka SQL Server Manager software by clicking on the  icon from the **Traka** program group in the **Start** menu.



2. Click on the User Management tab.

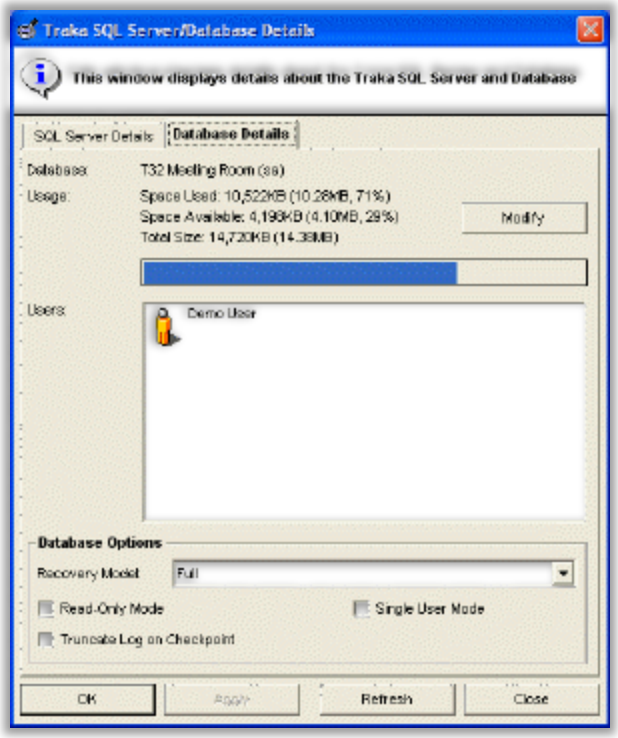


3. For each user that needs to login to Traka32 a new login must be created.
4. Enter a **Login Name**.
5. Enter a **Password**.
6. Click on **Create New Login**.
7. Repeat this for each user that requires a login.
8. Close the Traka SQL Server Manager software.

To view or delete the user accounts.

1. Load the Traka SQL Server Manager software by clicking on the  icon from the **Traka** program group in the **Start** menu.
2. Click **Details...** and the Database Detail screen will open.

3. Click on the **Database Details** tab.



4. A list of active user account will be shown.

5. To delete a user account, simply **right click** over the user account icon and click on **Remove User**.

Please note that a user account password cannot be changed. If the password needs to be changed the user account must be deleted and re-created again.

Setting up SQL Server User Accounts (Integrated Security Only)

This does not apply if you are using SQL Server Authentication.

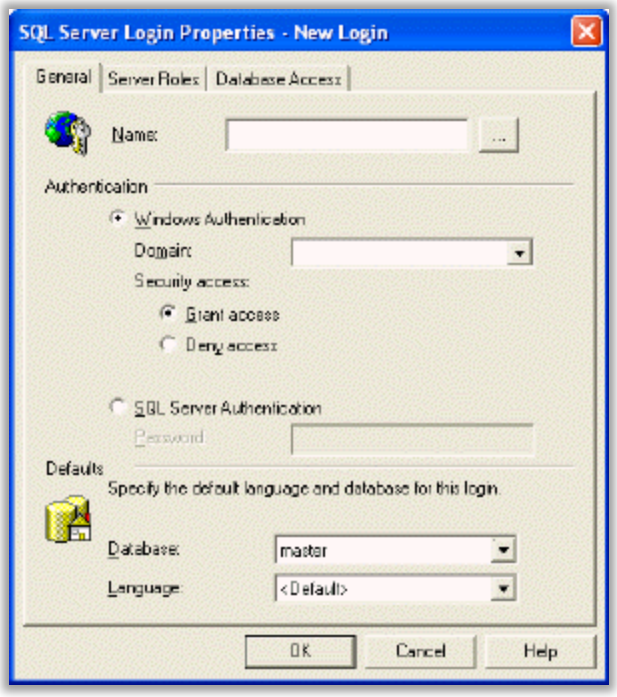
If Integrated Security is being used, the SQL Server Administrator must grant the users access to the database using SQL Server Enterprise Manager. This cannot be done using the Traka SQL Server Manager. If you are using MSDE as the database engine and you do not have access to a copy of Enterprise Manager then you cannot configure Integrated Security.

1. Load Enterprise Manager.

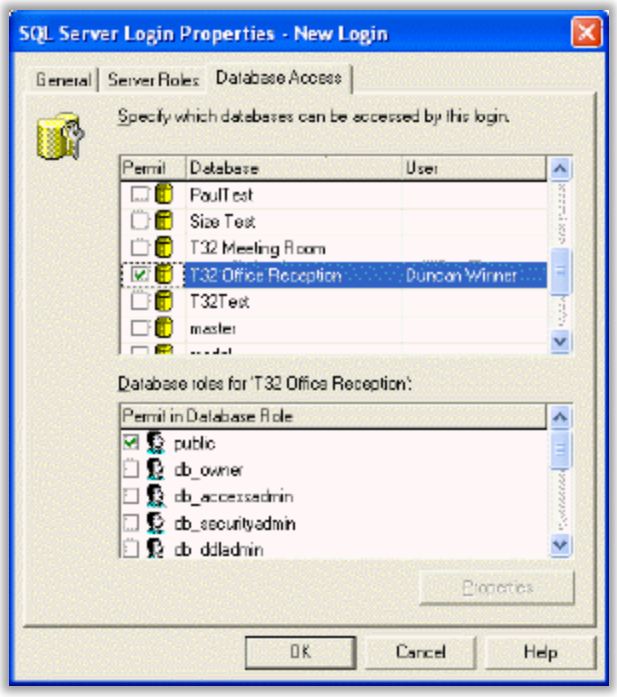
2. Expand the SQL Server that is hosting the Traka32 Database.

3. Expand the Security folder and click on Logins.

4. Right click over Logins and click on **New Login...**



5. Enter a user account **Name** or click on the ... button to browse for the user account name.
6. Select the **Windows Authentication** option.
7. Select the appropriate **Domain** name.
8. Select the **Grant Access** option.
9. Select the appropriate Traka32 Database as the **Default Database**.
10. Click on the **Database Access** tab.



11. Tick the **Permit** box for the appropriate Traka32 Database.

12. Click on **OK**.

Setting up Software Access

The next step is to create Software Access Groups.

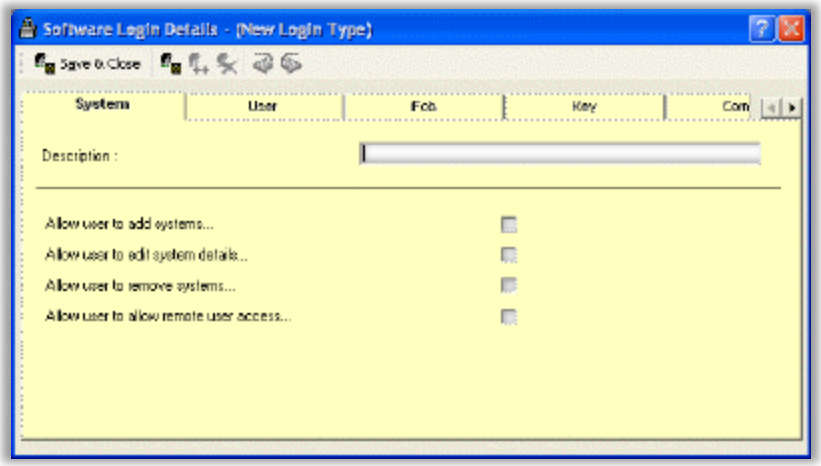
1. Load the Traka32 software by double clicking on the  icon.

2. If no users accounts have been configured yet, login using the SQL Server's SA account.

3. Click on **File**, **Options**.

4. The Options screen will open and you will see the **Software Access** tab is already selected. You will also notice that there is a predefined Login called **Administrator**. This login record cannot be edited or deleted and allows access to all areas of the Traka32 software except for the Engineer sections.

5. To add a new Login, click on **Options**, **Add New**.



6. Enter a **Description**.

7. Tick the relevant boxes to allow members of the Software Access Group access to the relevant areas of the software. The options are categorised, simply click on the tabs to view each category:

    - System
    - User
    - iFob
    - Key
    - Comms
    - Software

    For more details of the categories and options, please refer to the Software Access section.

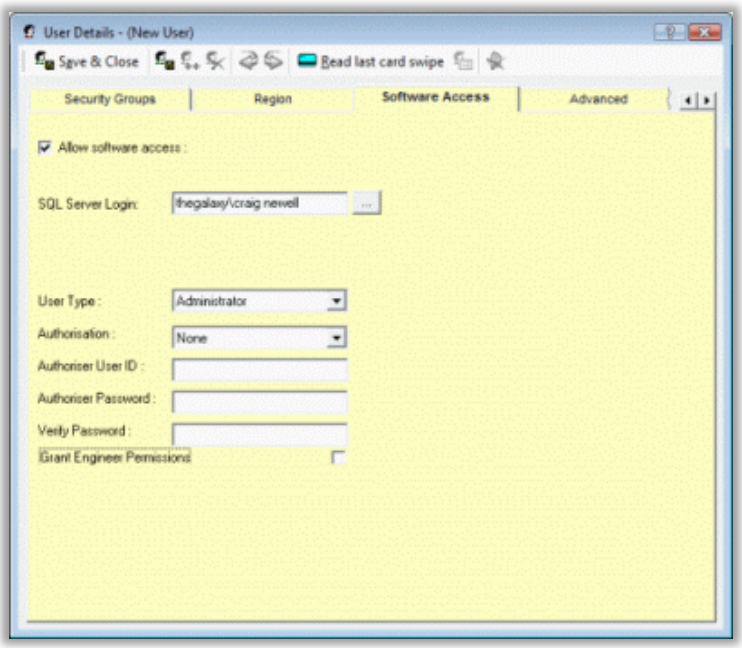
8. There is one final tab called **Access Levels**. Select the Access Levels that the members of the Software Access Group will be able to administer. This will allow the members to administer iFobs that have one of the Current Access Levels. This will also only allow the logged in user to administer Keys attached to iFobs that has one of the Current Access Levels. Also when administering User Details, the members will only be able to allocate users with the access levels listed in the Current Access Levels list.

9. Click on **Save & Close**.

Associate User Records to the SQL Server Login Account and Software Access Groups

Once the Software Access Groups have been the next step is to associate the users to the software access group.

1. Load the Traka32 software by double clicking on the  icon.
2. If no users accounts have been configured yet, login using the SQL Server's SA account.
3. Click on **View**, **User List**.
4. Click on Users, **Edit User** or **Add New** as required.
5. The User Details screen will open and you will see the **User Details** tab is already selected.
6. Enter a **Forename** and **Surname**.
7. Click on the **Software Access** tab.
8. Tick the **Allow Software Access** tick-box.



9. Enter the appropriate **SQL Server Login** name that was entered when setting up SQL Server User Accounts above. Click on the ... button to search for the users.

10. Select the **User Type**. This is the Software Access Group that was defined above.
11. Optionally select this option to grant engineering capabilities which will allow the user access to the Engineers menus.
12. Click on **Save and Close**.

4.18 MESSAGE NOTIFICATION SYSTEM

4.18.1 NOTIFICATIONS OVERVIEW

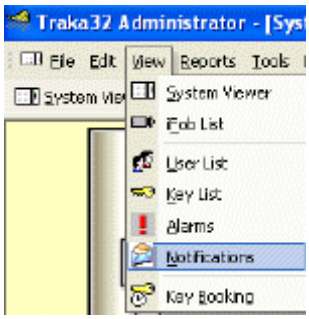
The Message Notification System allows 'rules' to be created where if the condition(s) of the rule are met, a message is sent to one or more users via Email or the Windows Network Messaging System (NetSend).

The Message Notification System allows the creation of rules to say for example:

- Message the Manager when anyone takes the key to the Safe.
- Message Site Services if there is a Fault logged against an iFob for a Vehicle.
- Message the I.T Dept. if a Power Failure occurs on any Traka System.

The system is versatile and allows the creation of many Notification Rules with different trigger conditions to suit the application.

The Message Notification System can be accessed by clicking **View > Notifications** from the Traka 32 menu.



NOTE: Messages are sent from the Traka32 software and not the Traka system cabinets. A message is generated (provided the rule conditions are met) after a  **Read All System Data has been completed.**

4.18.2 MESSAGE RULES AND TRIGGERS

A Notification Rule is created by the User in Traka 32. A Rule consists of various conditions where if the conditions are all met, the message will be created and sent. A user may setup as many Notification Rules as required by the application.

A Notification Rule is made up of the following criteria:

- The Trigger
- Any Special Conditions
- The Actual Message
    - How the Message is sent
    - Whom the Message is to be sent to

Triggers

The Trigger is part of the Notification Rule and is responsible for "triggering" a message to be sent. Triggers are made up of various sources of events generated by the Traka system.

These include:

- iFob Events from Systems (e.g. iFob Removed, iFob undetectable)
- System Alarms (iFob returned to wrong slot, Overdue iFob)

  See Alarm and Event Types a full description of all events generated by Traka.
- Faults entered/cleared on system from the cabinet
- Faults entered/cleared in Traka32
- Immobilisor iFob Events (e.g. Device Activated, Shock Occurrence etc.)

All of the above can be referred to as Triggers. Each Trigger has an associated Trigger Code and a descriptive Trigger Name. For example, Code 128 is "iFob Removed".

Filtering the Trigger Sources

When creating the Notification Rule, each Notification Rule can filter these Triggers in two ways:

1. One or multiple Trigger names can be selected from the Trigger List.
2. Who or what actually caused the trigger can be selected.

Trigger sources also have additional data associated to them other than their description such as:

- The Traka system where the trigger occurred
- The Key(s) attached to the iFob
- The User who was using the system at the time
- For Immobilisor systems, the Vehicle or Immobilisor

This, then, allows you to say, for example:

- I want to be notified for ANY Events from only System A (System Filter)

- I want to be notified when the Office Safe Key is taken – no matter which iFob it is attached to today (Key Filter)

- I want to be notified when John Smith replaces any iFob in any System (User Filter)

- I want to be notified when iFob 23 is removed OR replaced (iFob Filter)

- I want to be notified when a Fault is logged on a specific piece of equipment (iFob Filter)

Each Notification Rule also allows you to switch the Trigger Filter off so that the rule applies to ALL iFobs/Keys/Systems etc. This has the advantage that if a new iFob, Key, User or System is added to the system the Rule will automatically include the new one without having to revisit a list and manually include the new one.

Trigger Types

To make things easier, we have collected together the 'useful' combinations of Trigger Source (Events, Alarms, Faults etc.) and their Filters (iFob, User, System, Vehicle/Truck) and called it a **Trigger Type** :

- **iFob Events**: Where one or more selected Events (e.g. iFob Removed, iFob Returned) occurs on the selected [filtered] iFobs.

- **iFob Alarms**: Where one or more selected Alarms (e.g. Unauthorised iFob Taken, Overdue iFob) occurs on the selected iFobs.

- **User Events**: Where one or more selected Events (e.g. iFob Removed, iFob Returned) occurs when the selected user(s) have logged in to any System.

- **User Alarms**: Where one or more selected Alarms (e.g. Unauthorised iFob Taken, Overdue iFob) occurs when the selected user(s) have logged in to any System.

- **Key Events**: Where one or more selected Events (e.g. Key Removed, Key Returned) occurs on the selected Keys.

- **System Alarms**: Where one or more selected Alarms (e.g. Triple Primary PIN, Door Left Open) occurs on the selected System(s).

- **System Events**: Where one or more selected Events (e.g. Door Opened via iFob Reader) occurs on the selected System(s).

- **Locker Events**: Where one or more selected Events (e.g. Locker Opened) occurs on the selected System Positions.

- **iFob Faults**: Where one or more selected Faults (e.g. Battery, Heater) are created on the selected iFob(s) via Traka32 or the System.

- **iFob Critical Faults**: Where one or more selected Critical Faults (e.g. Brakes, Steering) are created on the selected iFob(s) via Traka32 or the System.

- **iFob Faults Repaired**: Where one or more selected Faults (e.g. Battery, Heater) are marked as Repaired on the selected iFob(s) via Traka32.

- **iFob Critical Faults Repaired**: Where one or more selected Faults (e.g. Brakes, Steering) are marked as Repaired on the selected iFob(s) via Traka32.

- **iFob Faults Cleared**: Where one or more selected Faults (e.g. Battery, Heater) are marked as Cleared on the selected iFob(s) via Traka32.

- **iFob Critical Faults Repaired**: Where one or more selected Faults (e.g. Brakes, Steering) are marked as Cleared on the selected iFob(s) via Traka32.

- **Immobilisor iFob Events**: Where one or more selected Immobilisor Events (e.g. Device Activated, Shock Occurrence) occur on the selected iFob(s).

- **Immobilisor User Events**: Where one or more selected Immobilisor Events (e.g. Device Activated, Shock Occurrence) occur for the selected User(s).

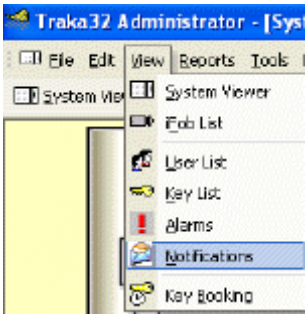
- **Immobilisor Truck Events**: Where one or more selected Immobilisor Events (e.g. Device Activated, Shock Occurrence) occur on the selected Truck[s] [Immobilisor(s)].

4.18.3 CREATING MESSAGE TEMPLATES

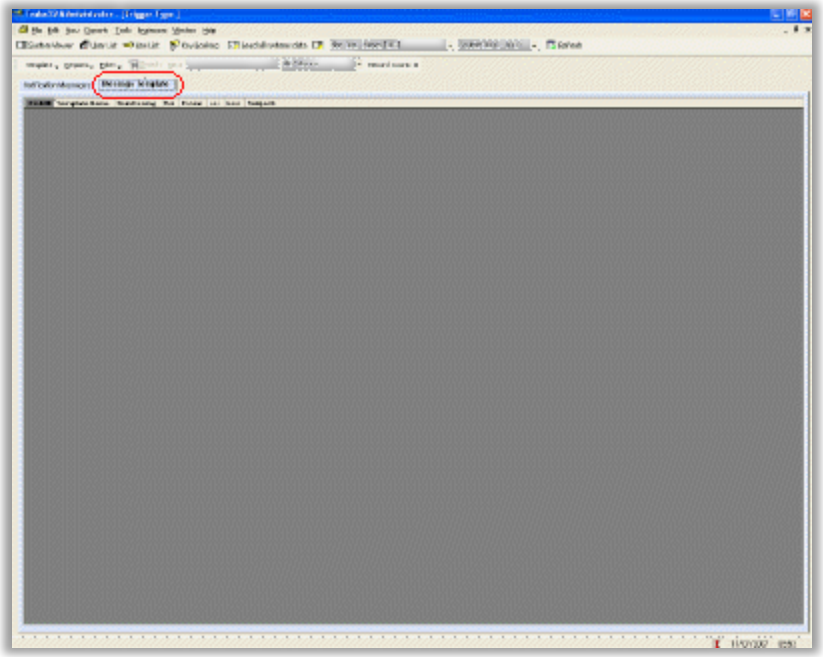
Traka uses a Message Template system so as a Message can be customized to include only references to data as required by the message recipient(s). Once created, a Template is saved allowing it to be shared by the Notification Rules. As many Templates as required can be created and saved allowing for ultimate flexibility.

To create a Message Template:

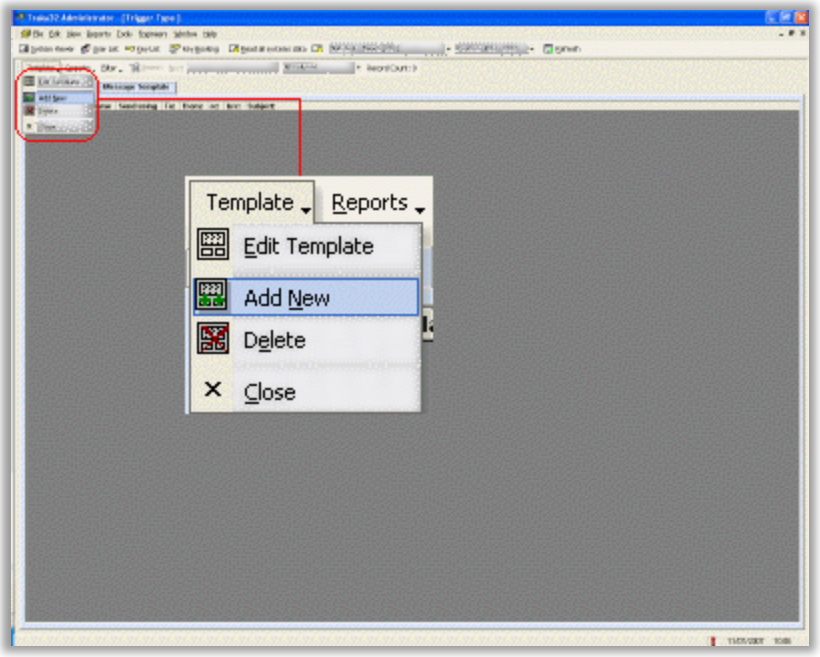
1. From Traka 32 System Viewer click **View > Notifications**:



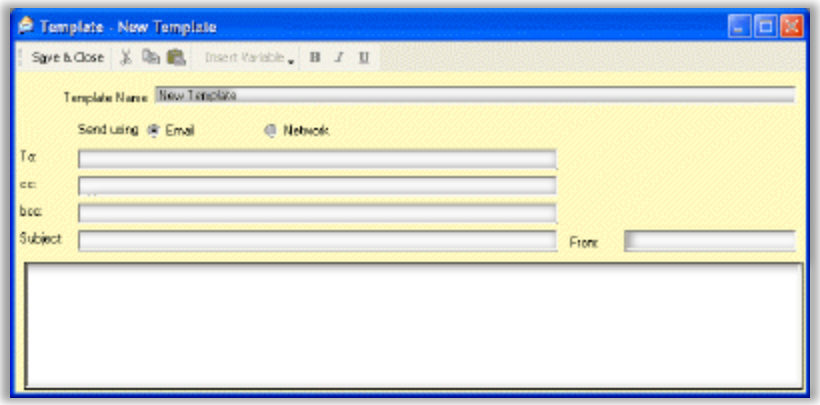
2. Click on the **Message Template** tab:



3. Click on **Template > Add New**:



4. A **New Template** window will open:



Template Name

Provide a Message Template name.

Send Using

Select if the message is to be sent using **Email, Network (Windows Network Messaging System) or SMS Message**.

Email

If email is selected

To:

Input the email addresses of the people who are required to receive this notification email separated by semicolons.

Cc:

Input the email addresses of the people who require a copy of this notification email separated by semicolons.

Bcc:

Input the email addresses of the people who require a blind copy of this notification email separated by semicolons.

Subject:

Provide a subject heading for the notification email.

NOTE: Email must be globally enabled by ticking Send Emails From Traka32 and entering the SMTP Server and SMTP Port from Traka 32 Properties. On certain SMTP servers such as Microsoft Exchange, relaying may have to be enabled in order allow Traka32 to send e-mails to the outside world. For a guide on how to safely configure Microsoft Exchange for relaying, please refer to the Relaying on Microsoft Exchange section.

NOTE: When using Email Notification, various response codes are sent and received between Traka32 and the email server. These codes must match in order for the Email Notifications to work correctly. Refer to the section Email Response Codes for more information.

Network

If Network is selected...

To:

Provide the windows login user name(s) of the people who are required to receive the Net Send (Windows Network Messaging Service) Message Notification.

From:

Provide a valid email address. If this is left blank the message may not be processed by the SMTP Server because it could think it is spam. Most systems require the senders email address to be verified.

NOTE: Consult Messenger on Microsoft Windows for how to configure the service for use with Traka32.

SMS Message

If SMS Message is selected

To:

Input the phone numbers of the people who are required to receive this SMS message separated by semicolons.

Subject:

Provide a subject heading for the SMS message.

Message Field:

Input the message the recipients of this notification will receive.

NOTE: Please read the section below on SMS Messaging for further details on how it works.

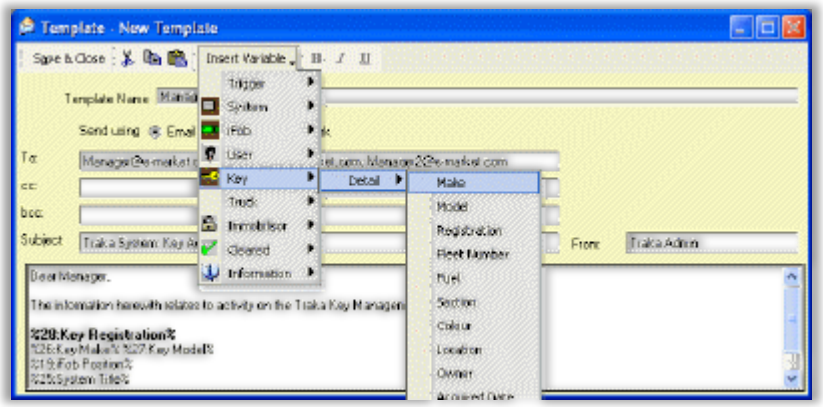
Message Box:

Enter the body of the message here and include the data variables (Traka system information) that are required to be included in this message template. To insert a variable:

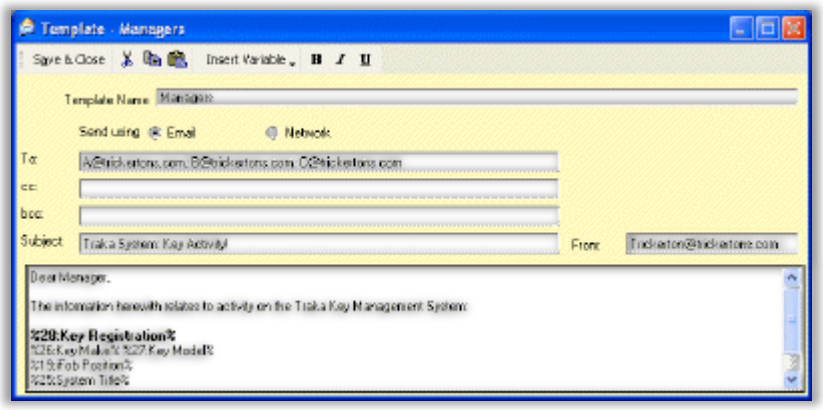
a. Click inside the **Message Box**

b. Click **Insert Variable** and select from the many available variables listed.

e.g **Key > Detail > Make** to insert the Make variable into the message...



Example Message Template Form:



The example above shows a Message Template called "Managers". The email addresses could easily be the managers of a company who are required to be sent this message when a message rule is triggered, e.g. perhaps relating to when a particular key is removed. The variables included are the Trigger Name, Date, Registration, Make, Model, iFob Position and System Title.

c. After completing the message template form click **Save and Close** to save the template to the Traka database.

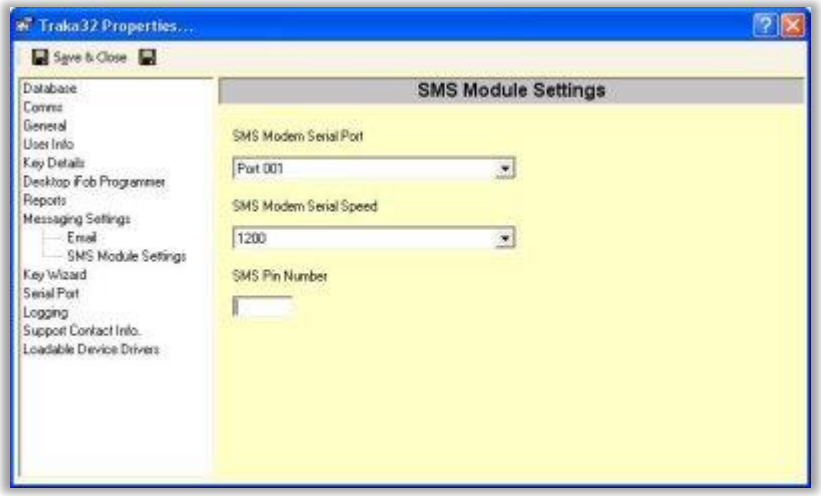
d. Now refer to the topic Creating Notification Message Rules.

SMS Notification

To use SMS...

Firstly you will need to have a GSM Module installed with your cabinet/system for this feature to work. On how to configure the GSM Module please refer to the Configuring the GSM Module section.

Secondly you will need to enable certain option within Traka32 by navigating to the Properties page, click *File* > *Properties.* You will be confronted by the Properties window, scroll down to the Message Settings tab and select 'SMS Module Settings'. Here you will need to enter/change the following fields as applicable.



SMS Modem Serial Port

Select the desired modem serial port number which Traka32 will use to send SMS messages.

SMS Modem Serial Speed

Select the appropriate speed you require for the modem you will be using.

SMS Pin Number

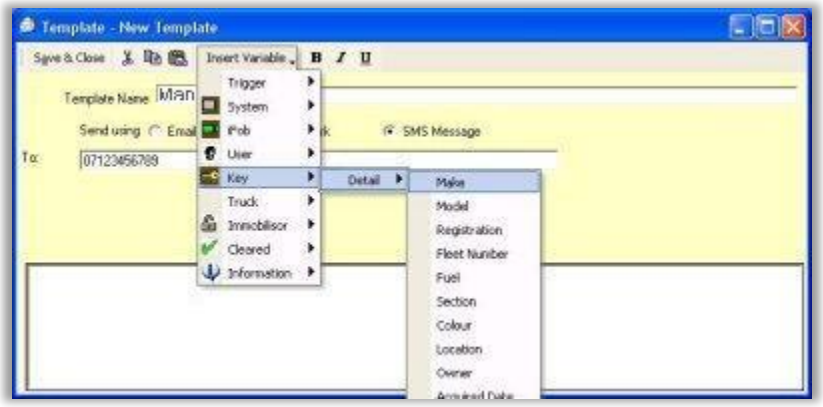
This field requires you to enter the pin number from the SIM card that you will be sending the SMS messages.

After entering/changing the configurable options above, from the Traka 32 System Viewer click **View > Notifications**, Click on the **Message Template** tab, Click on **Template > Add New**, and a **New Template** window will open.

1. Select the SMS button
2. Enter the phone number of the person you wish to notify
3. Click inside the **Message Box**

4. Click **Insert Variable** and select from the many available variables listed

   e.g. **Key > Detail > Make** to insert the Make variable into the message (see below)



   The example above shows a Message Template called "Managers". The phone number could be the managers of a company who is required to be sent this message when a message rule is triggered, e.g. perhaps relating to when a particular key is removed. The variables included are the Trigger Name, Date, Registration, Make, Model, iFob Position and System Title.

5. After completing the message template form click **Save and Close** to save the template to the Traka database.

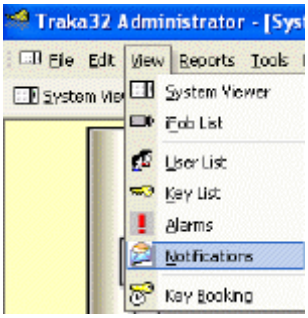
6. Now refer to the topic Creating Notification Message Rules.

4.18.4 CREATING NOTIFICATION MESSAGES

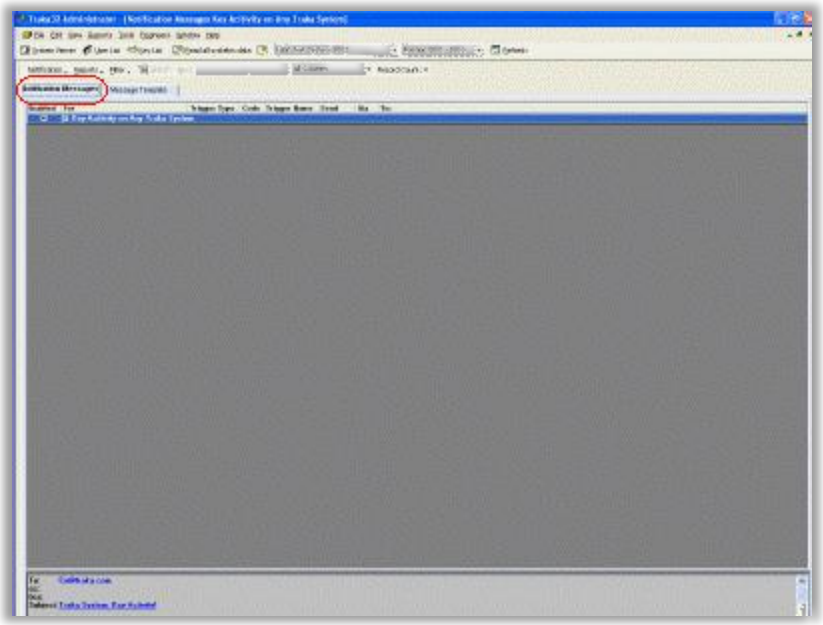
NOTE: Before creating a Message, at least one Message Template needs to exist in the Traka database so as it can be assigned to the Message Rule. Please view Creating Message Templates for a guide on how to create a Message Template.

To create a Notification Message:

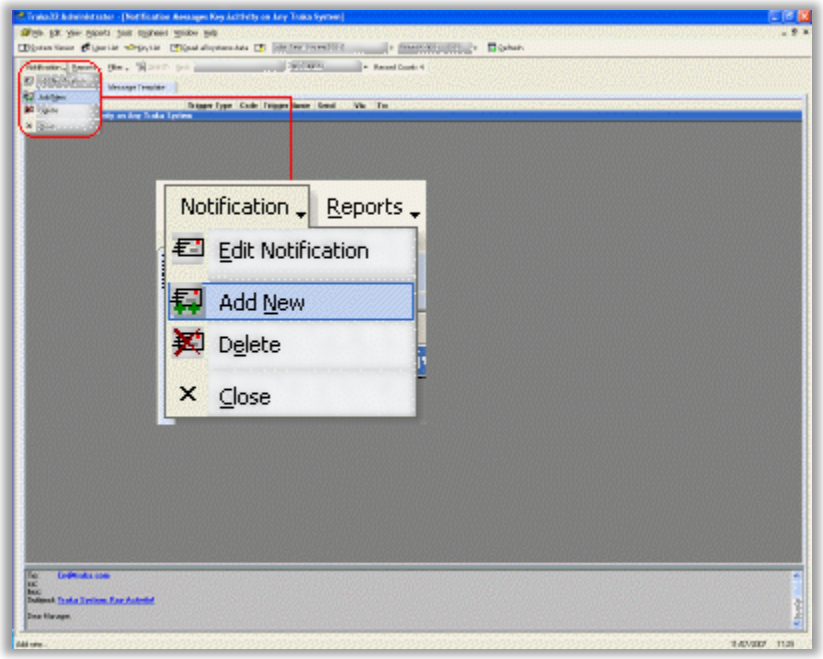
1. From Traka 32 System Viewer click **View > Notifications**:



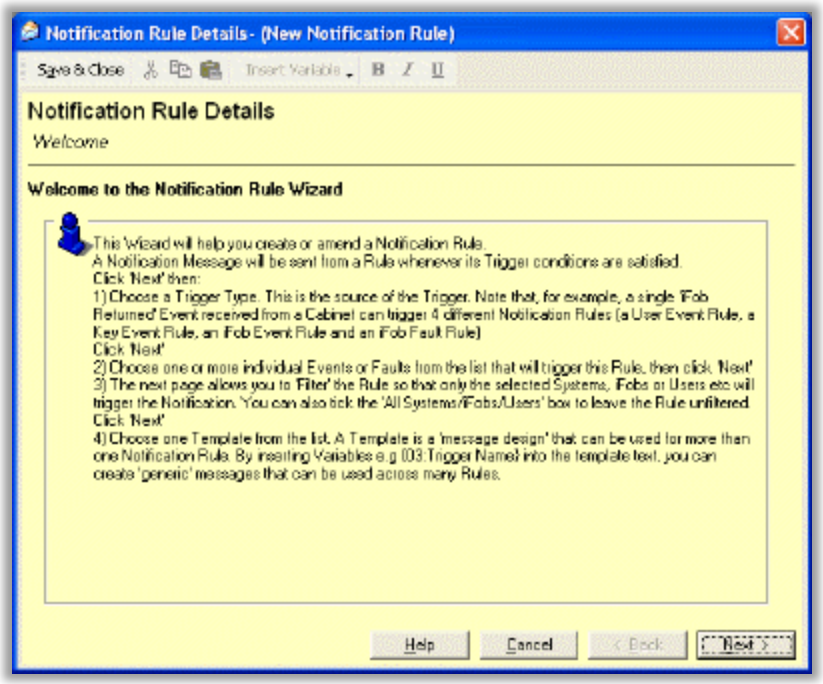
2. Click on the **Notification Messages** tab:



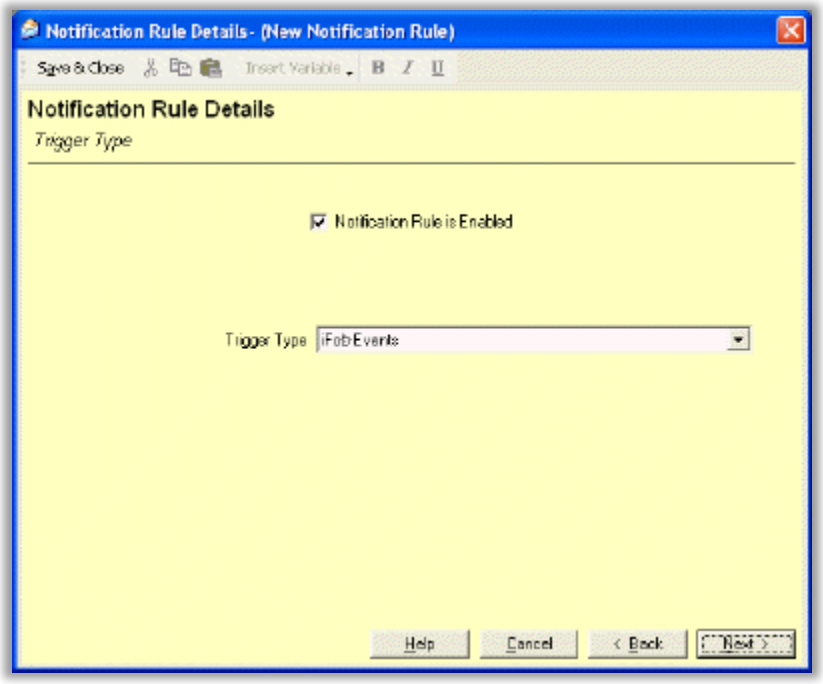
3. Click on **Notifications > Add New**:



4. The **Notification Rule Wizard** is displayed:



5. Click **Next** to display the ***Trigger Type*** window:



Notification Rule

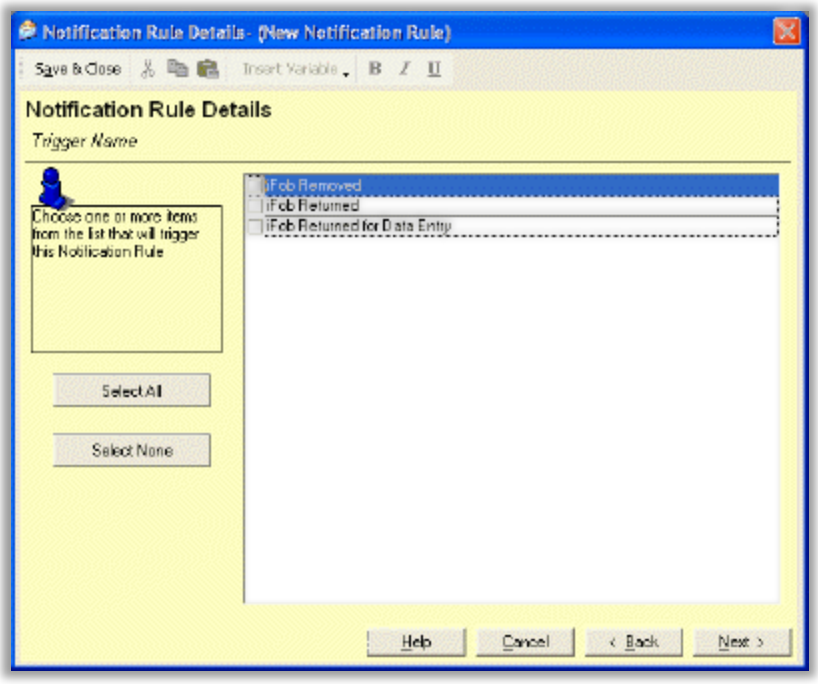
Tick the box to enable the Notification Rule.

Trigger Type

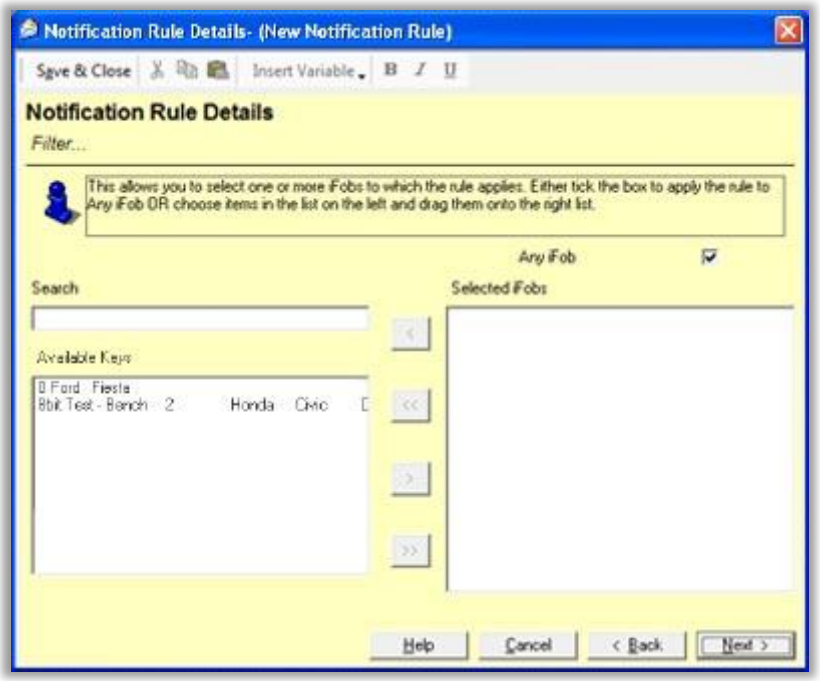
Select the Trigger Type that will cause a message to be sent.

6. Click **Next** to display the ***Trigger Name*** window.

7. **Select one or more Triggers** that will trigger the message to be sent:



8. Click **Next** to display the ***Filter*** window:



Any iFob

Tick the box to apply the rule to any iFob. If not ticked, the rule will only apply to the iFobs in the selected iFobs window.

Available iFobs Window

Lists all available iFobs for each system in the Traka database. If **Any iFob** is **not** ticked, this list will be greyed out.

Selected iFobs Window

Lists the selected iFobs to which the rule applies. If **Any iFob** is **not** ticked, there will be no iFobs listed here.

Use the  to move individual or multiple iFobs from the Selected iFob list to the Available iFob List.

Use the  to move ALL iFobs from the Selected iFob list to the Available iFob List.

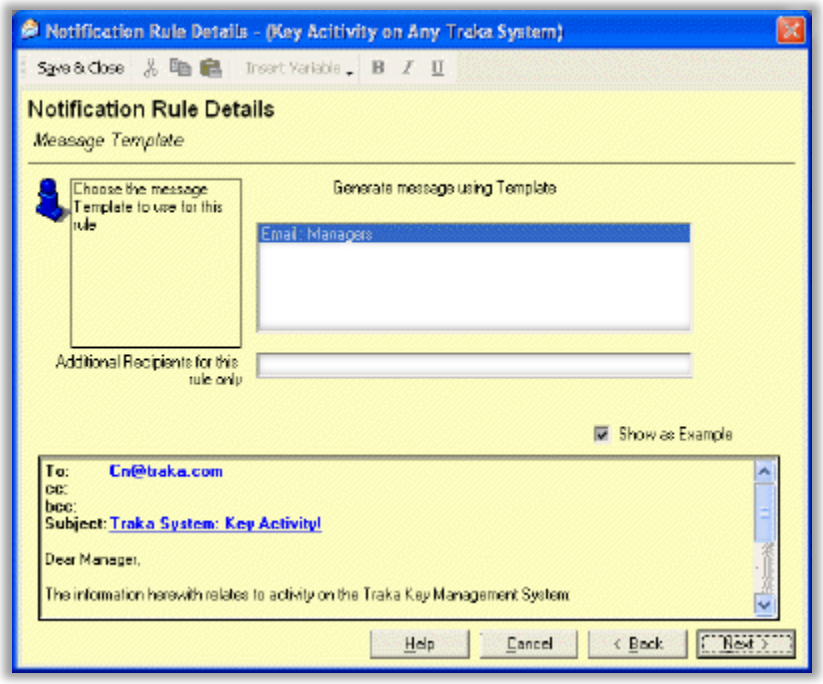
Use the  to move individual or multiple iFobs from the Available iFob list to the Selected iFob list.

Use the  to move ALL iFobs from the Available iFob list to the Selected iFob list.

Search

Allows you to search for specific iFobs via position number, description and system.

9. Click **Next** to display the ***Message Template*** select window:



Generate Message using Template

The available Message Templates are listed and are available for selection.

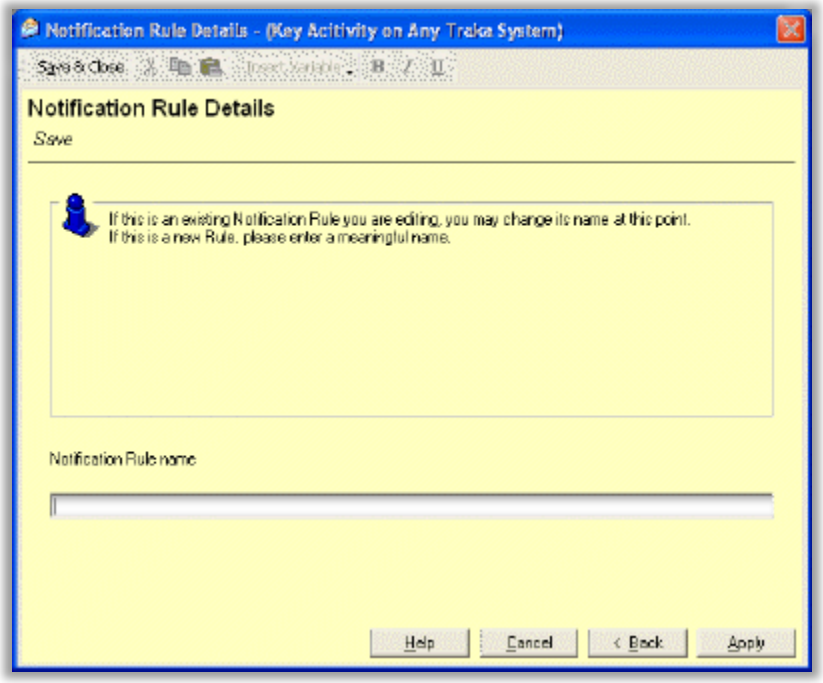
Additional Recipients for this rule only

Enter the email addresses or User name (if using NetSend) of any message recipients in addition to the recipients already included the selected Message Template.

Show Example

Tick this box to display an example of how the message will look.

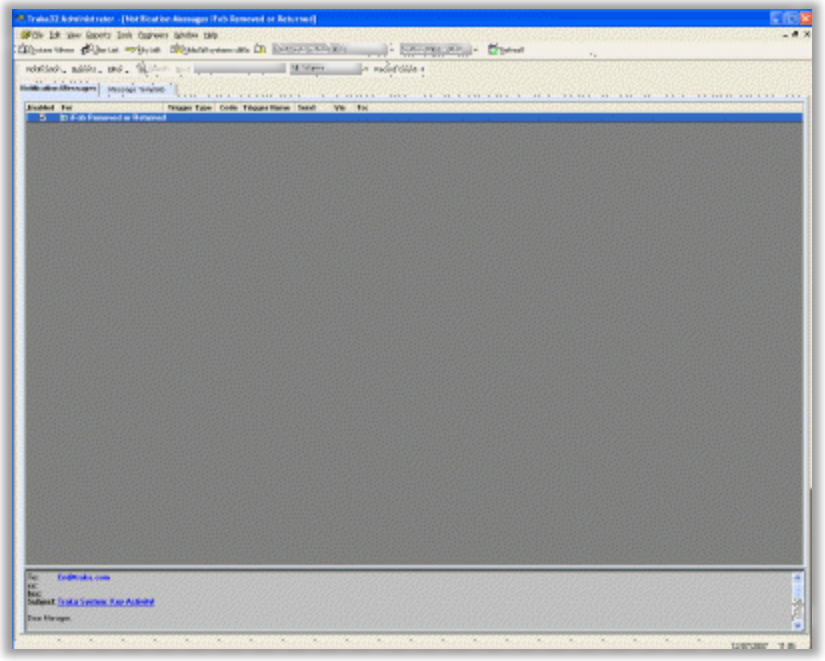
10. Click **Next** to display the ***Save*** window:



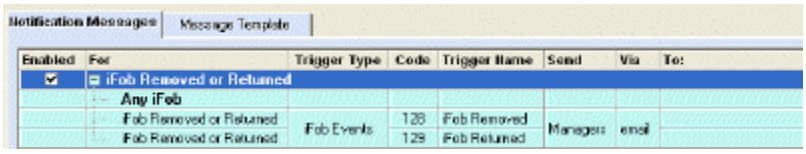
Notification Rule Name

Provide a meaningful name for the Notification Rule.

11. Click on **Apply** followed by **Finish** to save it to the database.
12. The Notification Message Rule will now be viewable in the Notification Messages list.

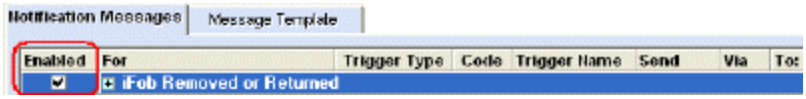


Tip 1. Click on ⊞ next to the Rule name to expand the Rule and display the details.



Tip 2. Double click on the Rule to edit from from the Notification Rule Wizard.

Tip 3. Click the Rule Enabled tick box to easily toggle the Notification Rule ON and OFF as required without entering the wizard.



4.18.5 EMAIL RESPONSE CODES

When using Email Notification there are various response codes sent and received between Traka32 and the customer email server. For example, before an email is sent Traka32 will send a code to the customer email server to ensure that there is a reliable connection. Once received the email server will send a code back to Traka32 confirming that the connection is made and communications are clear.

Some customer email servers send the wrong codes for certain messages, the data has been sent and received correctly however the code that the email server has sent is incorrect. It is possible to change the response codes that are expected back from the customers email server. Below is list of the SMTP codes that are sent to the email server and their default response codes:

Command	Response	Response No.
TELNET Mail Server IP 25	220	1
HELO Client IP	250	2
MAIL FROM: Traka32@Traka.com	250	3
RCPT TO: Email Address	250	4
DATA	354	5
TO: Email Address SUBJECT: Subject FROM: Traka32@Traka.com MIME-Version: 1.0 Content-Type: text/html; charset=utf-8 The message		
.	250	6
QUIT	221	7

Response Code Descriptions

220 - SMTP Service ready.

221 - Service closing.

250 - Requested action taken and completed.

354 - Start message input and end with <CRLF>.<CRLF>. This indicates that the server is ready to accept the message itself.

The following section will need to be added into the T32Settings.ini file, in the example below are all the response codes with their default values. On a customer site you only need to add in the lines that you want different from the default codes.

[Email]

Response1=220

Response2=250

Response3=250

Response4=250

Response5=354

Response6=250

Response7=221

For example, if you know that the response code you should receive for a particular message is 220 but you are receiving 250, then in the settings.ini file under email you will have the following.

[Email]

Response1=250

This allows Traka32 to accept the code 250 in place of 220 and receive the correct response code.

4.19 OPTIONAL FEATURES

4.19.1 ACCESS CONTROL INTEGRATION

4.19.1.1 ANTI PASS-BACK

Many Companies require a way in which they can prevent users from leaving the premises if they still have keys in their possession.

One method now available for Wiegand Readers is to link the Traka Key Control system directly to an existing Access Control system. Traka will update the Access Control system whenever a user has 1 or more keys booked out to them or whenever a user has returned all the keys.

There is no development required and minimal configuration on the Access Control system to implement this solution as it utilises the Anti Pass-Back feature of the Access Control system which is available in 99% of Access Control systems.

Within the Access Control system it will be possible to configure Anti Pass-Back with two zones:

Zone A: Users with no keys
Zone B: Users with 1 or more keys

It will be possible to configure certain Doors or Turn-Stiles that are controlled by the Access Control system to prevent users from passing through them if they are in Zone B.

So when a user takes 1 or more keys from the Traka Key Control system, the Traka Key Control system will inform the Access Control system which in turn will place that user into Zone B, preventing them from leaving the site.

When a user has returned all the keys booked out to them to the Traka Key Control system, the Traka Key Control system will again inform the Access Control system which in turn will place that user into Zone A, allowing them to leave the site.

How does the anti pass-back link work?

To enable the Traka Key Control system to link directly to the Access Control system it is possible to provide the Traka Key Control system with two Wiegand outputs. One output will relate to Zone A and the other output will relate to Zone B. These outputs will then be connected directly to the Access Control system it the same way as the other Access Control Card Readers.

When a user swipes their ID Card on the card reader attached directly to the Traka Key Control system, the Traka Key Control system will allow or deny access to the System / Keys in the normal way but also buffer the users Card ID.

If the user was allowed access by the Traka Key Control system and the user takes 1 or more keys from the Traka Key Control system, the Traka Key Control system will output the buffered Card ID on the Zone B Wiegand output, informing the Access Control system that the user has taken keys.

When returning keys if the user was allowed access by the Traka Key Control system and the user has returned all the keys booked out to them correctly to the Traka Key Control system, the Traka Key Control system will output the buffered Card ID on the Zone A Wiegand output, informing the Access Control system that the user has returned all the keys booked out to them.

The Traka Key Control system will also check if the keys have been returned to the correct slot and will not allow the user to leave site until correctly returned.

Things to note...

If a user already has a key in their possession and they access the Traka Key Control system to take 1 or more additional keys, the Traka Key Control system will not repeat the output to the Access Control system as it will already be aware that the user has keys. The same applies if the user has no keys in their possession and they access the Traka Key Control system and simply close the door without taking any keys.

The Access Control system will have to take into account emergency situations where it is not possible to return a key to the Traka Key Control system.

When using Doors rather than Turn-Stiles, it is possible for one person to authorise the opening of the door and for several people to walk through that door. This will make it difficult (if not impossible) to implement this type of solution.

If a User A hands a key over to User B without returning the key to the Traka Key Control system first (which is what they should do), the key status will not be cleared from User A and so User A will not be able to leave the site. On the downside, User B will be able to leave site (provided they have no keys booked out to them) with the keys that were handed to them. If this does happen, User A will not be able to leave and so users will quickly learn that they must always return keys to the Traka Key Control system.

4.19.2 AUTHORISED ACCESS

4.19.2.1 X SYSTEM AUTHORISERS

Overview

X System Authorisers is an optional feature that can be configured to require either 1 or 2 persons to authorise a user to access the system. Each User can be configured individually with no authorisation, 1 authorisation or 2 authorisations to be required to enable them to open the system door.

When a user that has been configured with 1 authorisation or 2 authorisations tries to access the system, the system will prompt for 1 or 2 authorisers to swipe their cards (and/or enter their PIN's) before opening the door. With the basic 'X System Authorisers' (with no additional options) selected, any user registered on the system can authorise and the door will open allowing access to the keys according to the users access rights.

A user can also be given the ability to self-authorise. To do this they must be given access level 199. With access level 199 a user can access the system without being prompted for any authorisation.

Additional Options

There are additional options that can be selected to further secure access to the system.

- **Force Access Level 199 To Authorise**

  If this option is selected in the firmware then the system will require the authoriser to have access level 199 to authorise other users to access the system. If this option is enabled and the authoriser does not have access level 199 then they will not be able to authorise. Users with access level 199 can also self-authorise, meaning they can access the system without needing another authoriser.

- **Force Access Level 193 To Authorise**

  If this option is selected in the firmware, users with access level 193 will have the ability to authorise access to the system, however they will be unable to self-authorise. Therefore if they try to access a system that requires authorisation then another authoriser will be required.

  NOTE: This option works much the same as 'Force Access Level 199 To Authorise' but without the ability to self-authorise. Both of these options can be used in conjunction with each other.

- **Force Authoriser from Different Group**

  This option forces each Authoriser to be from a different User Group than the user attempting to access the system. See the User Groups topic for more details on groups.

- **Check Authoriser has iFob Access Level**

  The feature called 'Check Authoriser has iFob Access Level' historically was used for X iFob Authorisers only. It has now been modified so that it works for X System Authorisers also. When enabled the system LEDs will illuminate green if both the logged in user and the authoriser have matching access levels. For example, if the logged in user has access to iFobs 1-5 but the authoriser has access to only 1&5, then only positions 1&5 will illuminate as the authoriser can only authorise the release of those iFobs.

- **Authorisation Access Levels**

  This feature can only be used with X iFob Authorisers.

- **X iFob Authoriser**

  X iFob Authoriser is an optional feature that can be configured to require either 1 or 2 persons to authorise the access to the system.

  8bit - On 8bit systems you cant use X System Authorisers and X iFob Authorisers together, they must be used separately.

  16bit - When using the latest 16bit firmware and Traka32 software you can combine X System Authorisers and X iFob Authorisers.

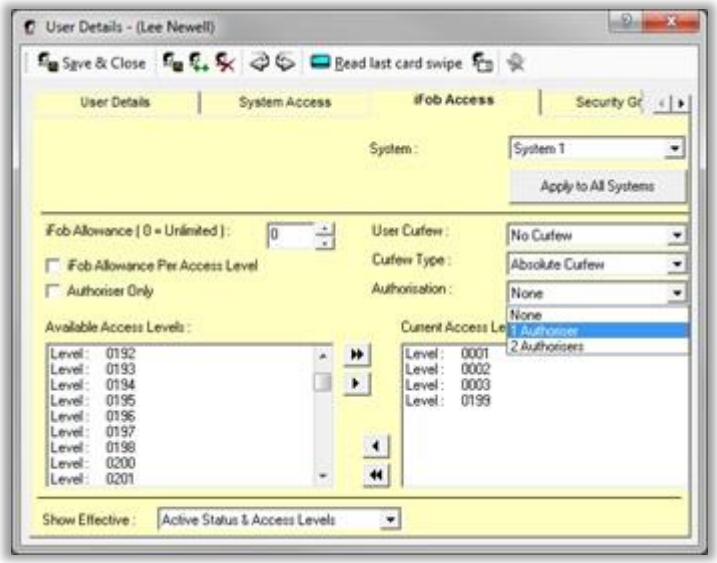
- **Authoriser Only**

  This option allows you to indicate that the user can only authorise other users. With this option selected the user will not be able to access the system themselves. See the setup section below for more details.
  NOTE: This option is available once 'X System Authorisers' is enabled in the firmware from version v3.13.03 onwards.

Setup

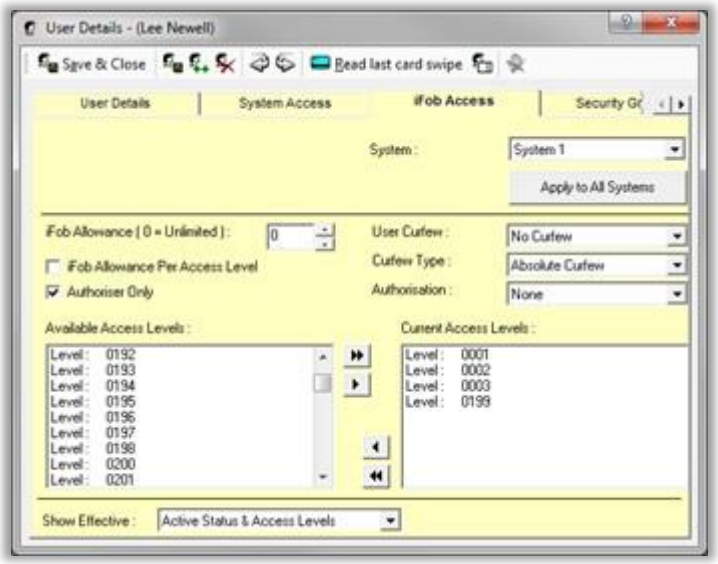
1. Navigate to the User List.
2. Open the desired user Detail window by double clicking the user name.
3. Navigate to the iFob Access tab.
4. From the Authorisation drop down box, select how many other authorisers this user will need before they gain access to the system.

   NOTE: If you leave the selection set to 'None' then the user will require no authorisation to access the system.

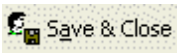


NOTE: If you give the user access level 199 then the system will not prompt for authorisation.

Alternatively, you can select the option to make the user an 'Authoriser Only' as shown below. This will restrict the user from accessing the system themselves but will allow them to authorise other users.



NOTE: The 'Authoriser Only' feature is only available for 16bit systems with firmware version v3.13.05 onwards.

5. Select the desired authorisation and click 

.

4.19.2.2 X IFOB AUTHORISERS

Overview

X iFob Authorisers is an optional feature that can be configured to require either 1 or 2 persons to authorise a user to access an iFob. Each iFob can be configured individually with no authorisation, 1 authorisation or 2 authorisations to be required to enable a user to take it.

If a user tries to take an iFob that has been configured with 1 authorisation or 2 authorisations, then the system will prompt for either 1 or 2 authorisers to swipe their cards (and/or enter their PIN's) before releasing the iFob. With the basic 'X iFob Authorisers' (with no additional options) selected, any user registered on the system can authorise, and the iFob will be released (providing the user has the correct access level). iFobs that are setup with no authorisation can be accessed as normal by any user who has to matching access level.

A user can also be given the ability to self-authorise. To do this they must be given access level 199. This can however, be overridden on an individual iFob basis by checking the 'Deny Single Authoriser Access' tick box in the Edit iFob Details page.

Additional Options

There are additional options that can be selected to further secure the removal of iFobs.

- **Force Access Level 199 To Authorise**

  If this option is selected in the firmware then the system will require the authoriser to have access level 199 to authorise other users to remove the iFob. If this option is enabled and the authoriser does not have access level 199 then they will not be able to authorise. Users with access level 199 can also self-authorise, meaning they can remove an iFob that requires authorisation without needing another authoriser.

- **Force Access Level 193 To Authorise**

  If this option is selected in the firmware, users with access level 193 will have the ability to authorise the removal of an iFob, however they will be unable to self-authorise. Therefore if they try to remove an iFob that requires authorisation then another authoriser will be required.

  NOTE: This option works much the same as 'Force Access Level 199 To Authorise' but without the ability to self-authorise. Both of these options can be used in conjunction with each other.

- **Force Authoriser from Different Group**

  This option forces each Authoriser to be from a different User Group than the user attempting to remove the iFob. See the User Groups topic for more details on groups.

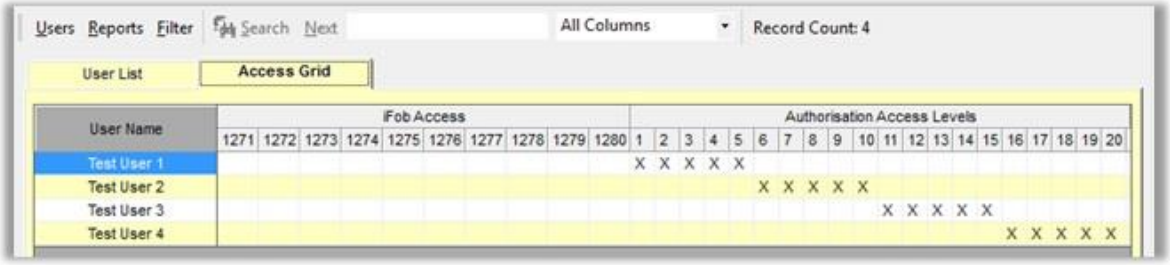
- **X iFob Authorisers - Check Authoriser has iFob Access Level**

  This option forces the authoriser to have the access level of the iFob before they are permitted to authorise its release for another user.

- **Authorisation Access Levels**

  This feature enables separate access levels for Authorisation only. The total number of access levels available is divided in half with the first half remaining as iFob Access Levels and the second half being allocated as Authorisation Access Levels. An authoriser must have an Authorisation Access Level that matches the access level of the iFob, to be able to authorise. For example, if a user has iFob Access Level 5 and tries to remove an iFob with access level 5, the authoriser must have Authorisation Access Level 5.

The simplest way to assign access levels to users using this feature is via the User Access Grid. Scroll along to the right to reveal the Authorisation Access Levels as shown below.



- **X System Authoriser**

  X System Authoriser is an optional feature that can be configured to force either 1 or 2 persons to authorise the access to the system.

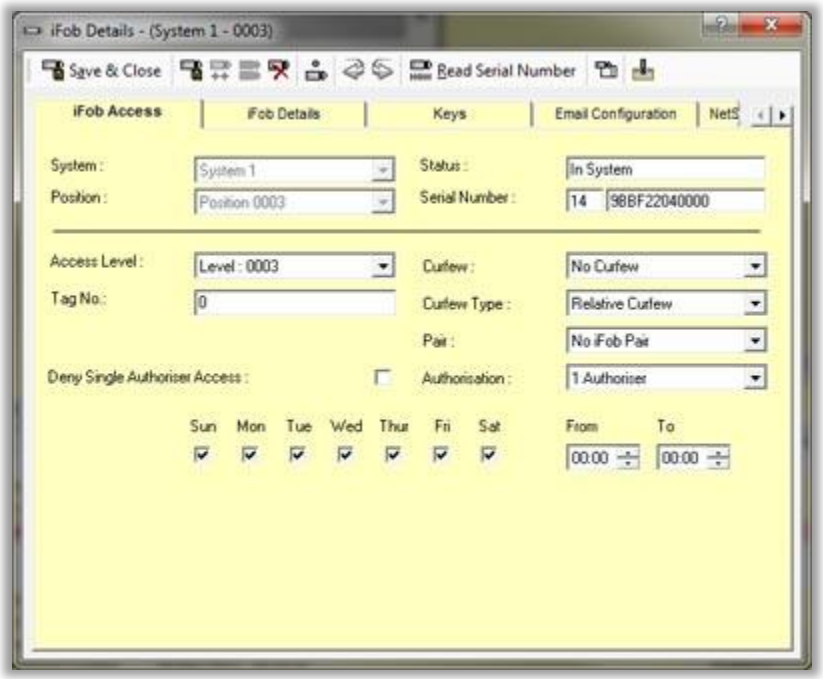
  8bit - On 8bit systems you cannot use X System Authorisers and X iFob Authorisers together, they must be used separately.

  16bit - When using the latest 16bit firmware and Traka32 software you can combine X System Authorisers and X iFob Authorisers.

Setup

1. Right click the desired iFob and select iFob Details.
2. On the iFob Access Tab you will see the Authorisation drop down box. From there you can select 1 or 2 authorisers.

   NOTE: If you leave the selection set to None than the iFob will require no authorisation and can be removed as a normal iFob.

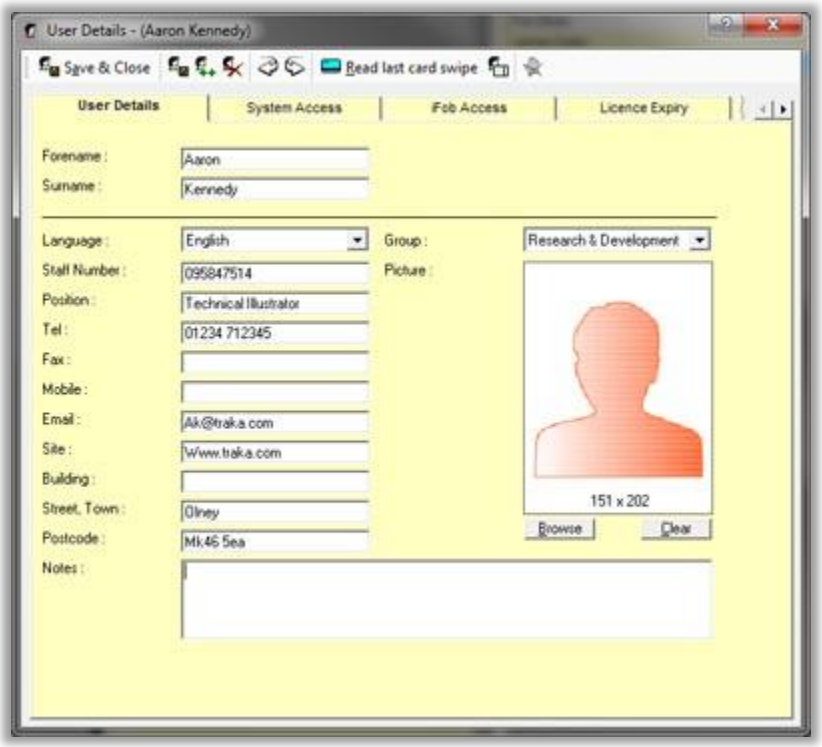


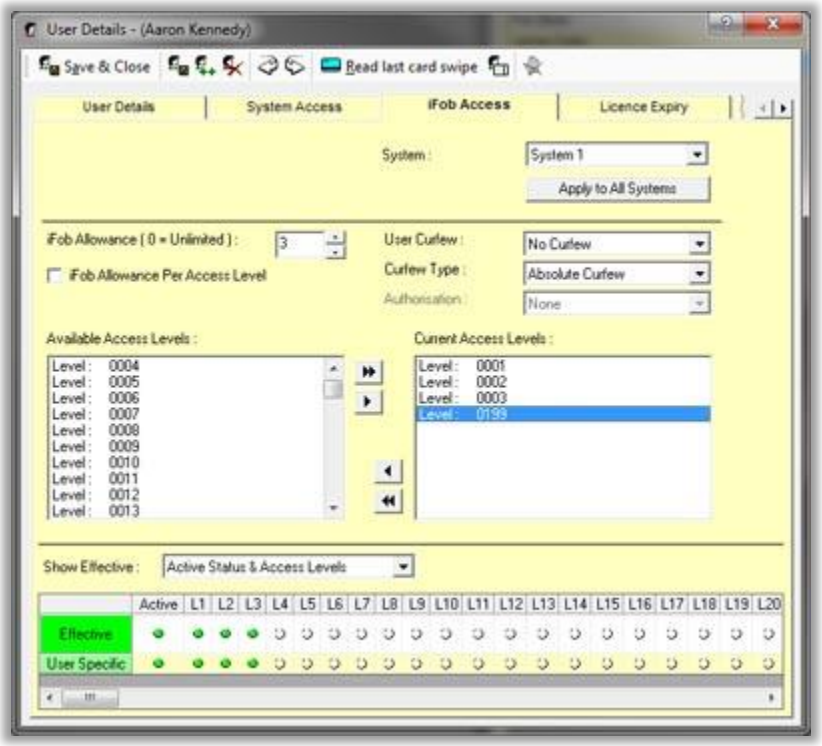
3. Select the desired authorisation and click.
4. Navigate to the User List and open the user details for the desired authoriser user. Depending on whether you have any of the additional options selected, will change which access levels you need to assign to the user.

a. If you selected 'Force Access Level 199 To Authorise' then you will need grant the user with access level 199.

b. If you selected 'Force Authoriser from Different Group' you will need assign the user a User Group that is different to that of the user whom they will authorise.

c. If you selected 'X iFob Authorisers - Check Authoriser has iFob Access Level' then you will need to ensure that you give the user the access level of the iFob they are authorising.

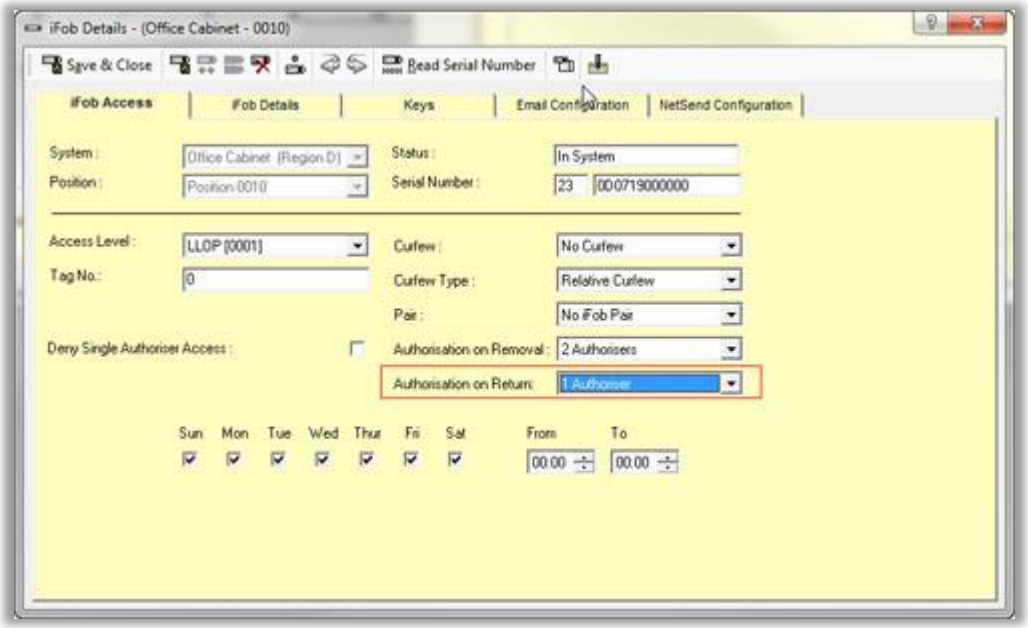




Multiple Authorisation on Return

An iFob can be configured so it requires none, 1 or 2 authorisers when it is returned to the correct position in the system. You will need X iFob Authorisers enabled in the firmware for this option to work.

1. Right click the iFob you wish to have the Multiple Authorisation on Return.
2. The form will open on the iFob Access Tab.
3. Click the Authorisation on Return drop down box and select the desired amount of users.

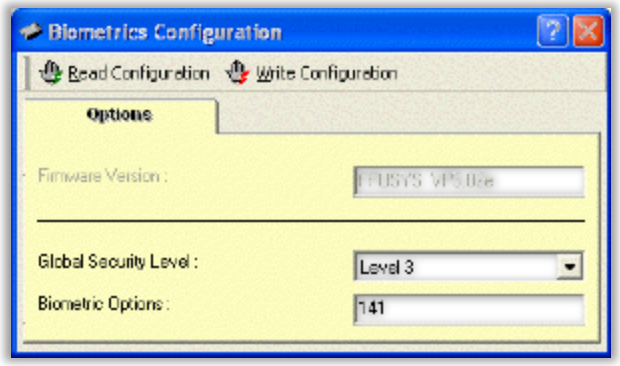


4. Click save & Close.
5. When a user returns the iFob, the system will ask for authorisation. If the no authorisation is given and the door is closed then an 'iFob Returned without Authorization' event is logged against the iFob.

4.19.3 BIOMETRICS

4.19.3.1 CONFIGURE BIOMETRICS

The System Configuration window allows you to view and edit the current configuration of the selected Traka System.



Read Configuration

Click on Read Configuration to read the current configuration of the biometrics reader's firmware in to the Biometrics Configuration window.

Write Configuration

When you are happy with the configuration changes, click on Write Configuration to write the configuration to the biometrics reader's firmware.

Firmware Version

This field shows the current version of the biometrics reader firmware.

Global Security Level

This field allows you to adjust the sensitivity of the reader. The following options are available...

- **PIN Only** - The biometrics reader will only ask for a PIN and not prompt for a fingerprint.
- **Any Fingerprint** - The biometrics reader will ask for a PIN and prompt for a fingerprint but will not check if the fingerprint matches the PIN.
- **Level 1 to 5** - The biometrics reader will ask for a PIN, prompt for a fingerprint and will check that the fingerprint matches the associated PIN. The level of sensitivity can be adjusted from 1 to 5, 1 being the lowest and 5 being the highest. Adjusting the level will not compromise the accuracy of the verification.

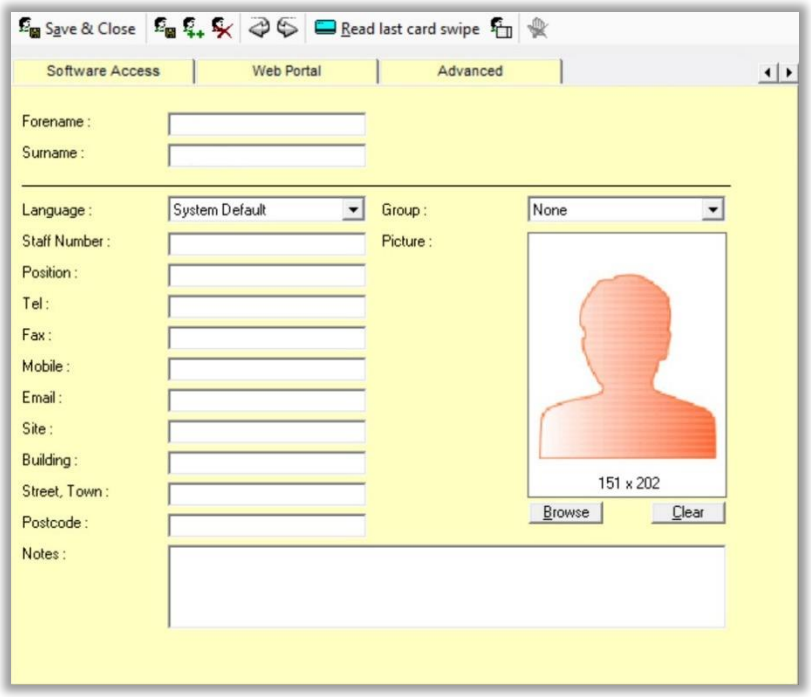
  TIP: If you are finding that it is difficult to enrol new users or if users that have been enrolled are having difficulties verifying their fingerprint then reduce the sensitivity.

Biometric Options

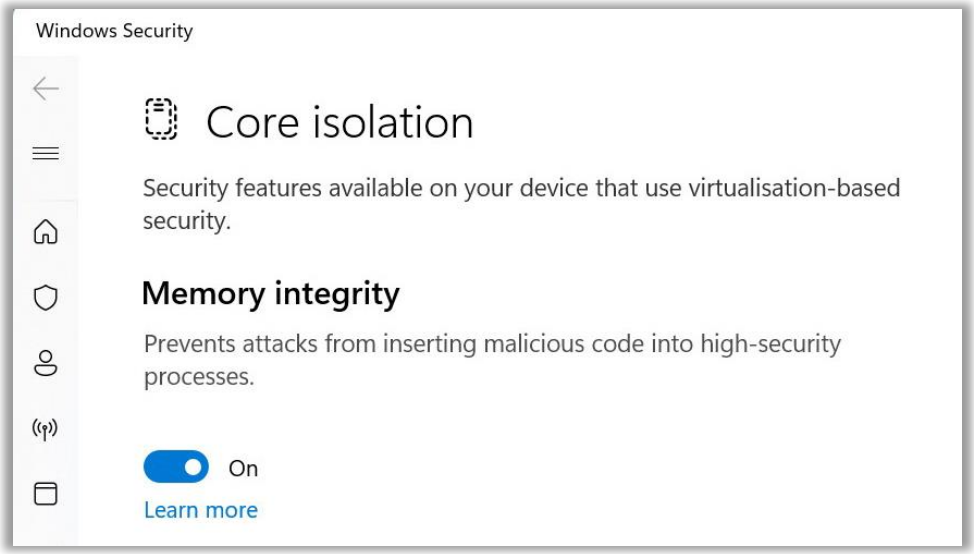
This field allows adjustments to be made to the biometrics reader operation. Please do not adjust this unless instructed to be a Traka Engineer. The default setting should be **141**.

4.19.3.2 CONFIGURE BIOMETRICS – WINDOWS 11

When using Traka32 with Windows 11, it will be noticed that the Biometrics tab is not available within User Details.



This is due to a security setting within **Windows Security** for **Memory Integrity.** By default, this option is enabled.



It will also be noted that if the fingerprint reader is connected to a PC, it will not be recognised as a Sagem device.

Disabling the Memory Integrity feature will resolve this issue. However, this may be considered a security risk.

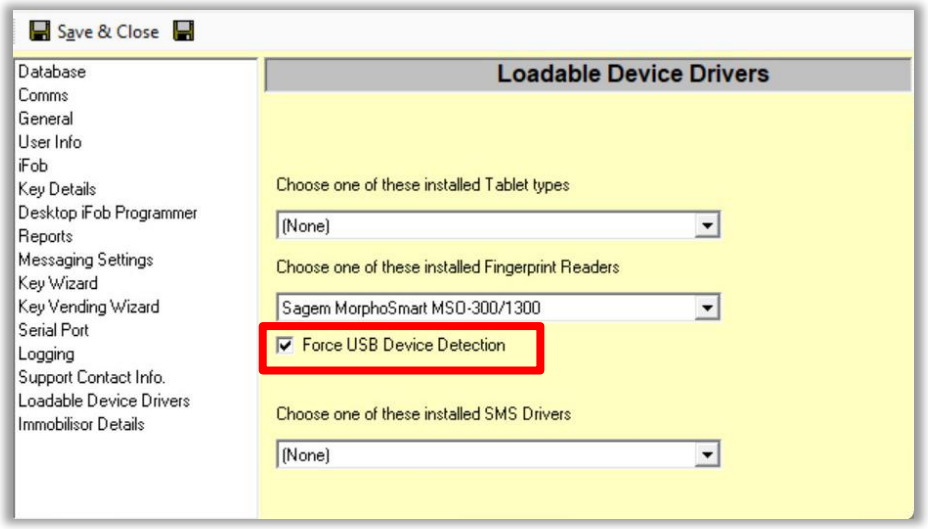
An alternative solution will be to install an additional USB driver that can located within:

Program Files (x86) / Traka Limited / Traka32 / Drivers / Biometrics.

1. Install the **MSO_USB_Driver x64** Windows Installer Package.

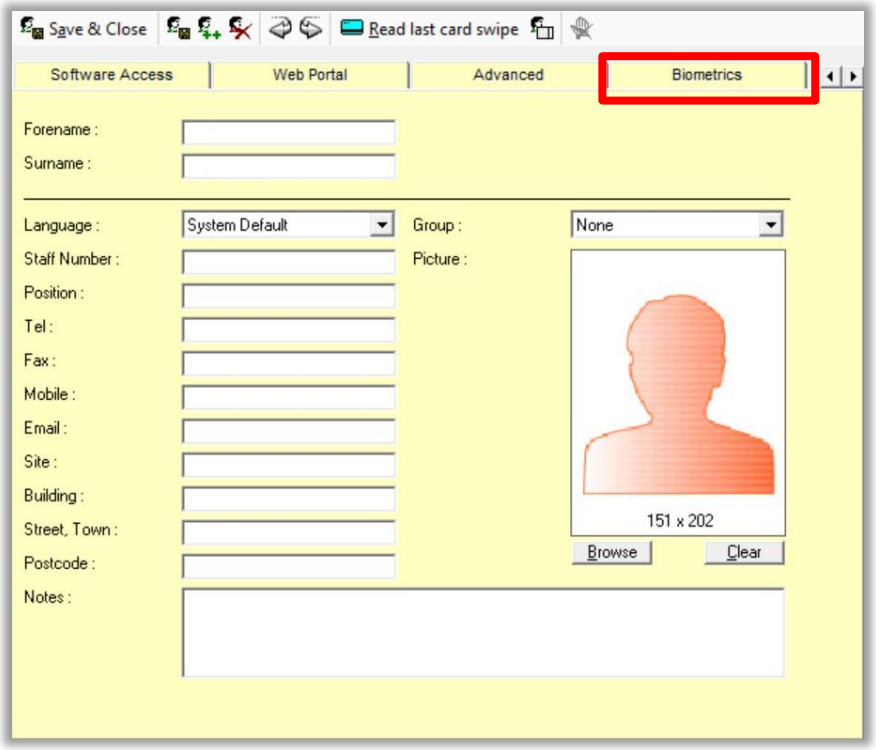
NOTE: The TrakaMSO300 Driver 32-bit and TrakaMSO300 Driver 64-bit are only compatible with Windows 11 when the Memory Integrity is enabled and only then can the new drivers be installed.

2. Withinin Traka32, navigate to the **Loadable Device Drivers** page and place a tick in the box for **Force USB Device Detection**.



This will enable the drivers to be detected with the Core Isolation/Memory Integrity enabled within Windows Security.

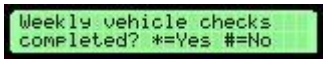
3. Navigate to the User Details Page. The **Biometrics** tab will now be visible.



4.19.4 DAILY / WEEKLY VEHICLE CHECKS

4.19.4.1 DAILY / WEEKLY VEHICLE CHECK OVERVIEW

When managing a fleet of vehicles it is important that checks are made on the condition of the vehicles. The daily \ weekly vehicle check option is designed to prompt a user to make their checks on a daily and/or weekly basis. The Traka System will prompt the user when they return their iFob and Keys and ask if they have completed their check.



An audit of if the users has made their checks is kept on the event reports.

4.19.5 FAULT LOGGING

4.19.5.1 FAULT LOGGING OVERVIEW

Fault Logging allows users to log and report problems or faults with the asset or equipment they have been using. Once activated, the user is prompted to key in a fault code whenever an iFob is returned to the system.

Faults can be split in to two categories, critical and non-critical.

- No fault has an index of 0.
- Critical faults have an index between 1 and 127. If a critical fault is logged when an iFob is returned, only users that have access level 200 in addition to the access level of the iFob can take the iFob until the fault is cleared.

- Non-Critical faults have an index between 128 and 255. If a non-critical fault is logged when an iFob is returned, users that have access to the iFob can still have access but they will be warned that a non-critical fault has been logged until the fault has been cleared.

In order to use Fault Logging it must first be enabled in the firmware configuration. There are 3 firmware configuration options available for Fault Logging:

1. Firmware has Fault Logging Enabled – a single fault can be logged per position and from Traka32 only.

2. Firmware Allows Faults to be Logged at Cabinet – as above but users can also log faults at the Traka System as well as Traka32. This option can only be selected in conjunction with option 1.

3. Firmware has Extended Fault Logging Enabled – this option allows up to 5 faults to be logged against one position. This option can only be selected in conjunction with option 1, and can also be used with option 2.

NOTE: It is also possible to enable / disable the fault logging option on a per iFob basis from the iFob Details window.

4.19.5.2 HOW TO IMPLEMENT FAULT LOGGING

NOTE: Fault Logging will only be available if the firmware of the selected system has Fault Logging enabled.

1. The first stage is to decide on a list of common faults and whether those faults are 'critical' on 'non-critical'.

2. The next step is to enter the fault details into the Traka32 software. Please refer to the Adding Fault Details section for more details.

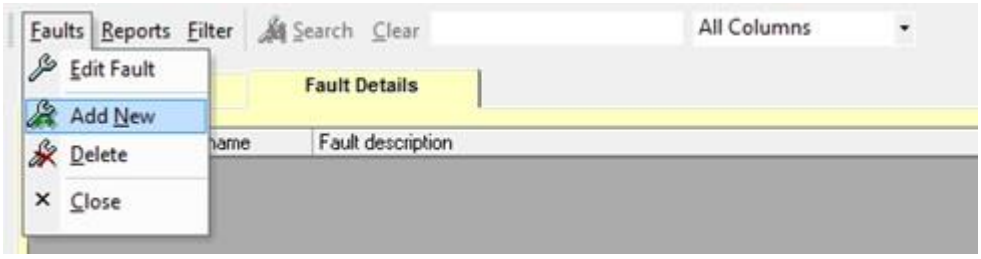
3. If your system is configured to allow faults to be logged at the cabinet, after you have added all the relevant faults, print a list of the fault indexes and descriptions, laminate them and stick them next to the Pod of each Traka System. When users return an iFob they will be prompted to enter a fault code. The fault codes can be looked up on the fault list next to the Pod.

4. Set up the user records of the engineers who will be repairing the faults and assign them with access level 200 as well the access levels of all the iFobs they will need access to. When a critical fault is logged, the only users that can remove the iFob are those with access level 200 as well as the access level of the iFob, until the fault has been cleared.

4.19.5.3 ADDING FAULT DETAILS

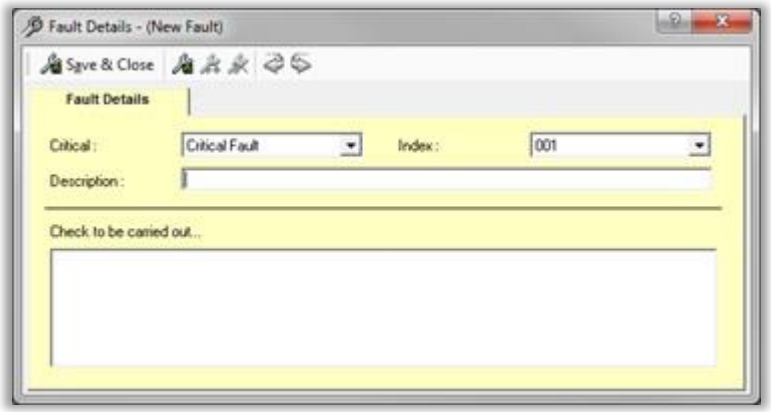
A Fault Detail is a type of fault applicable to the items your iFobs are managing. For example, if your iFobs are used to hold vehicle keys, one applicable fault detail could be 'Faulty Brakes'.

1. From the main toolbar click **View**, **Fault List**.
2. Select the **Fault Details** tab.
3. From the fault list click on the **Faults** menu followed by **Add New**.



NOTE: If you already have a fault record open you can create a new record by simply clicking on the  **button.**

4. Enter the relevant information for the Fault Detail…



Critical: Select whether the fault will be a 'critical' or 'non-critical' fault.

Index: Select the index number from the dropdown. The range of numbers available will be dependent on whether you selected 'critical' or 'non-critical', and only unused numbers will be displayed. Critical faults have an index range from 1 to 127, and non-critical faults are between 128 and 255.

Description: Enter a description for the Fault. This description will appear in the Outstanding Fault List in the 'Fault Name' column.

Check to be carried out: Enter a description for the work to be carried out in order to fix this fault.

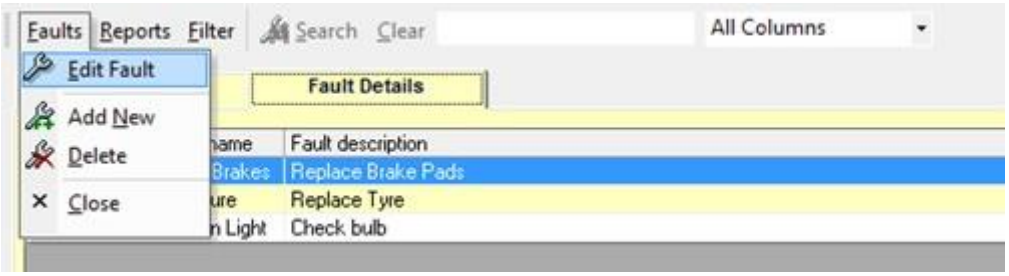
5. To **Save** your changes, simply click on  or, to **Cancel** your changes, simply close the window and click 'No' when asked to save the changes.

4.19.5.4 EDITING FAULT DETAILS

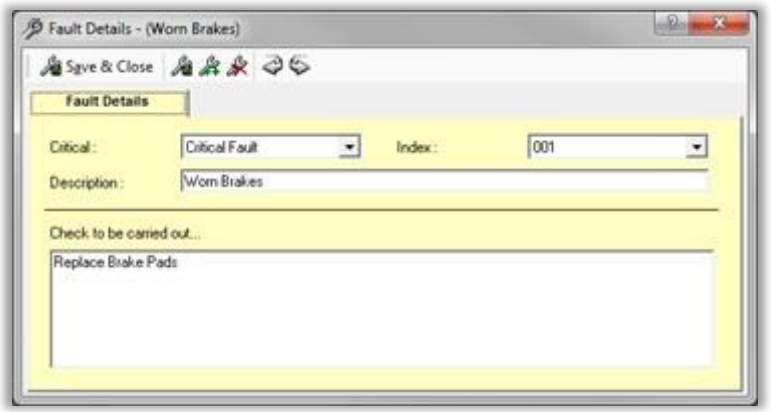
1. From the main menu click on **View**, **Fault List**.

1. Select the **Fault Details** tab.

2. From the fault list simply **double click** on the fault record you wish to edit or select the record and click on the **Faults** menu followed by **Edit Fault.**



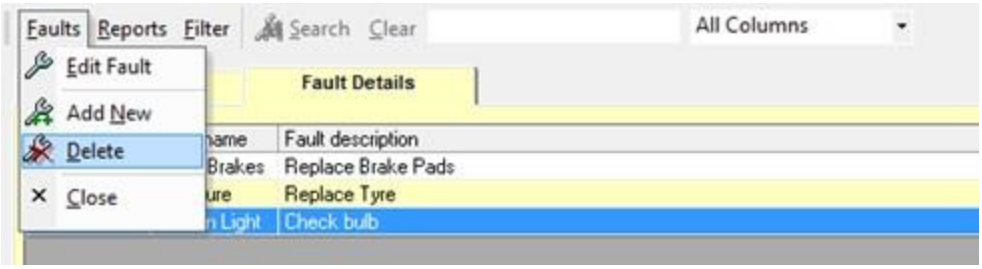
3. The selected fault record will open. Edit the appropriate details.



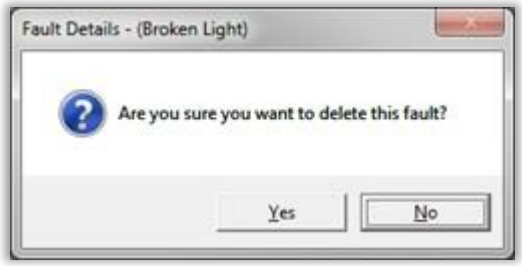
4. To **Save** your changes, simply click on  or . To **Cancel** your changes, simply close the window and click 'No' when asked to save the changes.

4.19.5.5 DELETING FAULT DETAILS

1. From the main menu click on **View**, **Fault List**.
2. Select the **Fault Details** tab.
3. From the fault list simply **click** on the fault record you wish to delete, click on the **Faults** menu followed by **Delete**.



4. Click **Yes** to confirm you want to delete the fault detail.

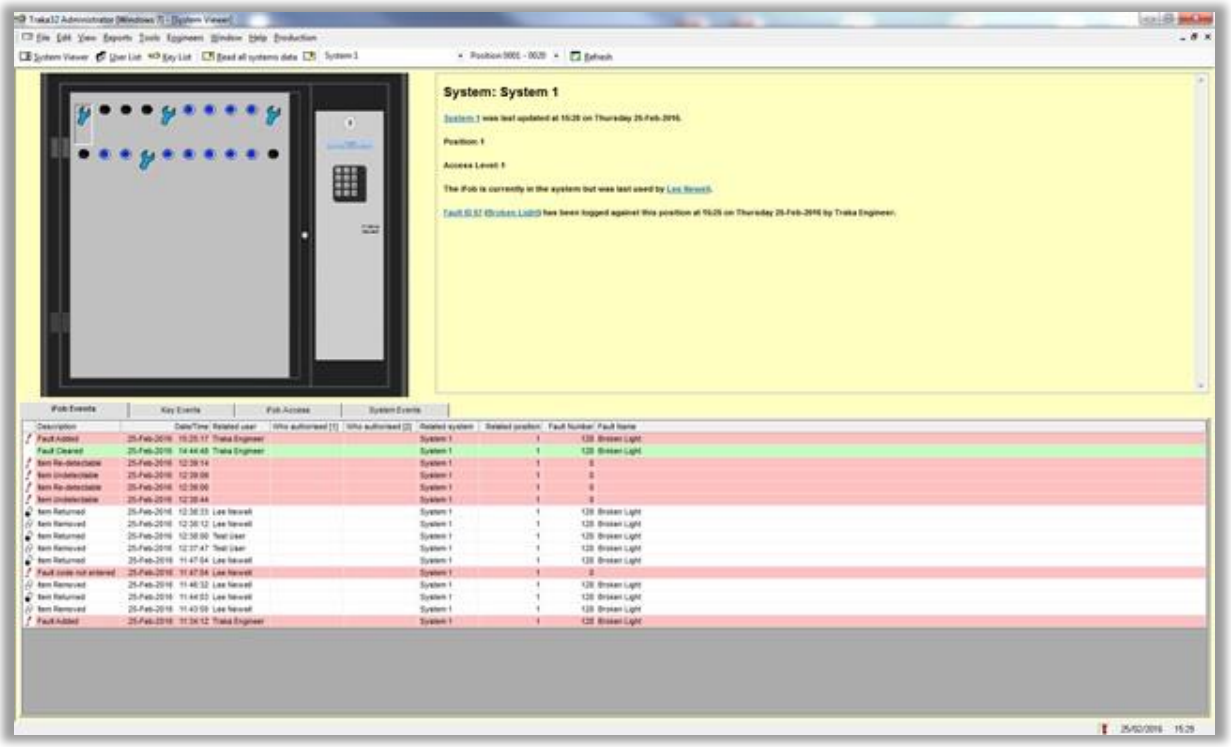


NOTE: If you already have a fault record open you can delete the record simply by clicking on the  **button.**

4.19.5.6 LOGGING FAULTS

Faults can be logged against an iFob directly from the Traka32 software and also at the Traka System when an iFob is returned. Once a Fault has been logged, it will appear in the Outstanding Faults list. Critical Faults will be coloured Red, and Non-critical Faults will be coloured Yellow in the Outstanding Faults list.

The system viewer will show iFobs with Faults logged against them highlighted with a blue spanner icon  . The panel to the right will show the fault that has been logged against the selected position. If there is more than one fault, and one of them is critical, the critical fault will be shown here. Otherwise, the fault shown will be the 'oldest' fault.



Logging a fault will also generate a 'Fault Added' iFob event. If no fault code is entered, a 'Fault code not entered' event will be generated.

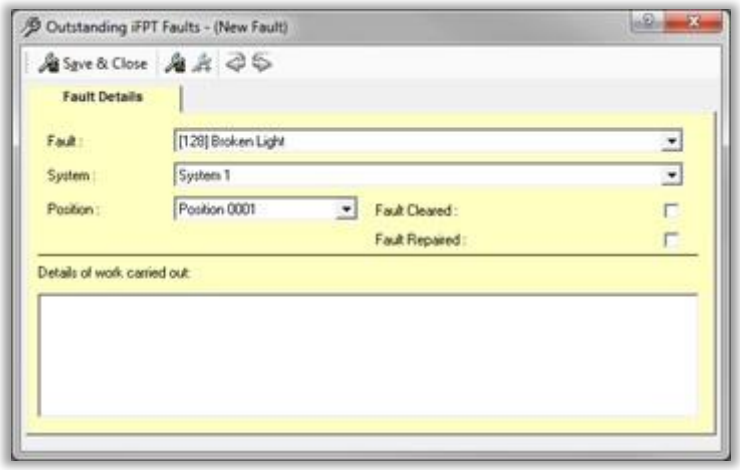
Logging Faults in Traka32

1. From the main menu click on **View**, **Fault List**.
2. Select the **Outstanding Faults** tab.

3. From the fault list click on the **Faults** menu followed by **Add New**.

NOTE: If you already have an outstanding fault record open you can create a new record by simply clicking on the  **button.**

4. A new blank outstanding fault record will be created.



5. Select the appropriate fault from the dropdown list, and then specify the system and position number you wish the fault to apply to.

6. To **Save** your changes, simply click on  or . To **Cancel** your changes, simply close the window and click 'No' when asked to save the changes.

7. Once a new fault record has been saved, Traka32 will communicate with the system and the fault will appear in the Outstanding Faults list.

Logging Faults at the Traka System

NOTE: To enable logging faults at the Traka System the option must first be enabled in the firmware configuration. See the Fault Logging Overview section for more details.

1. When a user returns an iFob to the system, if the iFob has no existing fault a message will appear on the LCD asking them if they wish to enter a fault code.

   If the iFob has an existing fault you can add another fault (up to a maximum of 5 faults) providing you have 'Extended Fault Logging' enabled in the firmware. The existing fault(s) will be displayed on the LCD briefly before then asking if you wish to enter a fault code.

   NOTE: A user with access level 200 will also be able to edit/clear any existing faults at this point. See the Clearing Faults section for more details.

2. Press the # (hash) key for 'Yes' and you will then be prompted to enter a fault code against the iFob.

3. Enter the appropriate fault number from the list of fault details generated in the Adding Fault Details section, and then press the # (hash) key.

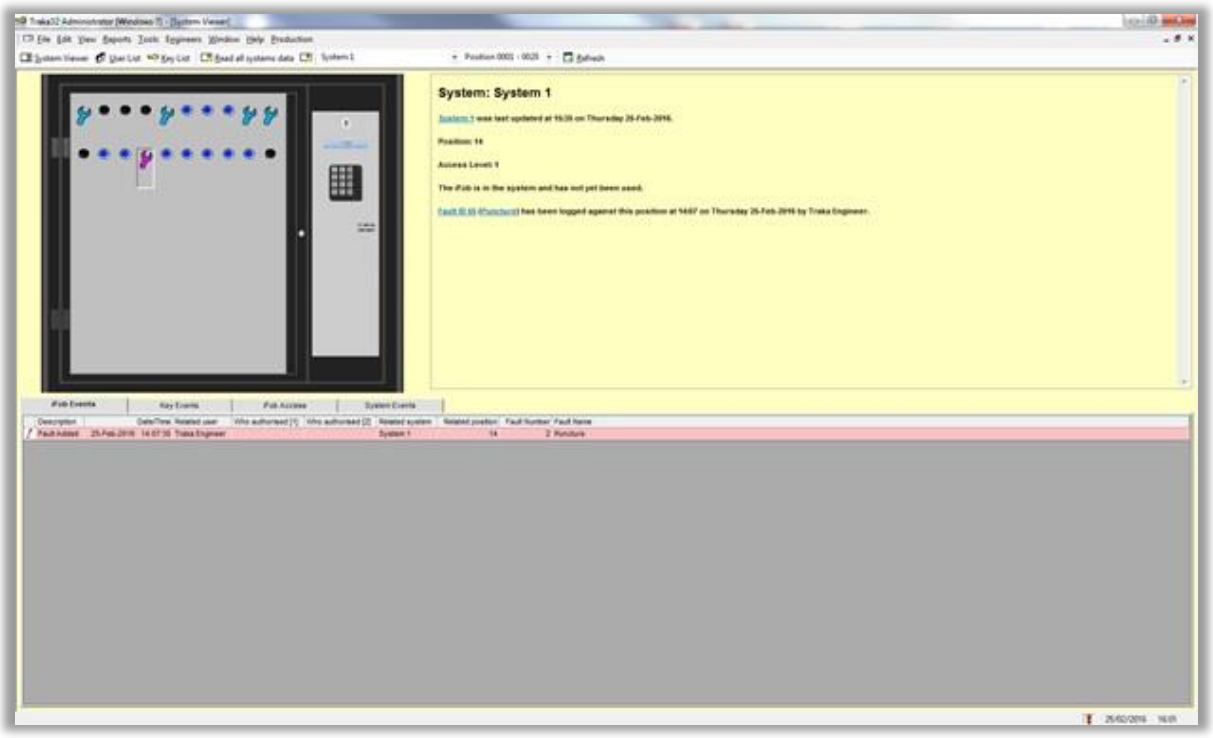
4. The system will then show you which fault code you have logged against the iFob.

5. If your system is configured with the 'Extended Fault Logging' option allowing multiple faults to be logged against one position, the LCD will then revert back to the fault screen allowing you to add more faults (up to a maximum of five). Select 'No' once you have finished adding faults.

6. Once any faults have been logged you can Read All System Data from Traka32 to update the Outstanding Faults list and System Viewer with the new faults. If your system has Auto-Comms enabled it will send the fault details to Trak32 upon the next communication.

4.19.5.7 CLEARING AND REPAIRING FAULTS

Faults can be cleared at the Traka system when returning the iFob, and can also be cleared or repaired from Traka32. Once a fault has been cleared it will disappear from the Outstanding Faults list. When a fault is marked as repaired, it will remain in the list but will be highlighted as repaired and shown in the system viewer with a pink spanner icon.

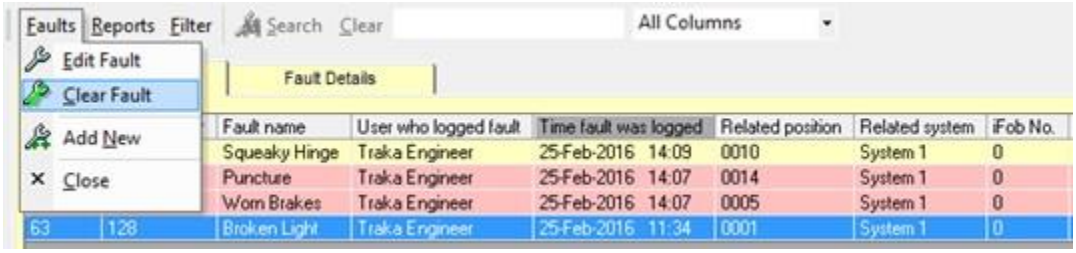


When faults are cleared the system will generate a 'Fault Cleared' iFob event.

Clearing and Repairing Faults in Traka32

1. From the main menu click on **View**, **Fault List**.
2. Select the **Outstanding Faults** tab.
3. From the Outstanding Faults List select the Fault you wish to clear or mark as repaired, and then click on the **Faults** menu followed by **Clear Fault**.

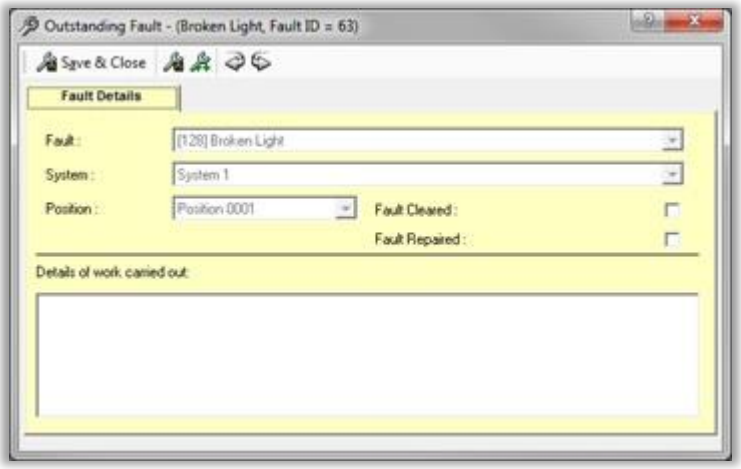
   NOTE: Faults shown in Red are critical, faults shown in Yellow are non-critical.



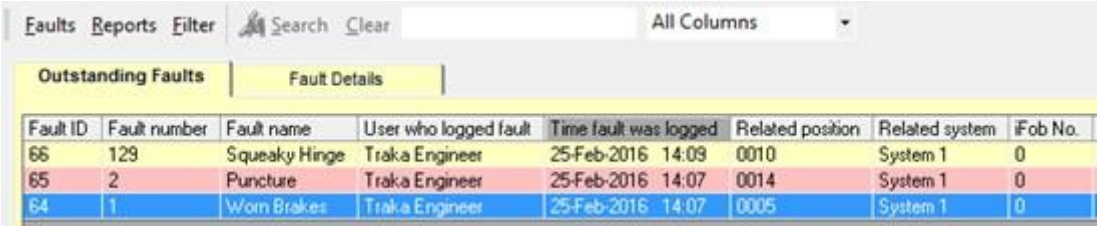
4. The Outstanding Fault window will appear. From hear you can select either 'Fault Cleared' or 'Fault Repaired' by checking the corresponding tick box, and also add details of any work carried out.

   Fault Cleared: Selecting 'Fault Cleared' will remove the fault from the iFob and delete the Outstanding Fault record from the list.

Fault Repaired: Selecting 'Fault Repaired' will highlight that the fault has been repaired but will not clear the fault or remove it from the list. This can be useful to highlight that a repair has been carried out but has not yet been approved or checked for clearing.



5. Select either 'Fault Cleared' or 'Fault Repaired' and click Save & Close. If you selected 'Fault Cleared', Traka32 will communicate with the Traka System removing the fault from the iFob. The fault will also have disappeared from the Outstanding Faults list.



Clearing Faults at the Traka System

NOTE: To enable clearing faults at the Traka System the option for Fault Logging at the cabinet must first be enabled in the firmware configuration. See the Fault Logging Overview section for more details.

In order for a user to clear a fault at the Traka System they must first have access level 200.

1. When a user with Access Level 200 returns an iFob with a fault to the system a message will appear on the LCD showing the current fault code(s) for a few seconds followed by a message asking them to enter a fault code. This second message will have the existing fault code already displayed.

2. If you wish to clear this fault, press the * (star) key to delete the fault code and then press the # (hash) key. If you do not wish to clear the fault, simply press the # (hash) key without deleting the number to keep the fault.

   If the iFob has multiple faults, the LCD will then display the next fault number allowing you to delete the number to clear that fault too.

3. Once you have cleared/skipped through all of the existing faults, the LCD will then ask if you wish to enter a fault code. This enables you to both clear faults and add any new faults that may have been found within the same transaction.

4. Once any faults have been cleared you can Read All System Data from Traka32 to update the Outstanding Faults list and System Viewer with the new status. If your system has Auto-Comms enabled it will send the cleared fault details to Trak32 upon the next communication.

4.19.5.8 FAULT LOGGING ON IFOB REMOVAL

NOTE: This option is only available on 8bit RFID Lockers with version 6.08.033 firmware.

NOTE: This section assumes the user has prior knowledge of the operation of the Fault Logging feature. Please read from the start of the Fault Logging section of this guide and then refer to this section on how to log a fault on iFob removal.

To be able log a fault when removing an iFob, the Fault Logging option will need to be enabled in the systems firmware. With Fault Logging enabled you have the option of entering a fault code when certain iFobs are removed from the system. This is configured on an individual iFob basis.

1. From the System Viewer right click the iFob you wish to configure.
2. Select 'Edit iFob Details'.
3. Tick the box that states 'Prompt For Fault On iFob Removal'.
4. Click 'Save & Close'.
5. When a user next removes that iFob they will be asked to enter a fault code.

4.19.5.9 FAULT LOGGING VIA IMMOBILISORS

Fault Logging allows users to log and report problems or faults with Data Loggers (Immobilisors). Whenever an iFob has had a fault logged against it via the Immobilisor and has been replaced in the cabinet, the user is prompted to key in a fault code for that particular Immobilisor.

NOTE: You can only log Critical Faults at the Immobilisor.

The first stage of implementing Fault Logging is to decide on a list of common faults that are split into the two categories of critical and non-critical.

- No Fault has an index of 0.
- Critical faults have an index between 1 and 127.
- Non-Critical faults have an index between 128 and 255.

Enter the fault details into the Traka32 software. Please refer to the Adding Fault Details section for more details.

After you have added all the relevant faults, print a list of the fault indexes and descriptions, laminate them and stick them next to the Pod of each Traka System.

Set up the user records of the engineers who will be repairing the faults with access level 200 as well the access levels of all the iFobs they will need access to.

When a critical fault is logged the only users that can remove the iFob are those with access level 200 as well as the access level of the iFob until the fault has been cleared.

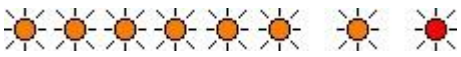
When users return an iFob they will be prompted to enter a fault code. The fault codes can be looked up on the fault list next to the Pod.

NOTE: Immobilisor Fault Logging is not compatible with our standard cabinet Fault Logging. If you require standard Fault Logging you must run this option on a separate System.

How to log a fault to the Immobilisor

Insert your vehicle iFob into the receptor barrel of the Immobilisor and the LED on the Acceptance button will be flashing green intermittently. Press and hold the acceptance button for 10 seconds to receive the following sequence of flashes.

NOTE: If the driver discovers a fault whilst the vehicle is active, they must remove the iFob and re-insert it to the receptor barrel to log a fault to the Immobilisor.



This indicates that the fault has successfully been written to both the Immobilisor and the iFob. This series of flashes will continue until you remove the iFob from the receptor barrel of the Immobilisor. You can now to go back to the cabinet and return the iFob, upon which you will be confronted by a message on the LCD requiring you to enter a fault code.

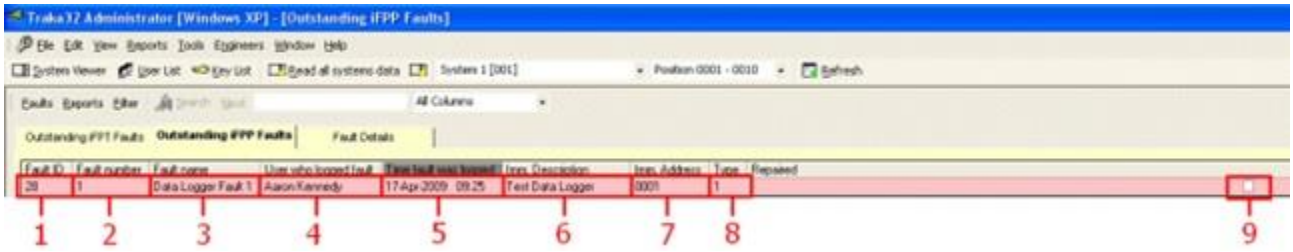
Enter your previously configured fault code and press # then close the door.

NOTE: Whilst you have a fault logged against an iFob, that particular iFob will not work in the Immobilisor again until the fault has been read from the iFob via Traka32 and the Immobilisor has been reset using a service iFob.

Viewing the Fault List

After returning your iFob to the cabinet go to the Traka32 software and Read All System Data, then at the top left of the screen click **View** > **Fault List**.

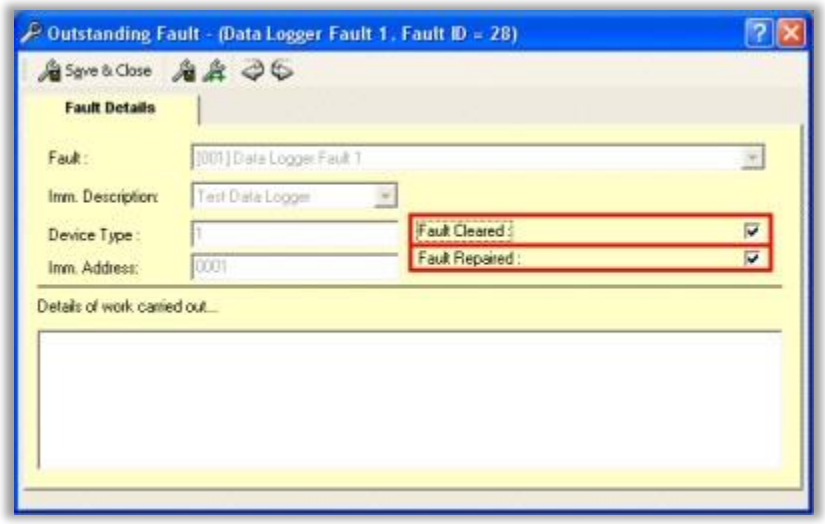
You will notice there is now an outstanding fault stored in the iFPP tab waiting to be repaired or cleared (see below).



1. The Fault ID box shows the unique number assigned to the fault by Traka32.
2. The Fault number shows which Fault Code was logged against this particular transaction.
3. This is the name of the fault that was given when creating the fault details.
4. The User who logged the fault.
5. The Date and time the fault was logged.
6. The description of the Immobilisor the fault has been logged to.
7. The Address of the Immobilisor.
8. The Immobilisor Type.
9. The repaired box (if ticked) shows that the Immobilisor has been repaired.

Double click the outstanding fault and the details window will appear. The greyed out section on the left is information about the Immobilisor and the fault itself and is unchangeable at this point.

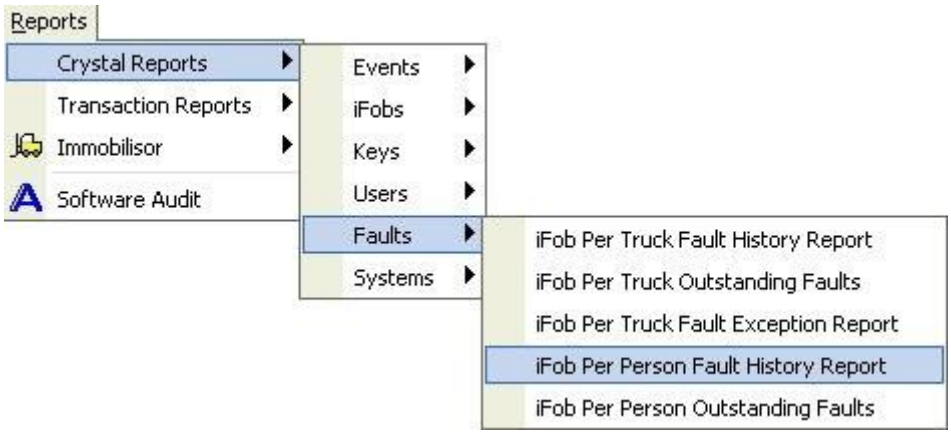
This window gives you the options of repairing the fault and/or clearing the fault, also there is a notes section at the bottom were you can specify the work carried out on the vehicle. After selecting the appropriate options click the Save & Close button in the top left corner.



NOTE: If a fault is repaired then the fault will still be present in the outstanding fault list within Traka32, also the box in the repaired section will now be ticked. Only when a fault is cleared will it be removed from the Outstanding Fault List completely.

Fault Reports

Each Immobilisor fault that is logged to Traka32 is saved in a report. You are able to view reports for Outstanding Faults and Fault History. To view the reports of the Immobilisors that have had faults logged against them and then been cleared and/or repaired click in the top left corner **Reports** > **Crystal Reports** > **Faults** > **iFob Per Person Fault History Report**.



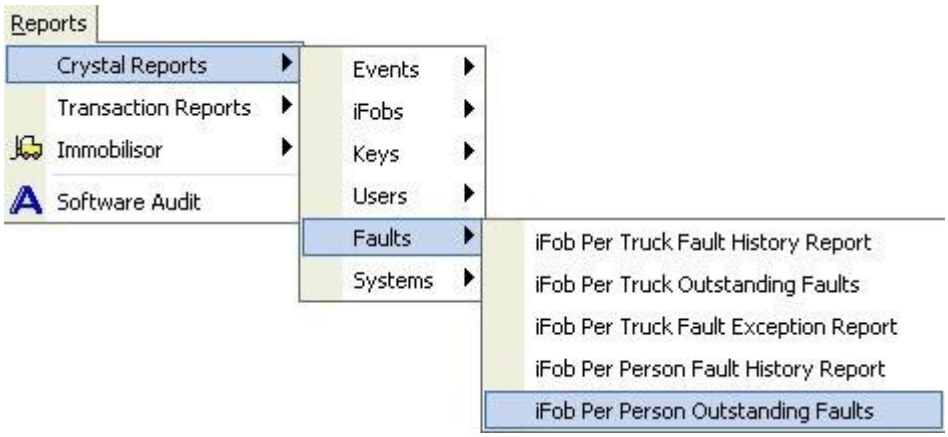
This report gives information on every fault logged, whether it's been cleared, repaired or just logged to the software. The report will look as pictured below.

iFob Per Person Fault History Report

Imm. Description	Type	Imm. Address	User who logged fault	Time fault was logged	Fault Number	Fault Name	Repaired	Cleared	User who cleared fault	Time fault was cleared
Test Data Logger	1	0001	Aaron Kennedy	14/04/2009 11:55:57	1	Data Logger Fault 1	True	True	Traka Engineer	14/04/2009 17:17:45
Test Data Logger	1	0001	Aaron Kennedy	17/04/2009 09:04:37	1	Data Logger Fault 1	True	True	Traka Engineer	17/04/2009 09:07:19
Test Data Logger	1	0001	Aaron Kennedy	17/04/2009 09:08:10	1	Data Logger Fault 1	True	True	Traka Engineer	17/04/2009 09:10:15
Test Data Logger	1	0001	Aaron Kennedy	17/04/2009 09:11:10	128	Data Logger Fault 2	True	True	Traka Engineer	17/04/2009 09:15:13
Test Data Logger	1	0001	Aaron Kennedy	17/04/2009 09:15:24	2	Data Logger Fault 3	True	True	Traka Engineer	17/04/2009 09:25:16
Test Data Logger	1	0001	Aaron Kennedy	17/04/2009 09:25:03	1	Data Logger Fault 1	True	False		

You will notice on the last line the sections that specify when the fault was cleared are empty because the fault has only been repaired and not yet cleared.

The other report shows you only the Outstanding Faults that have yet to been seen to. To view the reports of the Immobilisors that have only outstanding faults logged against them go to the top left corner of Traka32 and click **Reports** > **Crystal Reports** > **Faults** > **iFob Per Person Outstanding Faults**.



The Report will look as pictured below and is very similar to the Fault History report however this report only shows Outstanding Faults that have not been cleared or repaired. You can print off both versions of the reports if desired.

NOTE: A fault that has been repaired will remain on the outstanding fault list report until it has been cleared.

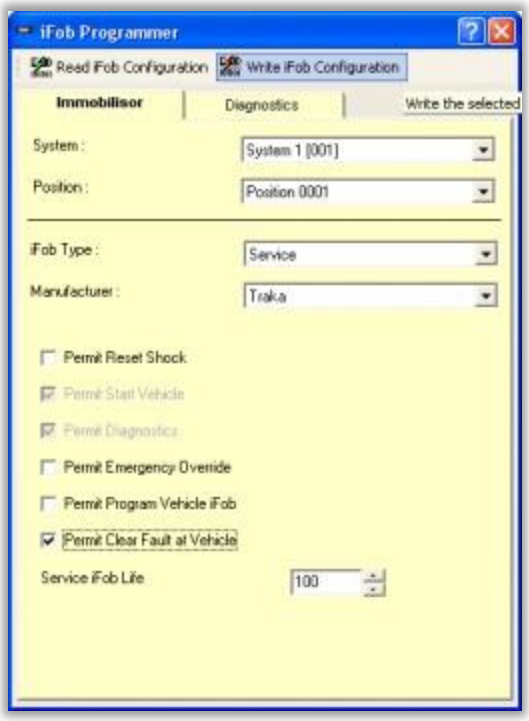
iFob Per Person Outstanding Faults

traka

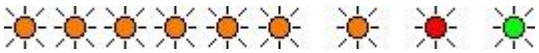
Imm. Description	Type	Imm. Address	User who logged fault	Time fault was logged	Fault Number	Fault Name	Repaired	Cleared	User who cleared fault	Time fault was cleared
Test Data Logger	1	0001	Aaron Kennedy	17/04/2009 09:25:03	1	Data Logger Fault 1	False	False		

Resetting the Immobilisor

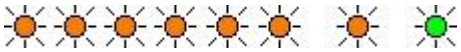
After you have cleared the fault from the Traka32 software the Immobilisor itself needs to be reset using a Service iFob. Service iFobs are usually Grey however with iFob Per Person systems we use Green Service iFobs. If you haven't done so already, you need to make sure your Service iFob has 'Permit Clear Fault at Vehicle' option enabled in order to reset and clear all the faults recorded at the Immobilisor. By default 'Permit Start Vehicle' & 'Permit Diagnostics' are automatically ticked and greyed out when the 'Permit Clear Fault at Vehicle' option is selected.



Insert the Service iFob into the receptor barrel of the Immobilisor and hold the acceptance button straight away before the ignition starts to receive the following sequence of flashes.



After holding the button for 10 seconds the sequence will change and the Red LED will be removed from the sequence.



This symbolizes that the fault has been cleared from the Immobilisor and that you can now reuse a vehicle iFob.

4.19.6 FIFO FOR KEY CABINETS

4.19.6.1 FIFO FOR KEY CABINETS OVERVIEW

First In, First Out (FIFO) is an option that automatically gives access to the iFob that has been in the cabinet for the longest time for each access level.

For example, if a user has access level 1, they have authorisation to remove any iFob with access level 1. However, using the FIFO option they will be restricted to only removing the access level 1 iFob that has been in the cabinet for the longest time.

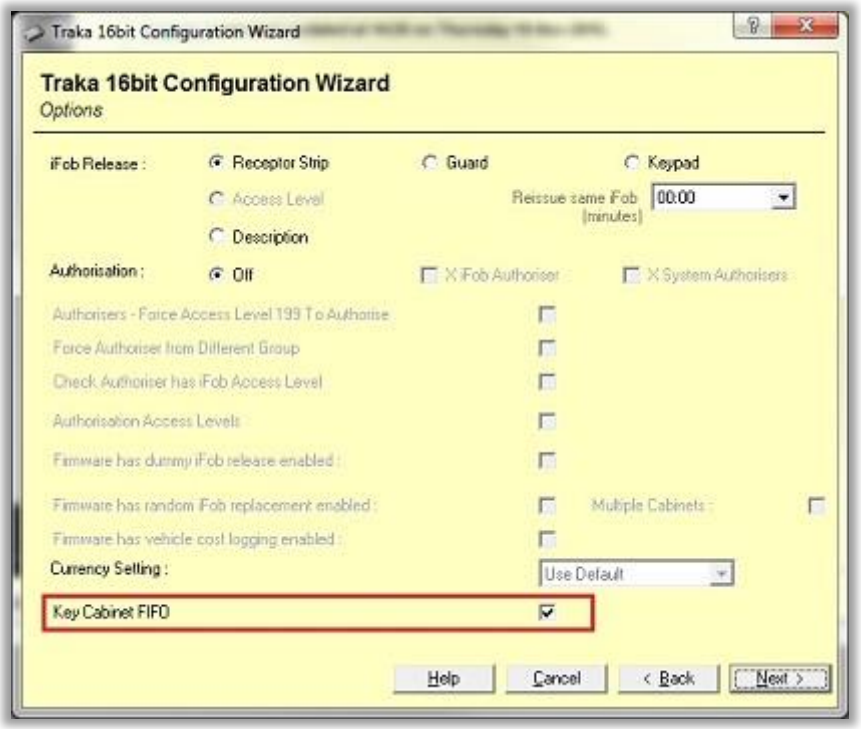
If a user has access levels 1 and 2, they have authorisation to remove any iFobs with access levels 1 and 2. However, with the FIFO option they will be restricted to only removing the iFob with access level 1, and the iFob with access level 2 that have been in the cabinet for the longest time.

FIFO is available from version 3.07.00 of the 16-bit firmware.

FIFO uses LED's to indicate the position of the authorized iFob(s). Therefore FIFO only Intelligent Receptor Strips (IRS) are supported with this option.

4.19.6.2 ENABLING THE FIFO OPTION

In order for the FIFO option to be used it must first be enabled in the 16-bit configuration file. Once enabled, it can be switched off if required from the 16-bit configuration wizard.



4.19.6.3 USING FIFO

Removing an iFob

When a user logs into the system, any iFobs the user can remove will be highlighted with a green LED. These will be the iFobs that have been in the cabinet for the longest time – one for each access level the user has access to.

If the Key Booking option is also being used on a system with FIFO, when a user logs into the system any iFobs with a key booking logged against them will be bypassed unless the booking has been made for that particular user.

If the Fault Logging option is being used on a system with FIFO, any iFobs with a critical fault will be bypassed unless that particular user has the correct access level to authorise them to remove an iFob with a critical fault.

Overriding the Option

It is possible to Override the FIFO option to enable a user to take any iFob regardless of how long it has been in the cabinet, provided that user has the correct access level for that particular iFob. In order to override the FIFO option for a particular user, they must be given access level 197.

4.19.7 FIRE ALARM ACCESS OVERRIDE

4.19.7.1 FIRE ALARM ACCESS OVERRIDE OVERVIEW

The Fire Alarm Access Override option allows the ability to connect a fire alarm or break glass switch to override system access and emergency release all of the iFobs. This means that all the iFobs can be removed from the system in the event of an emergency such as a fire.

NOTE: Fire Alarm Access Override is a firmware cost option; please ensure the correct firmware is loaded prior to using the system.

For more information please view the following sections:

Fire Alarm Access Override Operation

Fire Alarm Access Override Connections

4.19.7.2 FIRE ALARM ACCESS OVERRIDE OPERATION

NOTE: Fire Alarm Access Override is a firmware cost option; please ensure the correct firmware is loaded prior to using the system.

1. If the system detects an input from the fire alarm or break glass switch, the system LCD will display:

2. The door will open and the solenoids will fire in-turn starting from position 1. A user will be able remove the iFob indicated by the LCD:

   ...

   And so on...

   NOTE: The user is not required to press the button to remove the iFob because the solenoid is released automatically. Simply pull the iFob to remove it from the slot.

3. When the system detects the fire alarm or break glass switch has been reset, the system will return to normal operation. The LCD will briefly display the following:

Fire Alarm Access Override Events

The Traka system records 2 system events related to the Fire Alarm system viewable from the Traka 32 software:

- **Fire Alarm Activated** (code 60)

  Recorded when the system detects the fire alarm or break glass has been activated.

- **Fire Alarm Ended** (code 61)

  Recorded when the fire alarm has been reset indicating the system can return to normal operation.

For details on the all Event Codes please refer to the Alarm & Event Types.

For more information please view the following sections:

Fire Alarm Access Override Overview

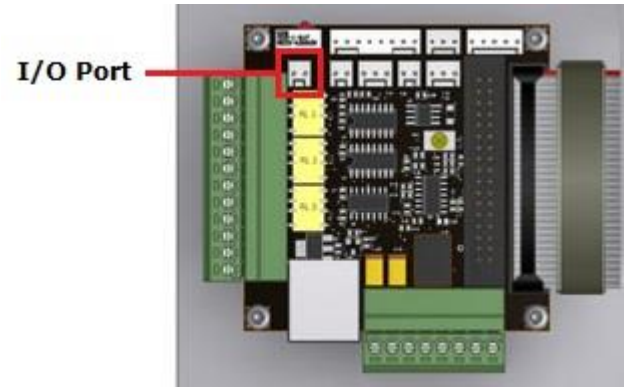
Fire Alarm Access Override Connections

4.19.7.3 FIRE ALARM ACCESS OVERRIDE CONNECTIONS

NOTE: Fire Alarm Access Override is a firmware cost option; please ensure the correct firmware is loaded prior to using the system.

16bit Systems

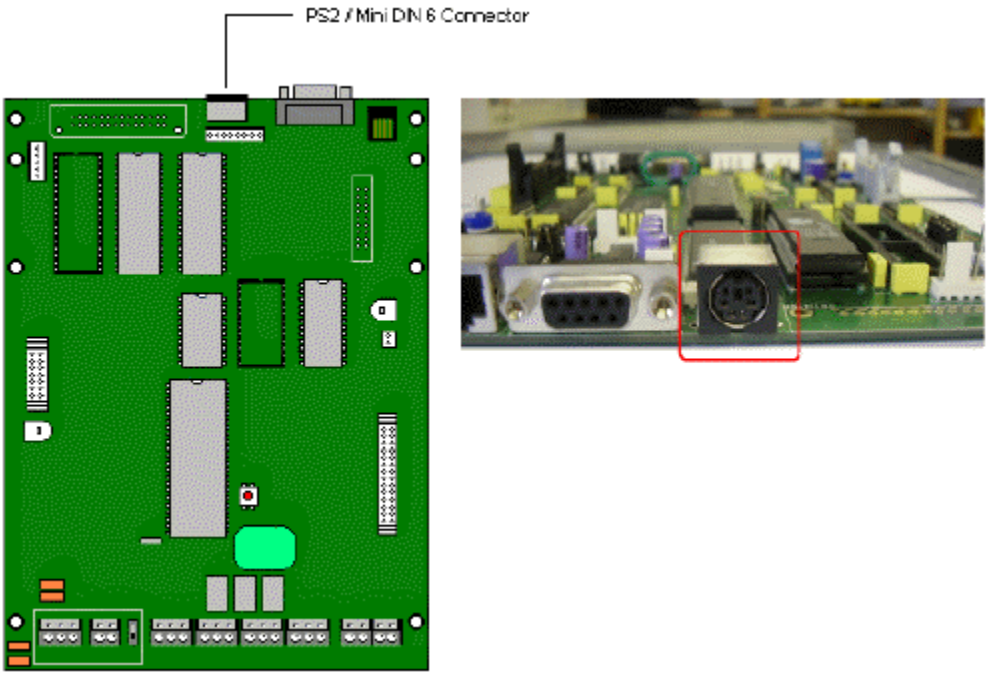
The fire alarm or break glass switch is required to be connected to the I/O Port on the 16bit I/O PCB, located just behind the On/Off switch as shown below.



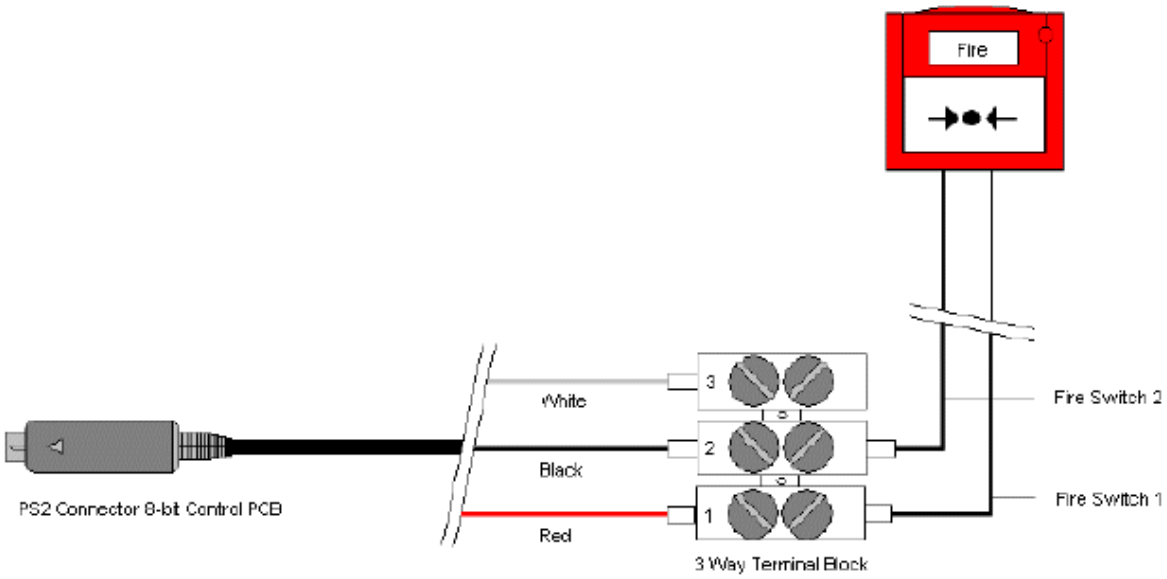
8bit Systems

The fire alarm or break glass switch is required to be connected to the PS2 port on the Traka 8-bit Control PCB.

1. The **PS2 connector** is not fitted as standard therefore if integrating the fire-alarm into an existing Traka system, a new Control PCB will be required. Alternatively, the connector will need to be soldered onto the existing 8-bit Control PCB. See below for a diagram of where the PS2 connector is located:



2. A **PS2 to Terminal Block Interface Cable** is required allowing termination of the fire alarm switch or break glass switch. The cable can be supplied upon request. See below for a diagram showing the connections required:



For more information please view the following sections:

Fire Alarm Access Override Overview

Fire Alarm Access Overide Operation

4.19.8 FUEL LEVEL LOGGING

4.19.8.1 FUEL LEVEL LOGGING OVERVIEW

Fuel Level Logging as its name suggests allows a user to record the current fuel level of a vehicle or battery level in the case of a forklift truck.

Every time a user returns an iFob they will be prompted for the vehicles fuel level. The fuel level must be a number between 0 and 4...

0 = Empty

1 = ¼ Full

2 = ½ Full

3 = ¾ Full

4 = Full

Once the value has been entered the user simply presses # to confirm the value or * to edit the value.

Each fuel level will appear in the Traka32 software against each iFob and Key transaction.

NOTE: Fuel Level Logging will only be available if the firmware of the selected system has Fuel Level Logging enabled. If the Fuel Level Logging option is enabled in the firmware, it is also possible to enable / disable the option on an iFob per iFob basis from the iFob Details window.

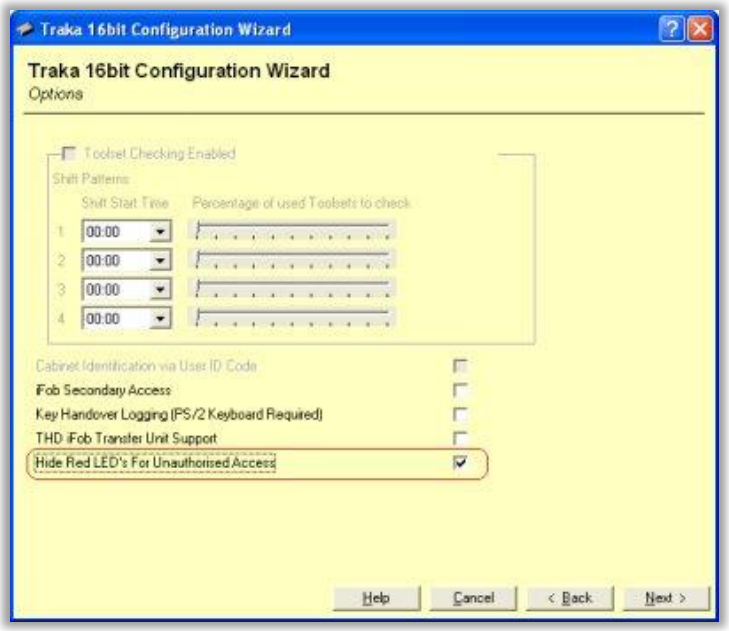
4.19.9 HIDE RED LED'S FOR UNAUTHORISED ACCESS

This feature is a 16-Bit only firmware option that when enabled will change the way the LED's display on the cabinet. When a user authenticates at the cabinet, LED's that illuminate green indicate that the user is allowed to take these iFobs. Some LED's may illuminate yellow, indicating that the currently logged in user has these iFobs out of the system. If a user authenticates at the cabinet and does not have access to the iFob the LED will **not** illuminate.

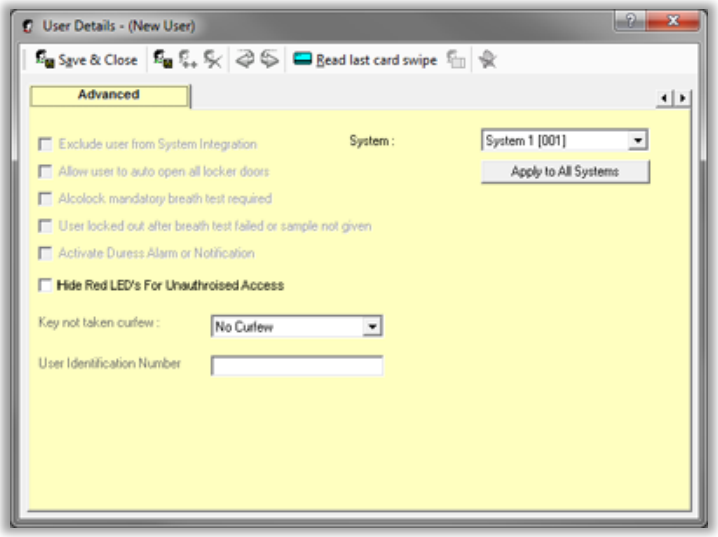
This feature makes it easier for users that are colour blind to help identify which iFobs they can or can't remove. If an iFob is returned to the wrong position then the LED will illuminate red and create a line between the correct slot (coloured green) and the wrong slot, this prompts the user to return the iFob to the correct position.

Hide Red LED's For Unauthorised Access is a cost option and must be enabled in the Traka32 Firmware Wizard. To enable/disable this option from your system right click your cabinet from the system viewer in Traka32, and select 'Configure Firmware'. Navigate to the fifth Options page and tick the 'Hide Red LED's For Unauthorised Access' box. Complete the wizard to update the cabinet with the newly made changes.

NOTE: When this option is initially enabled it applies to all users within the database. Please refer to the section below on how to active/deactivate this on a per user basis.



To enable/disable this option on an per user basis, an admin user must access the user details in Traka32 and navigate to the advanced tab. From there they can tick/untick the Hide Red LED's box for individual users.



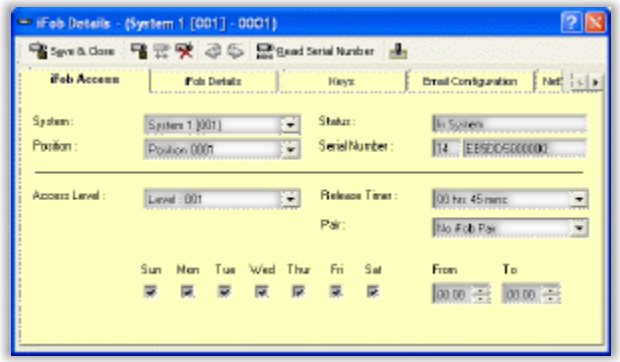
4.19.10 IFOB RELEASE TIMER

4.19.10.1 IFOB RELEASE TIMER OVERVIEW

The iFob Release Timer prevents iFobs from being re-used if they are returned to the cabinet early.

When the iFob is taken, the cabinet will add the Release Timer value to the current data and time. If the iFob is returned before the calculated time, the cabinet will not allow it to be taken again until the timer has elapsed.

For example, if an iFob is configured with a Release Timer value of 1 hour and a user takes it 13:30. If the iFob is returned at 14:15, the iFob cannot be taken again until 14:30.



NOTE: The iFob Release Timer option is only available on 8bit systems and when being used replaces the iFob Curfew and can be configured from the iFob Details window.

4.19.11 IFOB RETURN PROMPT

4.19.11.1 IFOB RETURN PROMPT OVERVIEW

With the Traka Systems collecting more data when iFobs are returned to the system, one of the issues faced is ensuring users input the data rather and closing the door and walking away.

With the current system this is physically impossible to prevent but iFob Return Prompt option goes along way to reducing the problem as it will not open the door on a system to allow a user to return an iFob unless they enter the data first.

NOTE: The current iFob Return Prompt option does NOT work with Random Return to Multiple Systems (RRMS).

4.19.11.2 IFOB RETURN PROMPT OPERATION

1. First access the Traka System. Please refer to the 'How to access the system?' section.

2. **Press *** to take an iFob or **press #** to return an iFob.

3. **To take an iFob press *** and iFobs can be taken as normal.

   If a user tries to return an iFob whilst in this mode the iFob will be rejected and the following message will show:-

   Also an' iFob Returned without Data Entry' event will be recorded to record the user that did not enter the data correctly along with the date and time. If the door is closed, the next user will be prompted to remove the iFob and an 'iFob Returned without Data Entry Now Removed' event will be recorded.

4. **To return an iFob press #.**

5. Enter an iFob No. to Return or press # when complete.

6. If valid, the system will prompt for data from any of the following options:-

   a. Fault Logging

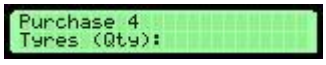
   b. Location Storing

   c. Mileage Logging

   d. Fuel Level Logging

   e. Reason Code Logging

   f. Vehicle Cost Logging



7. Repeat steps 5 and 6 for every iFob that is to be returned. When all the data is entered press # and the door will open ready to accept the iFobs that have had their data entered.

8. If data has already been entered for the selected iFob, the following error message will show:-

9. If an iFob is returned to the system without the data being entered in the above method, the iFob will be accepted into the system, however an 'iFob Returned without Data Entry' event will be recorded to record the user that did not enter the data correctly along with the date and time.

10. If a user tries to take an iFob whilst in this mode the following message will show:-

4.19.12 IFOB IN WRONG SLOT SYSTEM LOCKDOWN

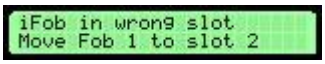
4.19.12.1 IFOB IN WRONG SLOT SYSTEM LOCKDOWN OVERVIEW

The iFob in Wrong Slot System Lockdown option will prevent ALL users from accessing the Traka system if a user has previously returned an iFob to the wrong slot, ignored the alarm condition and walked away. In this instance, a supervisor with access level 195 is the only user who can access the system and clear the condition by removing the iFob and returning it to the correct slot.

For more information please view the section on iFob in Wrong Slot System Lockdown Operation.

4.19.12.2 IFOB IN WRONG SLOT SYSTEM LOCKDOWN OPERATION

1. If a User has returned an iFob to the wrong slot, the LCD will show:



2. If the user chooses to ignore the "iFob in wrong slot" message and closes the door the system will enter a "lockdown" state and the LCD will show:

3. Whilst in System Lockdown, only a Supervisor / a user with Access Level 195 may open the system to clear the condition. To clear the condition simply:

    a. Access the system in the usual way by card, biometrics or pin as applicable.

    b. **Remove** the iFob from the wrong slot and return it to the correct slot.

    c. Close the door if applicable.

4. The System Lockdown condition will have now cleared allowing normal users to access the system.

4.19.13 INCORRECT IDENTIFICATION LOCKDOWN

This cost option allows the system to 'lockdown' when a user fails to correctly enter their access credentials within a pre-defined number of attempts.

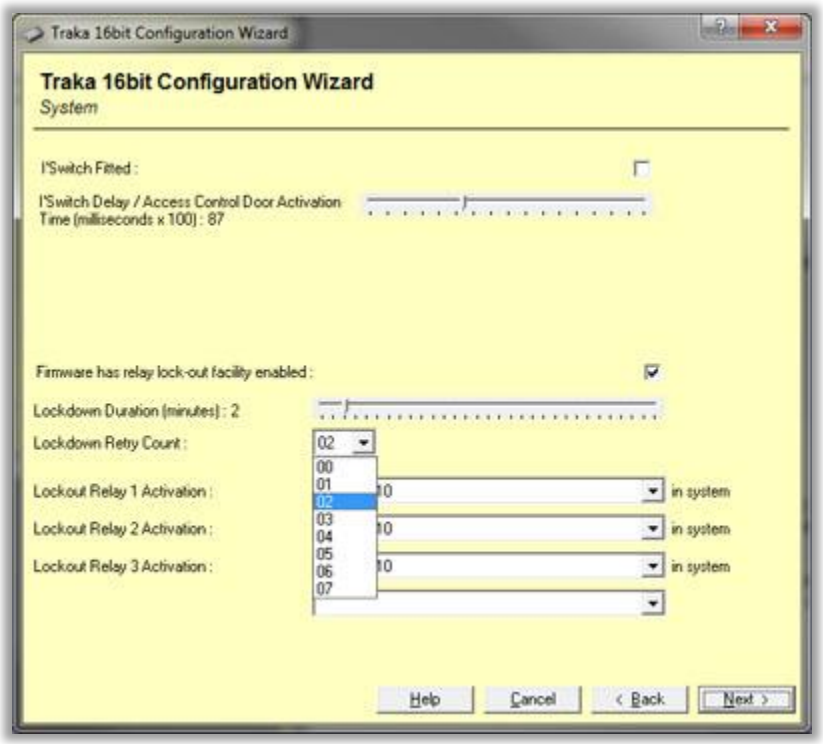
Setting up the System

To use this feature it will need to be enabled with the system configuration file.

If you are using a brand new system that was ordered with this feature, then this will already be configured for you. If you would like to add this option to an existing system, you will need a new configuration file created by Traka and loaded into your system. Please contact Traka for further details.

1. Right click the pod from the system viewer and select Configure Firmware.

2. Navigate to the System page. The option 'Firmware Relay Lock-out Facility Enabled' option will be ticked.



3. Using the sliding toolbar set the duration of the lockdown in increments on 1 minute. The maximum amount of time the system can be in 'Lockdown' is 30 minutes.

   NOTE: When 0 is selected the lockdown feature is disabled.

4. The Relay Count relates to how many tries a user will have correctly identify themselves at the system before it locks down.

   - Selecting 00 will set the count to 0 and mean that no retries are allowed.
   -
   -
   -
   -
   -
   - Selecting 07 will set the count to 7 tries before the system locks down.

5. Select the next button until you reach the end of the Configuration Wizard and click Apply. The configuration file will then write to the system.

6. Once communication is completed click Finish.

Methods of Access

The following methods of access work with Incorrect Identification Lockdown feature.

- PIN Entry
- PIN & Secondary PIN Entry
- Card Reader & Secondary PIN Entry (with 'Force Card & PIN' option selected)

Using the System

1. A user incorrectly identifies themselves to the system after a predetermined amount of tries.
2. The system will then Lockdown for the specified amount of time. And the following message will be displayed on the LCD.

   NOTE: During the lockdown period all users will be barred from using the system, except a user with access level 200 in their permissions. Having access level 200 will allow them to still gain access to the system even when the system is in Lockdown.
3. An 'Incorrect Identification Lockdown' event will be generated in Traka32. This can be viewed by selecting the system events tab from the System Viewer.
4. After the duration period the Lockdown will be lifted and users can remove/return items to the system as normal.

Clearing a Lockdown

When a lockdown is in effect a user with access level 200 has the authority to clear it and set the system back to normal.

1. The user must identify themselves at the system.
2. The LCD will then ask if they wish to cancel the lockdown.

   Select the **#** key for Yes or select the * Key for No.

4.19.14 IMMOBILISOR

4.19.14.1 IMMOBILISOR OVERVIEW

The Traka Immobilisor allows a standard Traka iFob to be used as an alternative to a conventional key for a vehicle. The Immobilisor comprises a black control box, which is mounted discreetly on the vehicle and a special electronic socket (receptor), which replaces the usual key barrel.

When used in conjunction with the standard Traka key cabinets, which control who may have access to the keys, as well as recording the date and time the key was taken and replaced, the Immobilisor provides an easy method for ensuring that only authorised drivers take vehicles they are allowed to drive and that every driver is fully accountable.

4.19.14.2 IFOB PROGRAMMER

The iFob Programmer allows you to program either a Data32 or Data512 iFob that is currently in the system with data that can be used in conjunction with other Traka products such as the Traka Immobilisor. The iFob Programmer can only be accessed if the current user of the software is logged in as an engineer.

NOTE: Traka32 versions 01.05.0005 or before does not include the iFob Programmer.

Read iFob Configuration

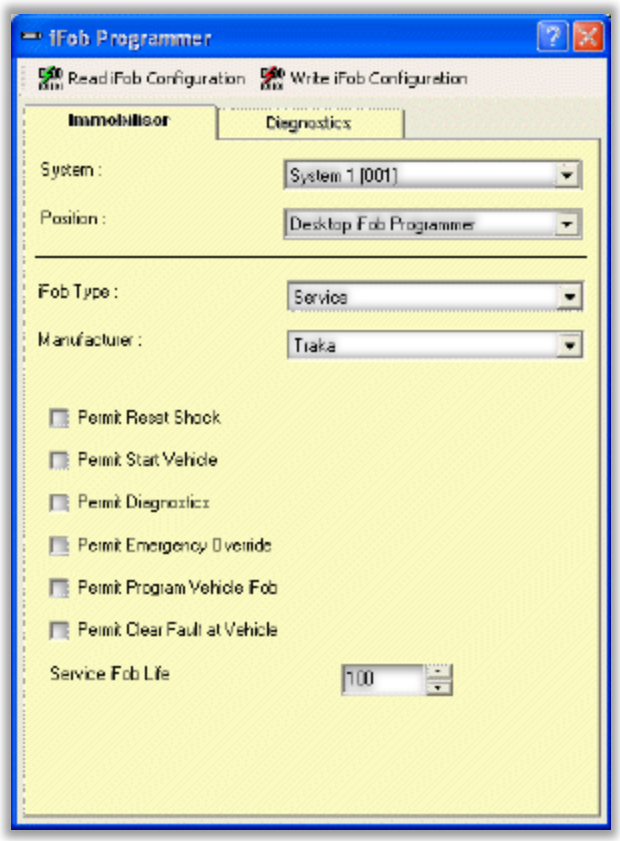
To read the configuration of an iFob, select the System and Position of where the iFob is located and click on Read iFob Configuration.

NOTE: If the iFob is not currently programmed or the iFob is not a Data32 or Data512 iFob or the iFob is not currently in the system a warning message will be displayed.

Write iFob Configuration

When you have selected the appropriate settings for the iFob, select the System and Position of where the iFob is located and click on Write iFob Configuration.

Immobilisor



System and Position

The system and position fields are used to select where the iFob is located that you wish to program.

Desktop iFob Programmer

To program an iFob using the Traka Desktop iFob Programmer, select Desktop iFob Programmer from the Posion dropdown menu.

iFob Type

There are two types of iFob the can be used with the Traka Immobilisor...

- Service iFob.

  A Service iFob has the following functions...

  a. allows a user to (re)program a Vehicle iFob.

  b. allows a user to drive any truck and access any on-board diagnostics fitted.

  c. allows a user to activate any vehicle permanently until the power is cut or the Service iFob or Vehicle iFob is replaced.

  d. allows a user to reset an Immobilisor after a shock.

- Program iFob

  A Program iFob has one function...

  a. allows a user to (re)program a Manufacturers Code, Acceptance Button timer and Shock Sensor Threshold.

- Vehicle iFob

  A Vehicle iFob has two functions...

  a. when programmed to an Immobilisor using a Service iFob, it allows a user activate that immobilisor.

  b. When the immobilisor is active, the Vehicle iFob can collect data such as shock detection and vehicle acceptance.

- Calibrate iFob

  A Calibrate iFob is used to calibrate the options Immobilisor Shock Sensor. This should only be used by qualified Traka engineers.

- Debug (RAM & ROM)

  A Debug iFob is used to diagnose problems with the Immobilisor system. This should only be used by qualified Traka engineers.

- Reset iFob

  A Reset iFob is used to reset the Minutes Used counter of the Immobilisor. This should only be used by qualified Traka engineers.

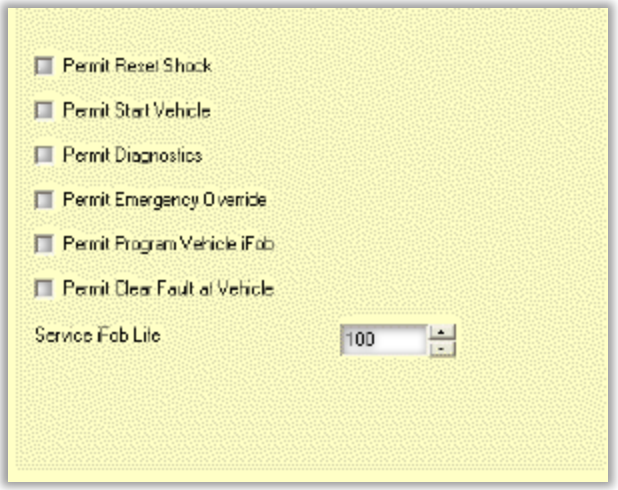
Manufacturer

A Traka Immobilisor can be programmed with a specific Manufacturers Code using a Program iFob. Once the Immobilisor has been programmed with a Manufactures Code, only Service iFobs that have been programmed with the same Manufacturers Code will work with that Immobilisor.

All new Immobilisors are programmed with a Manufactures Code of 'Traka'.

Service iFob

When configuring a Service iFob you can configure the settings that you wish to apply to the iFob.



Permit Reset Shock

If the Immobilisor is fitted with a Shock Sensor and the 'Reset via Service iFob Only' has been set via the Program iFob, setting this option will allow the Service iFob to reset an Immobilisor after a shock.

Permit Start Vehicle

Setting this option will allow the Service iFob to activate any Immobilisor.

Permit Diagnostics

Setting this option will allow the Service iFob to activate the diagnostics output on any Immobilisor.

Permit Emergency Override

Setting this option will allow the Service iFob to permanently activate any Immobilisor until either the power is cut or the Service or correct Vehicle iFobs are inserted.

Permit Program Vehicle iFob

Setting this option will allow the Service iFob to reprogram the allocated Vehicle iFob for the Immobilisor.

Permit Clear Fault at Vehicle

Setting this option will allow the Service iFob to clear faults logged at the vehicle.

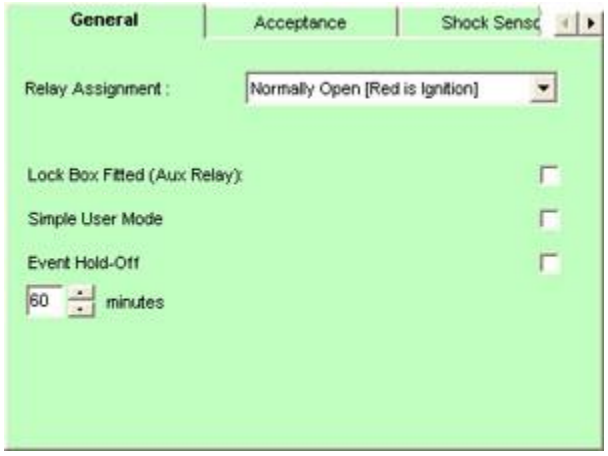
Service iFob Life

Enter a value for the number of times the Service iFob can be used before it expires.

Program iFob

When configuring a Program iFob you can configure the settings that you wish to program one or more Traka Immobilisors with.

General



Relay Assignment

Select the operation of the relay when the Immobilisor is active.

- Normally Closed [Red is Ignition]
- Normally Open [Yellow is Ignition]

Lock Box Fitted (AUX relay)

Select this option if the truck you are programming has a Traka Lock Box fitted to it.

Simple User Mode

Tick this box to enable the 'Small Fleet Immobilisor'. For more information on the Small Fleet Immobilisor please contact Traka.

Event Hold-Off

This tick box when enabled, allows you to set the number of minutes that must elapse before another event will be saved in the iFob.

Acceptance

Acceptance Button Fitted

Select this option if the Immobilisor is fitted with an Acceptance Button. You can configure a period of time (in minutes) in which the truck operator has to perform their pre-operational checks, this is located at the bottom of the window.

NOTE: Clear this option if the Immobilisor is NOT fitted with an Acceptance Button otherwise the Immobilisor will cut out after the delay. Please refer to the Immobilisor Acceptance section for more details.

Acceptance Warning

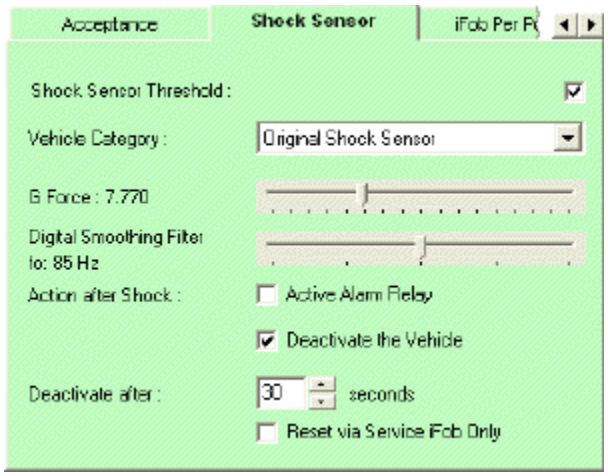
The Acceptance Warning option when enabled activates a beacon (to be wired into the Immobilisor on site) 30 seconds before the acceptance period expires.

NOTE: The Acceptance period is defined in increments of 1 minute via the field at the bottom of the Acceptance window and is only selectable when the 'Acceptance Button Fitted' option is selected.

iFob Per Person Single Acceptance

When this option is selected the driver of the Truck will only be asked to press the Acceptance button once, even if they leave the truck and come back later. If another driver uses the truck then they will have to press the Acceptance button.

Shock Sensor



Shock Sensor Threshold

Select this option if the Immobilisor is fitted with a Shock Sensor module. You can configure the shock sensor's g-force threshold level at which the Immobilisor will record a shock and act upon it.

NOTE: Clear this option if the Immobilisor is NOT fitted with a Shock Sensor module otherwise the Immobilisor will not program correctly.

Please refer to the Immobilisor Shock Sensor section for more details.

Vehicle Category

Select the type of shock sensor that you wish to configure...

- Original Shock Sensor
- Category A (Forklift Mass between 200 -1300 Kg's)
- Category B (Forklift Mass between 1300 -3400 Kg's)
- Category C (Forklift Mass between 3400+ Kg's)

G Force

Select the shock sensor's g-force threshold level at which the Immobilisor will record a shock and act upon it.

Digital Smoothing Filter

Select the frequency level at which the shock sensor filters out unwanted shock detection.

Action after Shock

If the Immobilisor is fitted with a Shock Sensor module, you can configure what actions should be taken after the Shock Sensor Threshold has been breached.

Active Alarm Relay

If this option is selected, the alarm relay will activate if an impact occurred. Immobilisor is fitted with a relay that can activate a siren or flashing light if an impact occurs.

If the option is not selected the alarm relay will not active under any circumstances.

Deactivate the Vehicle

If the option is selected, the vehicle will deactivate x number of seconds after impact depending on the deactivation delay set.

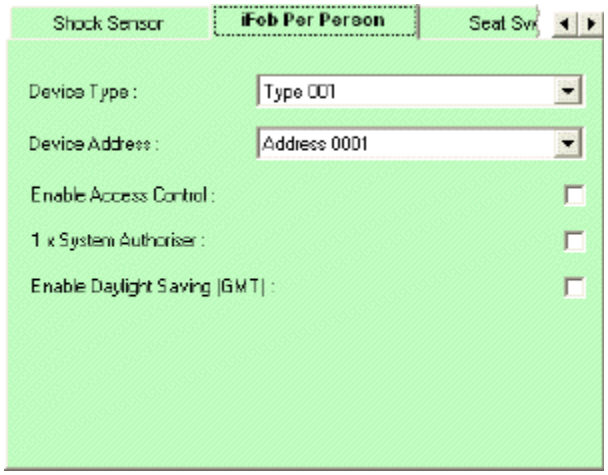
NOTE: Immediate deactivation of a vehicle after and impact may be dangerous as an operator may need to move the vehicle to avoid further injury; therefore a small delay is recommended.

Reset via Service iFob Only

If this option is selected, the Immobilisor can only be reset after an impact by a supervisor using their Service iFob even if the power to the vehicle or Immobilisor is cut.

If this option is not selected, the operator will be able to reset the vehicle by removing and re-inserting their Vehicle iFob.

iFob per Person



Truck type

Select the type of truck between 1 and 16. Users can only operate the types of truck they are authorised to by allocating access levels 101 to 116. For example if a truck type of 5 was programmed, a user authorised to operate the truck would be given access level 105.

Truck Address

Select the truck address between 1 and 255. Each truck should have its own unique address. The address is used by Traka32 to report on the events that have occurred for that truck.

Enabled Access Control

Select this option if the Immobilisor is used for Access Control.

Select this option if the iFob does not remain in the receptor socket for operation of the device e.g. where an iFob is "touched" to open a door. If enabled an event is recorded in the iFob before activating the device, this prevents the user from removing the iFob too quickly and losing the event. In this mode the standby LED is Solid Red so as there is as little time as possible before activation.

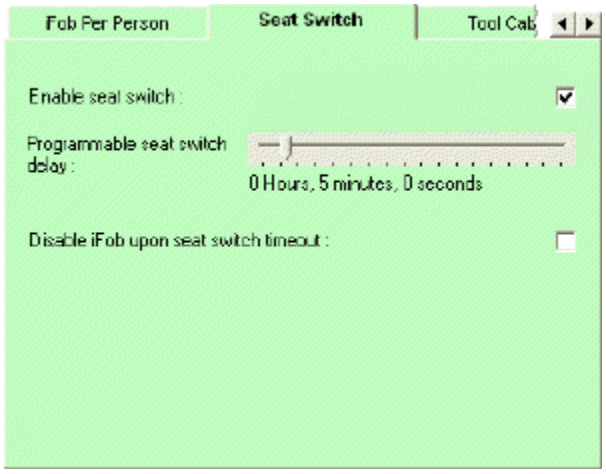
1 x System Authoriser

Select this option two Valid User iFobs are required to be inserted into the receptor socket to activate the ignition. A "request activation" event is logged in the first valid User iFob inserted. This must then be removed within 5 seconds. A "Device Activated" event is logged in the second Valid User iFob to be inserted within the next 5 seconds.

Enabled Daylight Saving (GMT)

Select this option to enable the real time clock to automatically update in accordance with U.K. GMT.

Seat Switch



Enable Seat Switch

Select this option if the Immobilisor is fitted with a Seat Switch module.

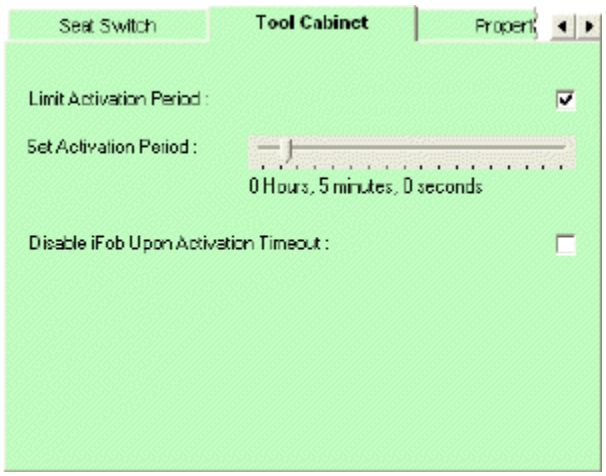
Programmable Seat Switch Delay

Set the Seat Switch Delay to the amount of time the driver must be away from the truck (i.e. not sitting on the seat) before the Immobilisor will automatically log an event and cut out the Ignition.

Disable iFob Upon Seat Switch Timeout

Select this option if upon the timeout of the Seat Switch Delay the Immobilisor will disable the iFob from being used again until returned to the Traka Cabinet.

Tool Cabinets



Limit Activation Period

Select this option if the Immobilisor is fitted to a Tool Cabinet.

Set Activation Period

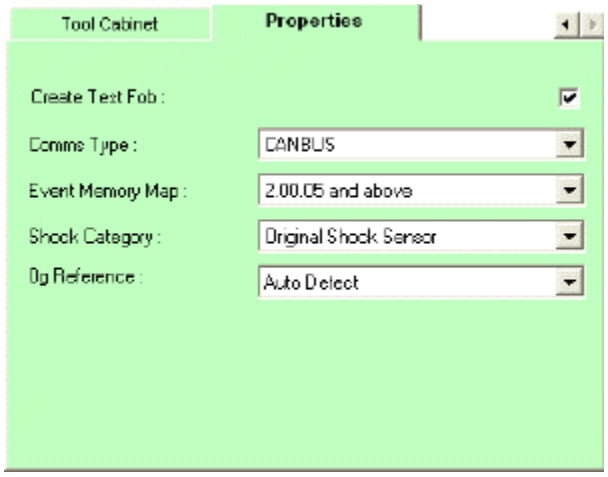
Set the Activation Period to the amount of time the Tool Cabinet will be unlocked whilst the iFob is inserted in the Immobilisor. If a timeout occurs the Immobilisor will automatically log an event and lock the Tool Cabinet.

Disable iFob upon Activation Timeout

Select this option if upon the timeout of the Activation Delay the Immobilisor will disable the iFob from being used again until returned to the Traka Cabinet.

Properties

Please refer to the Engineers Overview section before using the diagnostics utility of the iFob programmer.



Create Test Fob

Select this option to create a Test iFob. This is used to test the functionality of the Immobilisor LED's and Relays and also program the iFob with the parameters set below.

Comms Type

Select if the communications between the Data Logger and Shock Sensor use Clock & Data or CANBUS.

Event Memory Map

Select the iFob memory map used for the events. Select from version 2.00.04 and below or 2.00.05 and above.

Shock Category

Select the type of shock sensor that you wish to configure...

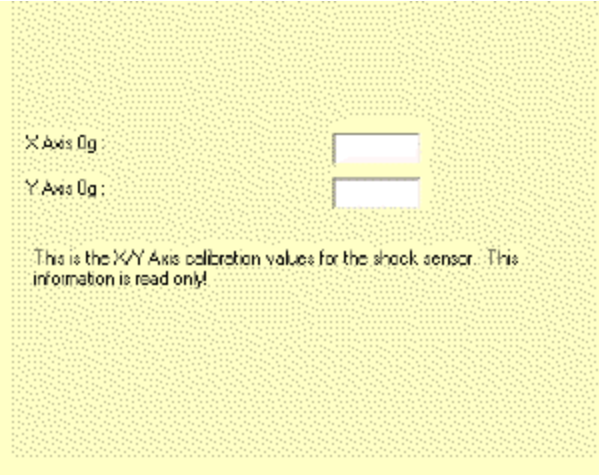
- Original Shock Sensor
- Category A (Forklift Mass between 200 -1300 Kg's)
- Category B (Forklift Mass between 1300 -3400 Kg's)
- Category C (Forklift Mass between 3400+ Kg's)

0g Reference

Select the 0g reference for the shock sensor.

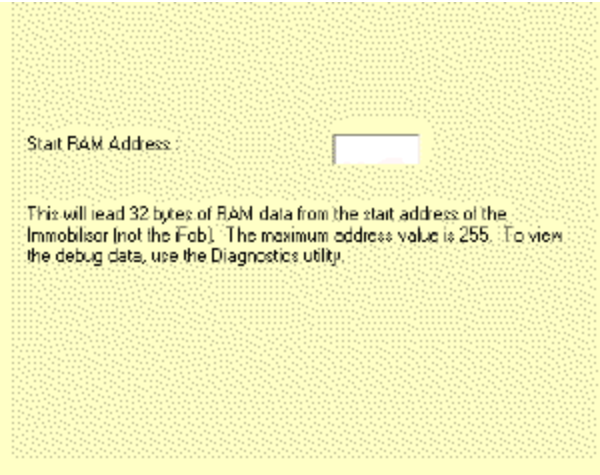
Calibrate iFob

When configuring a Calibrate iFob there are no settings to be configured however it is possible to read the X and Y Axis G Force settings.



Debug RAM / ROM iFob

When configuring a Debug RAM/ROM iFob you can configure the settings that you wish to debug with.



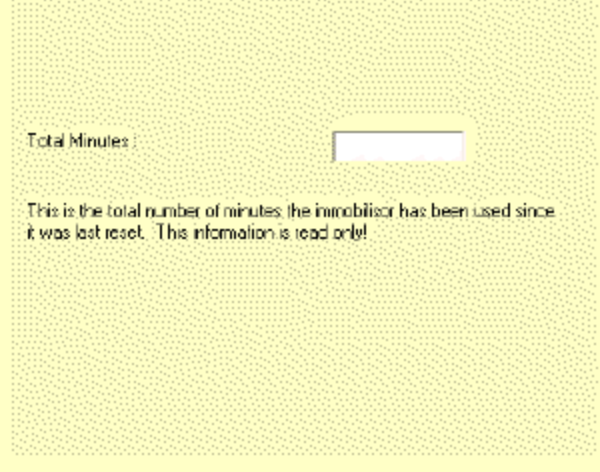
Start RAM/ROM Address

Enter the start address from where the debug iFob will read the RAM/ROM of the Immobilisor from. The debug will read 32 bytes from the start address.

NOTE: To view the debug data, use the Diagnostics utility.

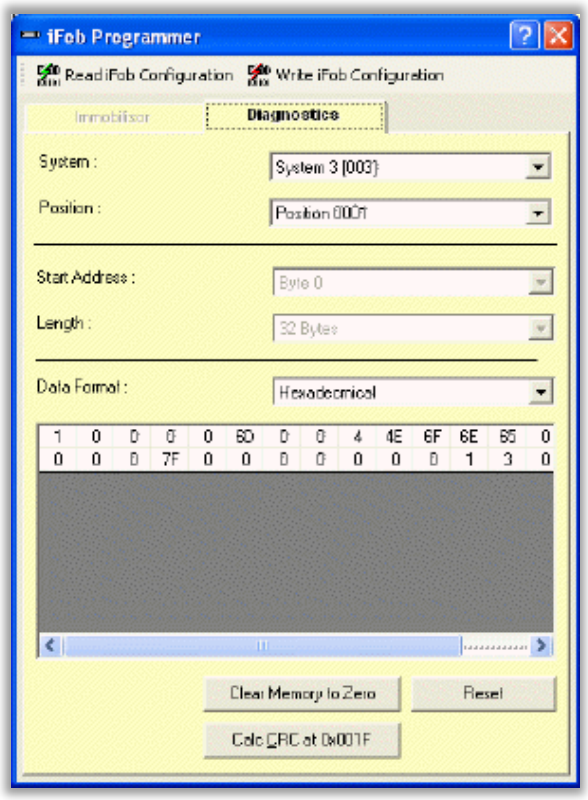
Reset iFob

When configuring a Reset iFob there are no settings to be configured however it is possible to read the total minutes used value that was read from the Immobilisor prior to being reset.



Diagnostics

Please refer to the Engineers Overview section before using the diagnostics utility of the iFob programmer.



System and Position

The system and position fields are used to select where the iFob is located.

Start Address

Select the address of the iFobs memory map that you wish to start reading from.

Length

Select the length of the data that you wish to read from the iFob, starting at the starting address above.

Once a **Start Address** and **Length** have been specified, clicking on the **Read iFob Configuration** button will read the data from the iFob and present it in the table below.

Data Format

Once the data has been read, the format of the data can be changed between...

- Hexadecimal
- Decimal
- ASCII

Data Table

If required, the data in the table can be altered by double clicking over the relevant data. The data can then be written back to the iFob by clicking on the **Write iFob Configuration** button.

Clear Memory to Zero

Click this button to set all the data in the data table to 0.

Reset

Once data has been read from the iFob, click the reset button to clear the data table and re-enable the Start Address and Length controls as well as the Immobilisor tab.

Calc CRC at 0x001F

Click this button to calculate a CRC value based upon the data present in bytes 0x0000 to 0x001E. The resultant CRC will replace byte 0x001F.

4.19.14.3 IFOB PER TRUCK

4.19.14.3.1 IFOB PER TRUCK OVERVIEW

In operation, simply inserting the correct iFob activates the vehicle and allows it to be driven. If an iFob is lost or broken it is an easy task to activate an alternative iFob using the special Service iFob, which is provided to the manager or supervisor and also to the vehicle service engineers. Only one Vehicle iFob can be active at any time.

4.19.14.3.2 IMMOBILISOR ACCEPTANCE BUTTON

This optional feature requests that a driver "Accepts" the truck within a defined period of time during which he can complete his Pre-op checks. Failure to press the button will cause the unit to time out, stopping the truck and necessitating the withdrawal and re-insertion of the iFob. Pressing the button writes a software token to the iFob which remains with the iFob until it is inserted back into the Traka cabinet. Once the software token is written to the iFob, the need to re-accept the vehicle is unnecessary. However, once the iFob is returned to the cabinet, the token transfers from the iFob to the cabinet and to the users' activity record allowing future Health and Safety checks to identify that a driver inspected the vehicle during his shift. When the next driver takes the iFob, the procedure starts again.

4.19.14.3.3 IMMOBILISOR SHOCK SENSOR

This optional feature monitors the g-forces exerted upon a vehicle as it is driven. The shock sensor is pre-programmed with a g-force threshold level and if that level is breached whilst the immobilisor is active for example by hitting another vehicle or racking, one or more pre-configurable actions can be taken. If the g-force level is breached a token will be automatically written to the iFob that will appear on the reports within Traka32. Optionally a relay can be activated on the Immobilisor to activate a siren or flashing light, the vehicle can be deactivated after a pre-set period of time and also the vehicle can be temporarily deactivated until reset by a supervisor using their Service iFob.

4.19.14.3.4 HOURS USAGE VIA CAN

This optional feature allows the Seat Hours, Traction Hours and Lift Hours of a vehicle to be recorded in a Vehicle or User iFob. The Traka Immobilisor continuously collects the Hours Usage information from the Vehicle CAN (Controller Area Network). This information is written to the iFob upon inserting it into the Immobilisor receptor barrel. Upon returning the iFob to the Traka cabinet the information is retrieved and downloaded to Traka 32 after a "Read All System Data". Traka 32 can generate reports on the Hours Usage per vehicle.

4.19.14.4 IFOB PER PERSON

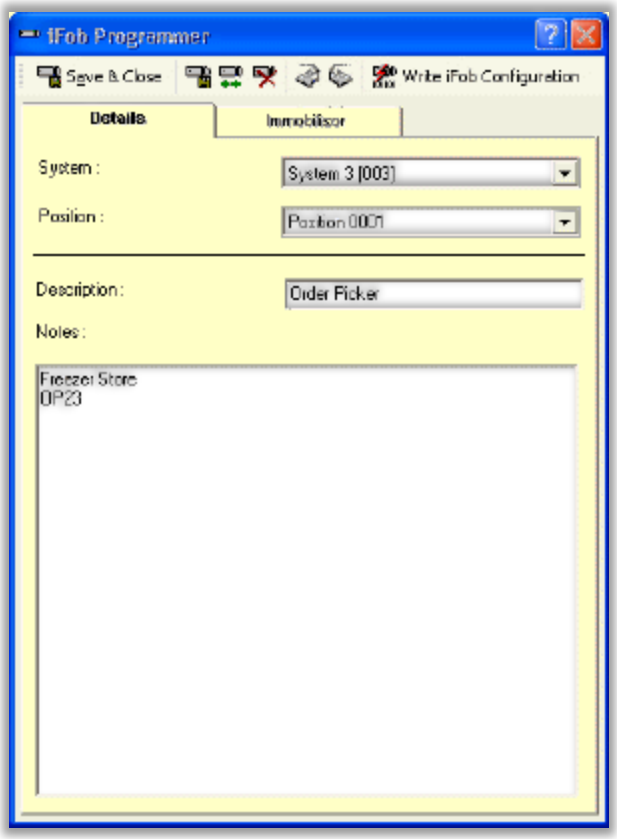
4.19.14.4.1 IFOB PER PERSON OVERVIEW

As with the iFob per Truck option, the operator will access Traka cabinet in conventional way. The operator will select an iFob and as the iFob is selected, the immobilisor access rights and time profile will be written to the iFob. Writing the time profile will ensure that the operative will have to return the iFob at the end of the day, as the iFob will effectively expire and therefore need to be "recharged". The operator will then take the iFob to the required MHE truck and insert into the Immobilisor data logger. If access to the profile is suitable, the truck will activate. The iFob will record time of insertion and the truck activated.

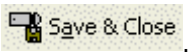
The Immobilisor Data Logger records events in the Data 512 User iFobs (yellow). A maximum of 60 events can be recorded into the iFob before it is required to be returned to the cabinet for download. With the 8bit board, each time a User iFob is returned; the Traka cabinet must read the event data from the iFob and immediately send this information back to the Traka 32 database. The iFob memory is then reset so it is ready for the next User. ONLINE or REMOTE HOST auto-communications used to be required in order for the Traka cabinet to send this information back to database immediately, however the 16bit board can store the events locally due to bigger memory and communicate in the background allowing the cabinet to still be used whilst the iFob details are being read to the cabinet memory. Normal Auto Communications can be used to frequent read the data from the cabinet. For further information on Auto Communication please refer to the appropriate section of the user guide.

4.19.14.4.2 ADDING IMMOBILISORS

1. From the main screen click on **View** followed by **Immobilisor List** and a list of the current immobilisors will be shown.
2. From the immobilisor list click on the **Configurations** menu followed by **Add New**.
3. A new blank immobilisor record will be created.



4. Edit the appropriate details, for more details refer to the Immobilisor Details section.

5. To **Save** your changes, simply click on  or 

.

6. To **Cancel** your changes, simply click on the **X** in the top right hand corner of the window and click on **No** to the message.

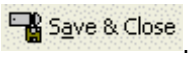
4.19.14.4.3 EDITING IMMOBILISORS

1. From the main screen click on View followed by **Immobilisor List** and a list of the current immobilisors will be shown.

2. From the immobilisor list simply **double click** on the immobilisor record you wish to edit or select the record and click on the **Configurations** menu followed by **Edit Configuration**.

3. The selected user record will open.

4. Edit the appropriate details, for more details refer to the Immobilisor Details section.

5. To **Save** your changes, simply click on  or 

.

6. To **Cancel** your changes, simply click on the **X** in the top right hand corner of the window and click on **No** to the message.

Truck Type and Truck Address Filtering Overview

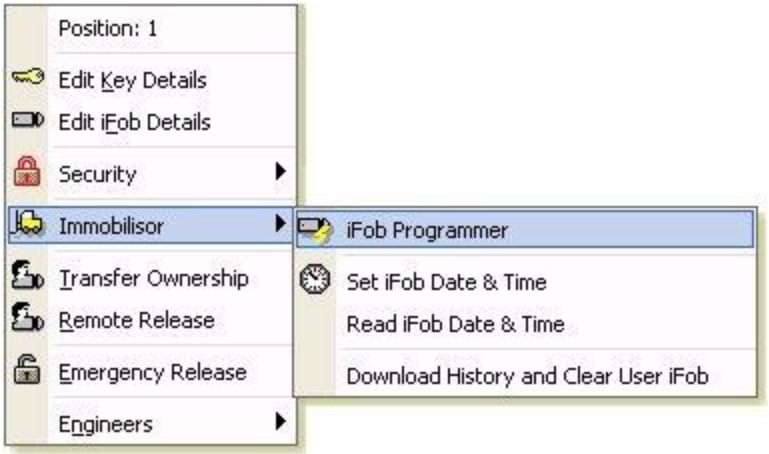
NOTE: This is a new feature is applicable to software versions 02.09.0000 and above.

If you wish to change the configuration of multiple trucks but do not wish to alter the Type or Address, then this option will allow you to program every truck with the same iFob without having to re-configuring the iFob.

For example, if you have 10 trucks with Type 001-010 and Addresses 001-010 and you wanted to enable the cost option **'Fault Logging'**, you would normally have to continuously go back and forth to the cabinet or Desktop Programmer each time to change the unique Type and Address of each truck. By selecting the 'No Change' option within the iFob Programmer, you will program the Data Logger with newly selected options without changing the Type or Address.

How to set up Type and Address Filtering

Right click the desired iFob you wish to turn into a Program iFob, and select iFob Programmer.



When you find yourself at the IPP tab, you will then have the option to set the device Type and Address to the 'No Change' option. This will ensure that when you are re-programming your Immobilisors the Device 'Type' and 'Address' won't change.

4.19.14.4.4 DELETING IMMOBILISORS

1. From the main screen click on **View** followed by **Immobilisor List** and a list of the current immobilisors will be shown.

2. From the immobilisor list simply **click** on the immobilisor record you wish to delete, click on the **Configurations** menu followed by **Delete**.

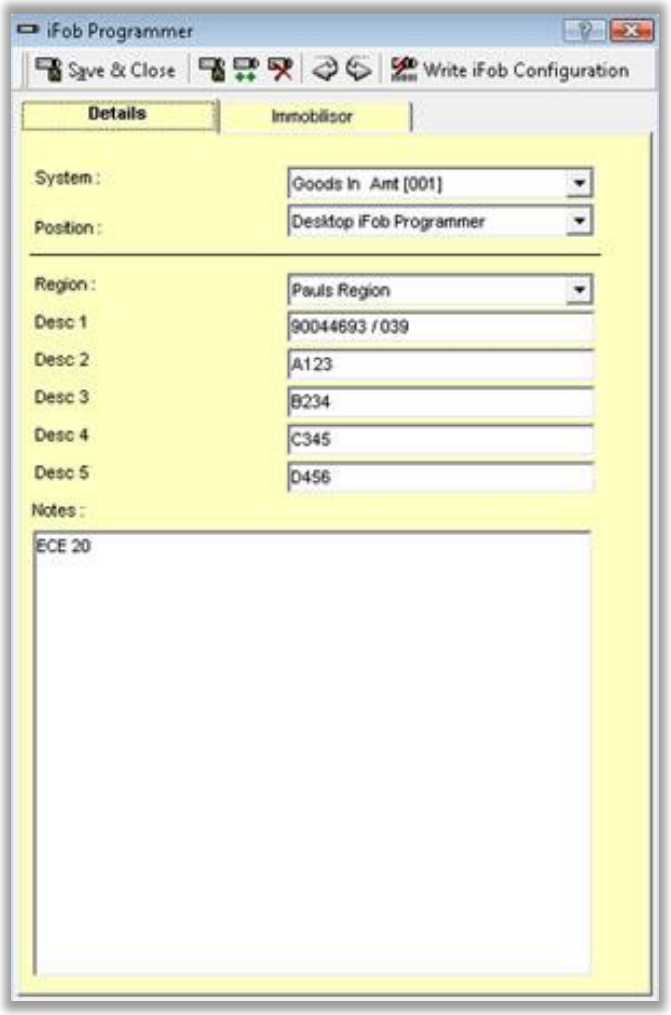
   NOTE: If you already have an immobilisor record open you can delete the record simply by clicking on the  **button.**

3. To delete the immobilisor simply click on **Yes**.

4.19.14.4.5 IMMOBILISOR DETAILS

The Immobilisor Details window allows you to add and edit the Immobilisor details.

Details Tab



System and Position

The system and position fields are used to select where the iFob is located.

Region

From this drop down box you can select which region you wish the truck to belong too. For information on how to create Immobilisor please review the Immobilisor Regions topic.

Detail Fields

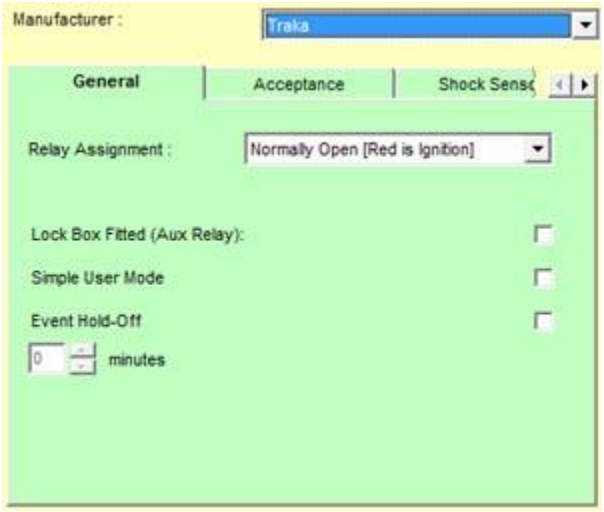
Here there are five definable detail fields for the Immobilisor. To change these field headings please refer to the Immobilisor Details section of Properties topic.

Notes

Enter any notes associated to the device.

Immobilisor Tab

Here you define the configuration of the Immobilisor.



Manufacturer

A Traka Immobilisor can be programmed with a specific Manufacturers Code using a Program iFob. Once the Immobilisor has been programmed with a Manufactures Code, only Service iFobs that have been programmed with the same Manufacturers Code will work with that Immobilisor. All new Immobilisors are programmed with a Manufactures Code of 'Traka' if the customer does not specify before installation.

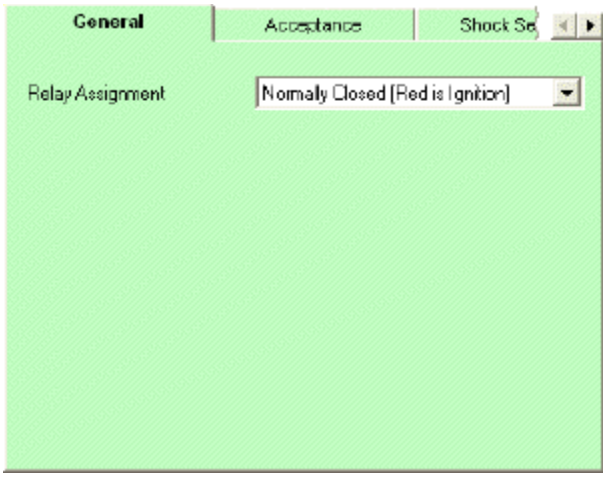
Default Manufacturer Code

As of software version V02.13.0000 it is possible to set a default manufacturer code for any detail form opened within the same database. For example, when opening the Immobilisor details window you will not need to worry about changing the manufacturer type as it will be set to the site default (e.g. Traka) in the Traka32 properties. This is beneficial as you will not need to change the manufactures code for each individual Immobilisor that needs programming. Please review the Immobilisor section of the Properties topic for more details on how to enable the option.

Region

From this drop down box you can select which region you wish the truck to belong too. For information on how to create Immobilisor please review the Immobilisor Regions topic.

General



Relay Assignment

Select the operation of the relay when the Immobilisor is active.

- Normally Closed [red is Ignition]
- Normally Open [Yellow is Ignitions]

Acceptance

Acceptance Button Fitted

Select this option if the Immobilisor is fitted with an Acceptance Button.

NOTE: this option if the Immobilisor is NOT fitted with an Acceptance Button otherwise the Immobilisor will cut out after the time-out delay.

Please refer to the Immobilisor Acceptance section for more details.

Acceptance Warning

The Acceptance Warning option when enabled activates a beacon (to be wired into the Immobilisor on site) 30 seconds before the acceptance period expires.

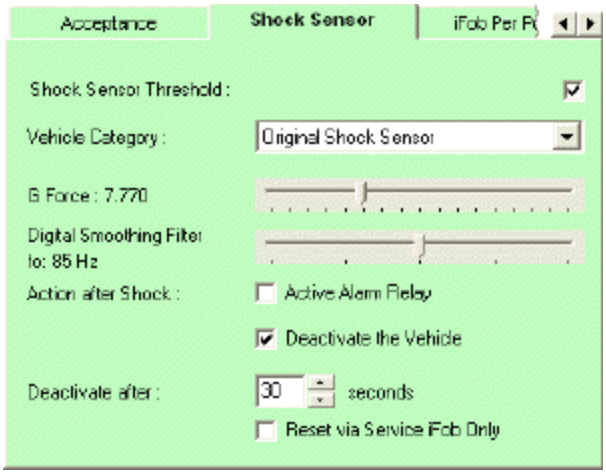
iFob Per Person Single Acceptance

When this option is selected the driver of the Truck will only be asked to press the Acceptance button once, even if they leave the truck and come back later. If another driver uses the truck then they will have to press the Acceptance button.

Time-out Delay

You can configure a period of time (in minutes) in which the truck operator has to perform their pre-operational checks.

Shock Sensor



Shock Sensor Threshold

Select this option if the Immobilisor is fitted with a Shock Sensor module. You can configure the shock sensor's g-force threshold level at which the Immobilisor will record a shock and act upon it.

NOTE: this option if the Immobilisor is NOT fitted with a Shock Sensor module otherwise the Immobilisor will not program correctly.

Please refer to the Immobilisor Shock Sensor section for more details.

Vehicle Category

Select the type of shock sensor that you wish to configure...

- Original Shock Sensor
- Category A (Forklift Mass between 200 -1300 Kg's)
- Category B (Forklift Mass between 1300 -3400 Kg's)
- Category C (Forklift Mass between 3400+ Kg's)

Action after Shock

Again, if the Immobilisor is fitted with a Shock Sensor module, you can configure what actions should be taken after the Shock Sensor Threshold has been breached.

Active Alarm Relay

If this option is selected, the alarm relay will activate if an impact occurred. Immobilisor is fitted with a relay that can activate a siren or flashing light if an impact occurs.

If the option is not selected the alarm relay will not active under any circumstances.

Deactivate the Vehicle

If the option is selected, the vehicle will deactivate x number of seconds after impact depending on the deactivation delay set.

NOTE: Immediate deactivation of a vehicle after and impact may be dangerous as an operator may need to move the vehicle to avoid further injury; therefore a small delay is recommended.

Reset via Service iFob Only

If this option is selected, the Immobilisor can only be reset after an impact by a supervisor using their Service iFob even if the power to the vehicle or Immobilisor is cut.

If this option is not selected, the operator will be able to reset the vehicle by removing and re-inserting their Vehicle iFob.

iFob per Person

Truck type

Select the type of truck between 1 and 56. Users can only operate the types of truck they are authorised to by allocating access levels 101 to 156. For example if a truck type of 5 was programmed, a user authorised to operate the truck would be given access level 105.

Truck Address

Select the truck address between 1 and 1023. Each truck should have its own unique address. The address is used by Traka32 to report on the events that have occurred for that truck.

Enabled Access Control

Select this option if the Immobilisor is used for Access Control.

Select this option if the iFob does not remain in the receptor socket for operation of the device e.g. where an iFob is "touched" to open a door. If enabled an event is recorded in the iFob before activating the device, this prevents the user from removing the iFob too quickly and losing the event. In this mode the standby LED is Solid Red so as there is as little time as possible before activation.

1 x System Authoriser

Select this option two Valid User iFobs are required to be inserted into the receptor socket to activate the ignition. A "request activation" event is logged in the first valid User iFob inserted. This must then be removed within 5 seconds. A "Device Activated" event is logged in the second Valid User iFob to be inserted within the next 5 seconds.

Enabled Daylight Saving (GMT)

Select this option to enable the real time clock to automatically update in accordance with U.K. GMT.

Enable Fault Logging

Check this box to enable the cost option Fault Logging on your Immobilisors. *Note: - Fault Logging must be enabled at the cabinet as well as the Immobilisor.*

Disable iFob Upon Logging Fault

This option automatically enables itself when you tick the 'Enable Fault Logging' box. With this option ticked, when a user logs a fault to the Immobilisor the iFob they used will not work again until it has been back to the cabinet and had the events downloaded from it.

4.19.14.4.6 LICENSE EXPIRY DATES

License expiry dates can be entered against the access level/Truck types 1-56 (Access Levels 101 – 156) from the user's details. This facility can be used to record when a user's license will expire for a given truck type. It will stop them from driving a truck once their license has expired.

Enabling the Option

There is an option in Traka32 properties that needs to be enabled before the license expiry option will work. To enable the option follow the steps below.

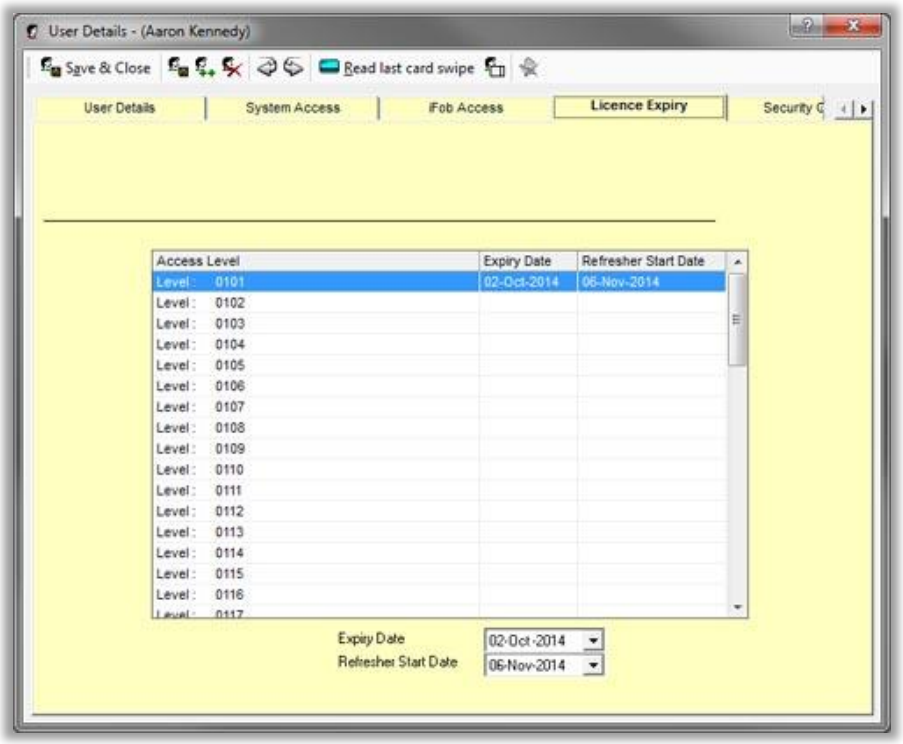
1. From the top of Traka32 select **File** > **Properties**.
2. When the properties window opens, select the **Comms** tab from the left hand side.
3. There will be an option called 'Revoke License Expired'. **Select** this tick box and click Save & Close.

   NOTE: You need a form of auto-comms enabled for this option to appear.

   NOTE: There is a setup procedure that a Traka engineer/project manager will have followed to ensure that the 'Revoke License Expired' option is available. If you have an iFob Per Person system with auto-comms and the option does not appear, please contact Traka.
4. Next you will need to add the expiry dates to the user details. From the top of Traka32 select the **User List**.
5. Highlight the desired user and double click, or select the **Users** button from the banner above and click the **Edit User** button.
6. When the user details window opens, navigate to the **License Expiry tab**.
7. Highlight the desired access level/s (which represents the truck type e.g. 101 type 1) and using the drop down selection box **enter an Expiry date**.

   NOTE: You can highlight multiple access levels at once.

   NOTE: If the user's expiry date is 48hrs prior to the next time the auto-comms runs past midnight, then the user will not get picked up by the license expiry option. To be safe, set the expiry date at some point in the future.



8. The Refresher Start Date selection box allows you to select a date when the user needs to have refresher training. Using the drop down selection box set a **Refresher Start Date.**

9. Click save and close.

10. The user is now set up and complete. Follow steps 7-9 for each user you wish to use the License Expiry option.

NOTE: Once the option is in use and a user's license has expired, the access level (truck type) will be removed from the user's details which will stop them driving the truck. The only way the user can drive the same truck again is to re-open the user details, navigate to the License Expiry tab and grant access to the desired access level (truck type).

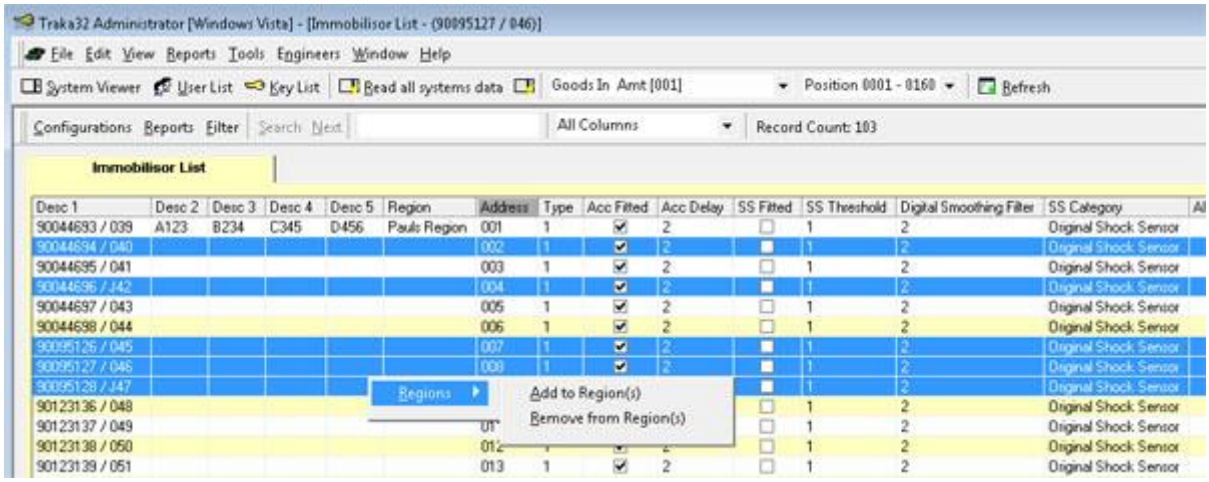
Running Reports

You can run a report to see who needs training within the coming months. This is called the MHE Equipment Refresher Training Report. It will list every user with a refresher date and how long they have until their training is required. Please refer to the Dock Door Training Reports for more details.

4.19.14.4.7 IMMOBILISOR REGIONS

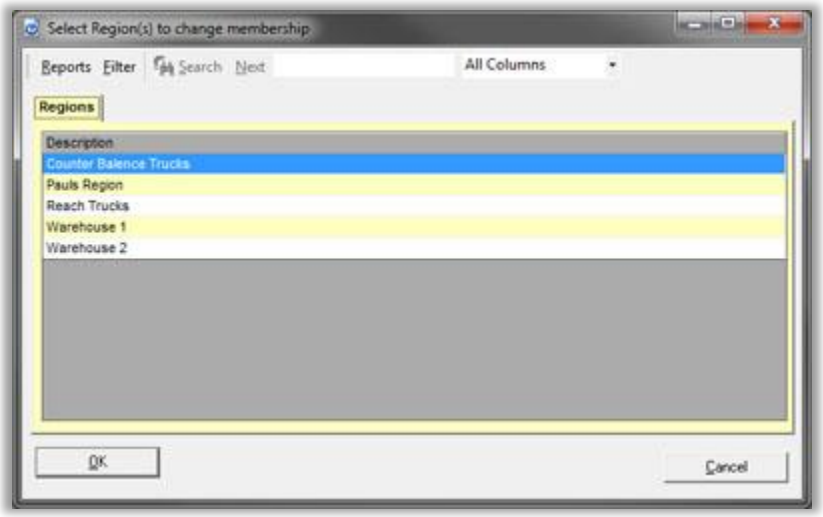
From the Immobilisor list it is now possible to assign an Immobilisor to a region.

To assign one or more Immobilisors to a region simply highlight the desired iFobs, right click and select Regions>Add to Region(s). To create regions please refer to the Regions section.



The Select Regions window will appear allowing you to select the desired region. Once selected click OK.

NOTE: The select regions window will be populated with the currently created regions. To create new regions please refer to the Regions section.



You will now notice that the region column for the selected truck(s) will now have the specified region.

4.19.14.4.8 IFOB PER PERSON DOWNLOAD STATION

The iFob per person download station is a fast effective way to download information from the iFob without having people queue up at a cabinet for long periods of time. The Download station is particularly beneficial to large customers who have a vast work force that have continuous shift changes, who wish to cut down the amount of time workers spend at the cabinet returning/removing iFobs. The Download Station allows users to insert their iFobs and recharge them at any point in the day.

The Data512 (yellow) iFob has more memory than the Data32 (blue) iFob which is why yellow iFobs are used with iFob per Person, however there isn't enough memory in the iFob to hold a large number of events so they need to be downloaded frequently, this is why the Download Stations are used. A Download Station is essentially a cabinet with no door, you then insert your iFob into a free position then swipe you card at the reader to recharge the iFob, which will only take a few seconds. The iFob does not have a fixed return position in the Download Station, you are able to return the iFob to any location and recharge it. When using the iFob per Person Download Station the users have their own personal iFobs which they get to keep, the iFob holds the users data such as vehicles they are licensed to operate, and holds certain events such as Shock Sensor breaches (if the vehicle is fitted with the appropriate hardware), also vehicles that have been used and the precise times they were operated.

How to set up an iFob per Person Download Station

Firstly an option is required in the firmware to enable the download station, check the tick box 'Download Station' next to the iFob per Person box.

Once your system is configured with the appropriate settings, you need to enroll your users to the system before attempting to assign them their individual iFobs, then 'Synchronise Users' to the cabinet. To find out how to add a new user and edit their details please refer to the Adding Users and User Details sections of the user guide. After creating the users and Synchronising them to the system, the Download Station is now ready for use. The user must now insert a blank Yellow (Data512) iFob into the Download Station and the following message will be displayed on the LCD...

NOTE: The * symbolises the position the iFob is inserted into.

The desired user now needs to swipe their card to receive the following message...

After a few seconds the iFob will be fully charged and the user may now remove their iFob.

This process assigns the iFob to the user. When the user next inserts their iFob into the download station they will be prompted to swipe their card, this will recharge the iFob and allow the user to remove it from the cabinet. All the transactions that have taken place will be downloaded to the cabinet.

Swiping the Incorrect Card

If a user inserts their iFob and swipes the incorrect card you will receive the following messages on the LCD...

After a few seconds the display will change. The next message shows whose iFob has been inserted and also whose card has been swiped against it...

And finally after a few more seconds the user will be prompted to remove the iFob from the download station.

NOTE: The * symbolises the position the iFob is inserted into.

Using a Sagem Fingerprint Reader with a Download Station

When using a Sagem fingerprint reader with a download station the user identification process is slightly different. Once the user inserts their iFob the following message will be displayed on the LCD...

NOTE: The * symbolises the position the iFob is inserted into.

The user now needs to place their finger on the reader to receive the following message...

After a few seconds the iFob will be fully charged and the user may now remove their iFob.

This process assigns the iFob to the user. When the user next inserts their iFob into the download station they will be prompted to swipe their card, this will recharge the iFob and allow the user to remove it from the cabinet. All the transactions that have taken place will be downloaded to the cabinet.

Sagem Reader using Secondary PIN access

In the example below the system has a Sagem fingerprint reader but the user is using their secondary PIN. Once the user inserts their iFob the following message will be displayed on the LCD...

NOTE: The * symbolises the position the iFob is inserted into.

The user now enters their secondary PIN into the keypad...

NOTE: There is no need to press any buttons, the user can simply begin to enter the secondary PIN straight away.

After a few seconds the iFob will be fully charged and the user may now remove their iFob.

This process assigns the iFob to the user. When the user next inserts their iFob into the download station they will be prompted to swipe their card, this will recharge the iFob and allow the user to remove it from the cabinet. All the transactions that have taken place will be downloaded to the cabinet.

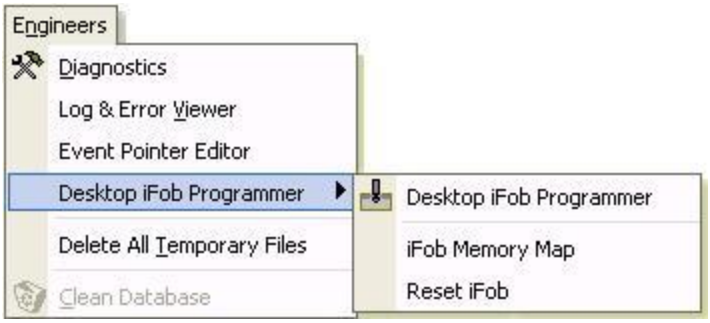
Desktop iFob Programmer

If you wish to use a Desktop iFob Programmer and you have not previously used one before, you will need to install the Drivers to your machine, please refer to the Desktop iFob Programmer Installation guide for further information. The Desktop Programmer is useful for several things such as resetting iFobs, creating Program iFobs, creating Test iFobs etc.

Resetting an iFob

The main function of the Desktop iFob Programmer when using it in conjunction with the Download Station, is resetting iFobs. For example if you have an iFob that was used before and you wish to assign it to a new user, you can reset the iFob and use it again.

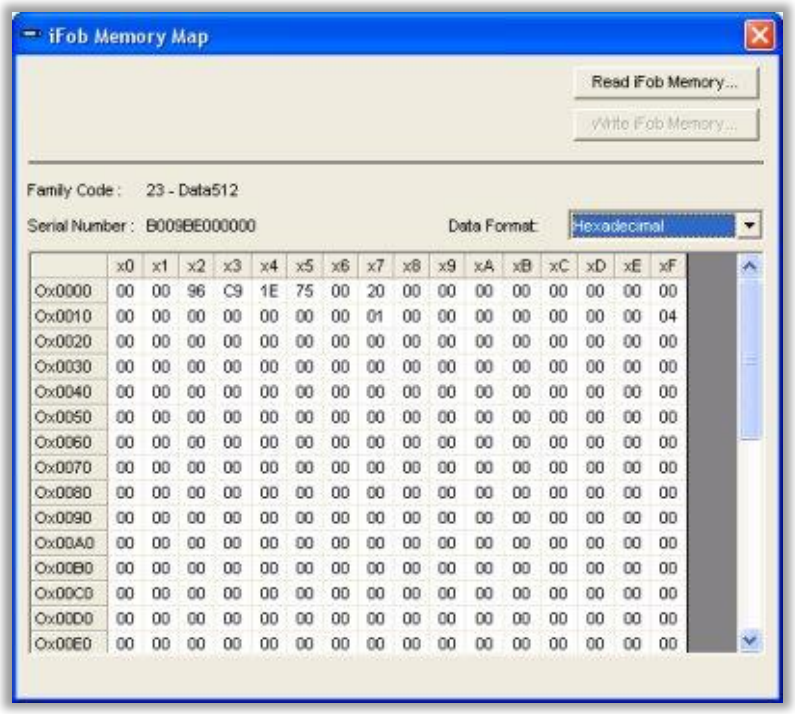
Once the correct Drivers have been installed successfully and you have plugged you Desktop Programmer in to a free USB port, you can insert the desired iFob into the barrel of the Desktop Programmer ready for resetting. Next on the tool bar at the top of the screen in Traka32 click *Engineers* > *Desktop iFob Programmer* > *Reset iFob.*



After a few seconds a window will appear informing you whether the reset was successful or not. If the reset is successful the message will read 'iFob Information Successfully Cleared'. You are now able to remove the iFob and use it as desired.

iFob Memory Map tab

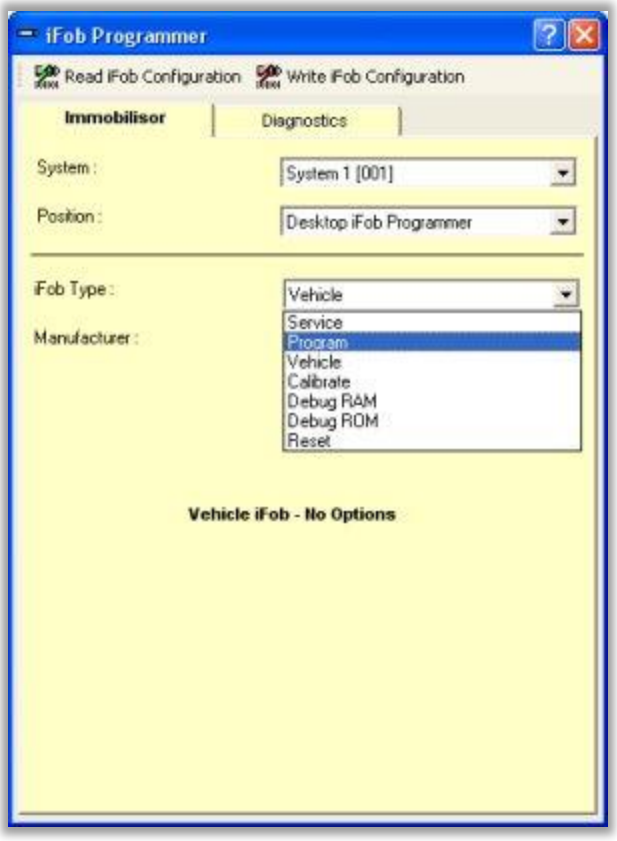
The iFob Memory Map allows you to view the data that is currently stored in the iFob.



	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x0000	00	00	96	C9	1E	75	00	20	00	00	00	00	00	00	00	00
0x0010	00	00	00	00	00	00	00	01	00	00	00	00	00	00	00	04
0x0020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x0090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0x00E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

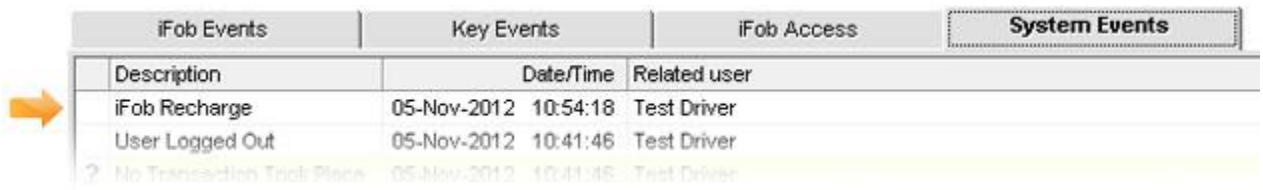
Desktop iFob Programmer tab

The Desktop iFob Programmer tab opens up the iFob Programmer that allows you to create iFobs such as Program iFobs, Test iFobs, Calibration iFobs etc. These iFobs are used for reprogramming and re-configuring Data Loggers and Shock Sensors.



Traka32

A new System event has been added called "iFob Recharge" which is created when a user recharges their iFob in a download station. This is available with the 16 bit firmware version 3.00.48. You can view the event details on the System Viewer screen, on the System Events tab.



4.19.15 JOB REFERENCE LOGGING

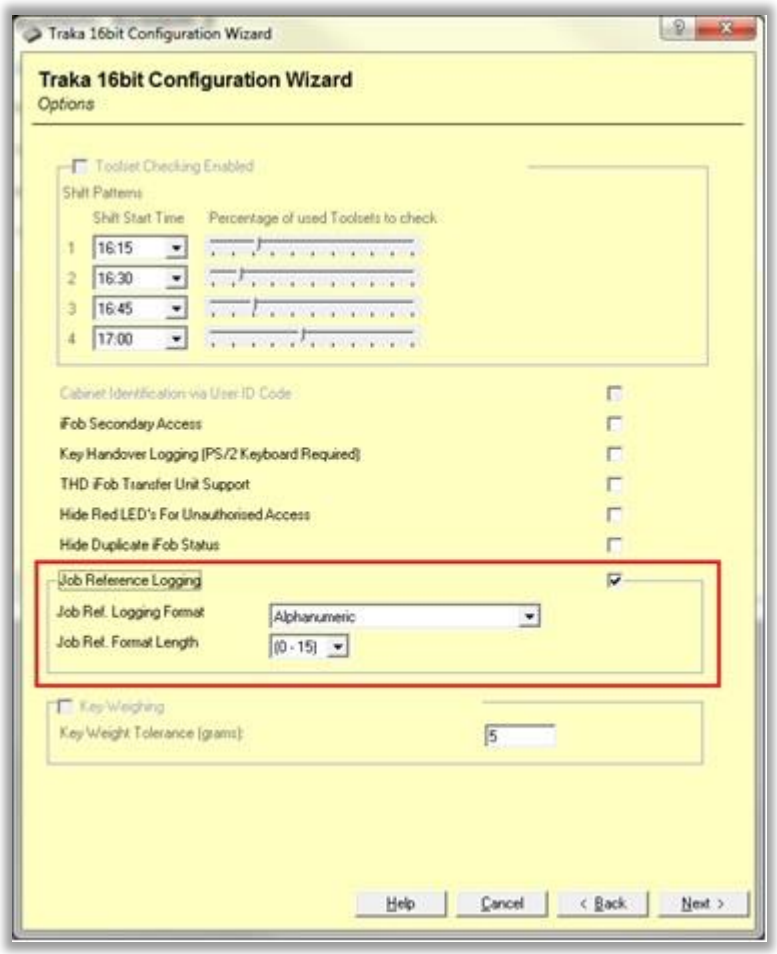
Job Reference Logging was developed for companies that give their employees reference numbers for each job they perform. This option allows a user to enter an alphanumeric reference number (up to 15 characters in length) into the cabinet when removing or returning an iFob. Job Reference Logging is a cost option and requires firmware version 3.00.14 and software version 02.09.0014 and above to work.

Job Reference Format and Length

1. The format and length of the Job Reference code can be specified in the Configure Firmware menu. Right click the Pod and select 'Configure Firmware'.

2. Click 'Next' through the pages until you reach the page shown below. From here you can select the format and length of the Job Reference code. The available options are listed below:

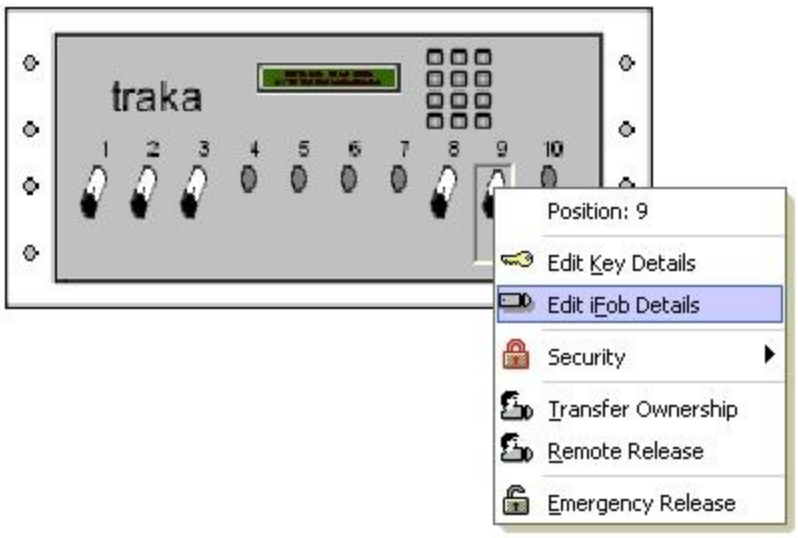
    - Alphanumeric with any number of characters between 0-15 characters in length
    - Alphanumeric with a fixed length of 1-15
    - Alpha with any number of characters between 0-15 characters in length
    - Alpha with a fixed length of 1-15
    - Numeric with any number of digits between 0-15 digits in length
    - Numeric with a fixed length of 1-15.



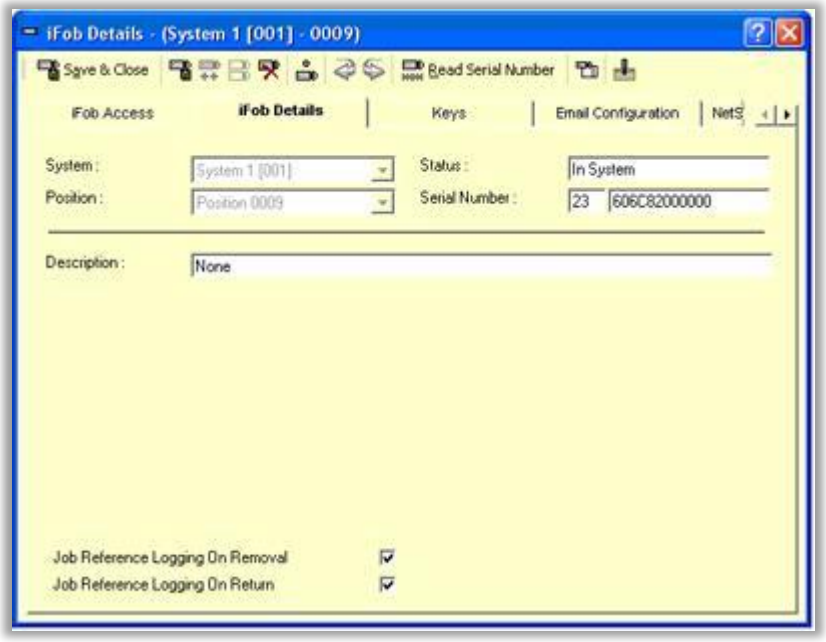
3. Click 'Next' through to the last page and then click 'Apply' to save the changes to the system.

Configuring the iFobs

1. Job Reference Logging works on a per iFob basis. To enable this option right click the iFob you wish to setup and select 'Edit iFob Details'.



2. Select the 'iFob Details' page. There will be two tick options at the bottom of the window, **Job Reference Logging on Removal** and **Job Reference Logging on Return.**



3. Select which options you would like and click the **Save & Close** button.

   NOTE: It is unlikely that you would need to have both of these options enabled at the same time however you can select them both if desired.

4. When a user now attempts to remove or return the iFob one of the scenarios below will take place...

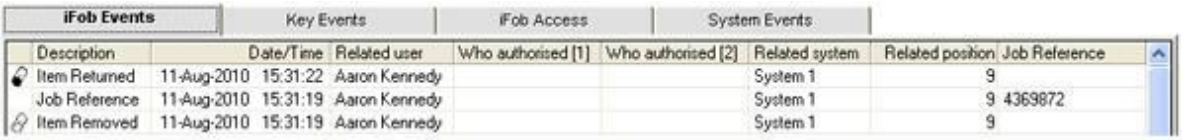
   Job Reference Logging on Removal

   With just this option enabled the user will only be prompted to enter a reference code before you remove the iFob.

   Job Reference Logging on Return
   With just this option enabled the user will only be prompted to enter a reference code when returning the iFob.

Job Reference Logging on Removal and Return
With option enabled the user will be prompted to enter a reference code when removing and returning the iFob.

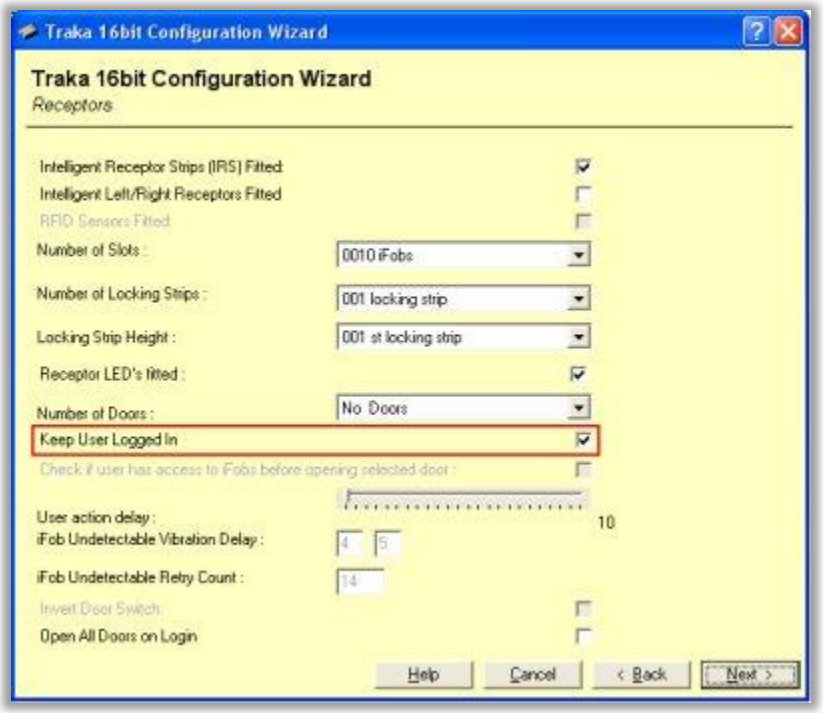
5. Click the read all system data button and navigate to the 'iFob Events' section. Here you will see the user who removed the iFob and the reference number they have entered.



4.19.16 KEEP USER LOGGED IN

This feature is a 16bit firmware only option that when enabled, allows a user to log into a 'No Door' system and stay logged in until the user presses the * key. If the user walks away from the system without logging off it will automatically log them off after the defined User Action Delay period.

This feature is a cost option and must be enabled in the firmware. To activate this option you must purchase a new configuration file from Traka and upgrade your system.



4.19.17 KEY BOOKING

4.19.17.1 KEY BOOKING OVERVIEW

Key Booking as its name suggests allows a user to pre-book an iFob / key. Using the Key Booking Wizard a key can be booked for a period of time in the future.

Fixed Return and Random Return to a Single System

Key Booking for Fixed Return and Random Return to a Single System works by specifically booking a specific iFob to an individual user between two given times.

During the booking period, only a user associated to the booking will be allowed to take and return the iFob / key.

The booking will remain active until the current time has passed the booking end time. If the user has finished with the iFob / key early, the booking can be cleared from the Booking List in Traka32 by deleting the booking. Alternatively if you are using a 16bit system with firmware V03.00.41 and up, you can delete the booking when you return the iFob/ key to the system.

It is possible for other authorised users to take the iFob outside of the booking time period unless iFob Access via Key Booking Only is enabled. For 8-bit systems, *Key Booking* and *iFob Access via Key Booking Only* options are mutually exclusive (cannot be used together on the same system). For 16-bit systems, only normal *Key Booking* is required. This is because on a 16-bit system it is possible to book an iFob to a user who does not have the access rights to the iFob outside the booking period, therefore eliminating the need for the *iFob Access via Key Booking* only option.

As the booking time approaches, it is possible for other authorised users to take the iFob but the user will be warned that there is an approaching booking. If an authorised user requests an iFob / key up to 12 hours prior to a booking, the user will be warned on the Traka Systems LCD that a booking is approaching along with the date and time of the booking.

If the iFob / key are not returned prior to the booking, the user will have to use the iFob Search Facility to lookup the current holder of the vehicle so that the iFob / key can be obtained. Alternatively the user will have to take an alternative iFob / key.

Each 8 bit Traka System can currently hold up to 100 bookings at a time, and each 16 bit system can currently hold up to 800 bookings at a time (firmware version 3.00.41 and above). Once a booking has expired the Traka System will automatically delete the booking from its memory freeing up the space for a new booking. The booking history is permanently kept by the Traka32 Software. The Key Booking System will not allow a user to pre-book the same key twice within a given period.

Notes:

- For 8bit systems, only a single user can be associated to the booking.
- On 8bit systems you can store up to 100 key bookings at a time.
- For 16bit systems, up to 3 users can be associated to a booking when using fixed return **ONLY**.
- On 16bit systems you can store up to 800 key bookings at a time from firmware version 3.00.41 and above.
- Key Booking with Fixed Return or Random Return to a Single System will only be available with 8-bit firmware version 6.05.02 and above and if the firmware of the selected system has Key Booking enabled.

Random Return to Multiple Systems

Key Booking has now been updated to work with Random Return to Multiple Systems however there are some differences in its operation compared with Fixed Return or Random Return to a Single System.

Key Booking for Random Return to Multiple Systems by booking an iFob Access Level to an individual user between two given times.

The Traka System will ensure that during the booking period that there are enough iFobs with the specified Access Level in the system to cover the bookings. This does not guarantee a user a specific iFob / key but does guarantee a particular type of iFob / key.

The booking will remain active until either the user removes a booked iFob or until the current time has passed the booking end time.

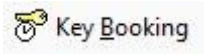
As the booking time approaches, it is possible for other authorised users to take the iFobs with the specified Access Level but the user will be warned that there is an approaching booking when there are not enough iFobs with the specified Access Level currently in the System. If an authorised user requests an iFob / key up to 12 hours prior to a booking, the user will be warned on the Traka Systems LCD that a booking is approaching along with the date and time of the earliest booking.

If the iFob / key are not returned prior to the booking, the user will have to use the iFob Search Facility to lookup the current holder of the vehicle so that the iFob / key can be obtained. Alternatively the user will have to take an alternative iFob / key.

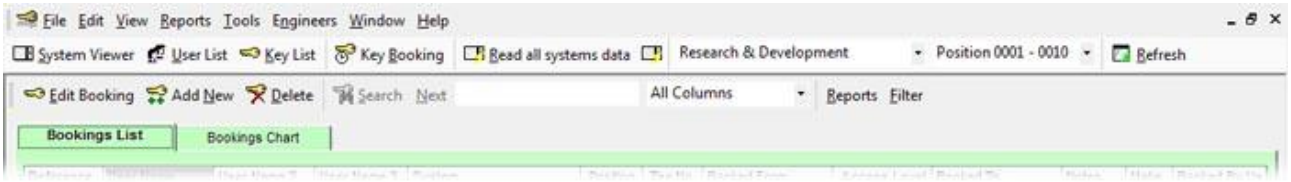
Each Traka System can currently hold up to 100 bookings at a time. Once a booking been completed or has expired the Traka System will automatically delete the booking from its memory freeing up the space for a new booking. The booking history is permanently kept by the Traka32 Software. The Key Booking System will not allow a user to pre-book the same key twice within a given period.

NOTE: Key Booking with Random Return to Multiple Systems will only be available with firmware version 6.07.34 and above and if the firmware of the selected system has Key Booking enabled.

4.19.17.2 KEY BOOKING FORM

This topic will detail the main tools of Key Booking and how they work. The main page of key booking is the Booking List, to access the booking list click 

from the main menu.



Edit Booking

Selecting this while highlighting an existing booking will allow you to make changed to that booking. For more details please refer to the Booking Wizard topic.

Add New

Selecting this button will allow you to add a new booking to the system. For more details please refer to the Booking Wizard topic.

Delete

Selecting this while highlighting an existing booking will allow you delete that booking. For more details please refer to the Deleting a Key Booking topic.

Search

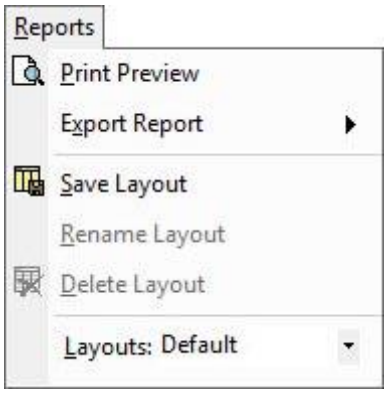
The search feature applies to the each column and line within the Booking List & Booking Chart. You can search for users who have keys booked to them or the system the key is booked from.

Reports

Print Preview will show a preview of the report for whichever page you are currently viewing, e.g. Booking List. This preview will also depend on the layout you are currently viewing.

Export Report gives you the option to export the report to an Excel spreadsheet.

The Layout options allow you to save a custom layout. For more information please refer to the Key Booking Layouts topic.



Filter

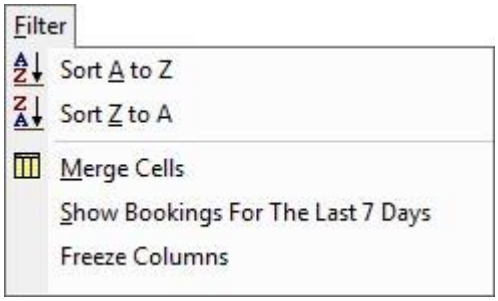
Sort A to Z will list all the data alphabetically from A to Z

Sort Z to A will list all the data alphabetically from Z to A

Merge Cells will combine multiple adjacent cells to be into a single larger cell. This can be toggled on and off depending on preference.

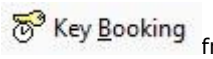
Show Booking from the last 7 days will display all the current and completed booking from the last seven days.

Freeze Columns will solidify all the data fields up to the first date column in the booking chart.

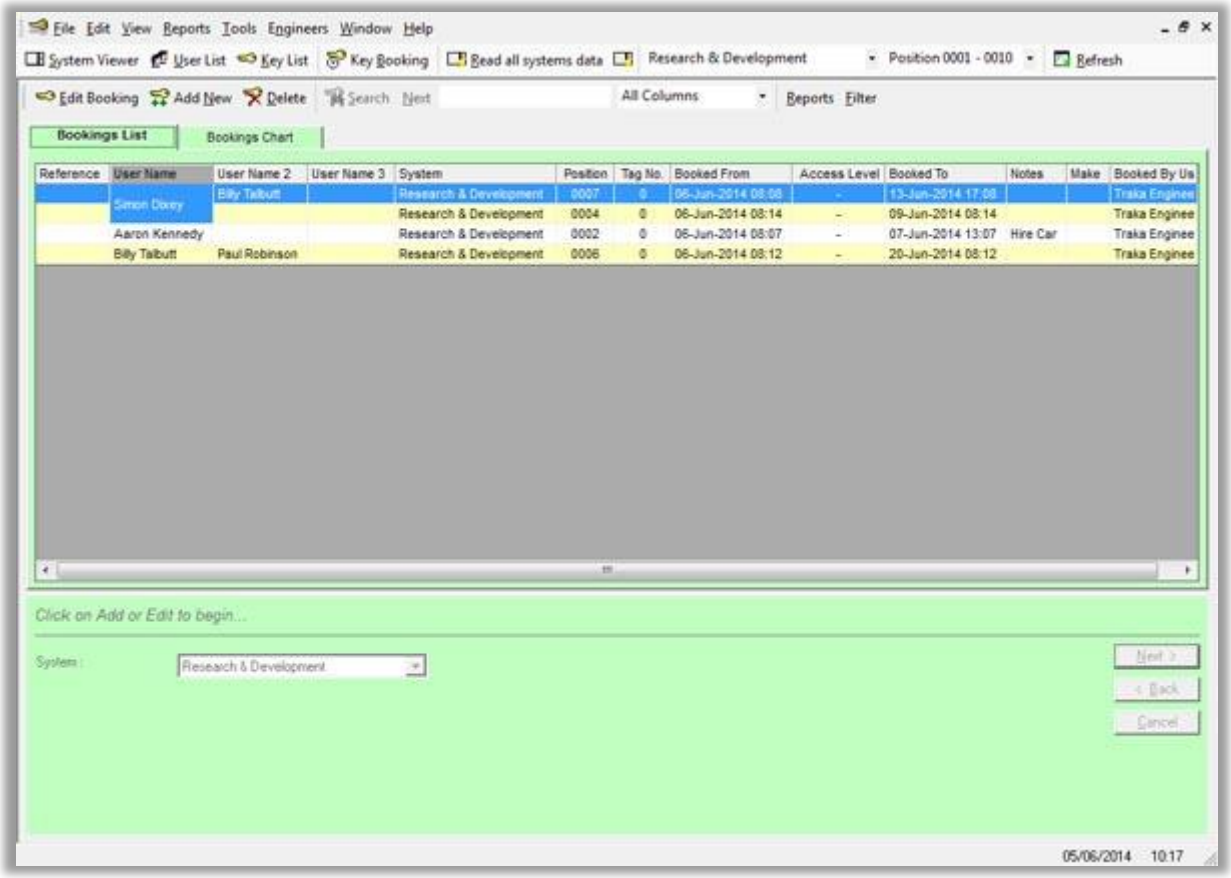


4.19.17.3 KEY BOOKING LIST

The Key Booking List allows you to view the current key bookings that have been made. From this list you can add and edit the bookings via the easy to use wizard or simply delete bookings.

To view the key booking list, click on 

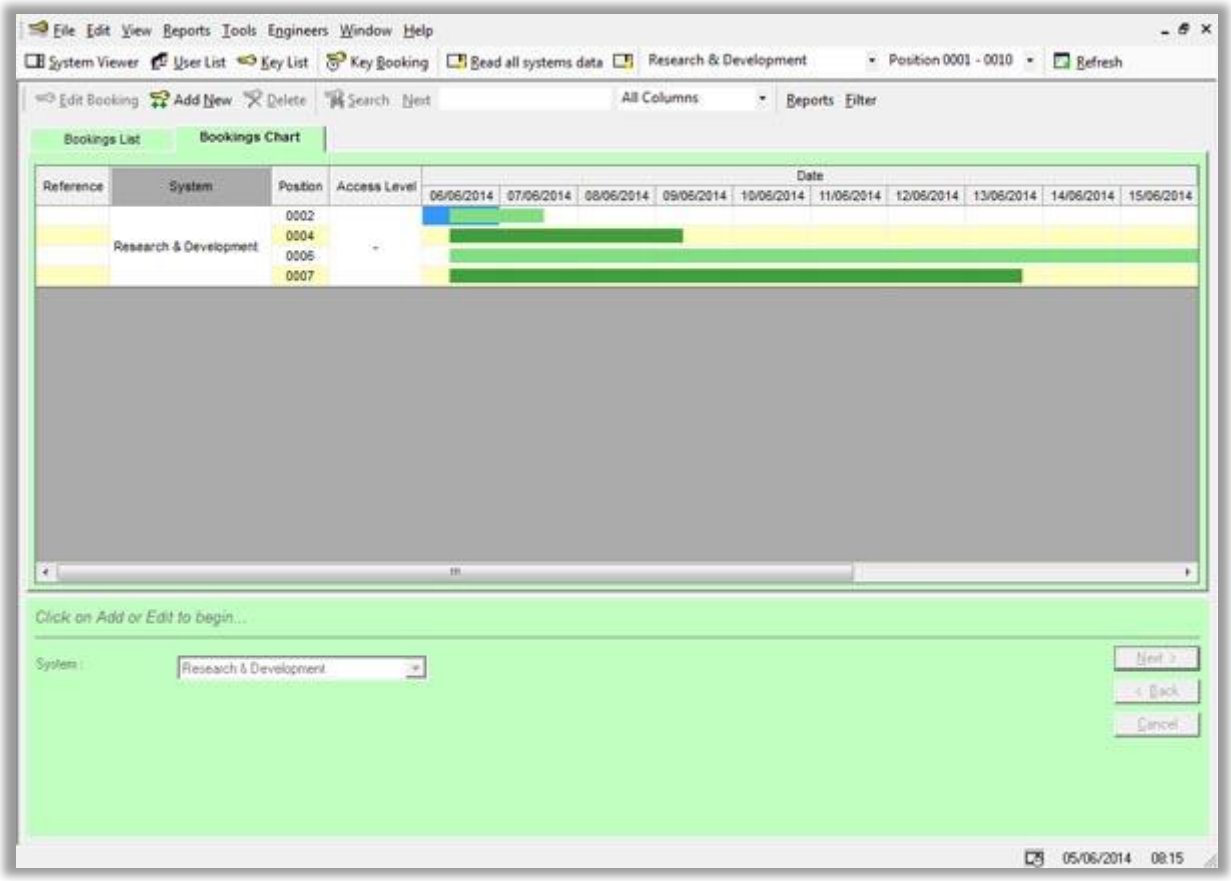
from the main menu.



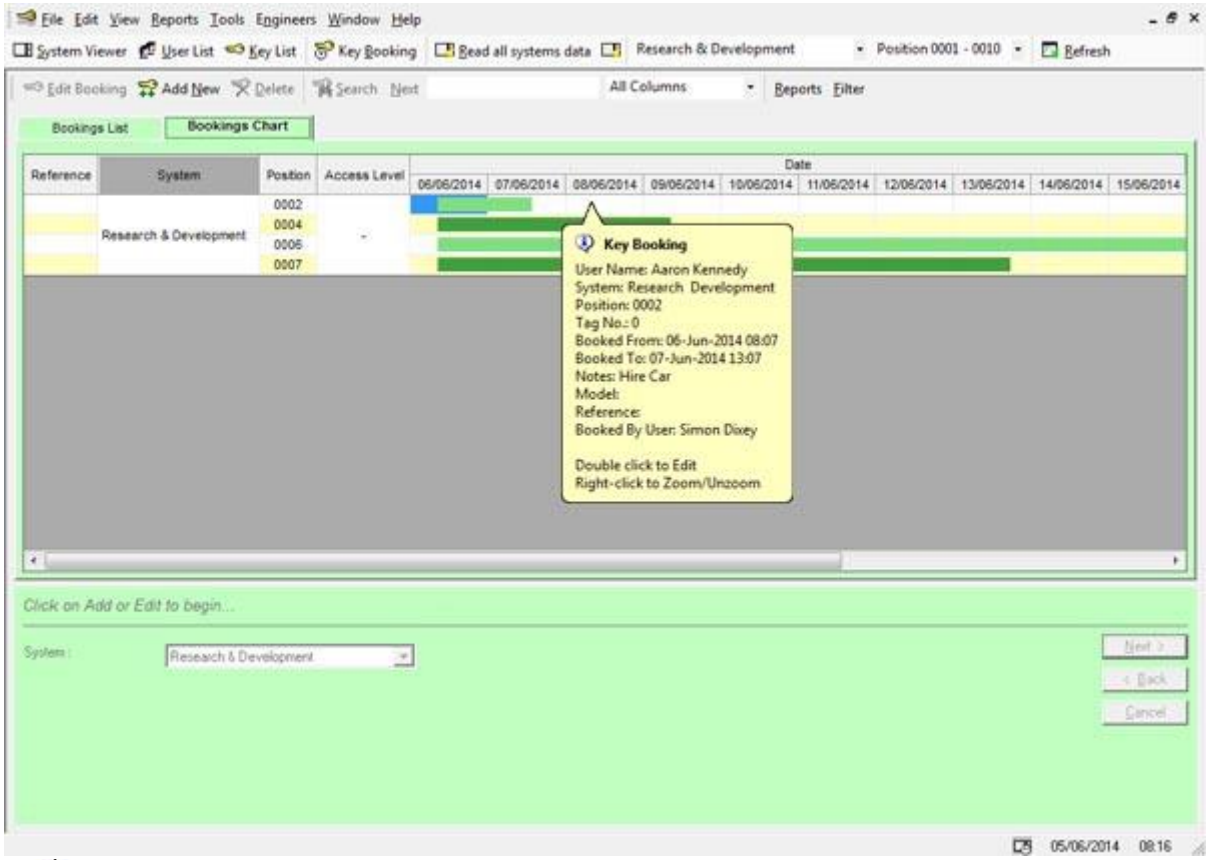
A user will only be able to view the bookings in the list that they have made. However it is sometimes beneficial for a user to be able to view all the bookings in order organise their own. As of software version v02.11.0002 there is an option in the software login details that allows the logged in user to view all booking. Please view the Login Details topic for more details.

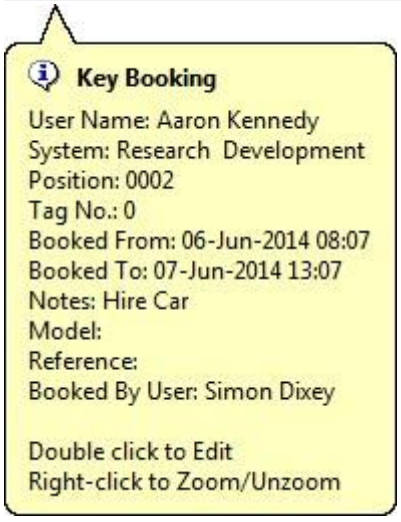
4.19.17.4 KEY BOOKING CHART

The Key Bookings Chart provides a graphical representation of all current bookings on the system.

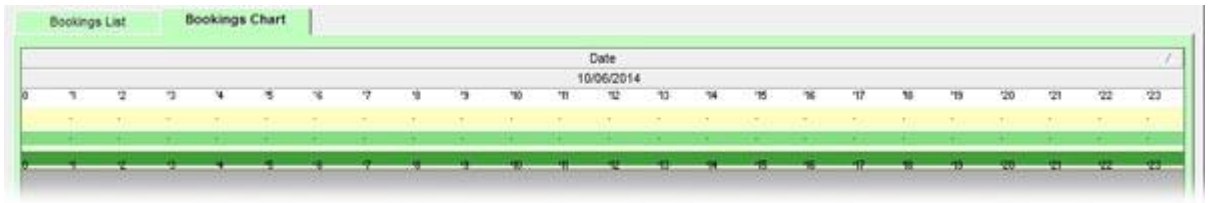


Booking details can be viewed by holding the mouse pointer over a booking record on the chart. A pop up is displayed with the booking details.





To view the bookings for a specific day, right click on the day of interest and the chart will zoom in to display this 24hr period. This also allows the user to easily see when an iFob is available (not booked) during the 24hr period.

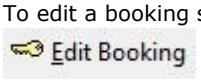


To edit an existing booking, double click on the booking directly from the chart and use the booking wizard at the bottom of the screen to edit the details as required. Please view Key Booking Wizard for more information.

4.19.17.5 KEY BOOKING WIZARD

To add a booking simply click on the 

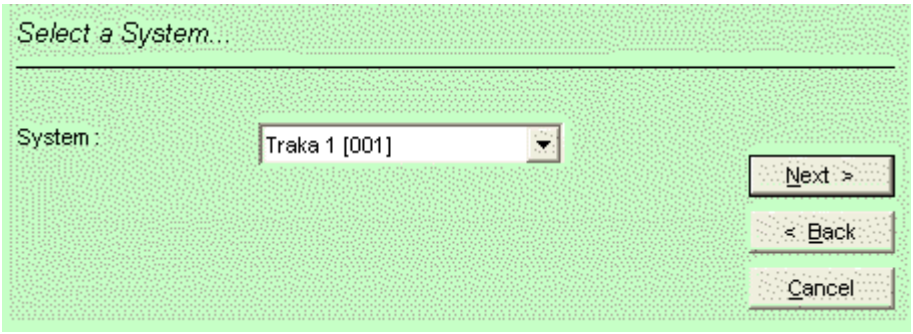
button.

To edit a booking simply **double click** on the booking record you wish to edit or select the booking and click on the 

button.

Step 1 – Select a System

Select a System from the drop down list and click on **Next**.

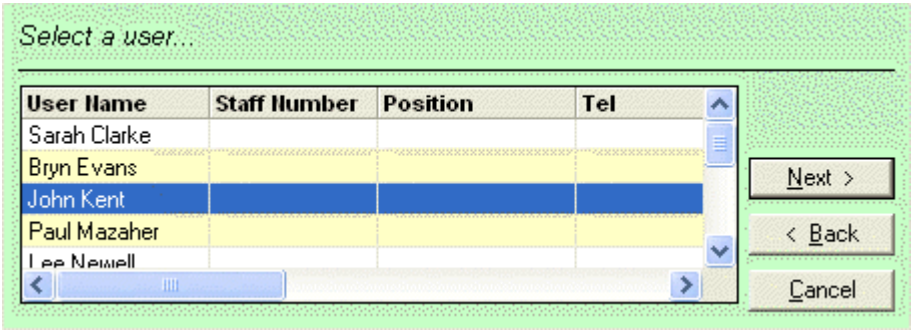


Step 2 – Select a User

Simply select a user from the list and click on **Next.** When the logged in user is a member of a region they can create key bookings for 'All Regions' users.

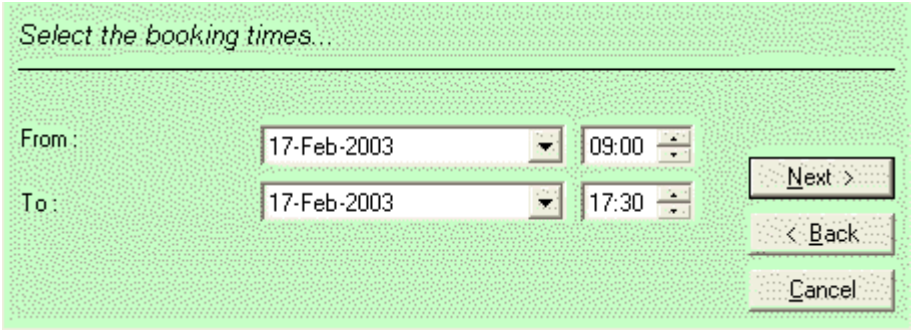
NOTE: For 16-bit systems up to 3 users can be associated to a single booking.

TIP: You can search the user list using the search box at the top of the key booking window



Step 3 – Select the Booking Times

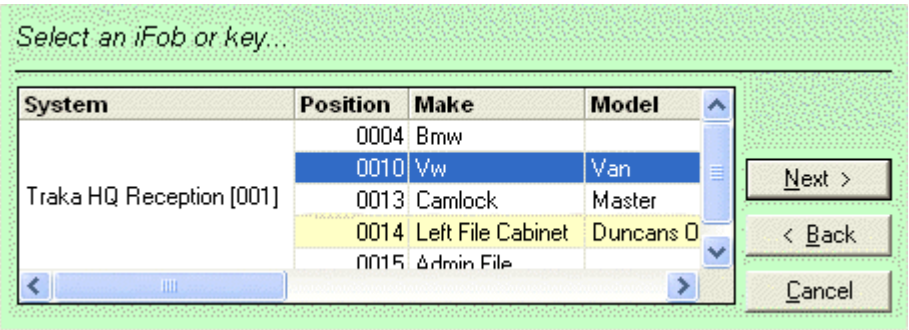
Select a start and end time for the booking and click on Next.



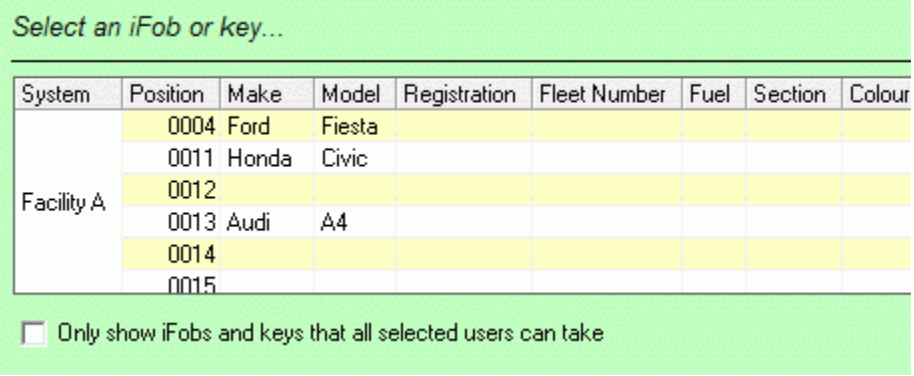
Step 4 – Select an iFob or Key / Access Level

If you have selected a System that is configured for Fixed Return or Random Return to a Single System, select an iFob or key from the list and click on **Next**.

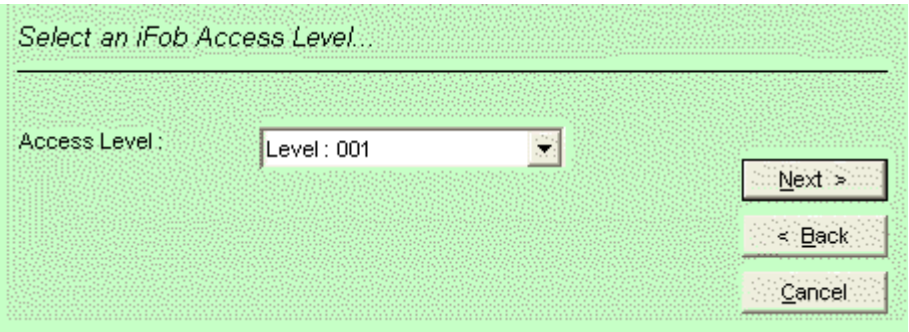
For **8-bit systems**, only the iFob or key the user is authorised to take will be displayed...



For **16-bit systems**, there is an additional tick box 'Only show iFobs and keys that all selected users can take'. This is useful as it allows a Traka32 administrator (with necessary privileges - see Login Details > Key) to book an iFob / key to a user who does not normally have the access rights to the iFob / key, therefore only allowing access during the booking period. View Key Booking Overview for more information.

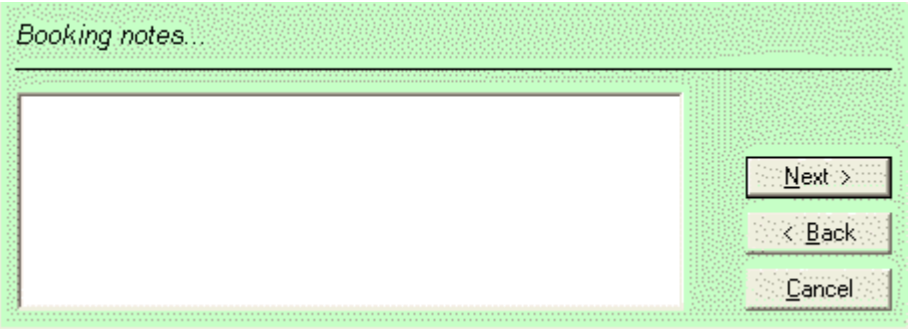


If you have selected a System that is configured for Random Return to Multiple Systems, select an iFob Access Level from the drop down list and click on Next.



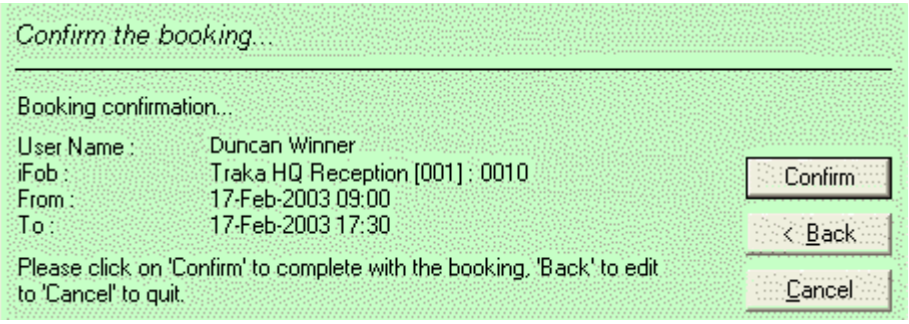
Step 5 – Booking Notes

Enter and notes that you want relating to the booking and click on **Next**.



Step 6 – Confirm the booking

Confirm the booking details, if you are happy and want to save the booking click on **Confirm** or if you want to change the details click on **Back** or to discard the booking click on **Cancel**.



If the booking is confirmed the Traka32 software will write the booking to the Traka System.

4.19.17.6 DELETING A KEY BOOKING

Traka32

To delete a booking in Traka32 you must have sufficient access to do so. Highlight the desired booking in the Bookings List and select the delete button. You will be asked to

At the System

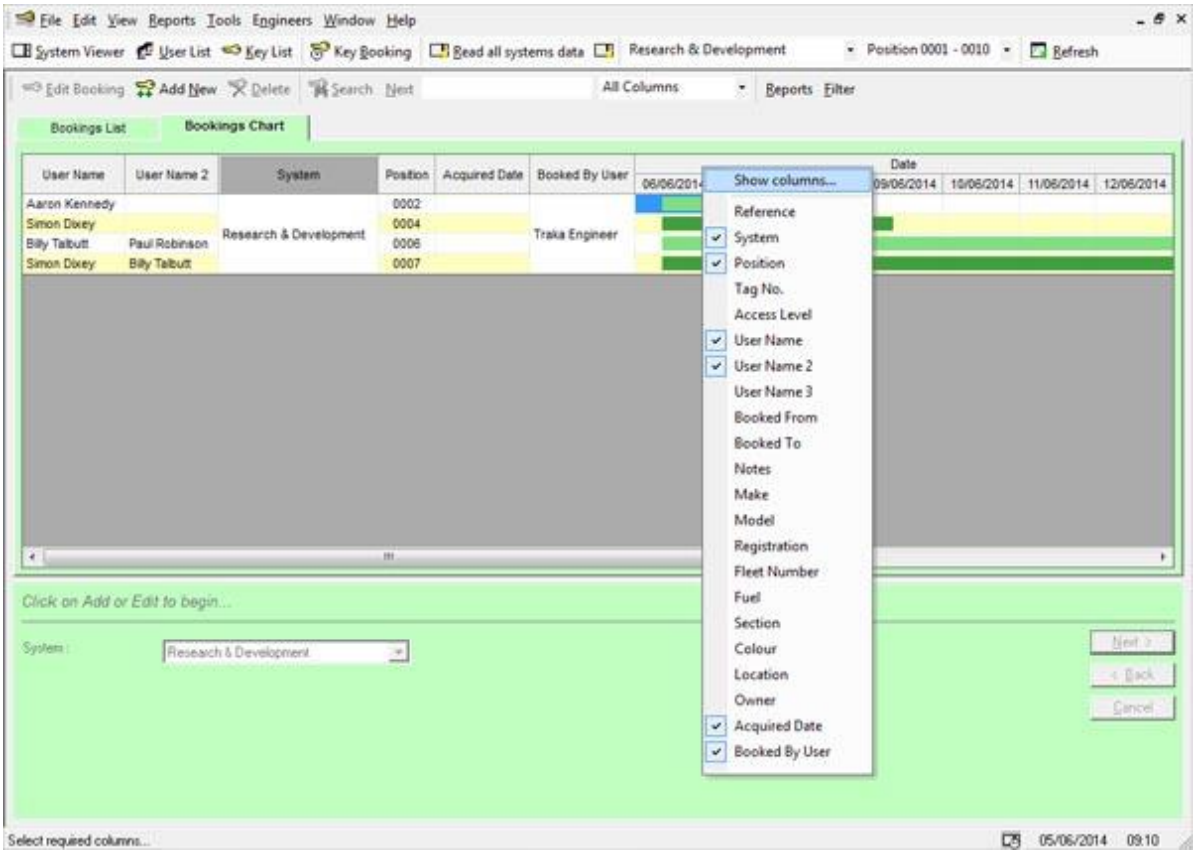
When a user returns an iFob that currently out of the system within the booking period, they have the option to complete the booking by pressing the # key, if they do this the booking will be removed or 'deleted' in Traka32, if they press the * key then the key booking will remain active until its expiry date.

4.19.17.7 KEY BOOKING LAYOUTS

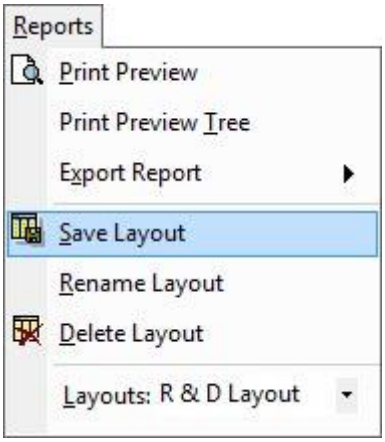
From software version v02.11.0001 onwards, it is possible to toggle the information columns that appear in the Bookings List & Booking Chart to create custom layouts.

1. To create a new layout, right click the header of any column.

2. The columns list will now appear allowing you to select and deselect the desired headings. As you do, the columns will be added and removed to the booking chart.

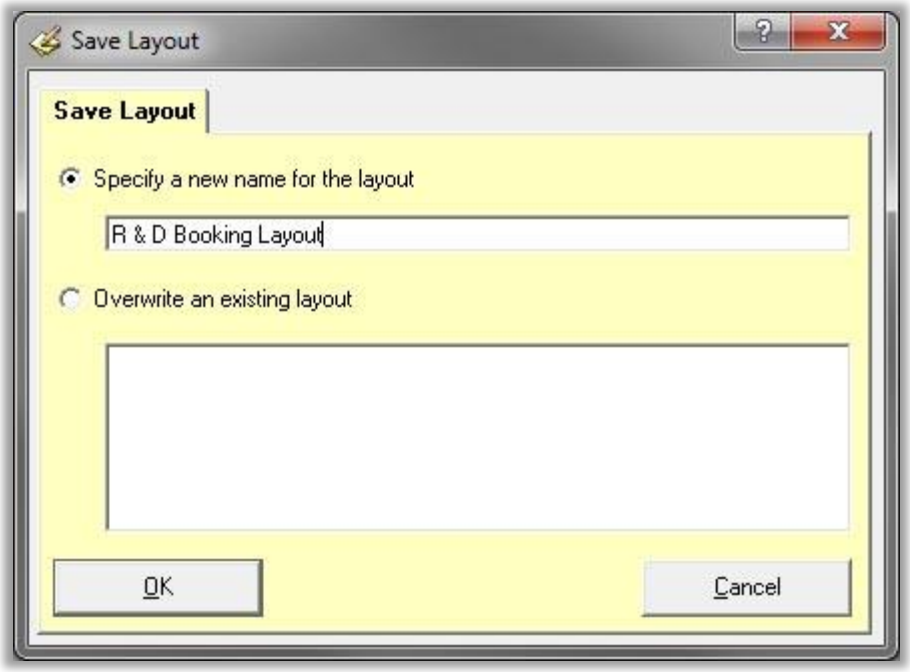


3. Once you have selected the desired layout, click the reports button and select Save Layout.

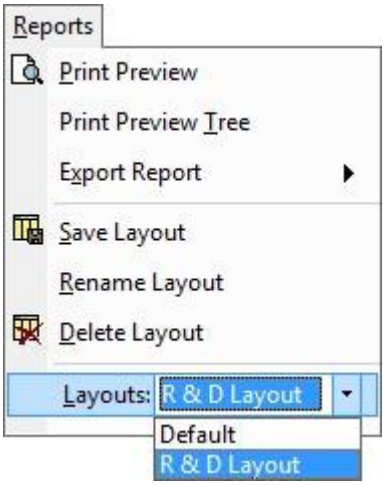


4. A window will appear allowing you to enter a name for the new custom layout.

   NOTE: You have the option to overwrite an existing layout. If a custom layout already exists you can overwrite it with the option you have previously selected.



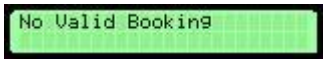
5. Once you have saved your layout Traka32 will automatically revert back to the default layout. To select your new layout click Reports, then select Layouts and choose your layout from the drop down list.



4.19.17.8 IFOB ACCESS VIA KEY BOOKING ONLY

When this option is enabled users are denied access to an iFob unless there is a valid key booking record associated with the iFob. If this option is not enabled, users can remove the iFob outside the key booking time period.

If a user tries to remove an iFob that does not have a key booking record associated or it is outside the key booking time period, the LCD will display:



4.19.17.9 OVERRIDE A KEY BOOKING

A User with Access **Level 195** can override a key booking and remove an iFob during the booking period even though the iFob has not been booked for them. See also How do access levels work.

4.19.17.10 KEY BOOKING BY REFERENCE

4.19.17.10.1 KEY BOOKING BY REFERENCE OVERVIEW

Key Booking by Reference will allow temporary users, who would not normally have access to the Traka System, to have a key made available to them via a booking reference number. This can be used for Hire Vehicles etc.

Once booked the user can go up to the Traka System, press 1 on the Keypad and the system will prompt for the Booking Reference number. The user can then enter the booking reference and if valid, the system will open the door and release the key. The booking reference will only be active between the booking start and end times as with standard key booking.

NOTE: The current Key Booking by Reference option does NOT work with Random Return to Multiple Systems (RRMS).

4.19.17.10.2 KEY BOOKING BY REFERENCE

Key Booking by Reference allows the selection of multiple keys when submitting the booking. Also, bookings can be made without specifying a user, by clicking the "Traka User" check box. This means that whoever registers for the booking at the cabinet (with the reference number) must also authenticate (e.g. swipe or PIN). This allows only internal staff members known to the system to complete the booking. Leaving this box unchecked requires a Forename and Surname as before, thus allowing for external visitors to access keys.

NOTE: Key Booking by Reference is only compatible with the 16bit control PCB.

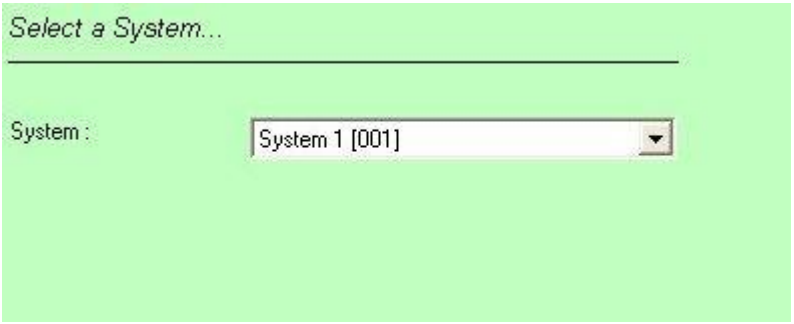
Ensure the cost option Key Booking by Reference is enabled in the system firmware.

To add a booking simply click on 

the button.

Step 1 – Select a System

Select a System from the drop down list and click 

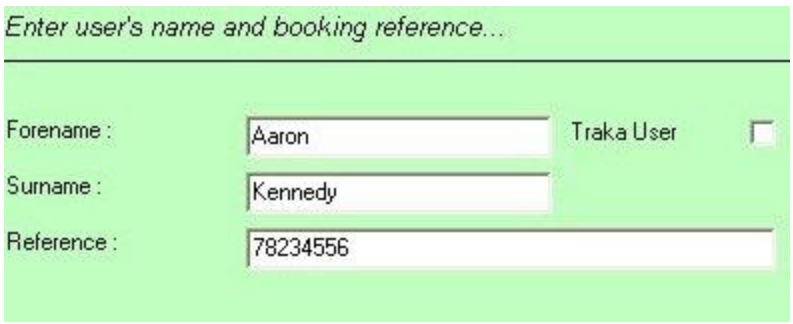


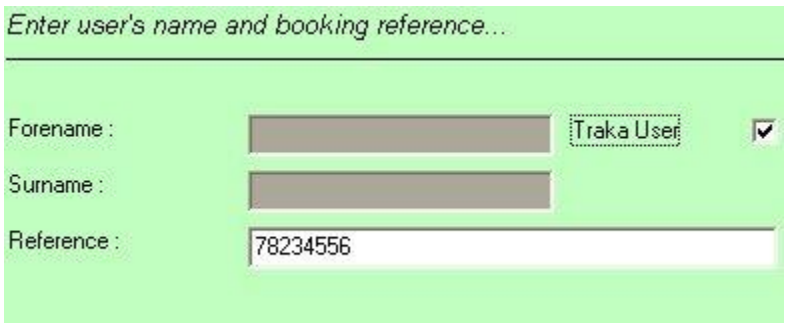
Step 2 – Enter User Name & Booking Reference

Enter a Forename, Surname and Reference and click 

. If the user completing the booking is Traka User, then check the 'Traka User' tick box. When this box is ticked, a Traka user will need to press 1 at the keypad and then enter the ref. number. The user is then prompted to enter his PIN (or swipe their card) and will be able to remove the key even they normally don't have access to it.

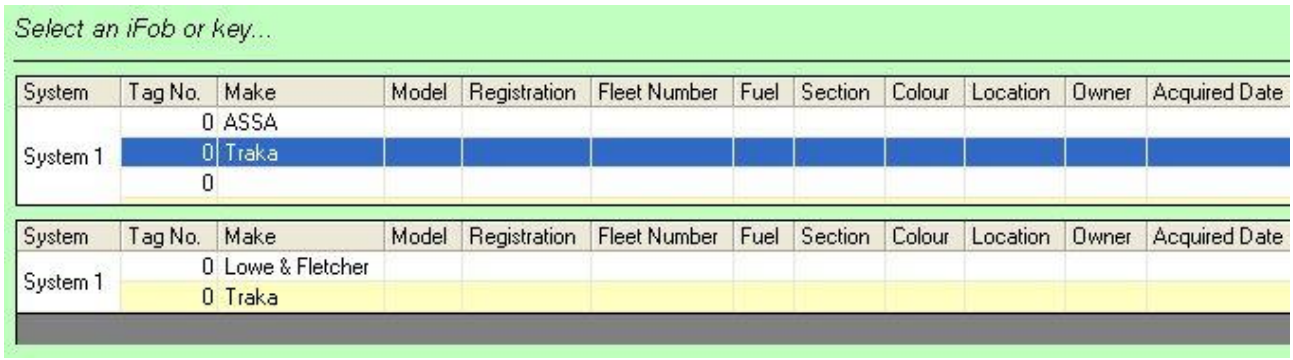
NOTE: The Reference must be a numerical reference and can be any length up to 12 digits long.





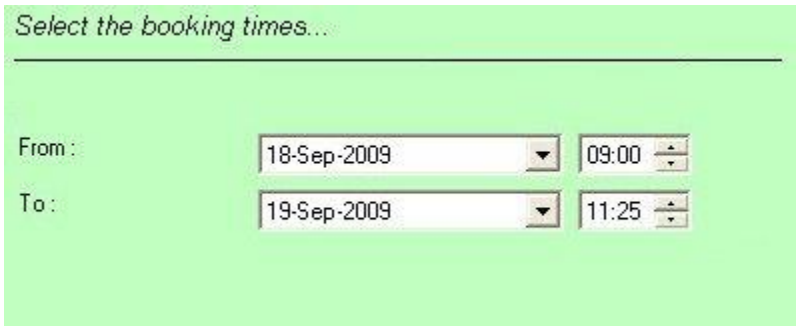
Step 3 – Select an iFob/s or Key/s

With Key Booking by Reference Enhanced, you can select up to five iFobs or Keys to be booked in one booking. Select the desired amount of iFob/s or key/s from the list and click 



Step 4 – Select the Booking Times

Select a start and end time for the booking and click 

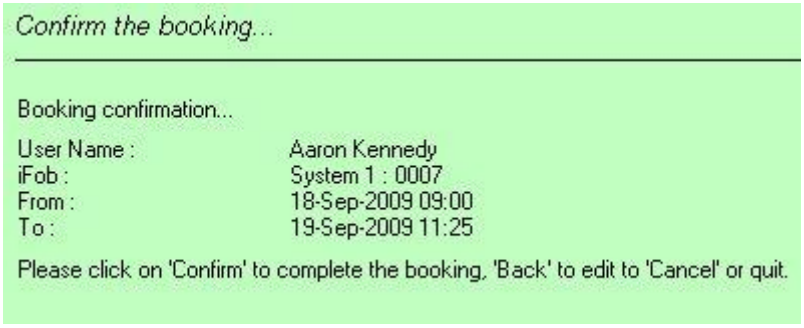


Step 5 – Booking Notes

Enter and notes that you want relating to the booking and click on Next >

Step 6 – Confirm the booking

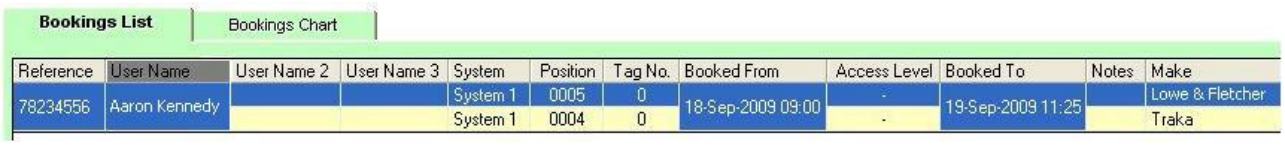
Confirm the booking details, if you are happy and want to save the booking click on Confirm or if you want to change the details click on < Back or to discard the booking click on Cancel



Step 7 – Viewing the Booking

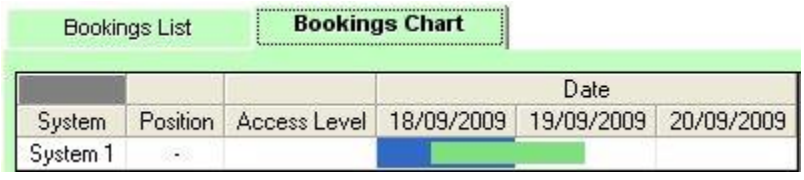
If the booking is confirmed the Traka32 software will write the booking to the Traka System. You can view the details of the booking by selecting the 'Bookings List' tab.

NOTE: Once a booking has been completed either by the user removing the booked keys or the booking time expiring, it will be removed from the booking list



The Key Bookings Chart provides a graphical representation of all current bookings on the system.

NOTE: Once a booking has been completed either by the user removing the booked keys or the booking time expiring, it will be removed from the booking chart



Step 8 – Editing a Booking

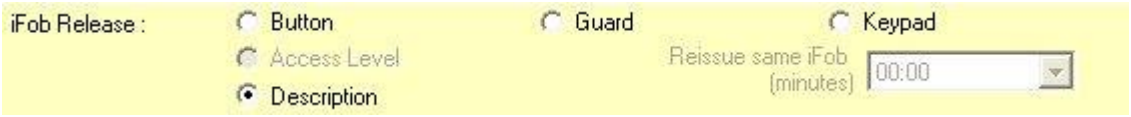
To edit a confirmed booking, simply click the 

button, the Booking Wizard will appear again and allow you to change the desired details.

iFob Release via Description Search

NOTE: This option is only compatible with 16bit control board.

With this option enabled, it is possible to release an iFob after entering the description via the alphanumeric keypad on the Traka system. The option must be enabled within the firmware in order to work. To enable this option right click the cabinet from the system viewer and select 'Configure Firmware'. The software will then communicate with the cabinet an you will be confronted by the 'Traka 16bit Configuration Wizard'. Click the 'Next' button until you come to a screen which allows you to select the iFob Release Types, and select release by Description.



After selecting release by Description, continue to click the 'Next' button until you come to the end of the Configuration Wizard then click the 'Finish' button. Traka32 will then communicate with the cabinet and update the Configuration File.

There are two different types of description searches that can be executed, a Numeric search and an Alphabetic search. When you come to enter your description on the key pad, if you hold the first key you press for one second you will notice a small symbol appear in the bottom left corner:- α. This symbolises that you have switched to 'Alphabetic Mode' and can now enter a description consisting of alphabetic characters. If however, you do not hold in the first key you press for one second you will remain in 'Numeric Mode' only allowing numbers to be entered for the description.

PIN access

To release an iFob, press the # button and then enter you 4 digit PIN code. You will then be prompted to enter a description using the key pad. When you begin to enter your description if you hold in the first key you push for a one second you will enter 'Alphabetic Mode', however if you press the key and release as normal you will remain in 'Numeric Mode'.

Reader Interface

To release an iFob, present your card/token at the reader to identify yourself. You will then be prompted to enter a description using the key pad. When you begin to enter your description if you hold in the first key you push for a one second you will enter 'Alphabetic Mode', however if you press the key and release as normal you will remain in 'Numeric Mode'.

4.19.17.11 KEY BOOKING WEB PORTAL

4.19.17.11.1 KEY BOOKING WEB PORTAL OVERVIEW

The Key Booking Web Portal application allows a user to create, edit and delete a booking from a web browser as well as the Traka32 software. The Key Booking Web application is designed to work with an existing Traka32/SQL Server installation. Communications with cabinets is performed by Traka32, either with Auto Comms enabled or preferably running as Traka as a Service (TAAS).

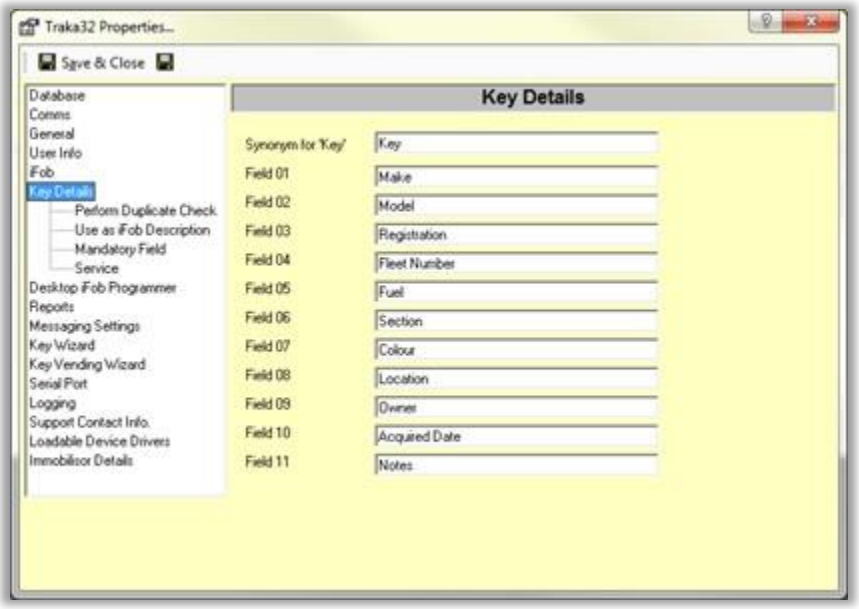
The Key Booking Web Portal connects to the existing Traka32 SQL Server database using the 'Traka Engineer' login account, which is created by default when the database is first initialised. (This account is also used by TAAS).

Firmware Options

The Traka cabinets you wish to create bookings for must have either the 'Key Booking' or 'Key Booking by Reference' option enabled in order to use the Key Booking Web Portal.

Key Details

There are certain aspects of the Key Booking feature which are user definable from Traka32, such as the Key Description fields. These fields can be changed to any description you desire, for example if the keys in your cabinet are specifically vehicle keys, your description fields may be as follows:-



To change the description fields simply open Traka32 and select **File>Properties>Key Details**. You can now enter a description of your choice into each field. These fields will then be shown in the Key Details section when adding a key.

Language

The Key Booking Web Portal application will automatically display in the language as set in your web browser. This is usually automatically set to the language of your operating system.

4.19.17.11.2 KEY BOOKING WEB PORTAL INSTALLATION

4.19.17.11.2.1 INSTALLING INTERNET INFORMATION SERVICES (IIS) AND .NET 4.0 FRAMEWORK

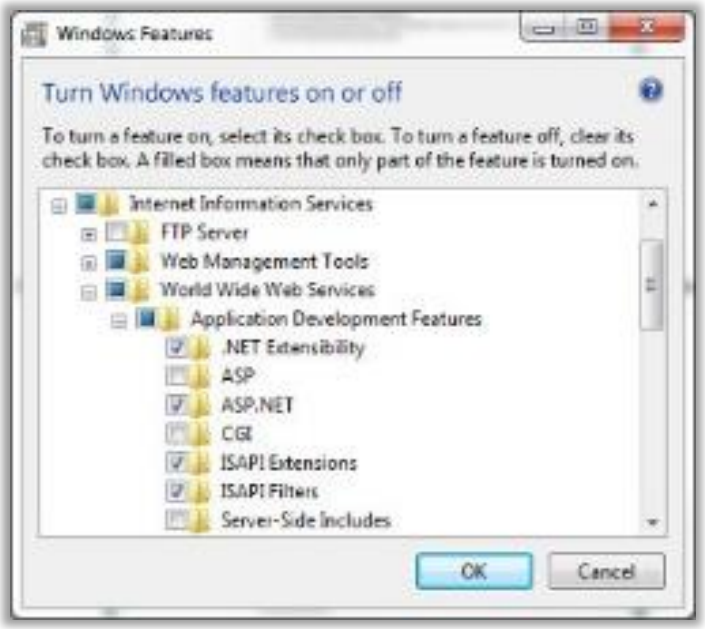
NOTE: It is important that you have installed IIS before proceeding to install the Key Booking Web Portal.

Installing Internet Information Services (IIS)

To Install IIS go to **Start>Control Panel>Programs>Programs and Features** and the select **Turn Windows features on or off** from the left hand sidebar.

Expand the options to navigate to the section shown below and check the box named **ASP.NET**.

NOTE: This process will differ depending on which operating system you are using. The example here is shown using Windows 7.



Once selected, click **OK**.

Installing .NET 4.0 Framework

In order to support this application, it is necessary to install the .NET 4.0 framework. This can be downloaded from here:

http://go.microsoft.com/fwlink/?LinkID=186913

To check the version of .NET your server is currently running, navigate to the following link on your server (not client):

http://www.smallestdotnet.com

This will detect which version of the .NET framework that is installed on your server. It will also let you know the necessary steps to install .NET 4.0.

Configuring IIS to Run ASP.NET Applications

Once installed, if you are running IIS 5.1 (on Windows XP) or IIS 6, you must configure it to support ASP.NET applications.

NOTE: IIS version 7 and later already supports ASP.NET, so you can skip this section and move on to Manually Installing the Key Booking Web Portal on Windows 7 Server.

Open IIS and expand the Web Sites folder to the left. You can check if ASP.NET has already been setup on IIS 5.1 or IIS 6 by right clicking Default Web Site and selecting Properties (see below).

You should then have an ASP.NET tab which will list the ASP.NET version as 4.0.30319.

If this tab does not already exist then ASP.NET will need to be enabled as follows:

Navigate to the following folder on the web server using a command line prompt:

- Select **Start>Run**
- Type **cmd** followed by **Enter**.
- Type **cd c:\Windows\Microsoft.NET\Framework\v4.0.30319**, then press **Enter**.
- Type **aspnet_regiis.exe-i**, followed by **Enter**.

Once this has finished, the ASP.NET tab as described above should be visible with the ASP.NET version listed as 4.0.30319.

NOTE: It is important that you have installed IIS prior to installing the Key Booking Web Portal. Please refer to the Installing IIS and .NET 4.0 Framework section.

Refer to the relevant section links below for your operating system.

Installing on IIS 7 on Windows Vista/7/2008 Server

Installing on IIS6 with Windows 2003 Server

Installing on IIS 5 with Windows XP

Installing on IIS 7 on Windows Vista/7/2008 Server

IIS7 supports ASP.NET 'out of the box', so doesn't need any of the special configuration required for IIS 5.1 and IIS 6. All that is required is the following steps.

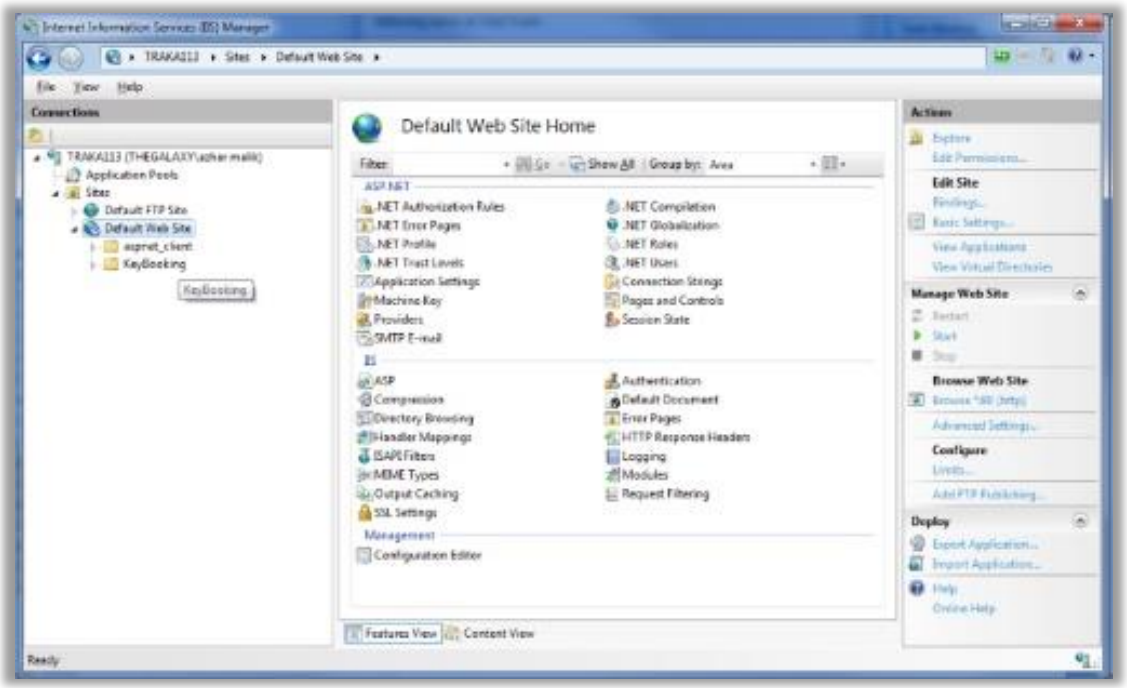
Install the Files

Extract the KeyBooking.zip file that is supplied with the Traka Install CD into a suitable folder under the **c:\Inetpub\wwwroot** folder, for example **c:\Inetpub\wwwroot\KeyBooking** on the hosts Windows VISTA /7/ 2008 server.

NOTE: If using the built in Windows zip extraction wizard, remove the Key Booking part of the destination folder since, since this will be generated automatically when the zip file extracts.

Installing a new Virtual directory under Default Web Site

Start IIS, by selecting **Start>Administrative Tools>Internet Information Services (IIS) Manager**. In IIS, select the **Default Web Site** node, then right click and select the **KeyBooking** node or the folder which you created earlier under the **wwwroot** folder.



From the popup menu select the **Convert to Application** option, and then from the **Add Application** screen, make sure the **Application pool** is set to **ASP.NET v4.0**

Installing on IIS 6 with Windows 2003 Server

It is recommended that Windows 2003 Service Pack 2 is installed before proceeding at this point. At the time of writing this is available at:

https://technet.microsoft.com/en-us/windowsserver/bb463273.aspx

Install the Files

Extract the KeyBooking.zip file that is supplied with the Traka Install CD into a suitable the folder, for example **c:\Inetpub\Traka** on the hosts Windows 2003 server.

NOTE: If using the built in Windows zip extraction wizard, remove the Key Booking part of the destination folder since, since this will be generated automatically when the zip file extracts.

Check Web Service Extensions

Start IIS by selecting **Start>Administrative Tools>Internet Information Services (IIS) Manager**.

On the left hand panel, click the bottom entry, **Web Service Extensions**. You should have an ASP.NET v4.0.30319 entry listed in the right hand side panel. If this is missing, then please refer to the section Configuring IIS to run ASP.NET applications and run the aspnet_regiis.exe -i command. Unless this is carried out, browsing the website will result in 'Page Not Found' errors.

You need to check that **IIS MetaBase Compatibility** is switched on. This can be found in **Programs and Features>Turn Windows Features on or off** then look in **IIS>Web Management Tools>IIS Management Compatibility** then switch on **IIS Metabase and IIS6 Configuration compatibility.**

Installing a new Web Site

The above should have created a new 'Default Web Site' otherwise you will need to create one and map it to the **inetpub\wwwroot** folder. Installing Traka KeyBooking as a new website is beyond the scope of this document. Please refer to the IIS documentation for further assistance. However, it will be necessary to add the 'Wildcard application map' as described below for adding a virtual directory.

Installing a new Virtual directory under Default Web Site

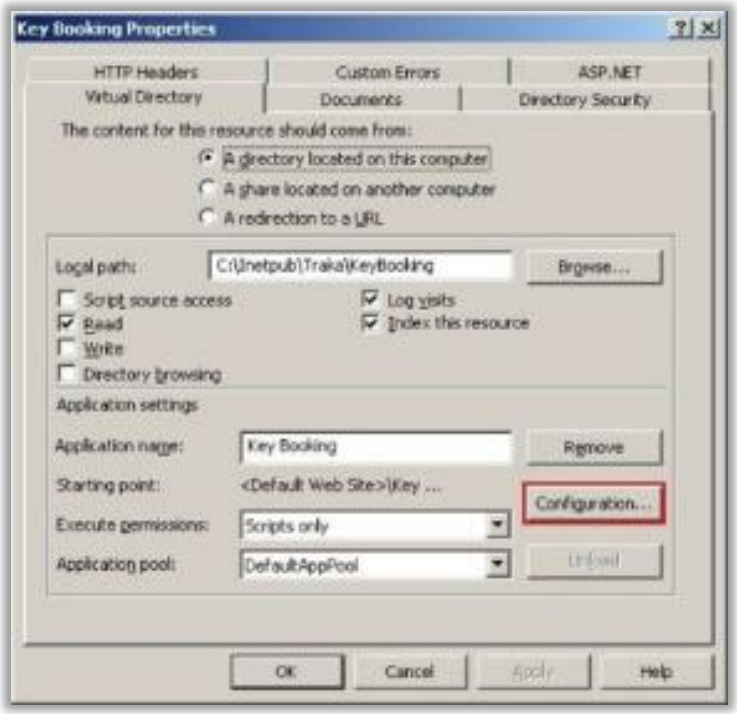
Start IIS, by selecting **Start>Administrative Tools>Internet Information Services (IIS) Manager**. In IIS, select the **Default Web Site** node, then right click and select **New>Virtual Directory** (see below).

You will then see the Virtual Directory Creation Wizard. Click the **Next** button, and then enter **KeyBooking** with no spaces (or a name of your choice), into the **Alias** field. For the Directory field, select the folder the software was installed to (e.g. c:\Inetpub\Traka\KeyBooking), then click **Next**.

You will then be taken to the Permissions screen, for Access Permissions check **Read** and **Run** scripts ONLY.

Now the Application Mappings need to be enabled. In IIS, right click the Key Booking virtual directory which has just been created, and select **Properties** (see below).

On the Virtual Directory tab, click the **Configuration** button (see below).



The **Application Configuration** window will now appear. On the Mappings tab, click the **Insert** button next to 'Wildcard application maps (order of implementation)'.

Then enter the following:-

Executable Field: c:\windows\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll

Verify that file exists Field: Unchecked (Important!)

Finally, on the ASP.NET tab, ensure that the ASP.NET version is set to 4.0.30319.

To test, navigate to http://localhost/keybooking (replacing 'keyBooking' with whatever Alias you used in the settings above.)

If you get a 'You are not authorized to view this page' error page (HTTP Error 403 – Forbidden), it is probably because the previous step has not been completed successfully. Ensure the settings are entered correctly and try again.

Installing on IIS 5 with Windows XP

Install the Files

Extract the KeyBooking.zip file that is supplied with the Traka Install CD into a suitable the folder, for example **c:\Inetpub\Traka** on the hosts Windows XP machine.

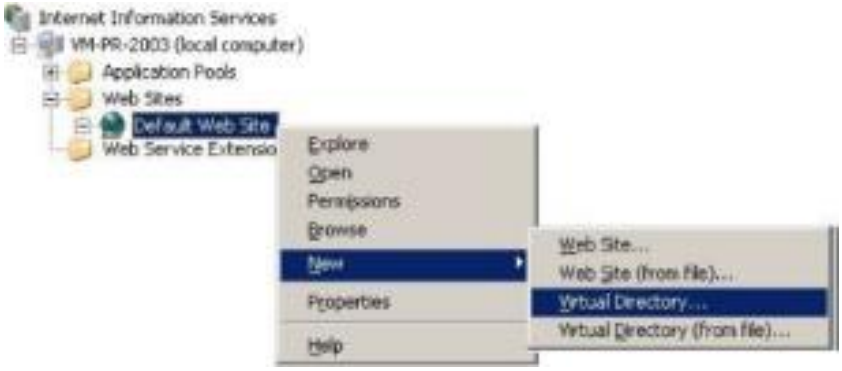
NOTE: If using the built in Windows zip extraction wizard, remove the Key Booking part of the destination folder since, since this will be generated automatically when the zip file extracts.

Installing a new Web Site

Installing Traka Key Booking as a new website is beyond the scope of this document. Please refer to the IIS documentation for further assistance. However, it will be necessary to add the "Wildcard application map" as described below for adding a virtual directory.

Installing a new Virtual directory under Default Web Site

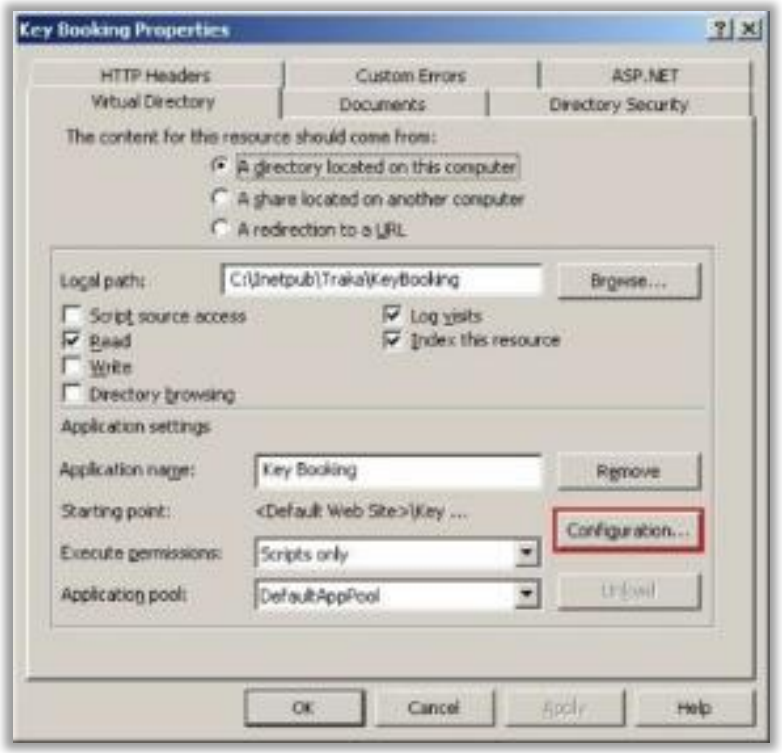
Start IIS, by selecting **Start>Administrative Tools>Internet Information Services (IIS) Manager**. In IIS, select the **Default Web Site** node, then right click and select **New>Virtual Directory** (see below).



You will then be confronted by the Virtual Directory Creation Wizard. Click the **Next** button, and then enter **KeyBooking** with no spaces (or a name of your choice), into the **Alias** field. For the Directory field, select the folder the software was installed to (e.g. c:\Inetpub\Traka\KeyBooking), then click **Next**.

Now the Application Mappings need to be enabled. In IIS, right click the Key Booking virtual directory which has just been created, and select **Properties** (see below).

On the Virtual Directory tab, click the **Configuration** button (see below).



You will be confronted by the **Application Configuration** window. Click the **Add** button and specify the following:

Executable Field: c:\windows\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll (Note: same executable file as for .aspx file extension)

Extension Field: .* (Note: The "dot" is important)

Limit to Field: GET, HEAD, POST, DEBUG

Script Engine Field: Checked

Verify that file exists: Unchecked (Important!)

NOTE: If the OK button is mysteriously disabled, just click into the Executable text box again and it should enable.

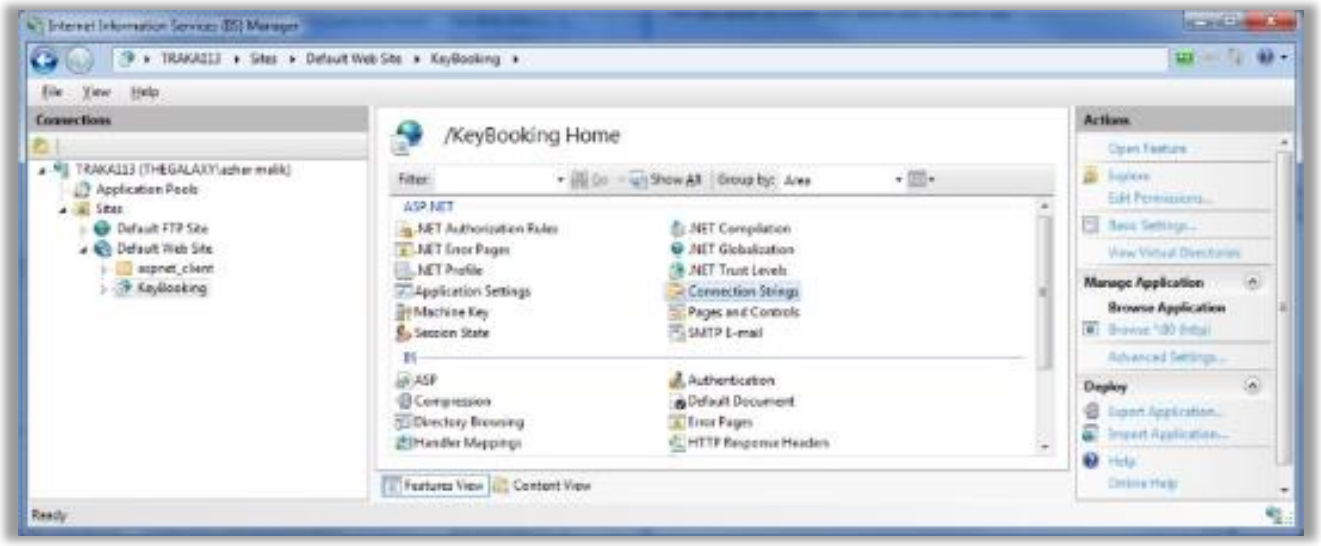
Finally, on the ASP.NET tab, ensure that the ASP.NET version is set to 4.0.30319.

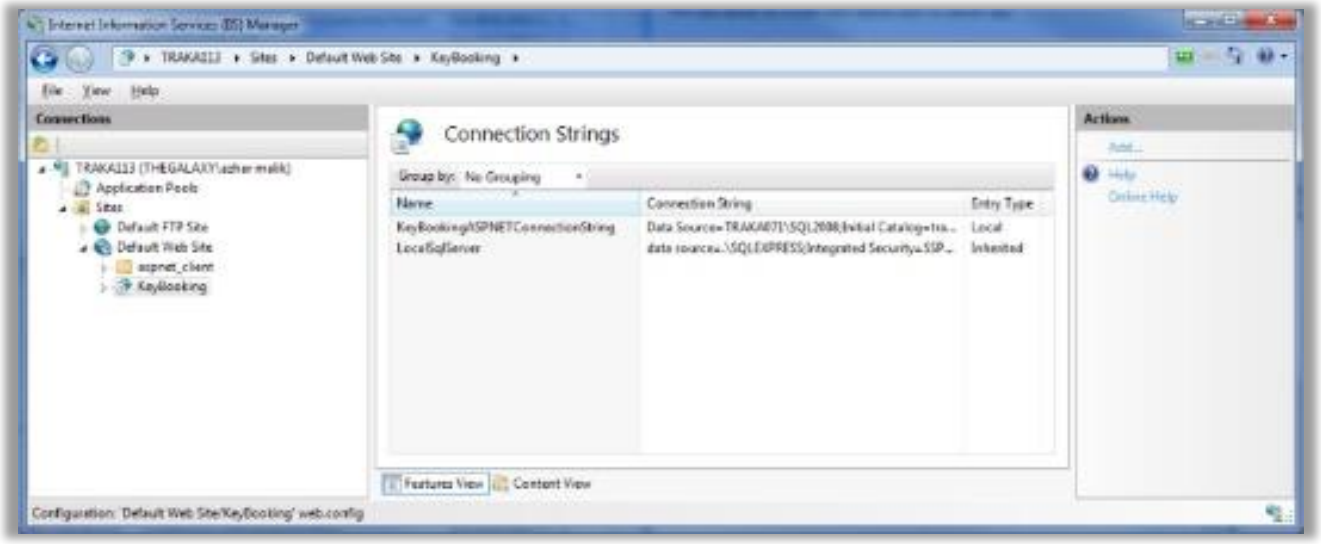
To test, navigate to http://localhost/keybooking (replacing 'keyBooking' with whatever Alias you used in the settings above.)

4.19.17.11.2.3 KEY BOOKING WEB PORTAL - CONNECTING TO THE TRAKA32 SQL SERVER DATABASE

In order to connect to your own database, in IIS 5.1 or IIS 6.1 right-click the **KeyBooking** website or Virtual Folder in IIS, and select **Properties**. On the ASP.NET tab, click the **Edit Configuration** button. On the General tab, edit the **KeyBookingASPNETConnectionString** entry, and replace 'Data Source' with your SQL Server database instance, e.g. **Data Source=MYSERVER\SQL2008,** and the 'Initial Catalog' with the Traka32 database, e.g. **Initial Catalog=MyTraka32Database**.

In IIS7, select the **KeyBooking** website, and then double-click the **Connection Strings** icon in the ASP.NET group, and edit the **KeyBookingASPNETConnectionString** entry.





This can also be carried out by editing the web.config file located in the wwwroot\KeyBooking folder. Open the file in a text editor, and scroll to the **<connectionStrings>** section. Modify the 'Data Source' and 'Initial Catalog' parts of the connection string named **KeyBookingASPNETConnectionString** as described above.

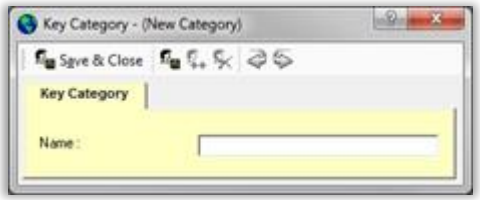
NOTE: The connection string must be named 'KeyBookingASPNETConnectionString'.

4.19.17.11.3.1 KEY CATEGORIES - KEY BOOKING WEB PORTAL

Key Categories can be used to group multiple keys together and narrow down searches. For example, when you are searching for a key using the Web Portal, as well as typing in a specific search term or selecting a key from the Key List, you can have a number of tick boxes with your desired Key Categories.

Adding a Key Category

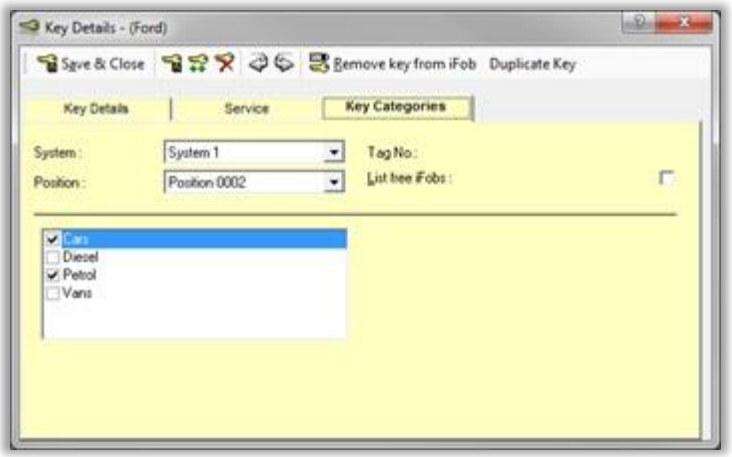
To add or edit a Key Category, simply open Traka32 and then select **File>Options**. From the options menu select the **Key Categories** tab. Next click the **Options** button and select **Add New**. Enter the desired category in the provided field and click **Save & Close**.



Assigning a Key to a Category

To assign keys to categories, click **Key List** and then double click a desired key from the list. If no keys have been created yet refer to the Adding Keys section.

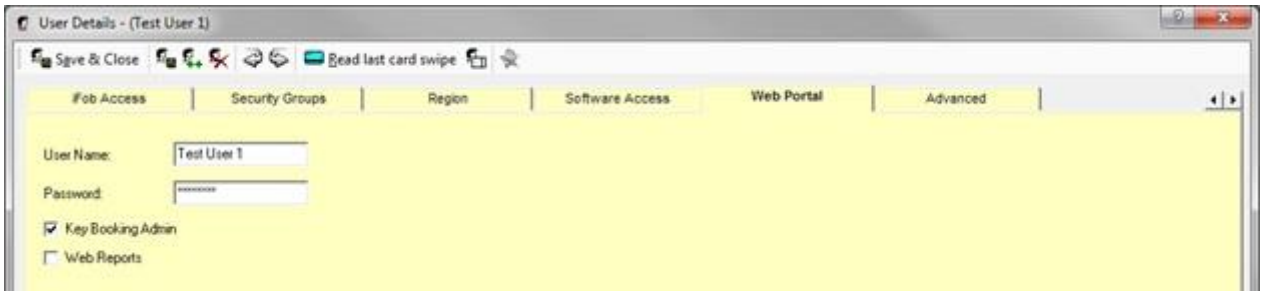
Select the **Key Categories** tab and then tick the categories you wish the key to be assigned to. Click **Save & Close**.



The categories will be available for selection when making a booking through the Web Portal.

To allow a Traka32 User to have access to the Key Booking Web Portal, a login must be created. To create the login you must have access to User Details.

Open Traka32 and select **User List**. From there double click the desired user to open their User Details window. Select the tab at the top of the details window named **Web Portal**. Here you can create the users 'Log In' for Key Booking Web Portal by entering a User Name and Password.



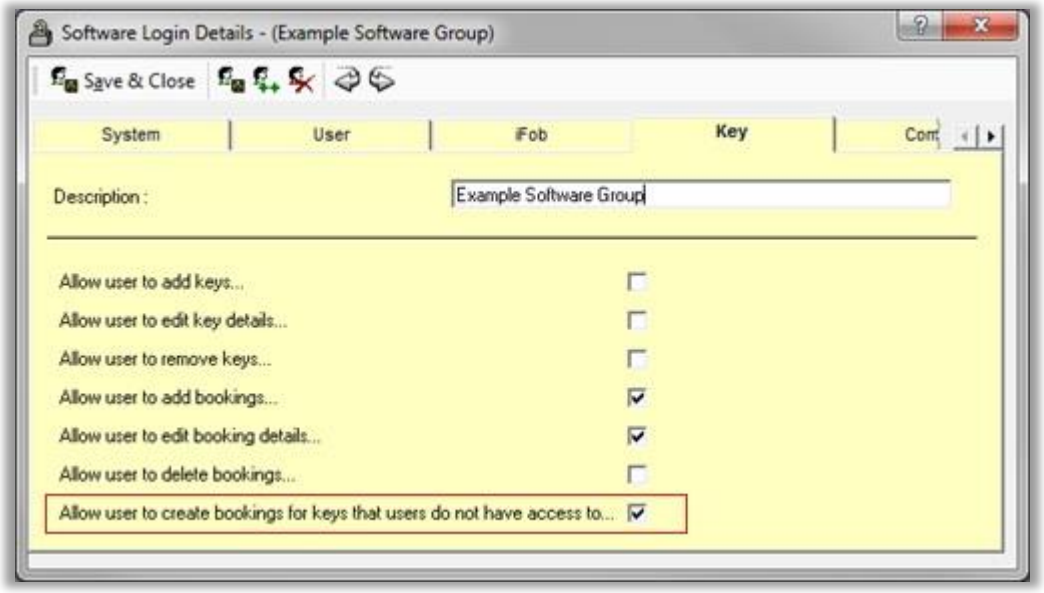
NOTE: The Web Reports tick box is for an obsolete feature and can be left unchecked.

Key Booking Admin

This option when enabled will allow the selected user to create bookings for other users, and up to 3 users at a time. It will also allow a user to book any key for another user.

If users are not a Key Booking Admin, they can still be given the option to book keys they do not have access to, by assigning them to a Software Access Group and selecting the option as shown below.

NOTE: This only applies to Fixed Return systems. For Random Return systems, this setting has no effect, you can only book the access level you have been assigned.



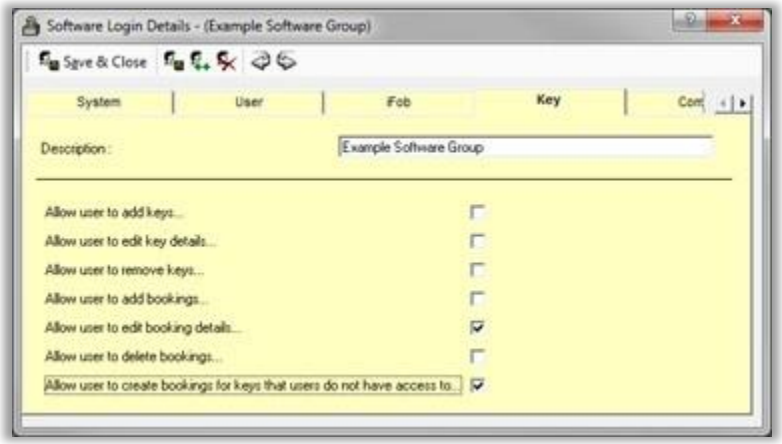
There are various configuration options which allow you to tailor the Web Portal to a customer's needs.

The options are explained here.

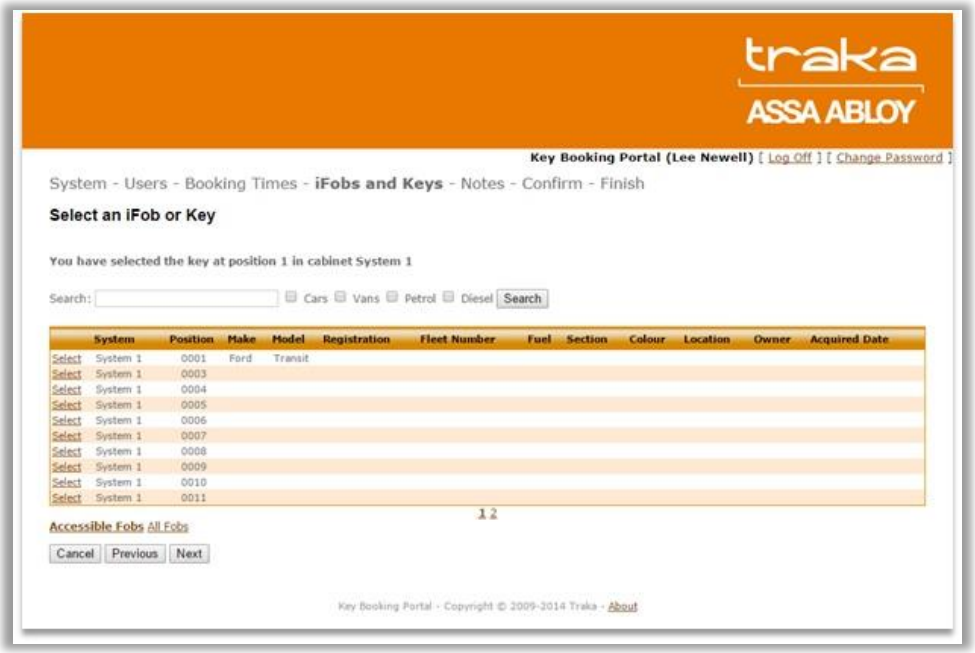
1. For **Fixed Return** Systems, allowing a user to be able to see **all iFobs/keys** for a system and book any one of them, in addition to just the iFobs/keys they have access to (default option).
2. Setting up a user as a Key Booking Admin user.
3. For **Fixed Return** Systems, show the iFobs that the user can book based on their Software Access Group.
4. For **Random Return** Systems, show the access levels that a user can book based on their Software Access Group.
5. Restricting how long users can book an iFob/key in advance.
6. Restricting the duration a user can book an iFob/key.
7. Adding a buffer to the booking start and end times.
8. Validating if a user expires within the booking period.
9. Changing the booking start date and end date defaults.
10. Allowing users to view other users' bookings.

1. Allow a user to see all iFobs/Keys

To allow a user to see all iFobs/keys for a system when creating a booking, the user must be in a software access group in traka32. The software access group must have the option **Allow user to create bookings for keys that users do not have access to** on the Key tab.



In the Web Portal they will then see the **Accessible iFobs** link and **All iFobs** link. The **Accessible iFobs** link when clicked will show the iFobs/keys they have access to.



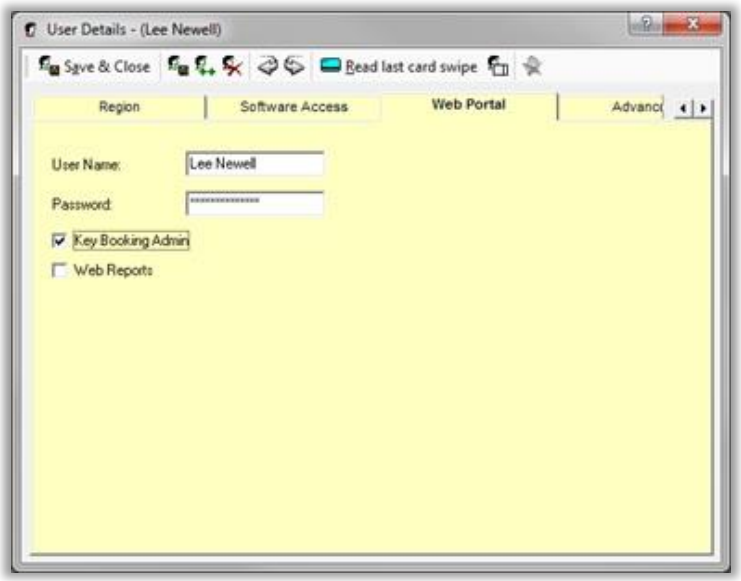
The **All iFobs** link when clicked will show all the iFobs/keys in that System.

2. Set up Key Booking Admin User

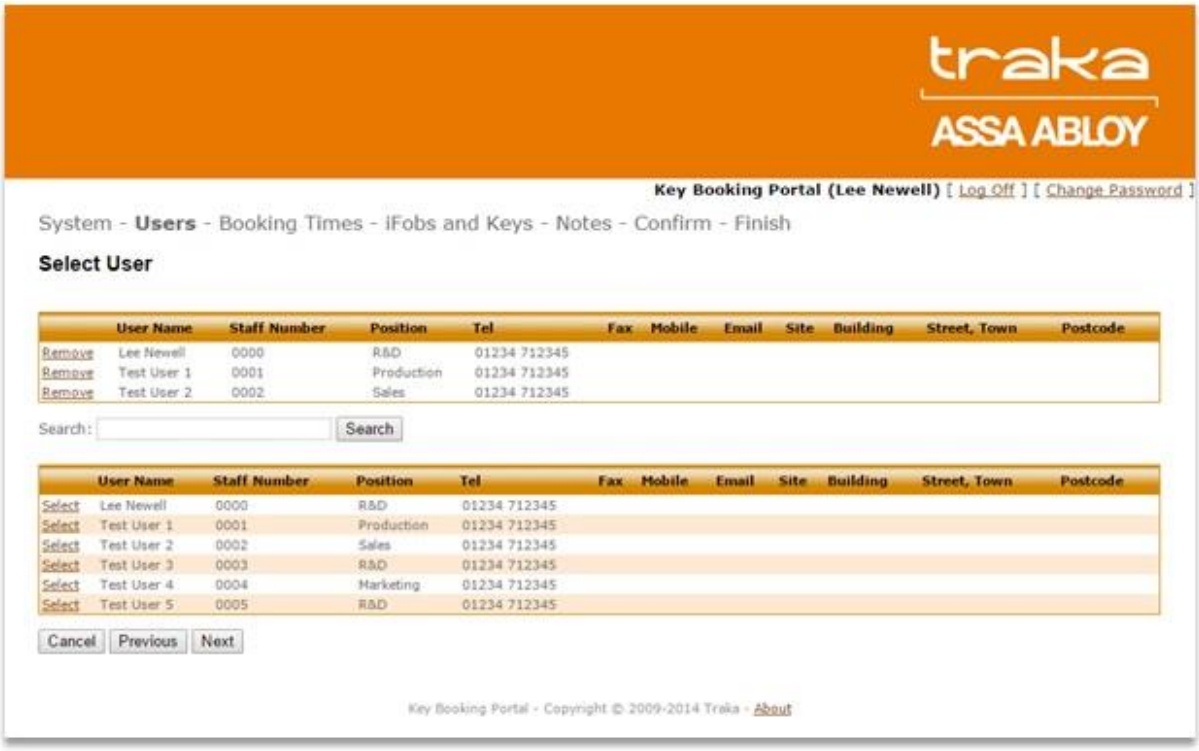
The Key Booking Admin has the following extra privileges over a standard user:

- For **Fixed Return** systems, they can see **all iFobs/keys** in that system and therefore book any of them for a user.
- For **Random Return** Systems, they can see **all access levels** in that system and therefore book any of them for a user.
- They can see **all users** in that System and therefore book iFobs/keys for **any user** and for up to **3 users** at a time. If an iFob/key is booked for more than one user, then any one of those users will be able to take the iFob/key from the System at the Booking Start time.

To setup a user as Key Booking Admin, in Traka32, go to the user details, Web Portal tab and select the option **Key Booking Admin**.



They will then see all users in the System, and be able to make a booking for up to 3 users.



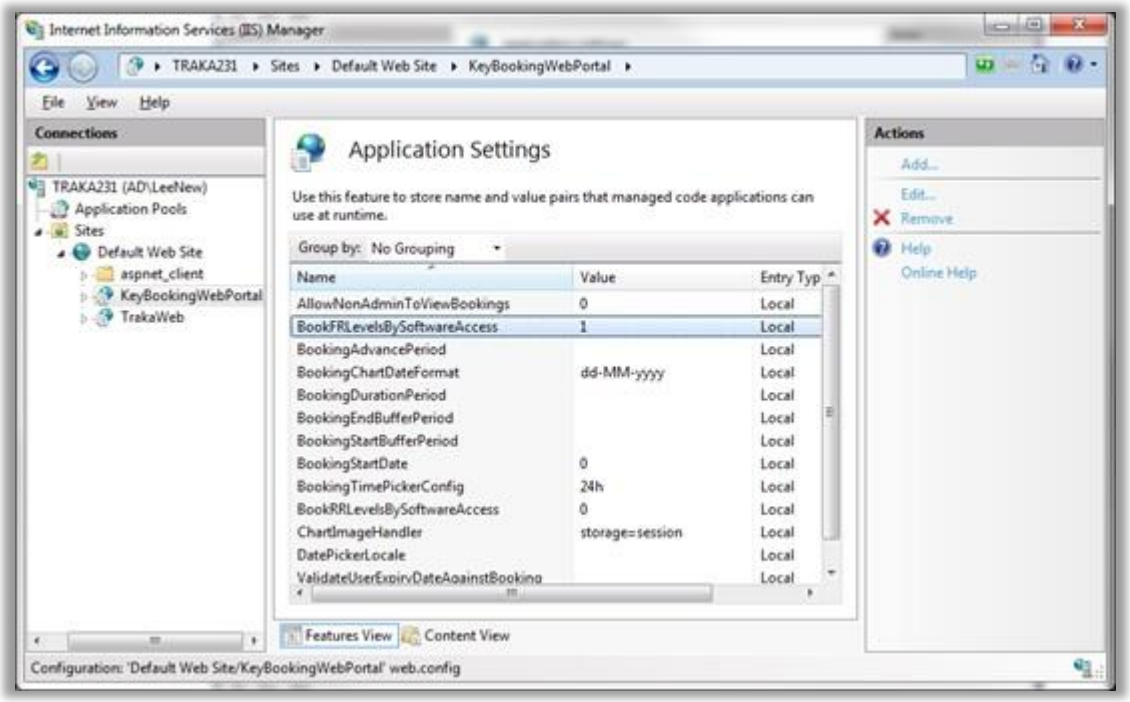
They will also see the **All iFobs** link and see **all iFobs/keys** in that System.

The bookings table will show the number of users for that booking.

3. Show iFobs based on Software Access Groups - Fixed Return Systems

For **Fixed Return** systems, when booking an iFob/key for a user, by default, the iFobs/keys that are listed are those that the user has access to from the cabinet (Traka32 user record). There are also access levels that can be set against a software access group, which can give more control over a group of users. In order for the Web Portal to use these access levels from the software access group, the following config setting needs to be set to 1, either in the web.config file or from IIS

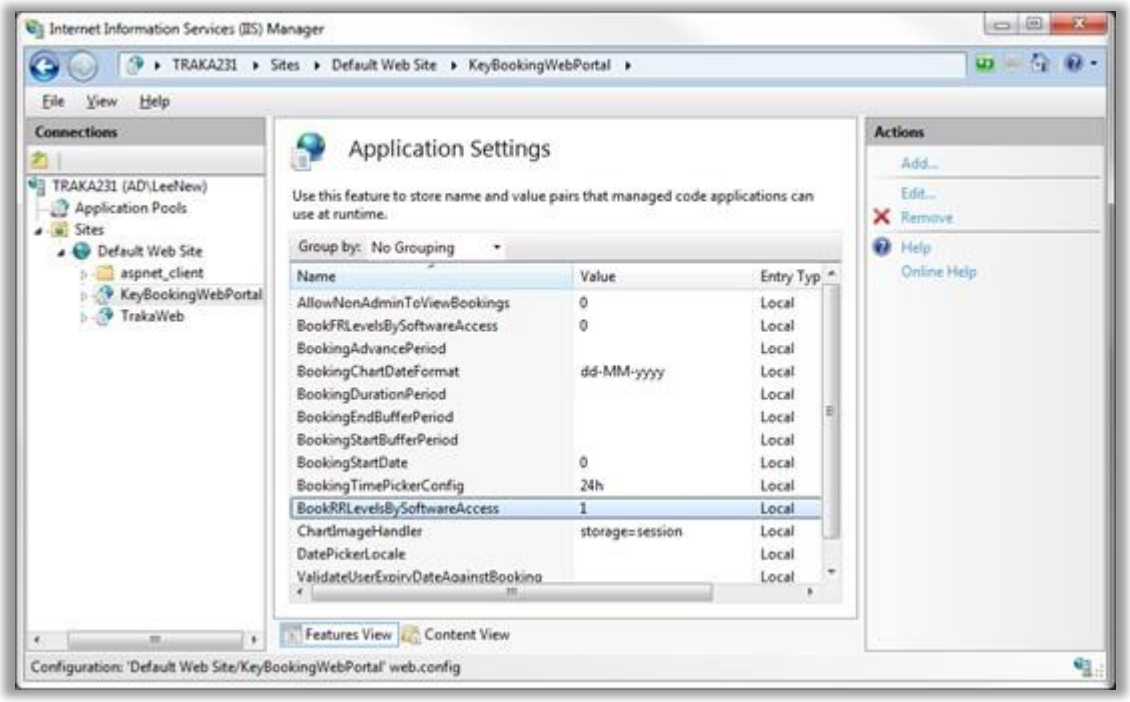
key="BookFRLevelsBySoftwareAccess" value="1"



4. Show Access Levels based on Software Access Groups - Random Return Systems

For **Random Return** Systems, when booking a iFob/key for a user, by Access Level, by default, the access levels that are listed are those that the user has been given for the cabinet (Traka32 user record). There are also access levels that can be set against a software access group, which can give more control over a group of users. In order for the Web Portal to use these access levels from the software access group, the following config setting needs to be set to 1, either in the web.config file or from IIS

key="BookRRLevelsBySoftwareAccess" value="1"



5. Restrict Booking Advance Period

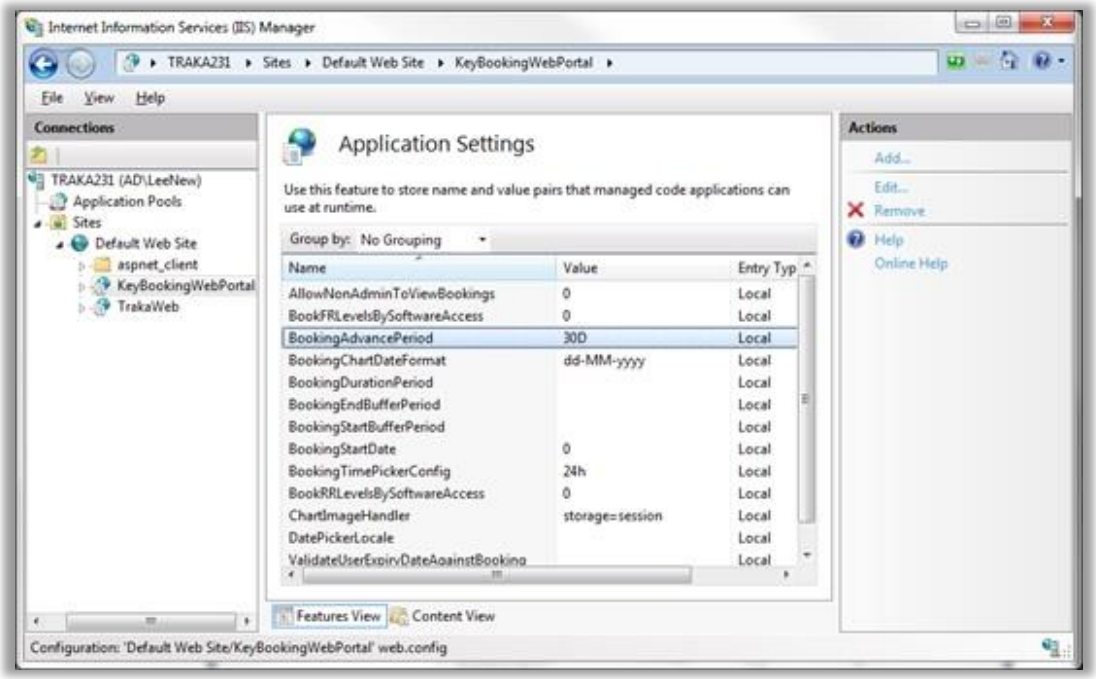
The **Booking Advance Period** option prevents the user from making a booking too far ahead in the future. This can be set to any number of days or months, e.g. setting to '30D' will restrict the user to only be able to make a booking for 30 days from the booking start date.

e.g.

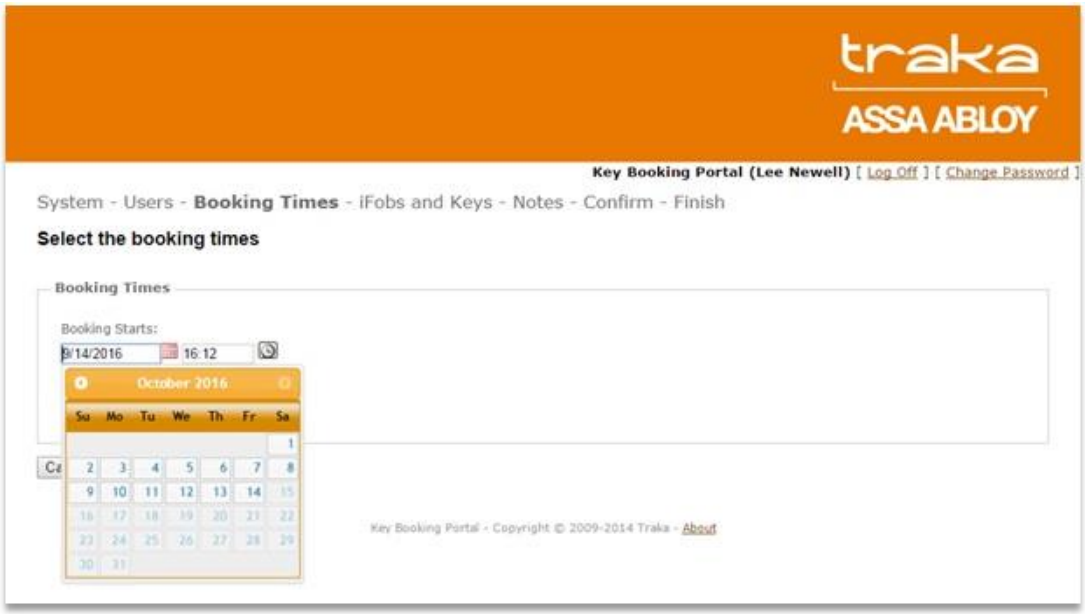
key="BookingAdvancePeriod" value="30D"/>

or

key="BookingAdvancePeriod" value="1M"/>



Here, the Booking Advance Period has been restricted to 30 days. Any start dates after 30 days are greyed out and cannot be selected.

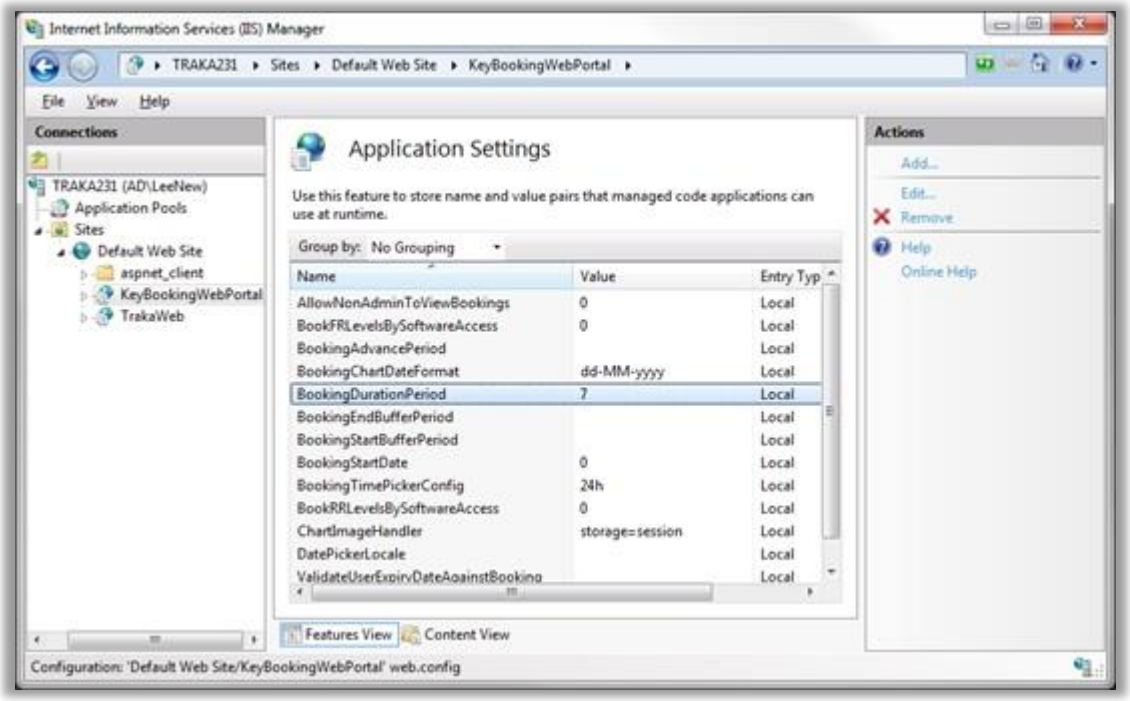


6. Booking Duration Period

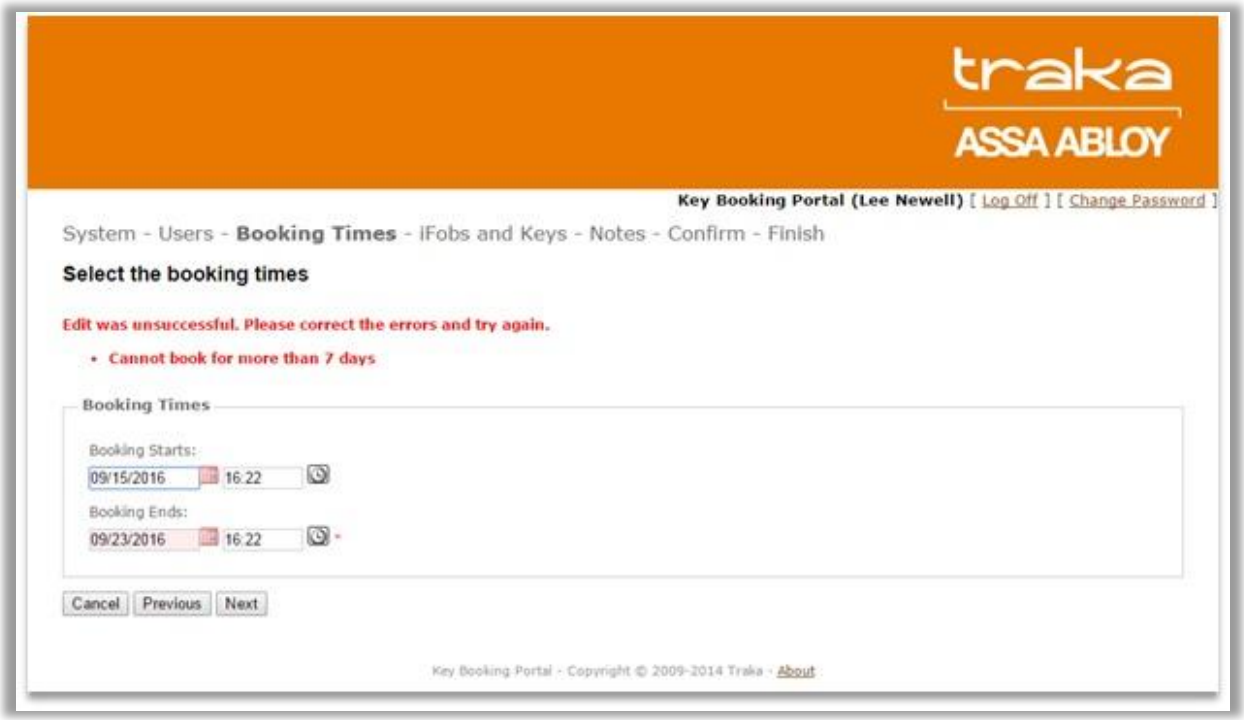
The **Booking Duration Period** option prevents the user from making a booking for longer than is necessary. E.g. setting to 7 will limit the calendar end date to 7 days after the selected start date

e.g.

key="BookingDurationPeriod" value="7"



Here, the Booking Duration Period has been set to 7 days. If you select an end date more than 7 days after the start date the system will prevent you from continuing.



7. Booking Start and End Buffer Periods

The **BookingStartBufferPeriod** and **BookingEndBufferPeriod** options add/remove minutes to the booking start and end times once the user presses next on the 'select booking times' page. This will make the booking start time and/or booking end time earlier or later. This allows for users who arrive early or late for a booking.

e.g.

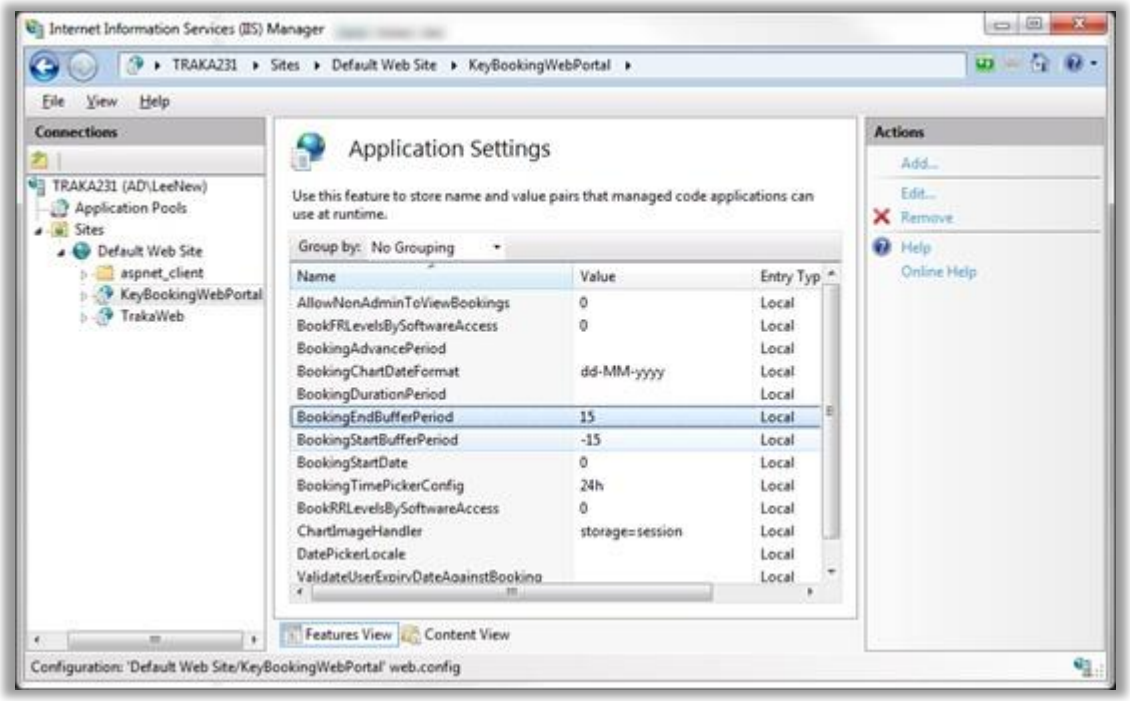
key="BookingStartBufferPeriod" value="-15

will make the booking start time 15 mins earlier

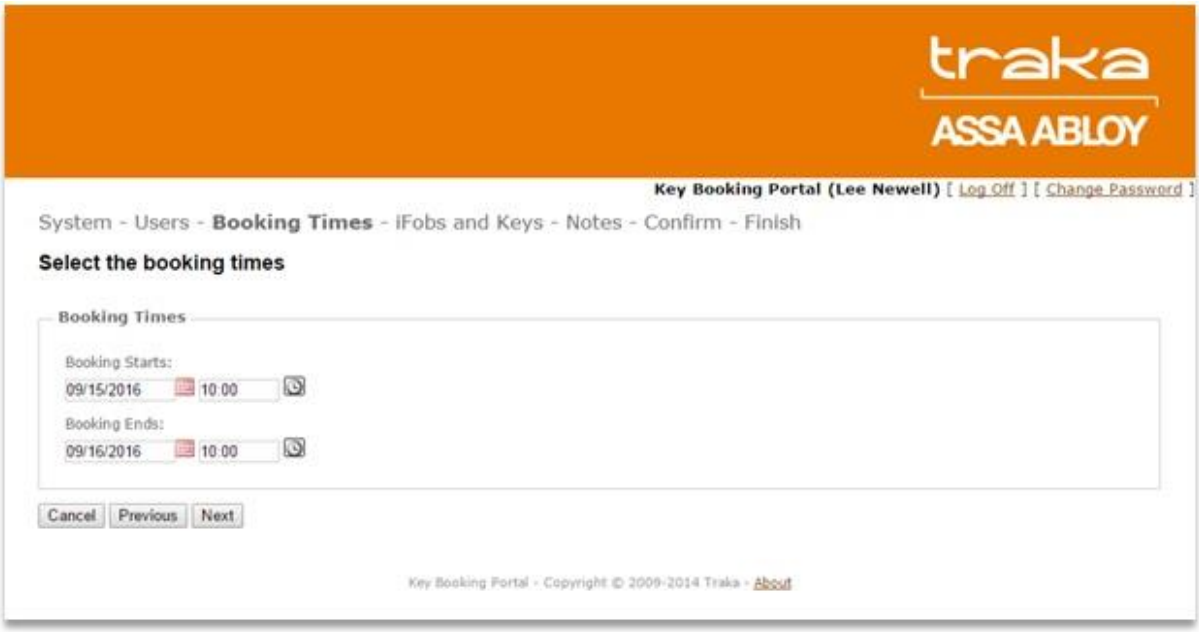
or

key="BookingEndBufferPeriod" value="15"

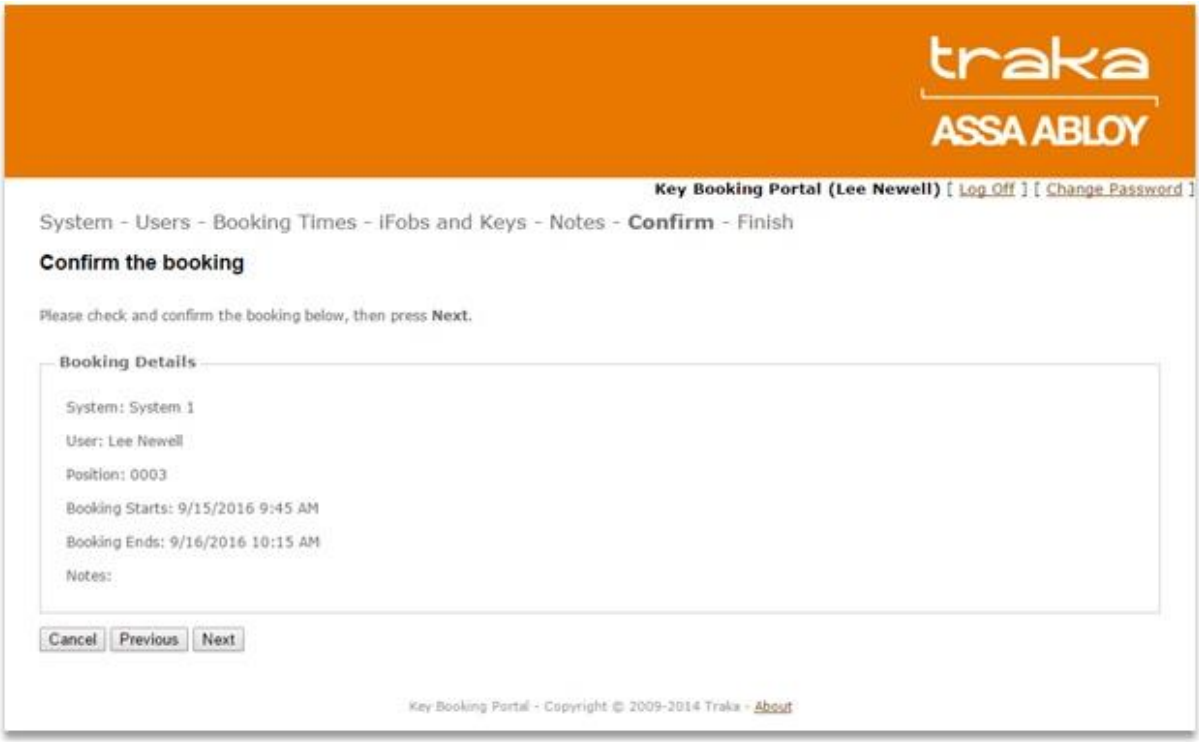
will make the booking end time 15 mins later



Here, a booking is made with a start and end time of 10:00am.



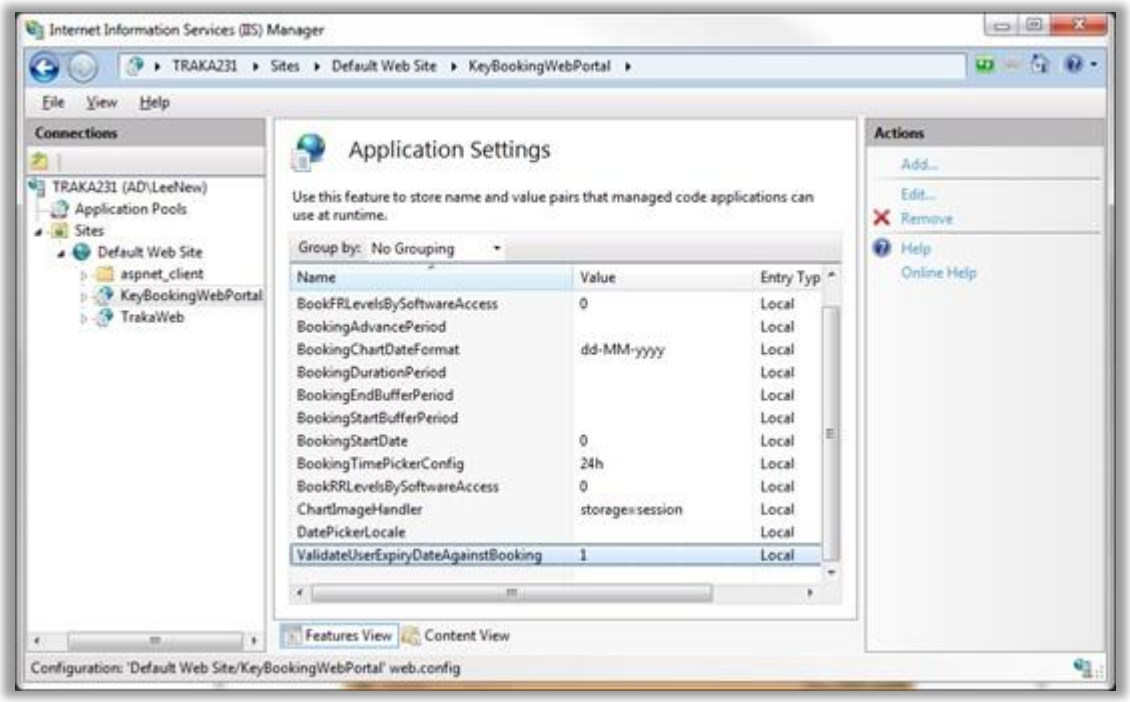
The booking confirmation screen shows the buffer minutes added to the booking start and end times.



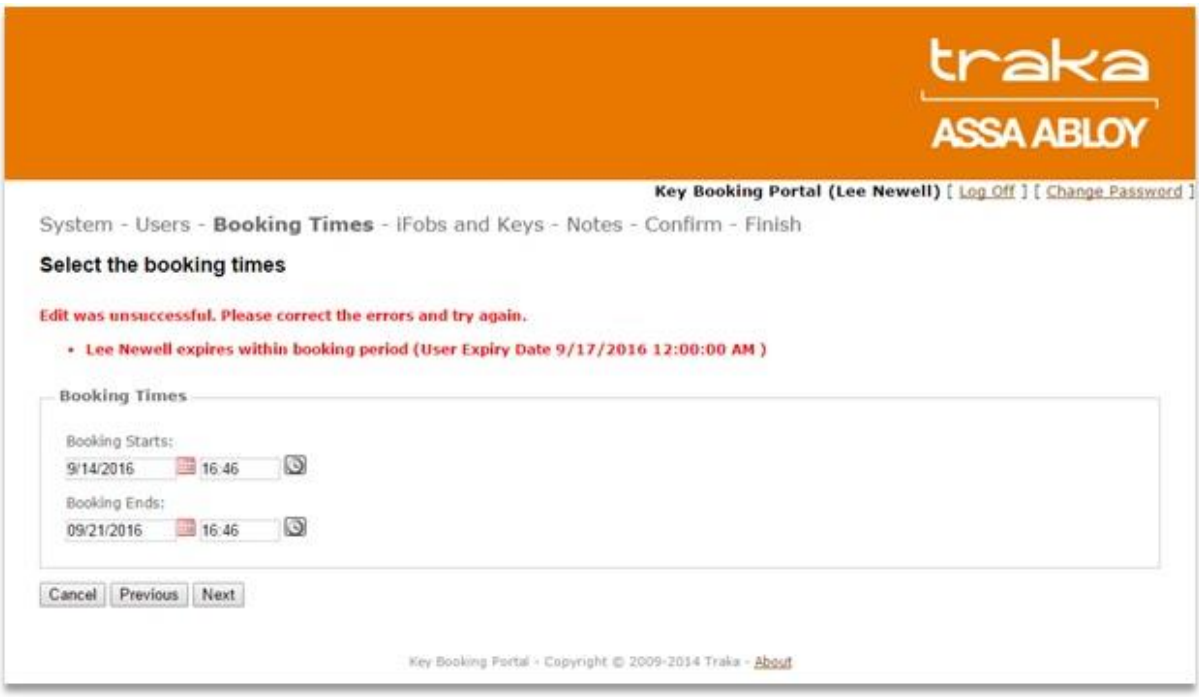
8. Validate User Expiry Date Against Booking

The **Validate User Expiry Date Against Booking** option prevents a user from making a booking if they expire within the booking period. Set the config setting to 1 to use this option.

key="ValidateUserExpiryDateAgainstBooking" value="1"



The validation stops a booking from being made for an expired user.



9. Start and End date Defaults

By default, the booking start date is set to the current day plus one, and the booking end date set to the current day plus 2. However if you wish the booking start date to start from today and the booking end date to end tomorrow, set the following config setting to 0.

key="BookingStartDate" value="0"

<!-- 0 = booking start date today, 1 = booking start date tommorrow, 5 = in 5 days time -->

You could also set the default booking start date in x days time by setting the value to the required number of days.

10. Allow users to view other users' bookings

Also by default, users can only view their own bookings unless they are a key booking admin. But if you would like users to view other users' bookings, set the following config setting to 1.

key="AllowNonAdminToViewBookings" value="0"

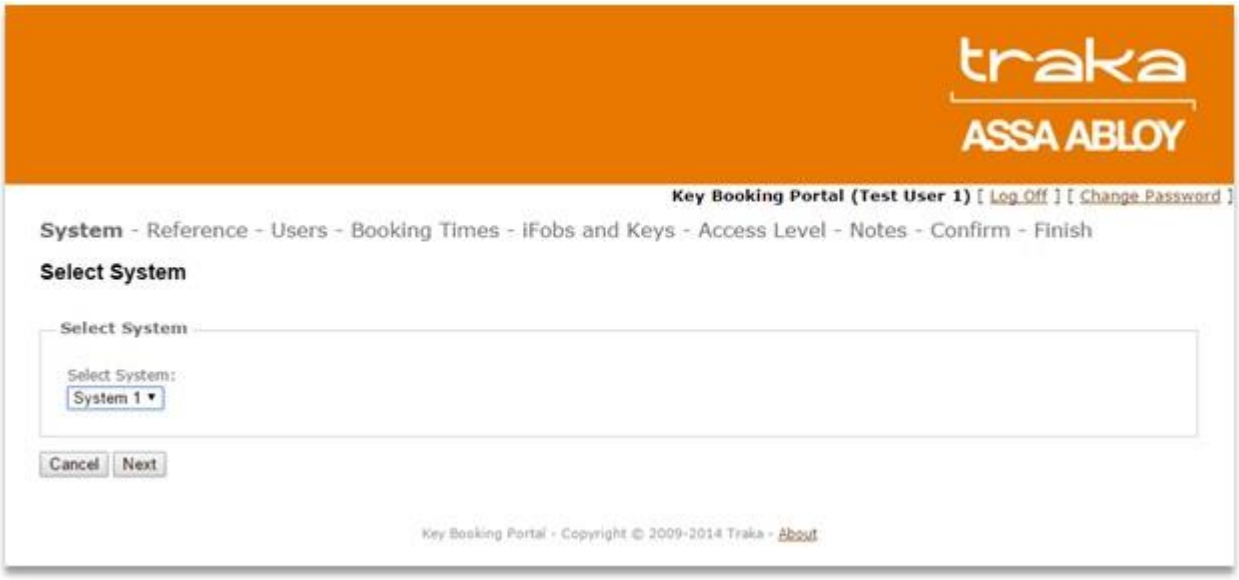
<!-- 0 = non-admin users can view own bookings, 1 = non-admin users can view other user's bookings -->

4.19.17.11.4 USING THE KEY BOOKING WEB PORTAL

After Installing the Key Booking Web Portal, navigate to http://localhost/KeyBookingWebPortal (replacing 'KeyBookingWebPortal' with whatever Alias you used in the installation process). You will then be confronted with the Key Booking Welcome page. From here you have the choice to add a new booking, view the bookings list or viewing the booking chart.

Click **Log On** in the top right corner of the screen and then enter your User Name and Password as previously configured. Once entered click **Log On.**

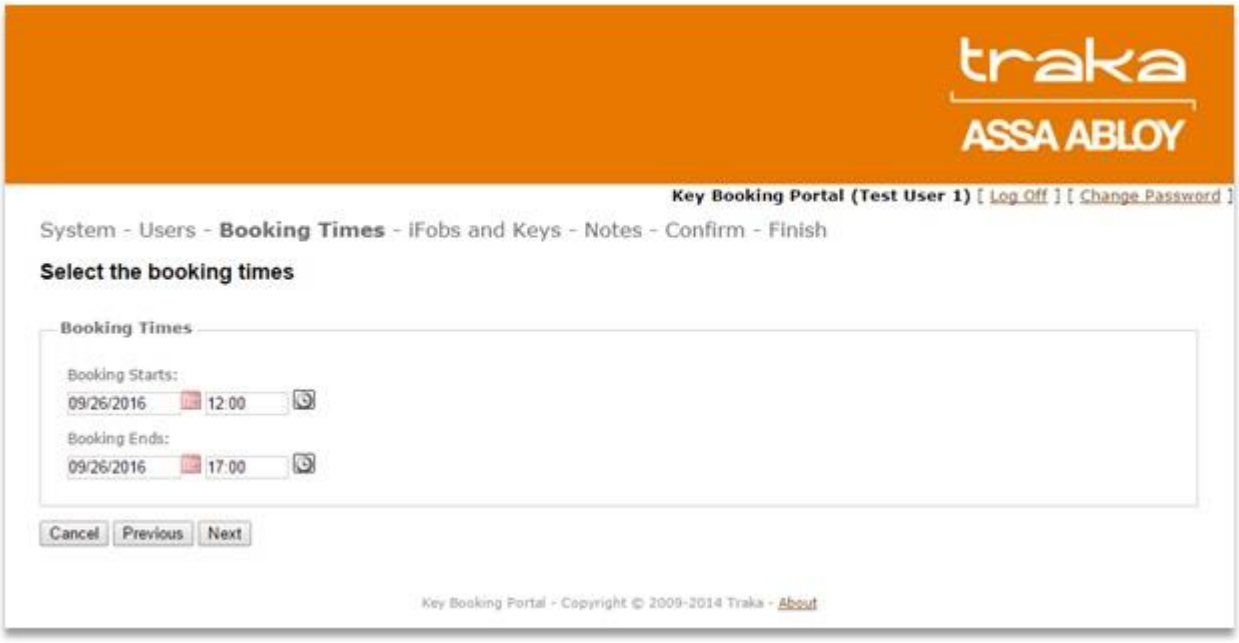
Once logged on you will return to the Welcome Page. To create a new booking simply click **Add New Booking**. You will then be taken to a screen where you can select which system you wish to book a key from. Select the desired system from the drop down list and click **Next**.



Next you will be prompted to select a user to book the key for. To find the desired user, browse the User List and click the **Select** button next to their name, or alternatively type the users name into the search bar and click the **Search** button. The selected user will be displayed above the search bar. Once you have selected a user click **Next**.

NOTE: If you are using Key Booking by Reference you will be asked to enter the name of the user and a reference number instead of the 'Select User' screen.

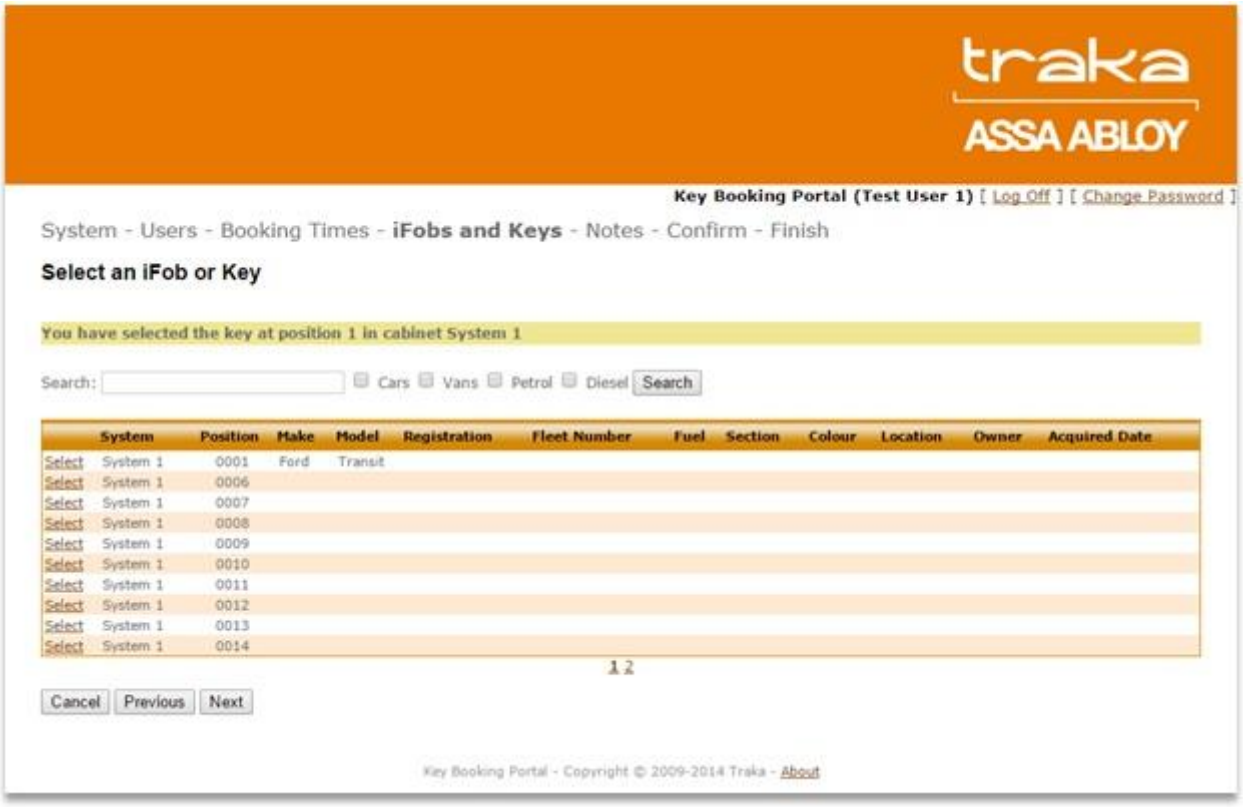
Once you have selected the user you will need to enter a Beginning and End time for the booking. Clicking the calendar and clock icons next to the fields will display a calendar and hours and minutes options to choose from. Alternatively manually enter dates and times, then click **Next**.



After selecting a beginning and end time for your booking you will need to select which key you would like to book. There are several ways to find the desired key:

- You can browse by scrolling down to find the desired key.
- Enter a valid description into the search bar, such as the Make, Model, Colour, Registration, Location and Owner etc (or whatever your key detail fields are configured to).
- Or select one or more of the Key Categories to filter the list.

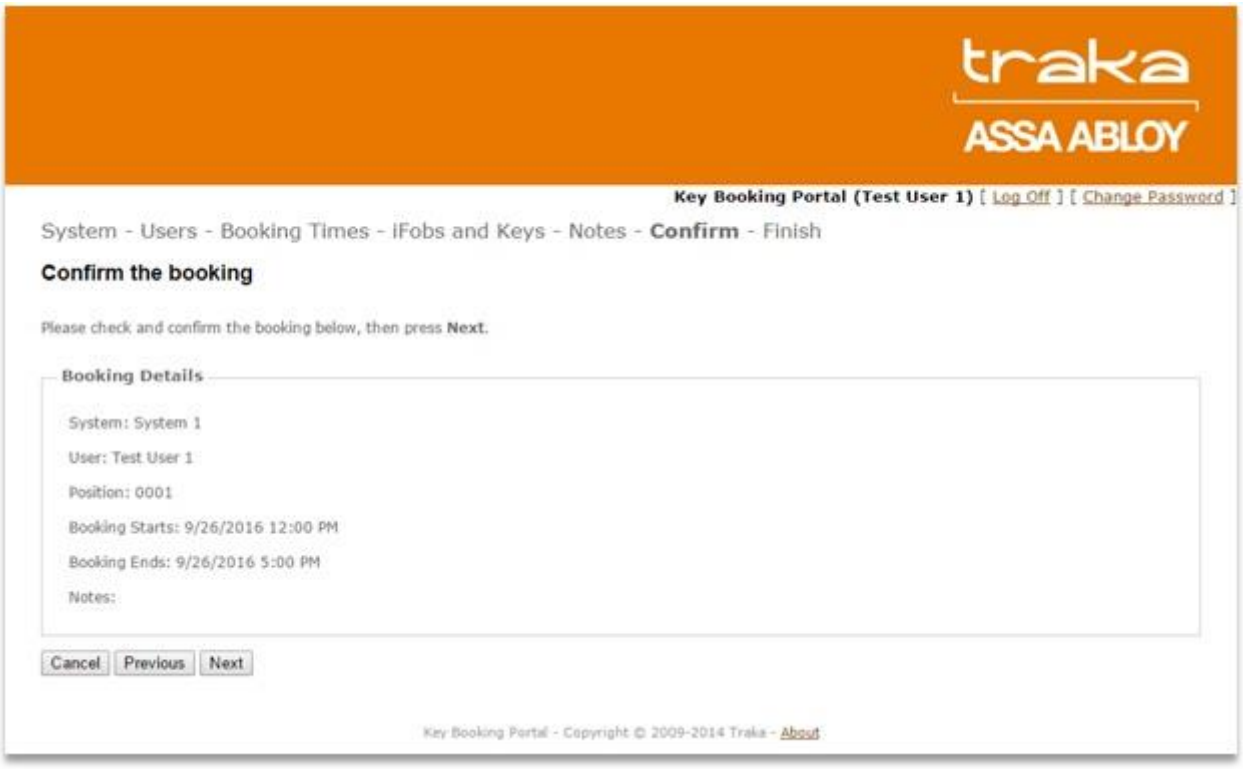
Click **Select** next to the key you wish to book. A message will appear above the search bar confirming which key you have selected.



Once you have selected the key you wish to book, click **Next**.

On the following screen you can enter any notes you wish to relate to the booking, then click **Next**.

The next screen shows the all of the booking details. If you are happy with the details and want to save the booking, click **Next**. If you want to make any changes click the **Previous** button, or to discard the booking completely, click **Cancel**.

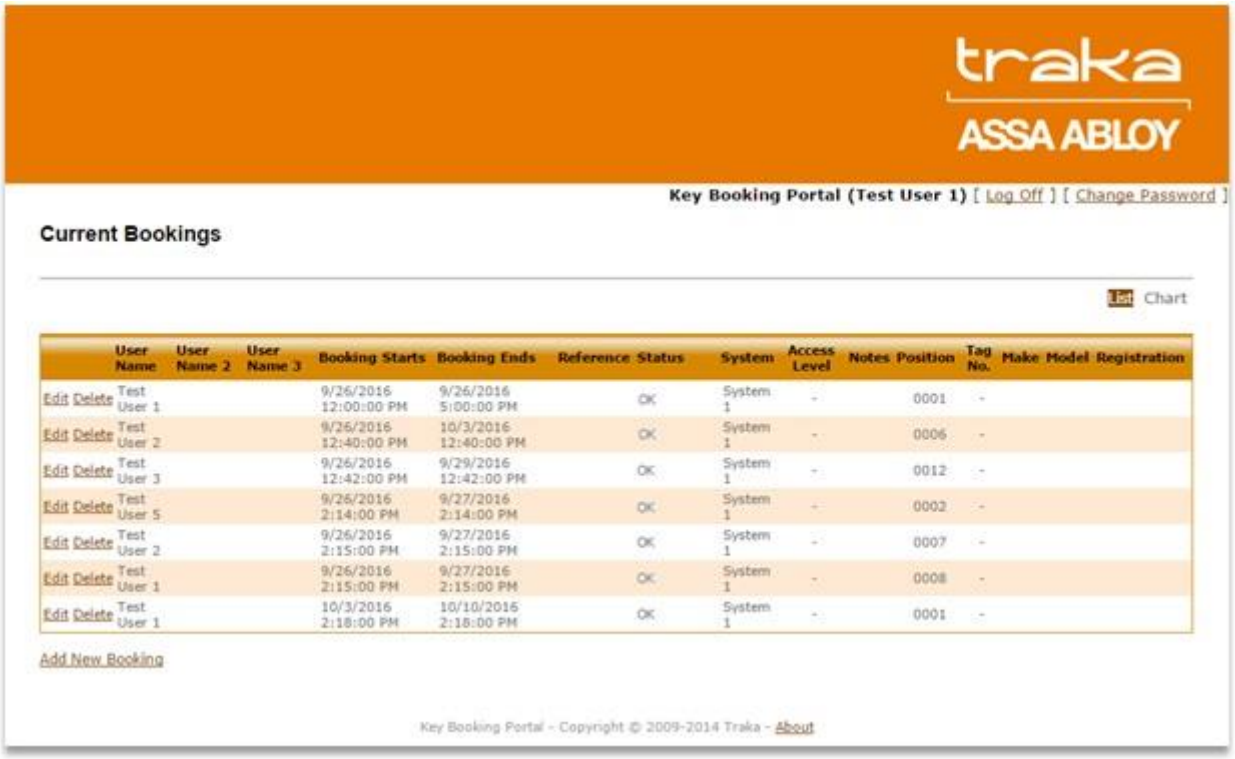


Once you've confirmed the booking the final screen will show you that the booking has been submitted successfully. From here you have the option to add another booking or click 'View Bookings' to see all current key bookings.

4.19.17.11.5 BOOKING LIST - KEY BOOKING WEB PORTAL

Once a booking is confirmed the Web Portal software will write the booking to the Traka System. You can view the details of any bookings by selecting the **Bookings List** button on the 'Welcome' screen and also from the 'Finish' page when you have completed a booking.

NOTE: You can only see bookings made by the Web Portal in the bookings list. In Traka32, you can see bookings made by both Traka32 and the Web Portal.



	User Name	User Name 2	User Name 3	Booking Starts	Booking Ends	Reference	Status	System	Access Level	Notes	Position	Tag No.	Make	Model	Registration
Edit Delete	Test User 1			9/26/2016 12:00:00 PM	9/26/2016 5:00:00 PM		OK	System 1	-		0001	-			
Edit Delete	Test User 2			9/26/2016 12:40:00 PM	10/3/2016 12:40:00 PM		OK	System 1	-		0006	-			
Edit Delete	Test User 3			9/26/2016 12:42:00 PM	9/29/2016 12:42:00 PM		OK	System 1	-		0012	-			
Edit Delete	Test User 5			9/26/2016 2:14:00 PM	9/27/2016 2:14:00 PM		OK	System 1	-		0002	-			
Edit Delete	Test User 2			9/26/2016 2:15:00 PM	9/27/2016 2:15:00 PM		OK	System 1	-		0007	-			
Edit Delete	Test User 1			9/26/2016 2:15:00 PM	9/27/2016 2:15:00 PM		OK	System 1	-		0008	-			
Edit Delete	Test User 1			10/3/2016 2:18:00 PM	10/10/2016 2:18:00 PM		OK	System 1	-		0001	-			

4.19.17.11.6 BOOKING CHART - KEY BOOKING WEB PORTAL

The Key Bookings Chart provides a graphical representation of all current bookings. It can be viewed by selecting **Chart** from the 'Welcome' screen or from the Booking List.

4.19.18 KEY HANDOVER LOGGING

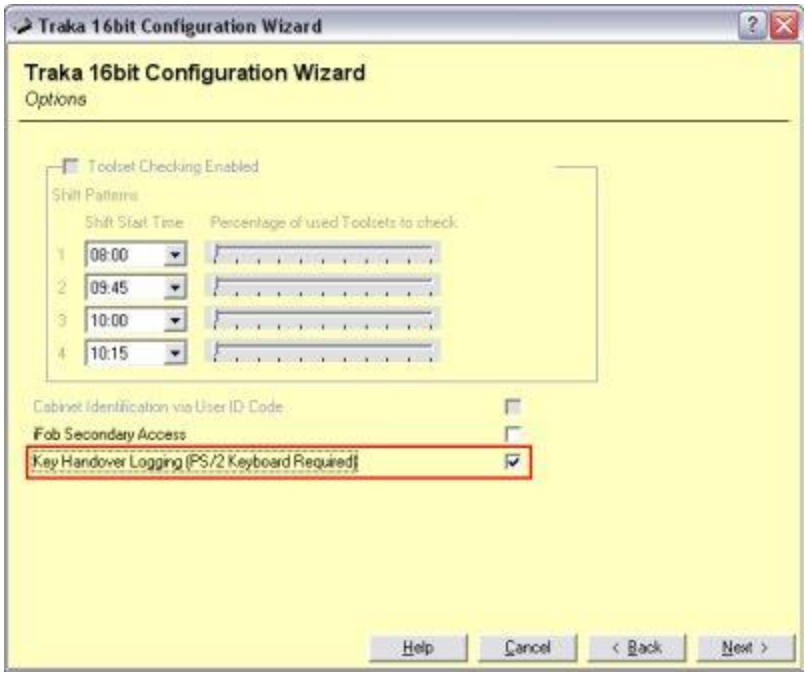
The Key Handover option was developed for a particular customer who wanted security officers to issue keys to other members of staff, who are not currently enrolled to the system. To make this feature more efficient Traka have included the interface of a QWERTY keyboard, allowing the security officers to record who they are giving the key to and where they are taking it, without typing all the information on the Traka keypad. This information then reads back to Traka32 and appears in the appropriate reports.

Setting up Key Handover Logging

Firstly an option is required in the 'Configure Firmware' to enable the use of the Key Handover Logging option. Right click your cabinet within Traka32 and click 'Configure Firmware'.

NOTE: To be able to see this option within the Configuration Wizard you must have software version 02.09.0001 and above.

The Configuration Wizard will appear allowing you to alter the cabinet's option and settings. Skip along to the last options page and tick the box named 'Key Handover Logging (PS/2 Keyboard Required)'. After selecting the option click 'Apply' to write the configuration to the cabinet.



Key Handover Logging Hardware and Software Requirements

As mentioned above the software version needed to operate Key Handover Logging is v02.09.0001 and above. To be able to interface a QWERTY keyboard with your Traka cabinet you must have the following hardware...

- Traka 16bit Cabinet
- QWERTY Keyboard with PS2 connection
- QWERTY-Traka Interface Cable (see below)

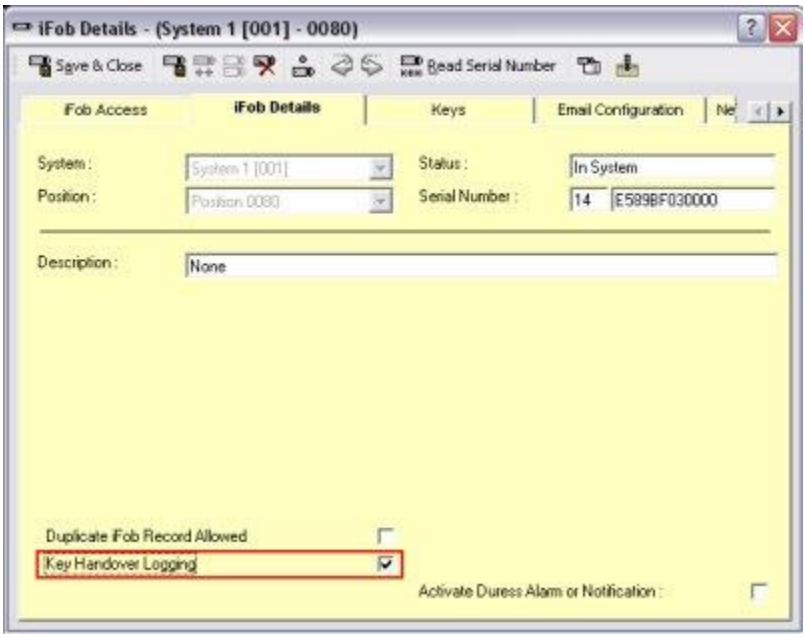
Key Handover Process

To handover the key to another member of staff the user must first enable the following option in the iFob Details. This has to be done for every iFob you wish to handover to another user.

1. Right click the desired iFob and select 'Edit iFob Details'.

2. The iFob Details window will now appear, select the iFob Details Tab. At the bottom of the screen you will see the option 'Key Handover Logging', tick this box then save and close.

   NOTE: If this option is not enabled on the iFob before the user attempts to remove it, then they will NOT be prompted to enter the Handover details. The iFob will be released as normal.



3. The user must next gain access to the system. On a locking system, when a user presses a button to request an iFob, the system will prompt for the user to enter in the Key Handover details (on a non-locking system the user will be prompted to enter the Handover details when an iFob is removed from the cabinet).

4. The user will then enter the name of the staff who they will hand the key over to using the QWERTY keyboard. Once the user has entered the name and pressed Enter, the system will then prompt for the user to enter in the location of where the staff member is visiting.

   NOTE: The maximum number of characters that can be entered for the Handover Name is 22.

5. The user will then enter the location the staff member is visiting using the QWERTY keyboard. Once the user has entered the location and pressed Enter, the key will be released.

   NOTE: The maximum number of characters that can be entered for the Handover Location is 24.

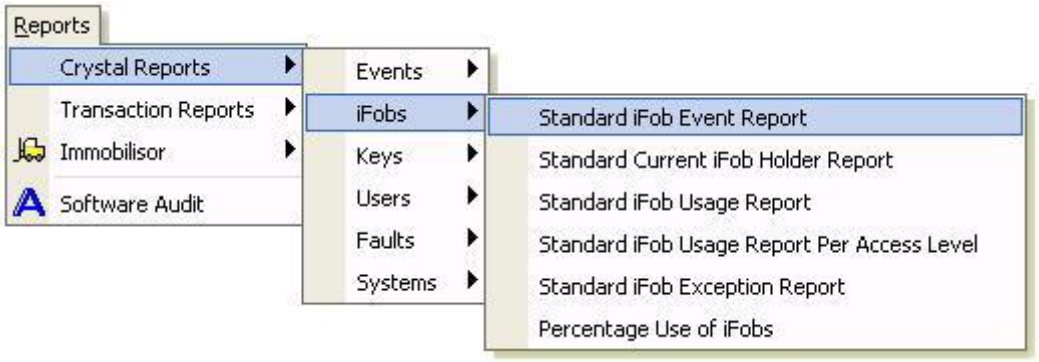
iFob Search Facility

When using the Standard Search Facility or the Advanced Search Facility, the LCD will display the Key Handover Name & the Key Handover Location along with the regular information such as iFob Description, iFob Status etc.

Reports

The Report on who has had the iFob Handed over to them and the location which they took it, is in the following location...

From the System viewer, click *Reports* > *Crystal Reports* > *iFobs* > *Standard iFob Event Report.*



This report will generate a list of all the people who have had an iFob 'handed' over to them and the location they used that iFob (see below)

Standard iFob Event Report

traka

Description	Date/time	Related system	Position	Tag No.	Related user	Authoriser 1	Authoriser 2
Key Handover Logging	26/06/2009 17:15:37	System 1	37	0	Fernando Bea		
Key Handover Name: 'Duncan Winner' Key Handover Location: 'back car park'							
iFob Returned	26/06/2009 17:13:25	System 1	40	0	Fernando Bea		
iFob Removed	26/06/2009 17:12:59	System 1	40	0	Fernando Bea		
Key Handover Logging	26/06/2009 17:12:59	System 1	40	0	Fernando Bea		
Key Handover Name: 'Duncan Winner' Key Handover Location: 'front car park'							

4.19.19 KEY VENDING WIZARD

4.19.19.1 KEY VENDING WIZARD OVERVIEW

The Key Vending Wizard provides a simple method for the issuing and returning of keys. A user (Key Requestor) requests a key from a Key Vendor. The Key Vendor issues a key via the Key Vending Wizard and a Traka USB Desktop Programmer, and the Key Requestor signs on the Signature Pad to accept receipt of the key. The same process is reversed upon a key being returned.

Key types are divided into 2 categories; 'Tenant Key' and 'Service Key'. These key types are selectable during the issuing of a key through the Key Vending Wizard.

Both Key Requestors and Key Vendors have a user record inside the Traka32 database, however only Key Vendors are given access to the Traka systems. Tenant Key Requestors can also be added to the Traka32 database via the Key Vending Wizard. The method for doing this is explained in the section Issue a Key.

Reports can be generated detailing all of the key issuing and returning transactions.

Emails are generated for overdue keys or keys that are removed or returned without using the Key Vending Wizard. An email address or email group can be specified as the recipient for the emails.

NOTE: The Key Vending Wizard has been designed to work with Random Return to Multiple Systems and is also best used with the Advanced Search option. If you wish to use this feature on a Fixed Return system, please contact Traka.

NOTE: This Key Vending Wizard section of the guide assumes your system is already configured and setup for Random Return to Multiple Systems. Refer to Random Return to Multiple Systems Setup for more information.

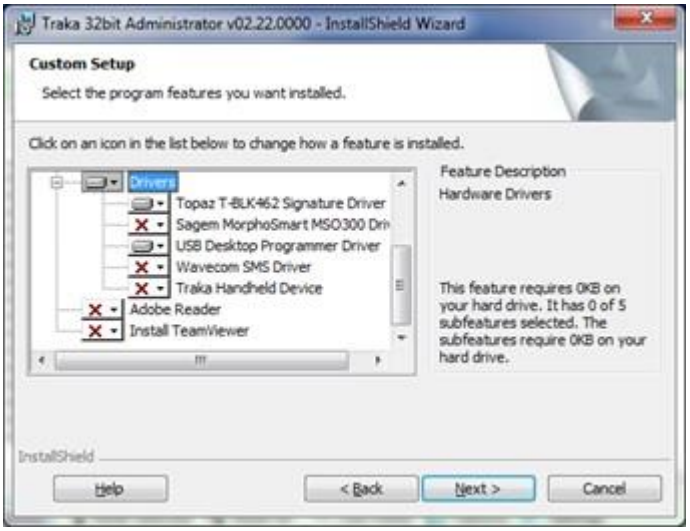
4.19.19.2 KEY VENDING WIZARD SETUP

4.19.19.2.1 KEY VENDING TRAKA32 SOFTWARE INSTALLATION

NOTE: The Key Vending feature uses Traka32 as a Service to process the automatic emails. For more information on installing Traka as a Service refer to the section Traka32 as a Windows Service.

During the **installation of Traka32** on any client PCs, the drivers for the Signature Pad and USB Desktop Reader must also be installed.

1. Install Traka32 selecting the **Custom** option.
2. Expand the Drivers folder and click to install both the **Topaz T-BLK462 Signature Driver** and the **USB Desktop Programmer Driver**.



3. Complete the installation.

The Key Vending Wizard feature is used in conjunction with the following devices:

- Topaz Signature Pad
- Traka USB Desktop Programmer

The following processes must be followed to configure the devices on all Client PCs.

Topaz Signature Pad Configuration

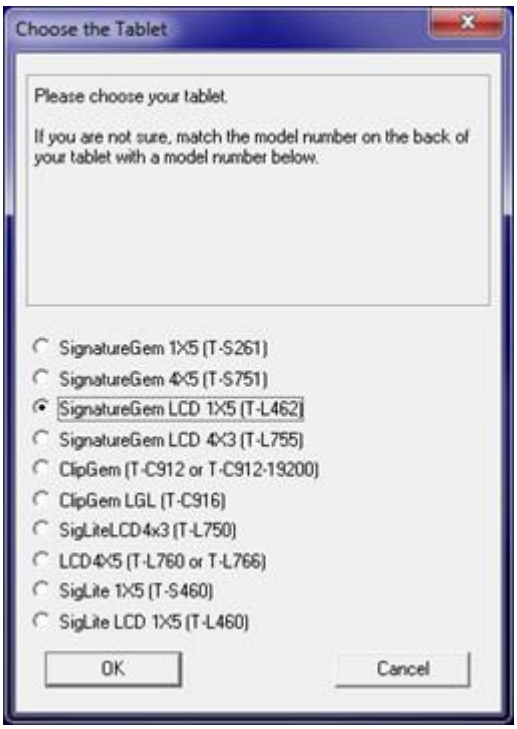
NOTE: Ensure the Signature Pad is <u>not</u> connected to the PC before beginning.

1. Navigate to c:\Program Files (x86)\Traka Limited\Traka32\Drivers\Signature
2. Run the sigplusbasic.exe application.
3. Click 'Next' and then click 'Agree' to the license agreement.
4. Select the correct operating system.
5. When asked if you will be viewing signatures in Word documents or Excel Spreadsheets select 'No' and then click 'OK'.

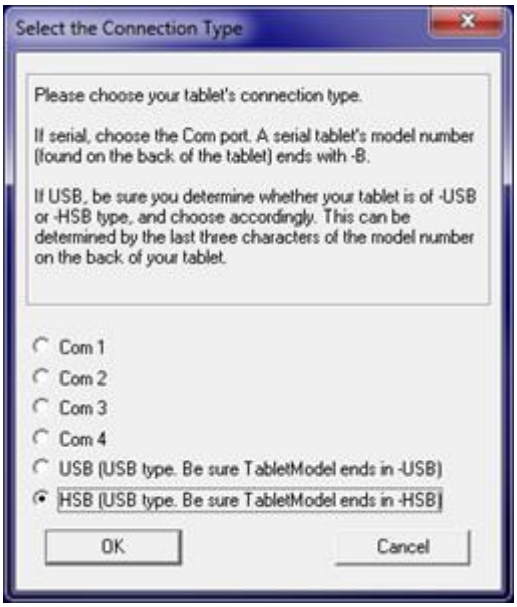
6. When asked if you will be signing and/or viewing signatures in Adobe Acrobat select 'No' and then click 'OK'.

7. Select the option ‘I have a tablet, and want to sign eDocuments’ and click ‘OK’.

8. Select the tablet ‘SignatureGem LCD 1X5 (T-L462)’ and click ‘OK’.



9. Select the connection type ‘HSB (USB type…) and click ‘OK’ to begin the software installation.



NOTE: Wait for the installation to complete before moving on to the next step.

9. Plug the USB cable from the signature pad into the PC to complete the setup.

USB Desktop Programmer Configuration

NOTE: Ensure the Desktop Programmer is <u>not</u> connected to the PC before beginning.

1. Navigate to c:\Program Files (x86)\Traka Limited\Traka32\Drivers\USB Desktop Programmer
2. Install the correct one of the following depending on your system type:
    - Install_1_wire_drivers_x64_v402.msi (use this on 64-bit systems)
    - Install_1_wire_drivers_x86_v401r2.msi (use this on 32-bit systems)

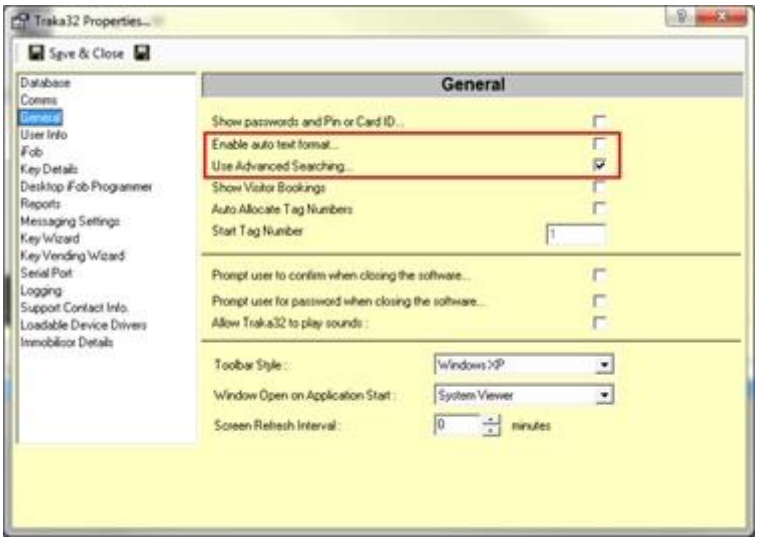
NOTE: Wait for the installation is complete before moving on to the next step.

3. Plug the USB cable from the desktop programmer into the PC and check that the software installs correctly.

4.19.19.2.3 KEY VENDING TRAKA32 CONFIGURATION

4.19.19.2.3.1 KEY VENDING - TRAKA32 PROPERTIES

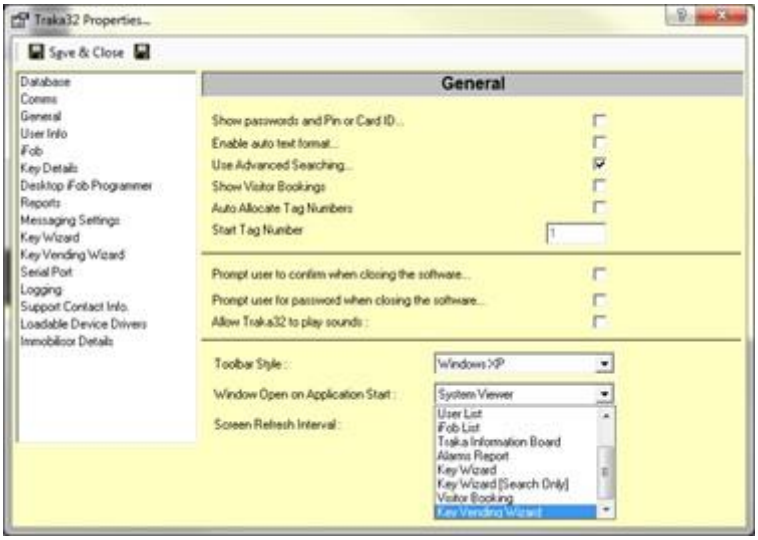
1. Select the **General** page and tick the **Use Advanced Searching** box. Also ensure the **Enable Auto Text Format** option is unticked.



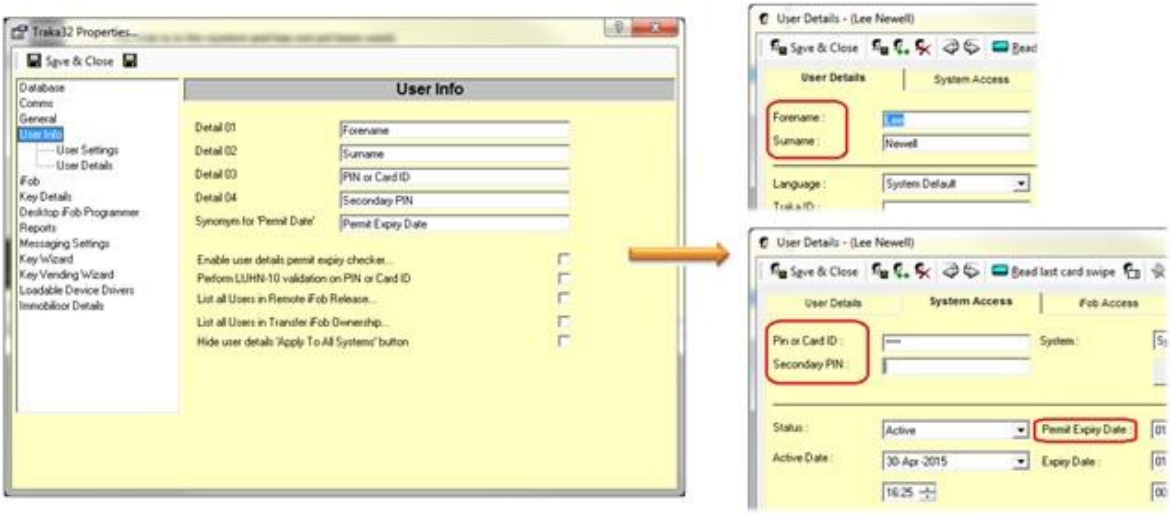
2. If this PC is to be used by a Key Vendor user and the user will not be administering the Traka32 software (such as adding/editing users) it is possible to set the default screen to be the Key Vending Wizard. This means whenever Traka32 is opened on this PC by any user it will only show the Key Vending Wizard, and no other functions of Traka32 will be accessible.

   To enable this, select **Key Vending Wizard** from the 'Window Open on Application Start' dropdown and then click **Save**. The next time Traka32 is opened from this PC it will open the Key Vending Wizard only.

   NOTE: To restore this setting back to default please contact Traka.



3. Select the **User Info** page. From here you can change the terminology used for some of the user detail fields, such as 'Forename' and 'Surname'. Changing the descriptions here will update the headings wherever they are displayed across Traka32 and the Key Vending Wizard.



4. Select **User Details**. Specify the correct user definable labels. Changing these fields will update the field headings in the User Details page. An example of what these fields could be changed to is shown below:

   Field 01 = Traka ID (this could be employee number or student ID etc.)

   Field 02 = Email Address

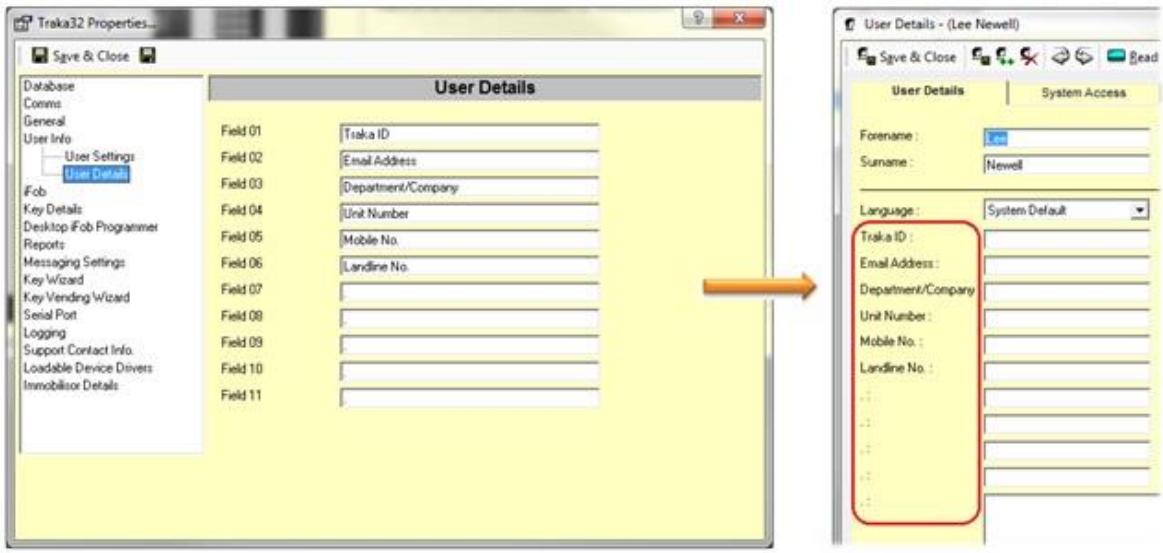
   Field 03 = Department/Company

   Field 04 = Unit Number

   Field 05 = Mobile No.

   Field 06 = Landline No.

   To make things clearer it is advised to specify a'.' in any unused fields.



NOTE: These fields must match the fields in the User Import Spreadsheet if you are importing users.

5. Click **Save** before moving on.

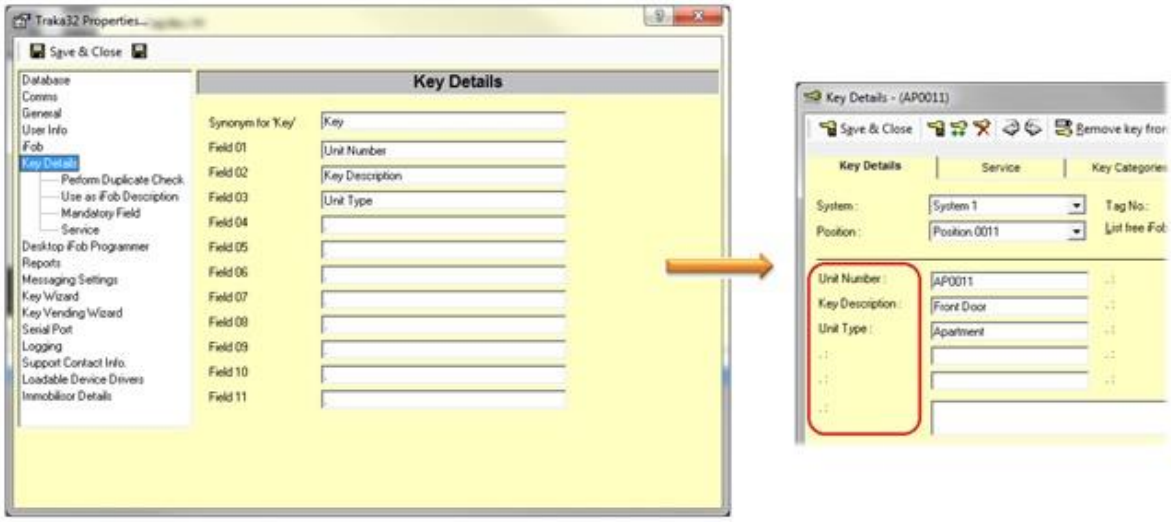
6. Select the **Key Details** page. Specify the correct user definable labels. Changing these fields will update the headings in the Key Details pages. An example is shown below:

   Field 01 = Unit Number

   Field 02 = Key Description

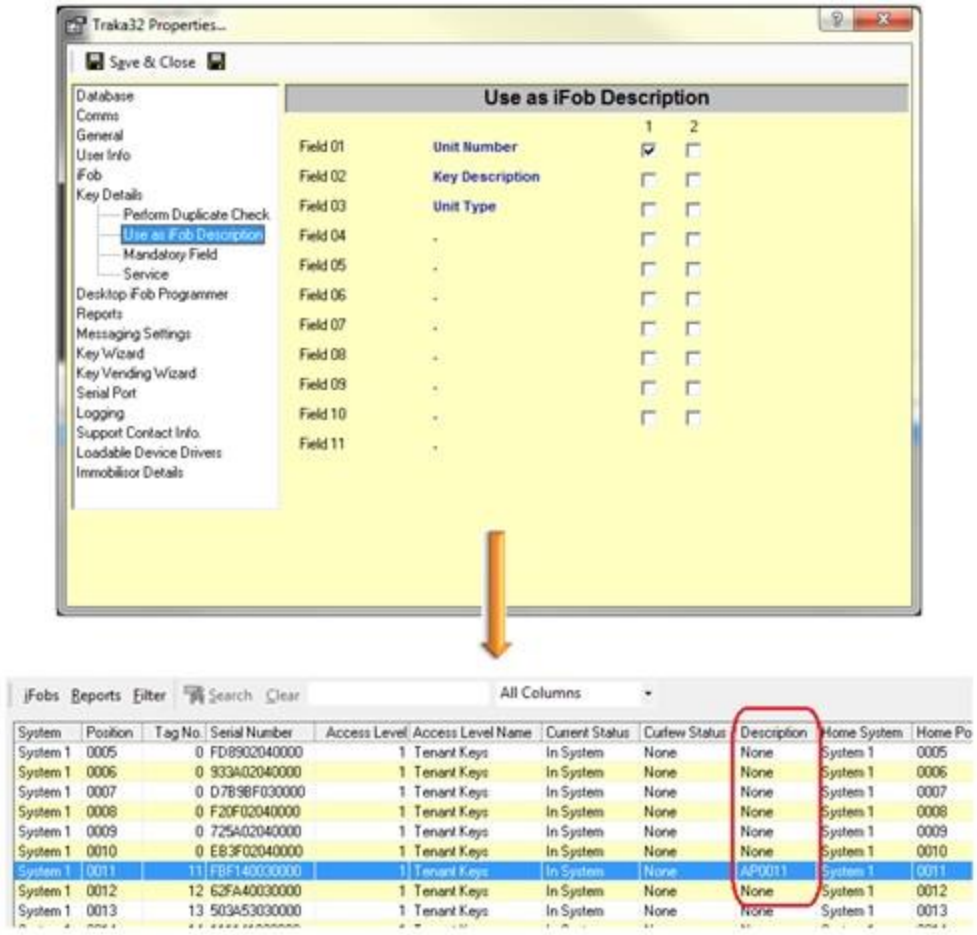
   Field 03 = Unit Type

   To make things clearer it is advised to specify a'.' in any unused fields.



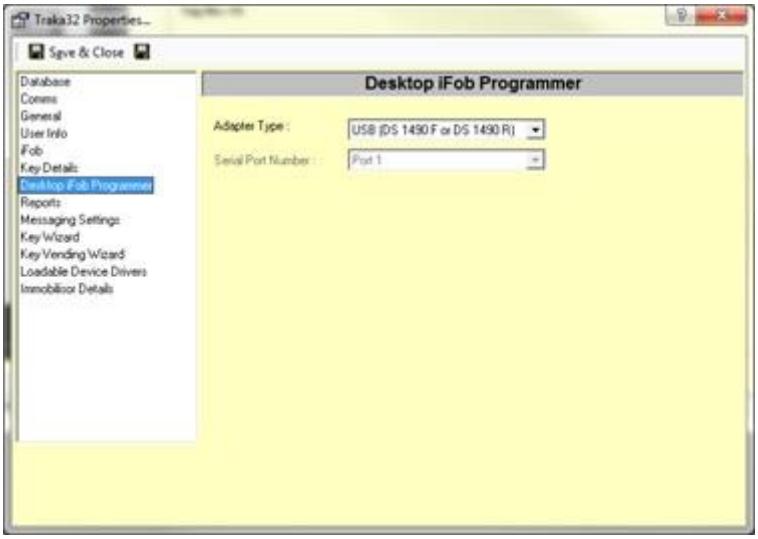
NOTE: These fields must match the fields in the Key Import Spreadsheet if you are importing keys.

7. Select **Use as iFob Description** and select which field (from the list in the previous step) you wish to use as the iFob description. In the example below, 'Unit Number' is used as the iFob Description. Anywhere the iFob description is displayed in Traka32 (for example in the iFob list) will now be populated with the Unit Number.

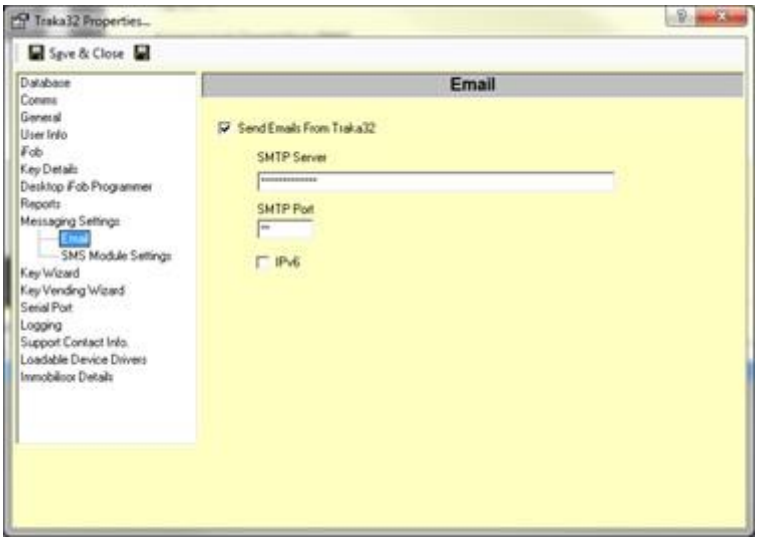


8. Click **Save** before moving on.

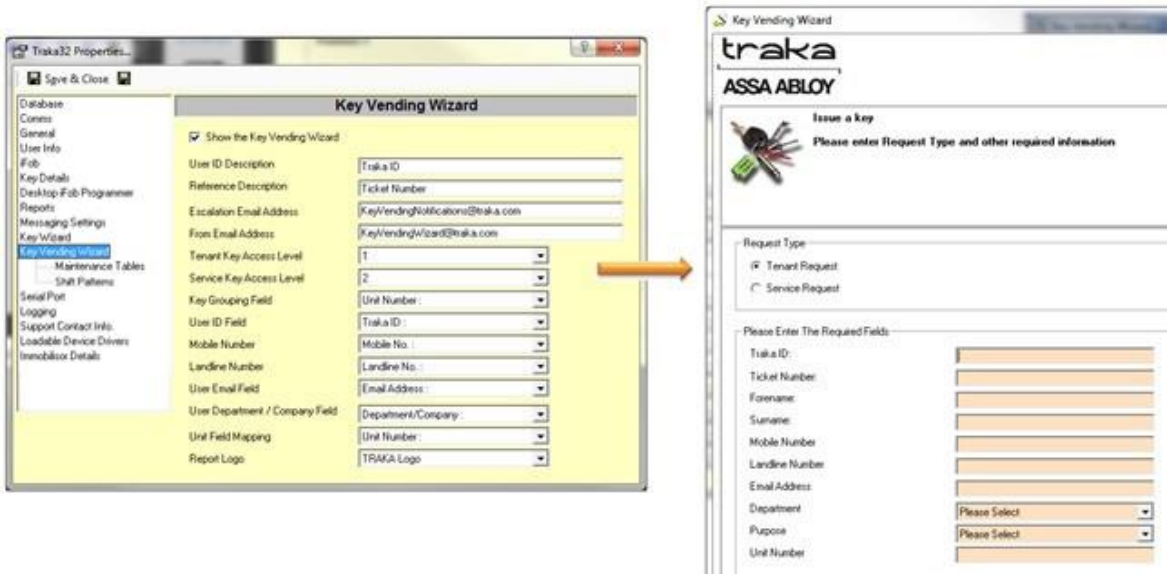
9. Select the **Desktop iFob Programmer** page. Set the Adapter Type to **USB (DS 1490 F or DS 1490 R)** and then click **Save**.



10. Select **Message Settings>Email**. Enter the correct details for your email server and click **Save**.



11. Select the **Key Vending Wizard** page. Ensure the 'Show the Key Vending Wizard' tick box is ticked. From this page you can also specify various details specifically for the Key Vending Wizard as detailed below:



NOTE: To open the Key Vending Wizard select View>Key Vending Wizard.

User ID Description: Specify the field heading used for the User ID field in the Key Vending Wizard.

Reference Description: Specify the field heading used for the reference field in the Key Vending Wizard.

Escalation Email Address: Specify the email address of a person or group who you wish to receive email notifications from the Key Vending Wizard.

From Email Address: Specify the email address that will be displayed as the 'sender' of the notifications.

Tenant Key Access Level: Specify the Access Level you wish to use for Tenant Keys (usually access level 1).

Service Key Access Level: Specify the Access Level you wish to use for Service Keys (usually access level 2).

Key Grouping Field: Specify the field that determines a duplicate key. This is used to warn if a duplicate key to one that is already out of the system is requested. In the example, if 'Unit Number' is referring to an apartment, it will warn the Key Vendor if a service key is requested for an apartment that is already occupied by a tenant.

User ID Field: Specify the data that will be used for the User ID field in the Key Vending Wizard. The options available in this list will be those that were specified in the User Details earlier in this section.

NOTE: The user ID Field requires the data entered to be numerical and between 6-8 digits in length.

Mobile Number: Specify the data that will be used for the Mobile Number field in the Key Vending Wizard. The options available in this list will be those that were specified in the User Details earlier in this section.

Landline Number: Specify the data that will be used for the Landline Number field in the Key Vending Wizard. The options available in this list will be those that were specified in the User Details earlier in this section.

User Email Field: Specify the data that will be displayed in the Email Address field in the Key Vending Wizard. The options available in this list will be those that were specified in the User Details earlier in this section.

User Department/Company Field: Specify the data that will be displayed in the User Department/Company field. The options available in this list will be those that were specified in the User Details earlier in this section.

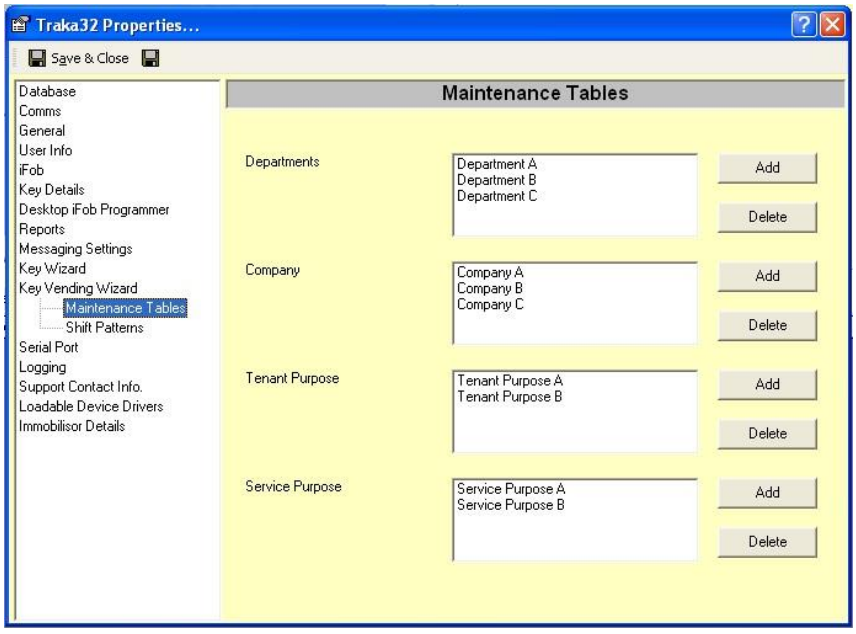
Unit Field Mapping: Specify the data that will be displayed in the Unit Field. The options available in this list will be those that were specified in the User Details earlier in this section.

Report Logo: Specify the logo that will be shown on all reports. As well as the Traka Logo, customers' own logos will be listed. To have your own logo available here please contact Traka.

12. Click **Save** before moving on.

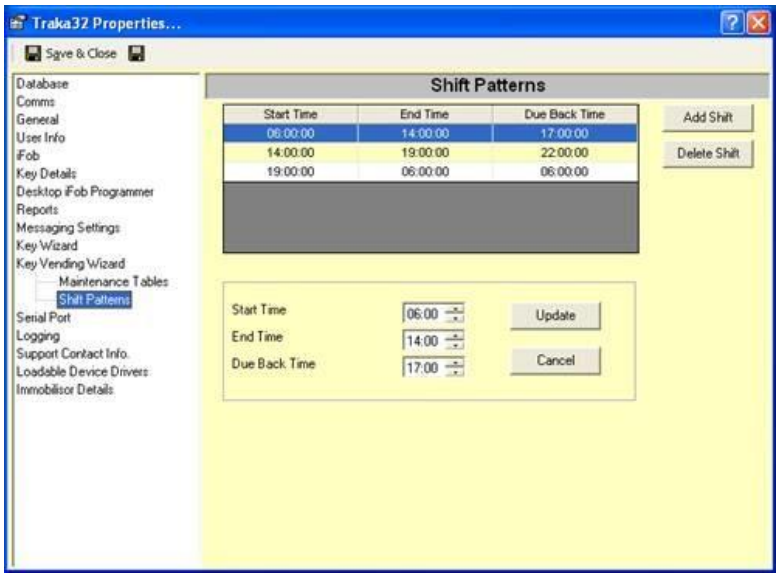
13. Select **Maintenance Tables**. Here you can specify a list of departments and companies, and also list common purposes for the issuing of keys for both service and tenants. These are then selectable in the Key Vending Wizard during the process of issuing a key.

    To add to any list, click the **Add** button next to the field. Type in the relevant description and then click **OK**.



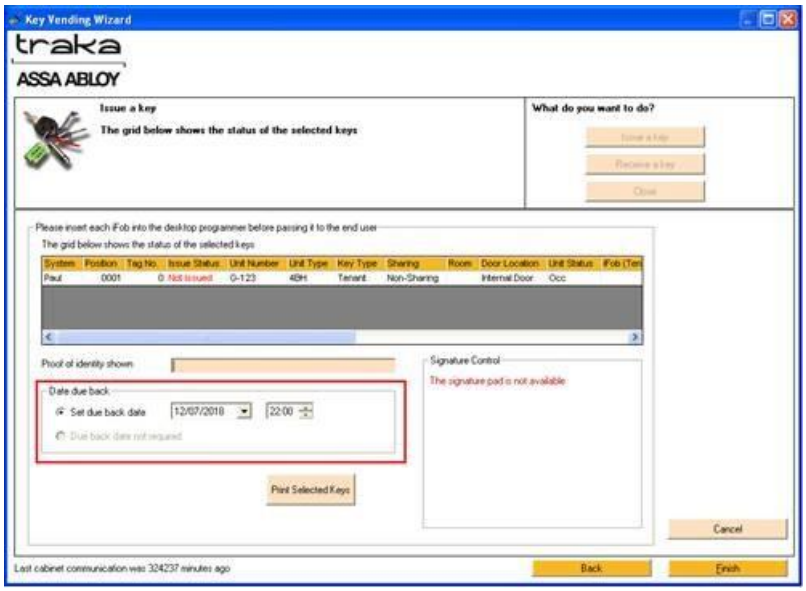
14. Click **Save** before moving on.

15. Select **Shift Patterns**. This maintenance form will enable you define multiple shift patterns. Shifts can be added by entering a Start Time, End Time and a Due Back Time followed by clicking on the **Add Shift** button. This can be repeated to add multiple shifts.



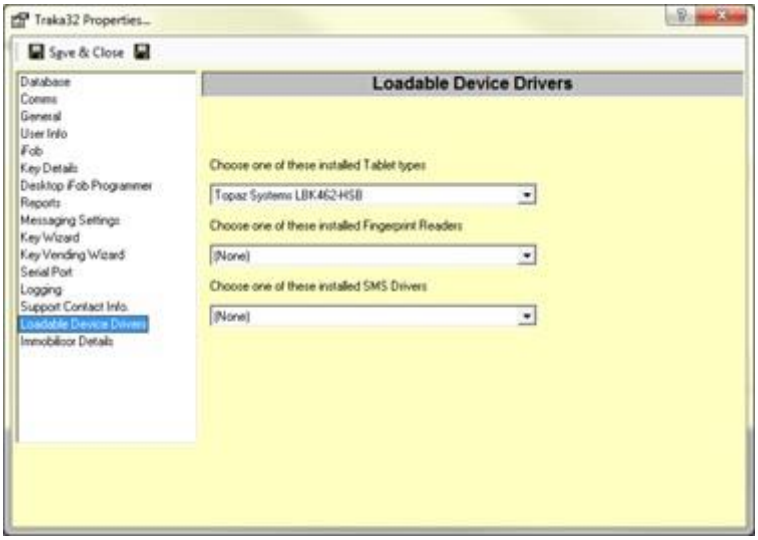
When an iFob is issued, the table will be referred to in order to determine the Due Back Time. This will then be used as the default curfew time.

The Example below shows that the due back date and time has been automatically set according to the issue time.



16. Click on **Save** before continuing.

17. Select the **Loadable Device Drivers** page and select **Topaz Systems LBK 462-HSB** from the 'Tablet types' dropdown.



18. Click **Save & Close**.

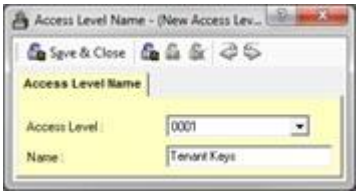
4.19.19.2.3.2 KEY VENDING ACCESS LEVELS

The Key Vending feature divides keys into 2 types; 'Tenant Key' and 'Service Key'. These 2 types must each be given an Access Level. For example, Tenant Keys can be assigned with Access Level 1 and Service Keys can be assigned with Access Level 2. These Access Levels can also be assigned names.

1. Go to **File>Options** and select the **Access Level Names** tab.

2. Select **Options** and **Add New**.

3. Select the Access Level number you wish to use for the Tenant Keys and type 'Tenant Keys' into the Name field and then click **Save & Close.**

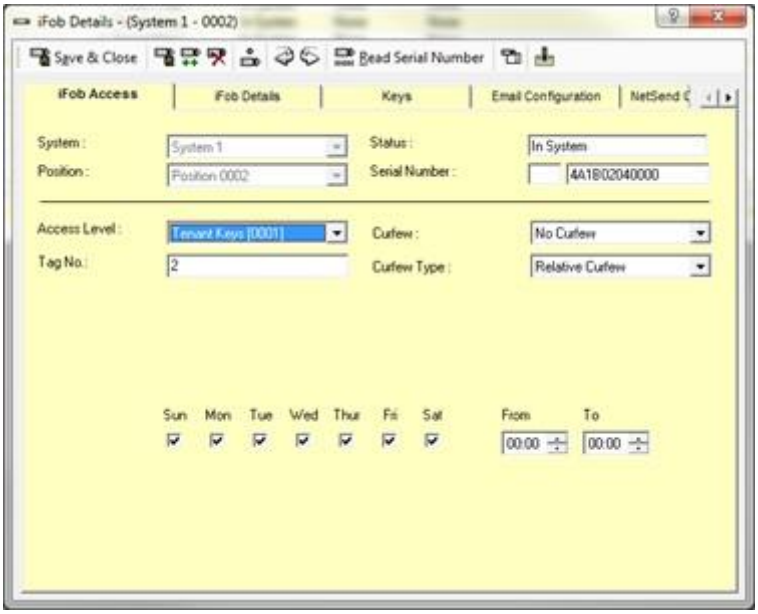


4. Repeat this process for the Service Keys, selecting the required Access Level number and entering the name 'Service Keys'.

5. To assign the Access Levels to the iFobs, from the System Viewer window go to **View>iFob List**.

6. Select the required iFob from the list and then go to **iFobs>Edit iFob**.

7. On the **iFob Access** tab select the required access level from the **Access Level** drop down list, and then click Save & Close.



Key Vending User Setup

There are 2 types of users that must be added to the user database:

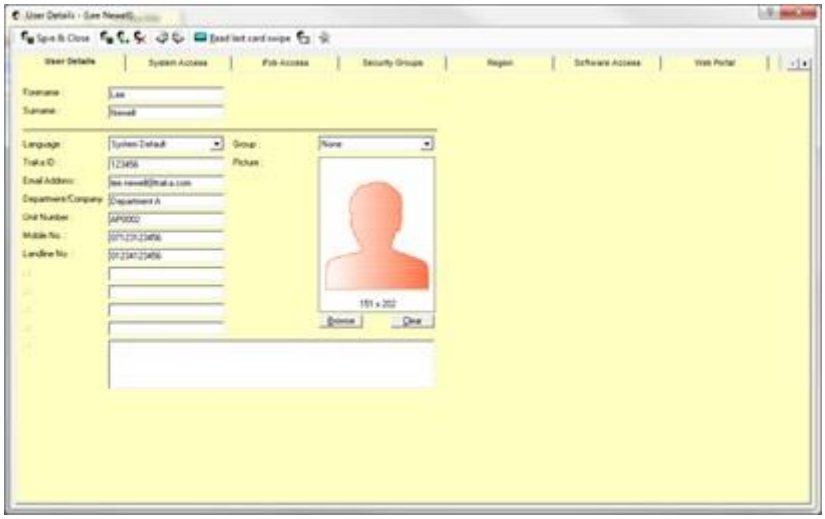
- Key Requestors – able to request keys from the Key Vendors but have no access to the Traka systems.
- Key Vendors – process the key requests and must be given access the Traka systems and Traka32 software.

Users can be added either via the User Import Spreadsheet or manually through the Traka32 software. A brief guide on manually adding both Key Requestor and Key Vendor users is outlined below. For more specific details on adding users, please refer to the section Adding Users for more details.

NOTE: It is also possible to add Tenant users directly from the Key Vending Wizard. This is explained during the Issue a Key process.

Key Requestor

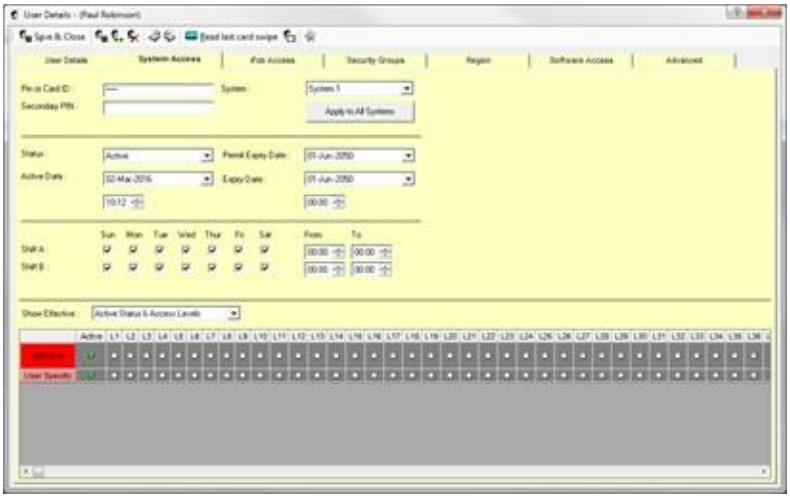
When adding a new Key Requestor user, simply fill in the required details on the User Details tab and click **Save & Close**. No other settings or details are required as Key Requestors will have no access to the Traka System itself.



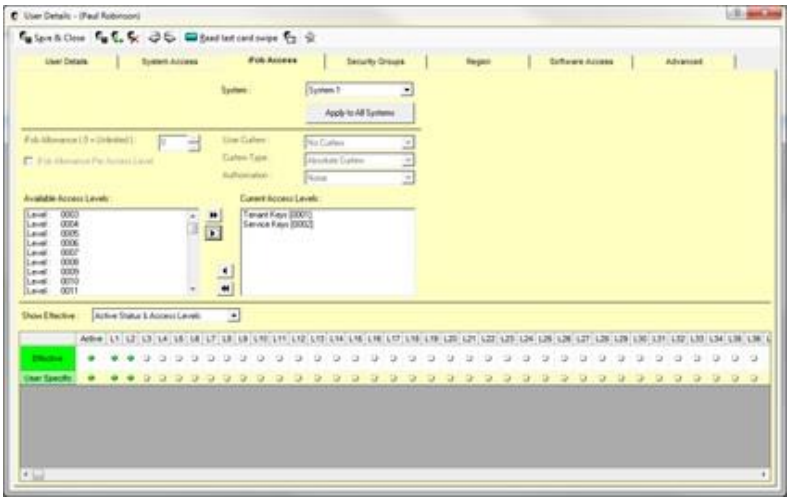
Key Vendor

When adding a new Key Vendor user, in addition to adding the required details on the User Details tab the user will also need to be given access to the Traka System(s) and the Traka32 software.

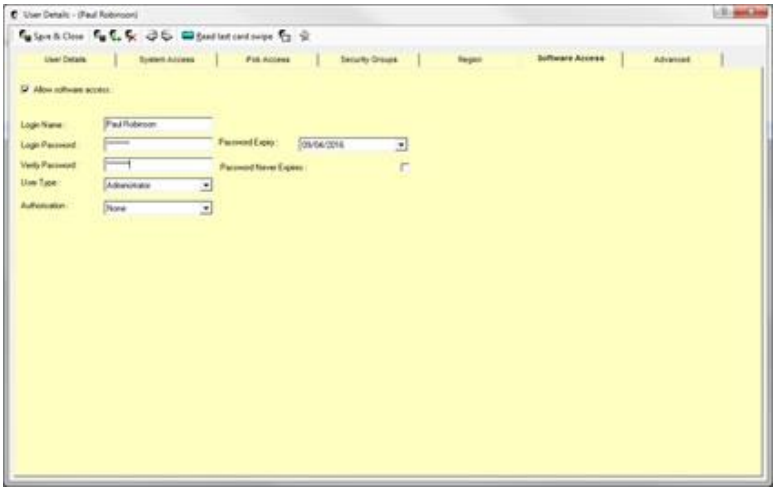
1. Enter the user's Pin or Card ID on the System Access tab and set the Status to 'Active'.



2. From the iFob Access tab, assign both the Tenant Key and Service Key access levels to the user.



3. On the Software Access tab, tick the 'Allow Software Access' tick box and enter login details for the user. Enter any other required details and click **Save & Close**. For more information on assigning software access refer to the User Details section of this guide.



4.19.19.2.3.3 KEY VENDING - ADDING KEYS

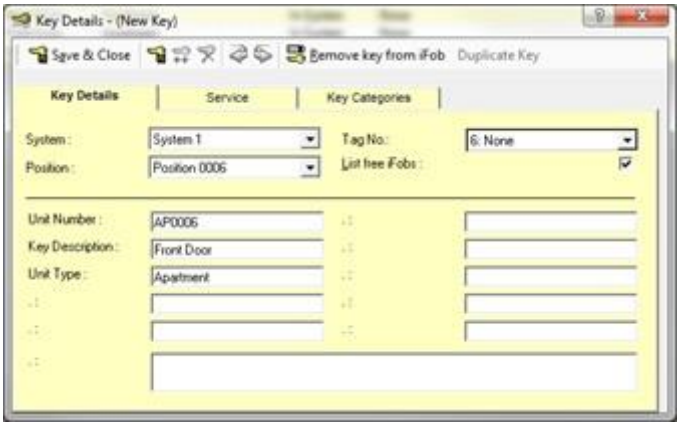
Keys can be added either via the Key Import Spreadsheet or manually through the Traka32 software. A brief guide on manually adding keys is outlined below. For more specific details on adding keys please refer to the section Adding Keys for more details.

1. From the System Viewer window select **Key List** and then **Keys>Add New**.
2. Select the required System and then the position number or tag number of the iFob you wish to add the key to.

   NOTE: This section of the guide assumes the system is already setup with tag numbers. Refer to the section Random Return to Multiple Systems for more information.

3. Enter the relevant details into the provided fields and then click Save & Close.

   NOTE: These are customisable fields that were setup in the Key Details part of the Key Vending - Traka32 Properties section.

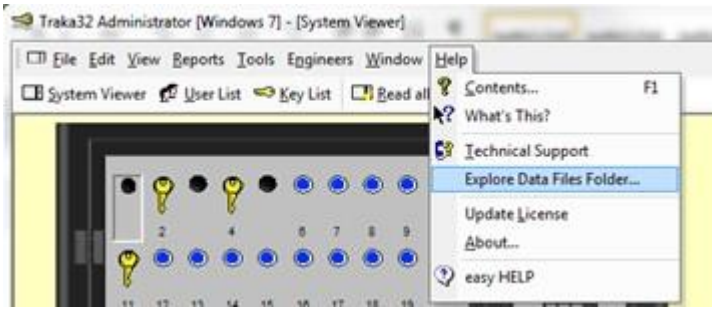


4.19.19.2.3.4 KEY ISSUE EXCEPTION TIME DELAY

By default, a Key Vendor is given 15 minutes to complete the Key Issue process in the Key Vending Wizard after an iFob has been removed from the Traka system. After 15 minutes has passed, if the Key Vending Wizard has not been completed an escalation email is sent, and the key issue exception will appear in the Key Issue Exception Report.

This time delay can be adjusted by editing the T32Settings.ini file.

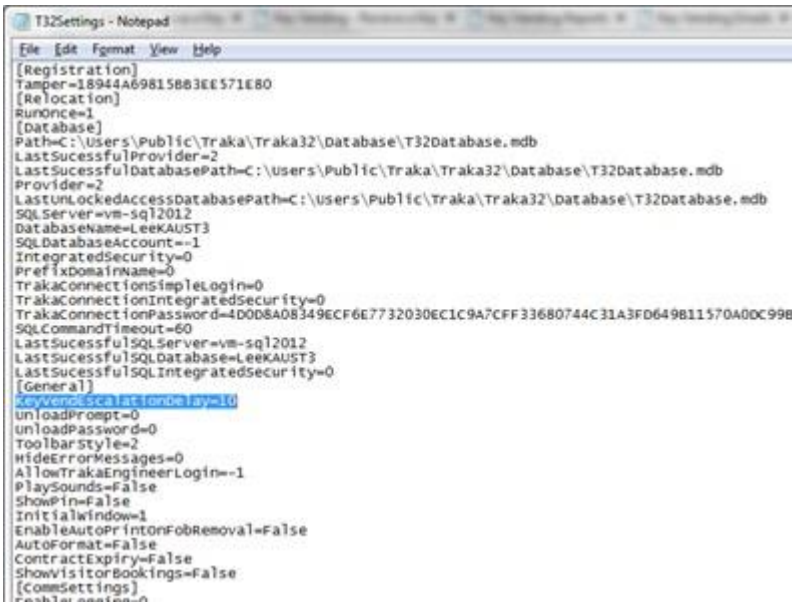
1. To locate the file, go to **Help>Explore Data Files Folder...**



2. Open the **Settings** folder, and then open the **T32Settings.ini** file.

3. Under the **[General]** section type **KeyVendEscalationDelay=(number of minutes).**

   For example, to change the time delay to 10 minutes, type **KeyVendEscalationDelay=10** as shown in the example below.



4. Save and close the file. The time delay will now be set to the specified time.

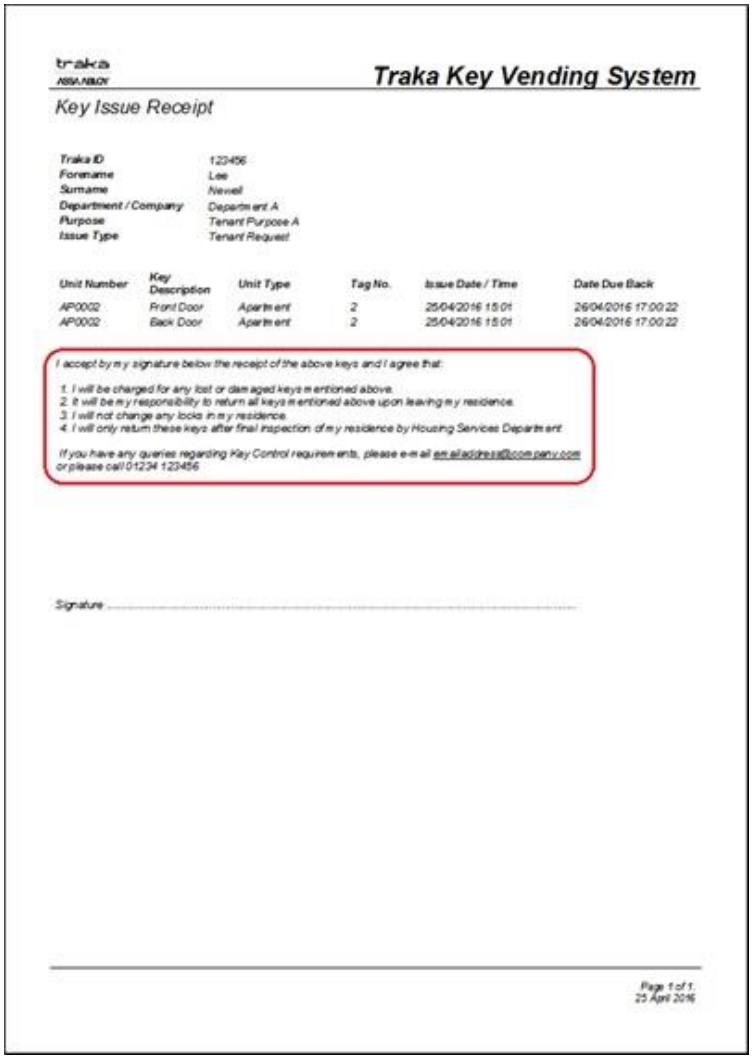
   To edit the time again, simply open this file, change the number of minutes and then save and close the file.

   To return to the default of 15 minutes, either edit the number to 15 or delete the 'KeyVendEscalationDelay' line completely.

4.19.19.2.3.5 CUSTOMISE KEY RECEIPTS

During the key issuing and returning processes a Key Receipt can be printed to be signed to accept receipt of the keys. As well as displaying a list of the keys being issued or returned, it also has a default section of text that can be edited to suit the customers' specific requirements.

The example image below shows the Key Issue Tenant Receipt with the customisable text highlighted.



traka

Traka Key Vending System

Key Issue Receipt

Traka ID	123456
Forename	Lee
Surname	Newell
Department / Company	Department A
Purpose	Tenant Purpose A
Issue Type	Tenant Request

Unit Number	Key Description	Unit Type	Tag No.	Issue Date / Time	Date Due Back
AP0002	Front Door	Apartment	2	25/04/2016 15:01	26/04/2016 17:00:22
AP0002	Back Door	Apartment	2	25/04/2016 15:01	26/04/2016 17:00:22

I accept by my signature below the receipt of the above keys and I agree that:

1. I will be charged for any lost or damaged keys mentioned above.
2. It will be my responsibility to return all keys mentioned above upon leaving my residence.
3. I will not change any locks in my residence.
4. I will only return these keys after final inspection of my residence by Housing Services Department

If you have any queries regarding Key Control requirements, please e-mail an.alladdress@company.com or please call 01234 123456

Signature .....

Page 1 of 1
25 April 2016

1. Go to **Help>Explore Data Files Folder...**
2. Open the **Templates** folder. There are 4 receipt templates in total.

   KeyVend_IssueService - Key issue receipt for Service requests

   KeyVend_IssueTenant - Key issue receipt for Tenant requests

   KeyVend_ReturnService - Key return receipt for Service returns

   KeyVend_ReturnTenant - Key return receipt for Tenant returns

   Right click the receipt you wish to edit and ensure it is not set to 'Read Only', and then open the file with Notepad or a HTML editor.

   NOTE: It is advised to make a backup copy of the receipt files before editing.

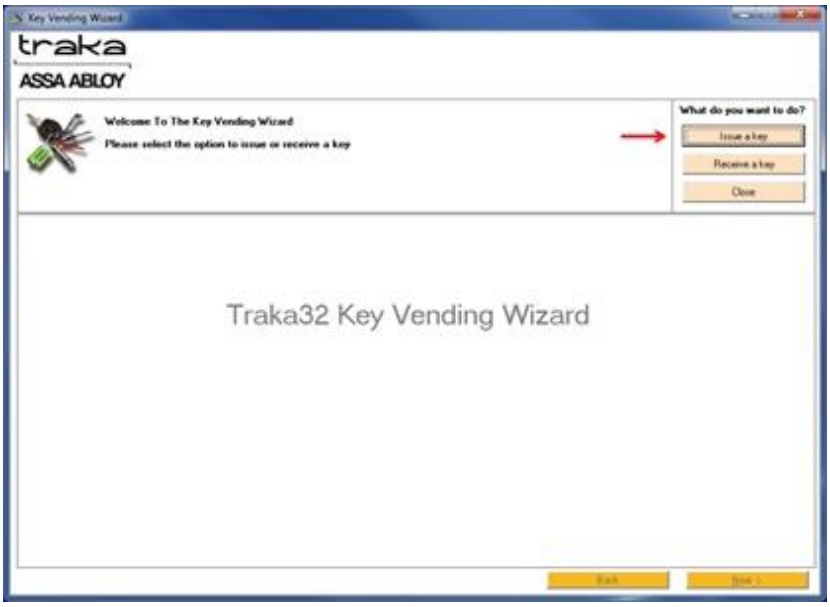
3. Make the required changes and then save the file. Ensure you select to save as 'All Files' if you are using Notepad.

   The next time the receipt is opened it will display the new text.

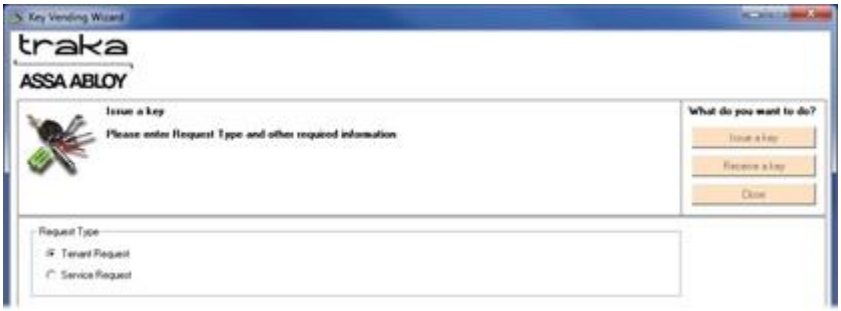
4.19.19.3 KEY VENDING WIZARD OPERATION

4.19.19.3.1 KEY VENDING - ISSUE A KEY

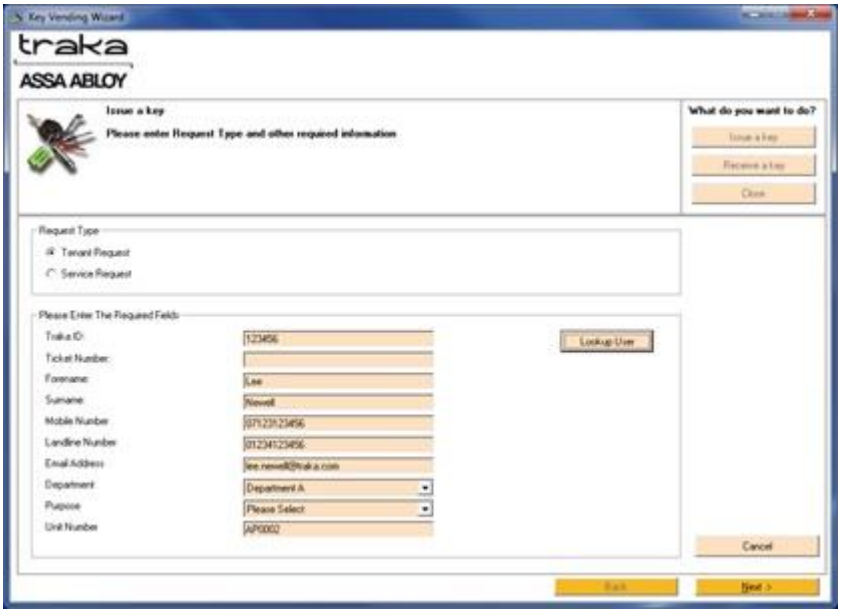
1. From the Key Vending Wizard home screen click **Issue a Key**.



2. From the 'Request Type' section select whether the Key Requestor is a Tenant or Service Person.



3. Enter the ID number of the Key Requestor and select **Lookup User**. If the ID number is in the Traka32 User Database, the system will populate the fields with any details already entered in the User Record in Traka32.

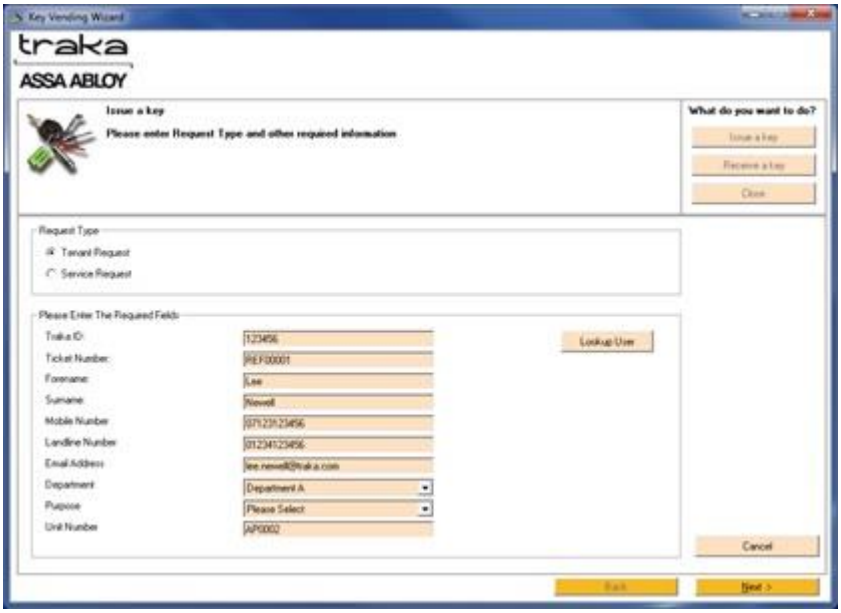


If the ID number is not known, you can leave the field blank and this can be added upon the return of the key.

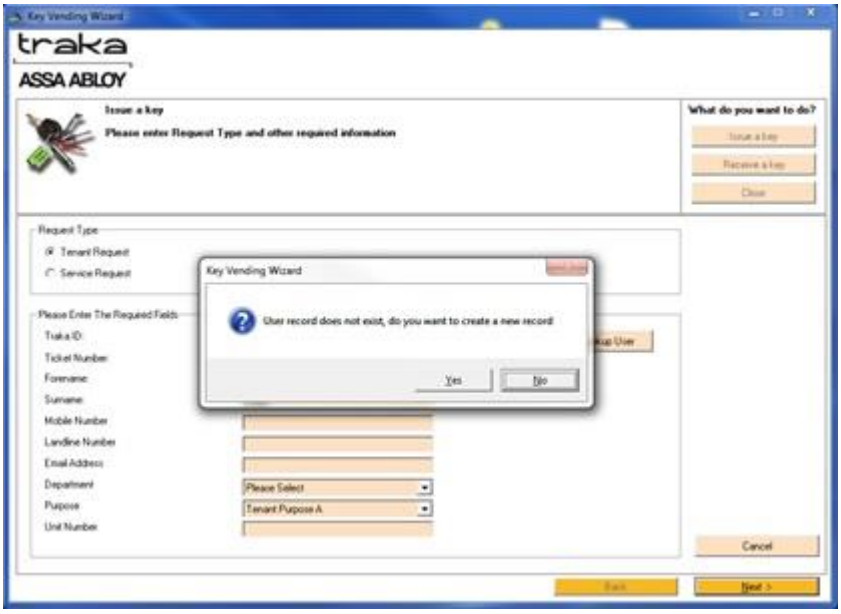
NOTE: It is compulsory to enter an ID number for a Service Key Request.

If the ID number is not in the database a message will pop up saying the User Record does not exist. If the request is for a Tenant Key, it is possible to create a new user directly from the Key Vending Wizard. To do this, enter the user's details into the provided fields and continue to the next step.

4. Enter a Ticket Number (reference number) if applicable, and also specify the purpose for the key request. The list of purposes will be those you specified during the setup on the Key Vending Wizard page of the Properties.

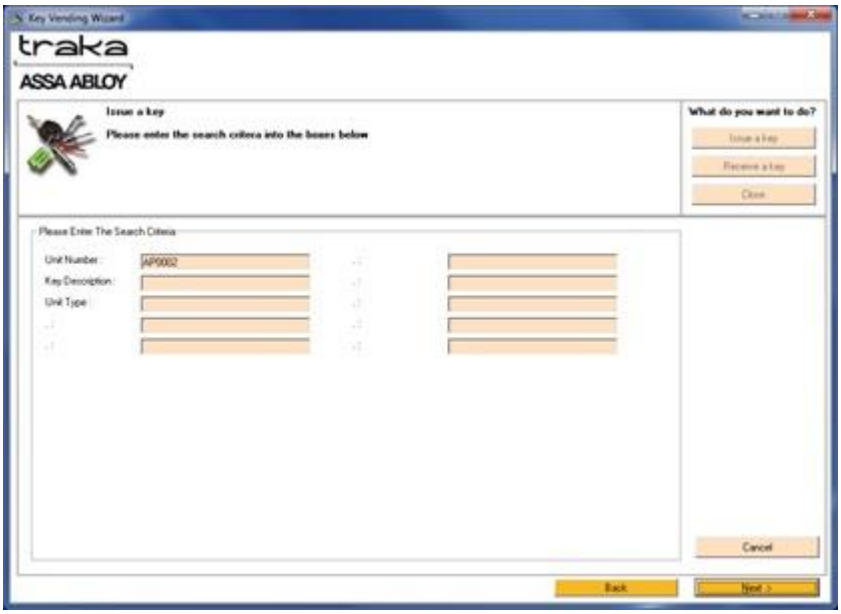


5. Once you have entered the necessary information click **Next**. If the user is not currently in the Traka32 database a message will pop up asking if you wish to create a new user record. Click **Yes** and the user will be added to the Traka32 database.



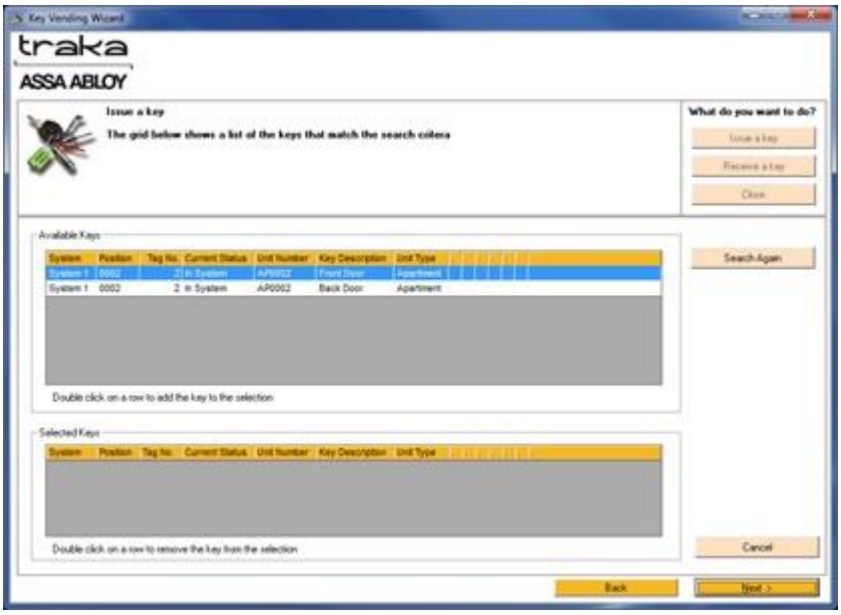
6. From the next page you can enter search criteria to find the requested key. The searchable fields available will be those specified during the setup in the Key Details of the Properties.

   In the example below the available fields are 'Unit Number' and 'Key Description'. The Unit Number has already been populated as this detail is already specified in the User Record in the example. However if you wanted to search for a different key, this field can be edited. Leaving the fields blank will search for all keys.



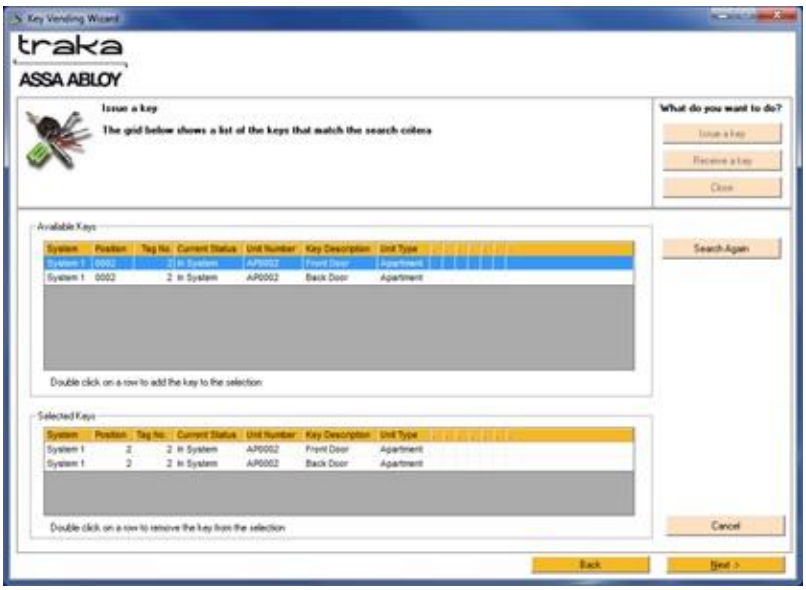
   Once you have entered the relevant search criteria click **Next**.

7. This page shows a list of keys that match the search criteria you entered on the previous page.



   Double-click on the key(s) you wish to select and they will be added to the selected keys list. You can add up to a total of 5 iFobs. If you wish to remove a key from the selected list simply double-click it.

   NOTE: If you select a key that is attached to an iFob containing other keys, all of the keys on that iFob will be added to the selected list.

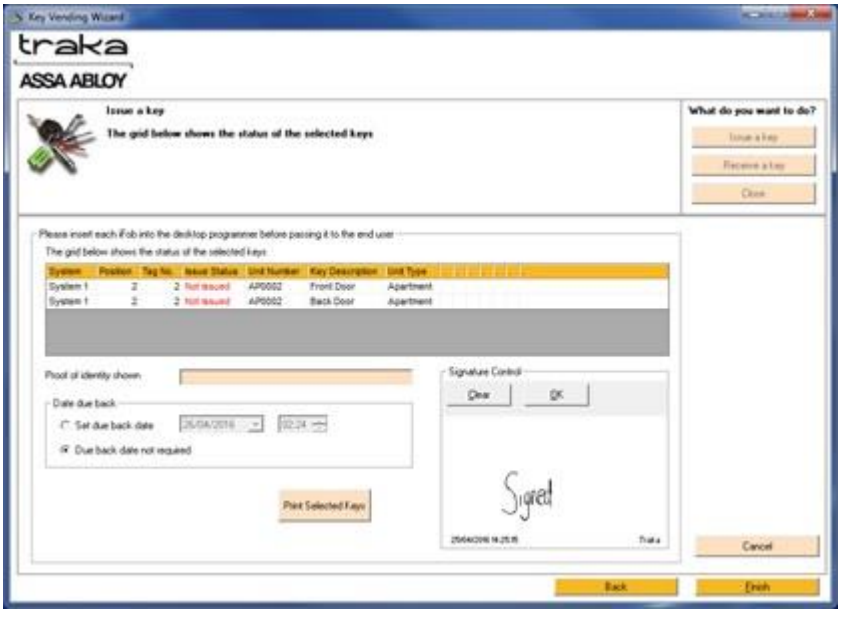


If you want to search for more keys using different search criteria, click the 'Search Again' button and you will be taken back to the search criteria page. The currently selected keys will remain selected allowing you to add to the list from your new search results.

If you select a key, or an iFob that contains a key that is a duplicate (or accesses the same apartment) of one that has already been issued, a message will pop up to warn the user that the Unit/House could be occupied.

NOTE: In this example the 'Unit Number' field is used to determine if a duplicate key (or key to the same apartment) is requested. This field can be changed on the 'Key Grouping Field' dropdown on the 'Key Vending Wizard' page of the Properties section.

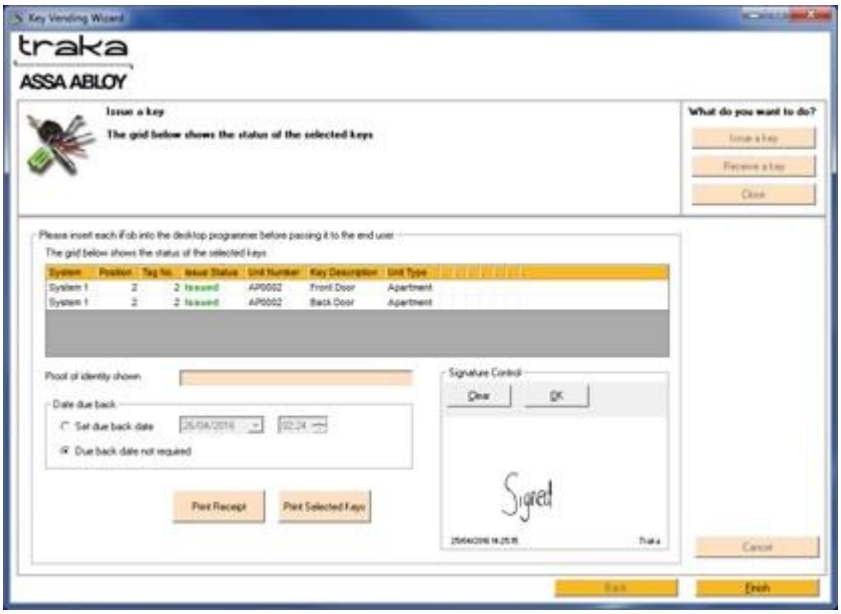
8. Once you have selected the required key(s) click **Next**. This will activate the Signature Pad allowing the Key Requestor to sign to accept receipt of the key. The signature will be displayed in the Signature Control window. Once the signature is complete the Key Requestor can select 'OK' on the Signature Pad or the Key Vendor can select 'OK' from the Signature Control window.



Note that the current status of the selected key is 'Not Issued'. The key will only become 'Issued' when it is removed from the Traka System and inserted into the USB Desktop Programmer as outlined in the next steps.

9. The Key Vendor must now remove the iFob/Key from the Traka System. The grid showing the selected keys indicates the system and position number of which they are located.

   Once the iFob has been removed from the system, insert it into the Desktop Programmer and the Issue Status will change from 'Not Issued' to 'Issued'.



NOTE: If the wrong iFob is inserted into the Desktop Programmer a warning message will pop up telling the Key Vendor that the iFob should not be issued.

10. Specify any proof of identity shown and also if there is a date and time for which the key is due back.

NOTE: It is compulsory to set a 'due back date' for a Service Request.

11. You can print a receipt for the issue of the key(s) by clicking **Print Receipt**. The receipt shows details of the Key(s) and Key Requestor and can be signed by the user to accept receipt of the key(s).

Traka Key Vending System

Key Issue Receipt

Traka ID	123456
Forename	Lee
Surname	Newell
Department / Company	Department A
Purpose	Tenant Purpose A
Issue Type	Tenant Request

Unit Number	Key Description	Unit Type	Tag No.	Issue Date / Time	Date Due Back
AP0002	Front Door	Apartment	2	25/04/2016 15:01	26/04/2016 17:00:22
AP0002	Back Door	Apartment	2	25/04/2016 15:01	26/04/2016 17:00:22

I accept by my signature below the receipt of the above keys and I agree that:

1. I will be charged for any lost or damaged keys mentioned above.
2. It will be my responsibility to return all keys mentioned above upon leaving my residence.
3. I will not change any locks in my residence.
4. I will only return these keys after final inspection of my residence by Housing Services Department.

If you have any queries regarding Key Control requirements, please e-mail ...@company.com or please call 01234 123456

Signature .....

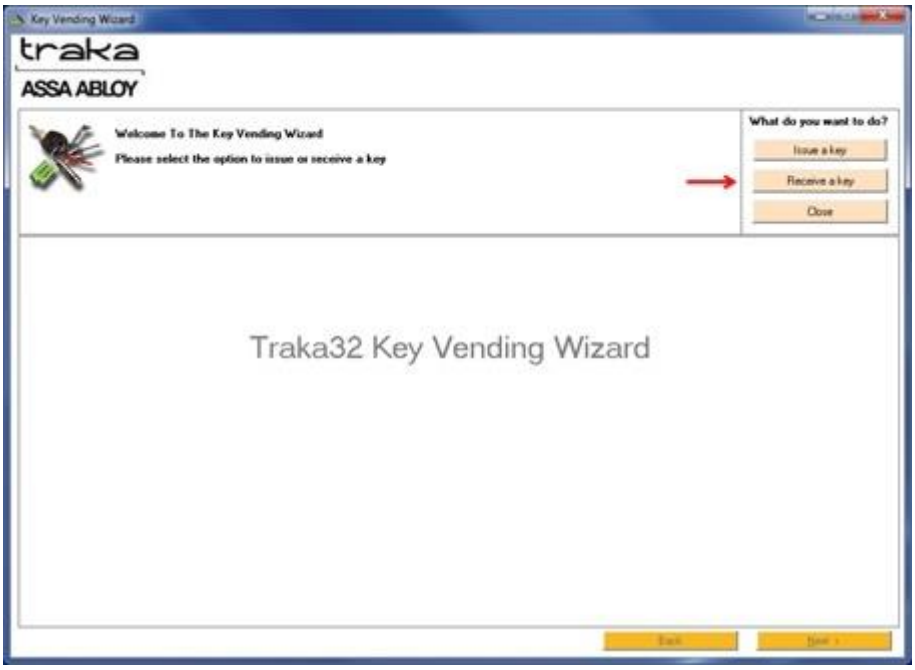
Page 1 of 1
25 April 2016

NOTE: It is possible to change the text in the paragraph beneath the key list. For more information on how to do this, refer to the section Customise Key Receipts.

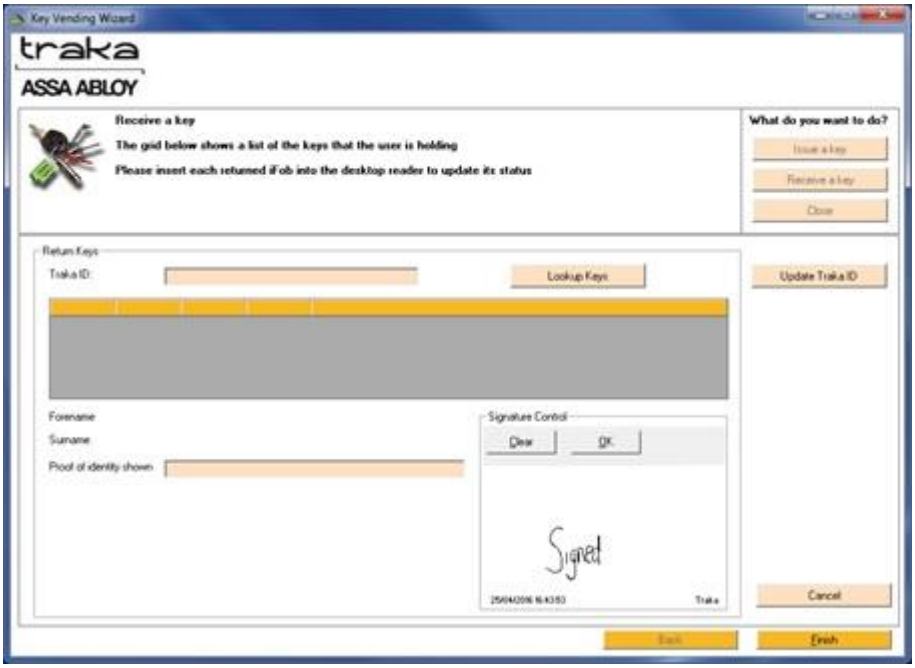
12. Click **Finish** to save the details, and the keys can then be handed over to the user.

NOTE: If the keys have been removed from the Traka System before the Key Vending Wizard process has been completed, by default you will have 15 minutes to complete the Wizard before the system assumes the key(s) have been issued without using the Wizard. If 15 minutes passes the system will generate a Key Issue Exception. More information on Key Issue Exceptions can be found in the Key Vending Reports section. To change the default time delay, refer to the section Key Issue Exception Time Delay.

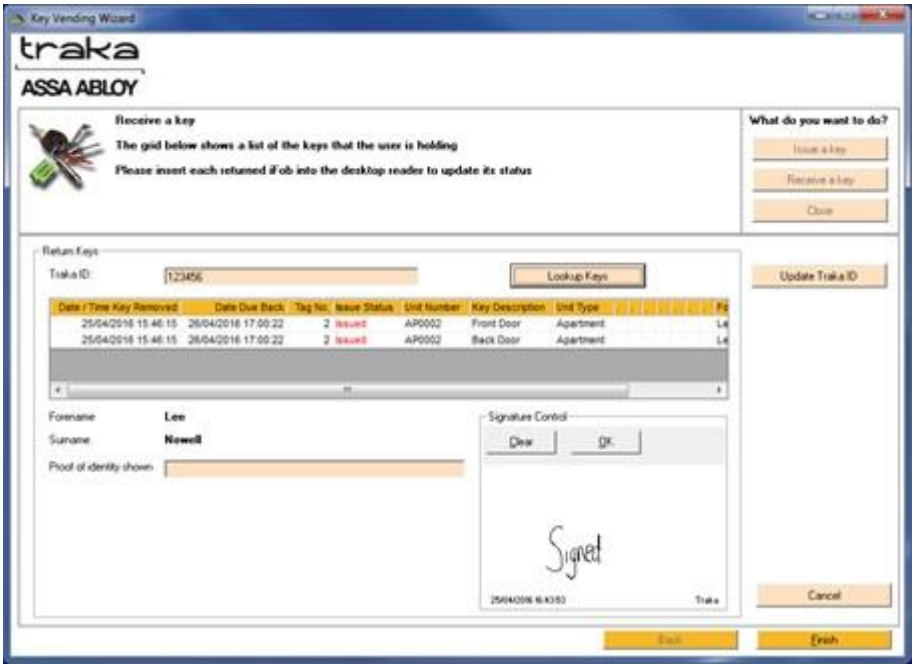
1. From the Key Vending Wizard home screen click **Receive a Key**.



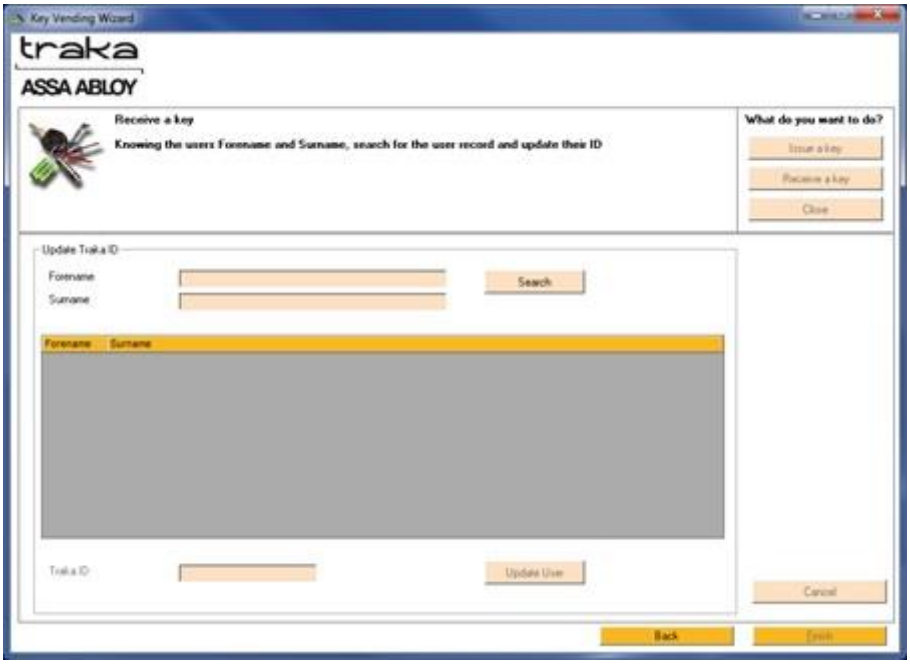
2. This will activate the Signature Pad to allow the user to sign to confirm the return of the key(s). The signature will be displayed in the Signature Control window. Once the signature is complete the Key Requestor can select 'OK' on the Signature Pad or the Key Vendor can select 'OK' from the Signature Control window.



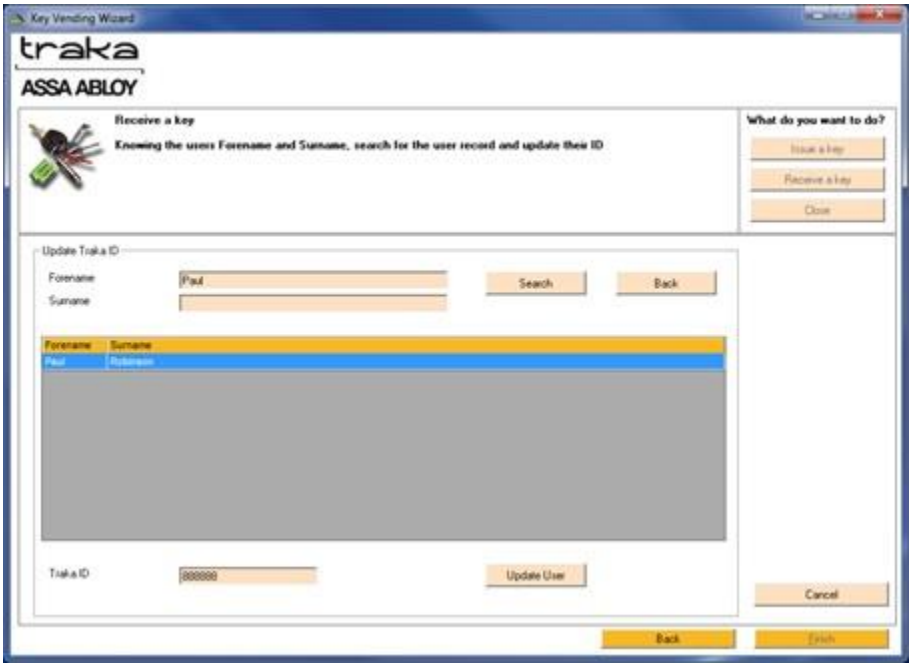
3. Enter the ID number of the user into the provided field and press **Lookup Keys**. This will display a list of the keys currently issued to that user.



If no keys are displayed it's likely that the ID number was not entered when the key was issued. In this case, click Update ID (Update Traka ID in the example). You will be prompted to enter the user's name.

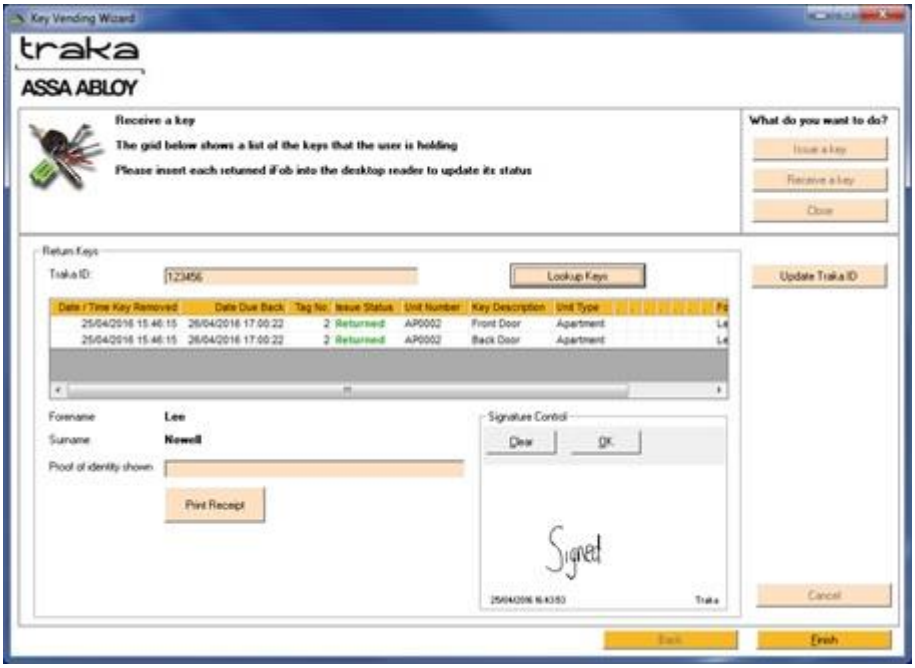


4. Enter the user's name and click **Search**. Select the correct user from the list, enter the ID number in the field at the bottom of the window and then click **Update User**.



A message will appear asking you to confirm the update. Click **Yes** and **OK** to the confirmation, and then click **Back** to return to the Key selection screen to enter the ID number as shown at the beginning of this step.

5. Insert the iFob(s) into the Desktop Programmer. This will change the Issue Status from 'Issued' to 'Returned'.



6. Specify any proof of identity shown in the provided field.

7. You can print a receipt for the return of the key(s) by clicking **Print Receipt**.

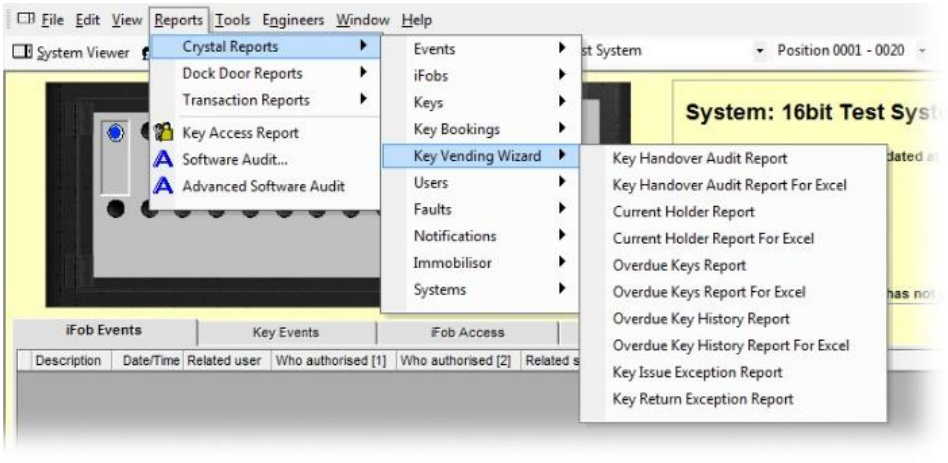
8. Click **Finish** to save the details.
9. Return the key(s) to the Traka System.

4.19.19.3.3 KEY VENDING REPORTS

The following reports can be generated for the Key Vending Wizard feature:

- Key Handover Audit Report
- Key Handover Audit Report for Excel
- Overdue Keys Report
- Overdue Keys Report for Excel
- Current Holder Report
- Current Holder Report for Excel
- Overdue Keys Report
- Current Holder Report for Excel
- Key Issue Exception Report
- Key Return Exception Report

To generate one of these reports go to **Reports>Crystal Reports>Key Vending Wizard>...**



NOTE: For details on how to filter and save reports refer to the section Event Report Viewer.

Key Handover Audit Report

The Key Handover Audit Report shows all of the transactions for keys that have been issued and returned. It shows the date and time of the key issue/return and various details of the keys and user including the user's signature that was signed during the transaction.

Key Handover Audit Report for Excel

The Key Handover audit Report for Excel will generate an Excel document based on the Key Handover Audit Report

Overdue Keys Report

The Overdue Keys Report lists all of the keys currently out of the system that haven't been returned by the date/time specified at the time they were issued. Once the key has been returned it will be removed from this list. If you require separate reports for Tenant Requests and Service Requests, simply filter by the Request Type and click 'Refresh'. This report can then be saved and will appear in the Key Vending Wizard Reports menu for future use.

Overdue Keys Report for Excel

The Overdue Keys Report for Excel will generate an Excel document based on the Overdue Keys Report.

Current Holder Report

The Current Holder Report displays a list of all the keys currently out of the system, which user they were issued to and various other details including when the key is due back.

Current Holder Report for Excel

The Current Holder Report for Excel will generate an Excel document based on the Current Holder Report.

Overdue Key History Report

The Overdue Key History Report displays a list of overdue key events that have occurred even after keys have been returned to the system.

Overdue Key History Report for Excel

The Overdue Key History Report for Excel will generate an Excel document based on the Overdue Key History Report.

Key Issue Exception Report

The Key Issue Exception Report lists all of the keys that have been removed from the Traka System but have not been issued using the Key Vending Wizard. Keys will appear in this report 15 minutes after being removed from the system if they have not been issued via the Wizard.

NOTE: If you wish to adjust the standard 15 minute time delay, please refer to the section Key Issue Exception Time Delay.

Key Return Exception Report

The Key Return Exception Report lists all of the keys that have been returned to the Traka System but have not been returned using the Key Vending Wizard. Keys will appear in this report upon the next communication after being returned to the system if they have not been returned via the Wizard.

Keys returned in this way will also show in the Key Vending Current Holder Report, despite having been returned to the system. To correct this, the iFob must be removed from the system and returned again via the Key Vending Wizard, against the user that is shown as the current holder.

4.19.19.3.4 KEY VENDING EMAILS

An email is generated for any keys that are overdue, or if they have been removed from or returned to the Traka System without using the Key Vending Wizard (Key Issue Exception and Key Return Exception).

The recipients of the emails can be specified in File>Properties>Key Vending Wizard in Traka32. Refer to the Properties section in this guide for more information.

An example of an email sent for returning a key without using the Key Vending Wizard is shown below:


From: Traka Key Vending System
To:
Cc:
Subject: Key Return Exception For Tag Number: 11
Sent: Thu 24/03/2016 10:58

The following key has been returned to a cabinet but it was not returned using the Key Vending Wizard:

Date / Time Key Issued	24/03/2016 10:57:43
Date / Time Returned To Cabinet	24/03/2016 10:58:09
Key Returned by	Lee Newell
Tag	11
Access Level	1
System Title	System 1
Position	11
Unit Number	AP0011
Key Description	Front Door
Unit Type	Apartment

NOTE: 'Key Issue Exception' emails are generated 15 minutes after the key has been removed from the system. To edit the length of this time delay refer to the section Key Issue Exception Time Delay.

'Key Return Exception' emails are generated immediately.

4.19.20 KEY WEIGHING

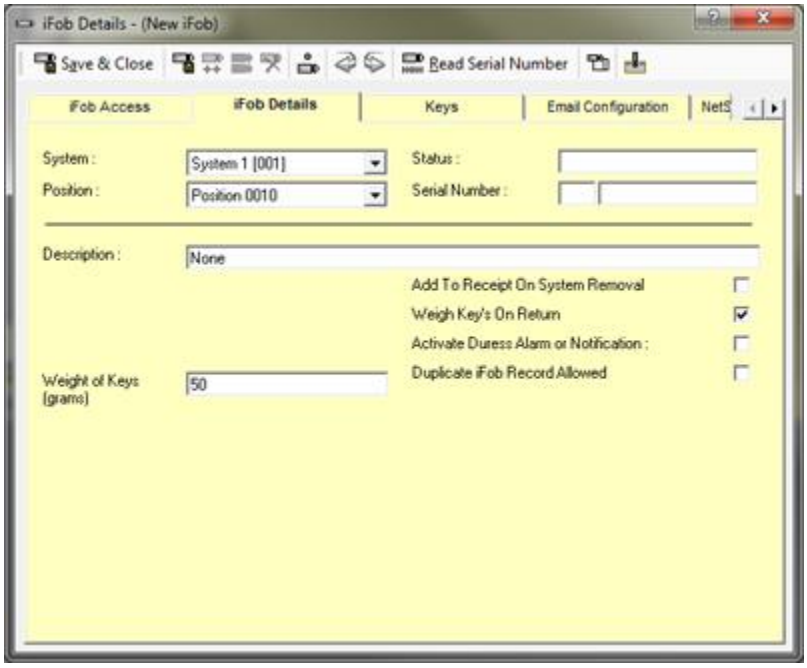
Traka32 has the facility to weigh keys when they are returned to the cabinet, this is designed to check that no keys have been removed from the iFob or tampered with whilst they have been out of the cabinet. Key Weighing is a cost option and will need to be enabled in the firmware. You will also need to have your own set of scales that Traka can integrate into the system.

The Key Weighing feature allows you to set a weight for individual sets of keys. You can also set a tolerance weight within the firmware which means when the keys are returned to the cabinet the software will check if the key bunch is within the tolerance set. If the key bunch is over or below the tolerance, then an event will be generated in Traka32 to display this.

NOTE: The Tolerance set in the firmware applies to all keys in the system.

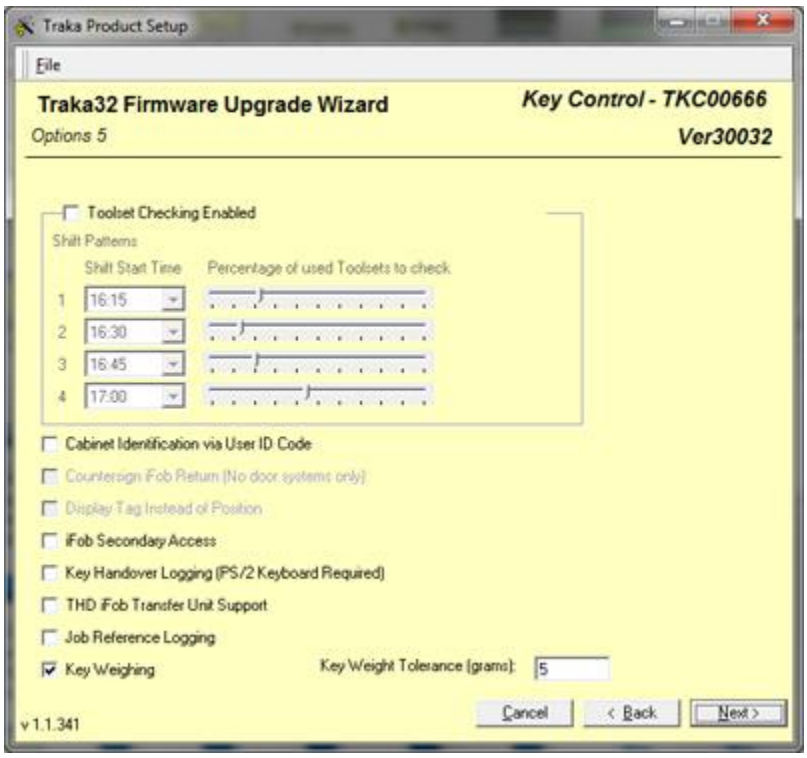
Setting the Key Weight Tolerance

Right click the desired iFob and select iFob Details. From there navigate to the iFob Details Page. You will then be able to tick the weigh keys on return option. This will enable the use the 'Weight of Keys' field, simply enter the weight of the keys and click Save and Close.



Setting the Key Weight Tolerance

Right click the cabinet pod in the system viewer and navigate to 'Configure Firmware'. Navigate to the Options 5 page and at the bottom you will see the Key Weighing option enabled along with a Tolerance field, simply enter the desired tolerance and continue through the wizard and save and close at the end.



4.19.21 KEY WIZARD

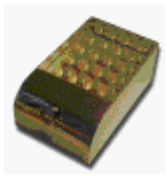
4.19.21.1 KEY WIZARD OVERVIEW

The new Traka32 Key Wizard allows quick and easy access to adding, maintaining and searching key records within Traka32. It incorporates a quick lookup facility using the Traka Desktop iFob Programmer allowing users to identify the keys in an instant and also allow quick allocation and de-allocation of keys. The Key Wizard also includes optional links through to third party systems such as Dealer Management software to import existing key information and also third party key readers.

The Key Wizard is a simple user interface that has three modes of operation that allows a quick way to find a key record in Traka32.

- This allows a quick text search to be carried out to find a key record.

- This allows a search to be carried out by inserting a Traka iFob into the Traka Desktop iFob Programmer.



- This allows a search to be carried out by inserting a BMW Key into the BMW Desktop Key Reader.

If no key record can be found in the Traka Database, the key record can be quickly imported from Kerridge.

Once a key record has been found it can be allocated too or de-allocated from an iFob at the click of a button.

Key records can also be edited if required.

4.19.21.2 CONFIGURATION AND GENERAL

Configuration

Optionally you can get Traka32 to launch the Key Wizard automatically when Traka32 is loaded.

Set the **Window Open on Application Start** to...

a. Key Wizard – This will open the key wizard in full edit mode allowing keys to be allocated, de-allocated and edited.

b. Key Wizard [Search Only] – This will open the key wizard in search only mode. The use will not be able to allocate, de-allocate or edit key records.

General

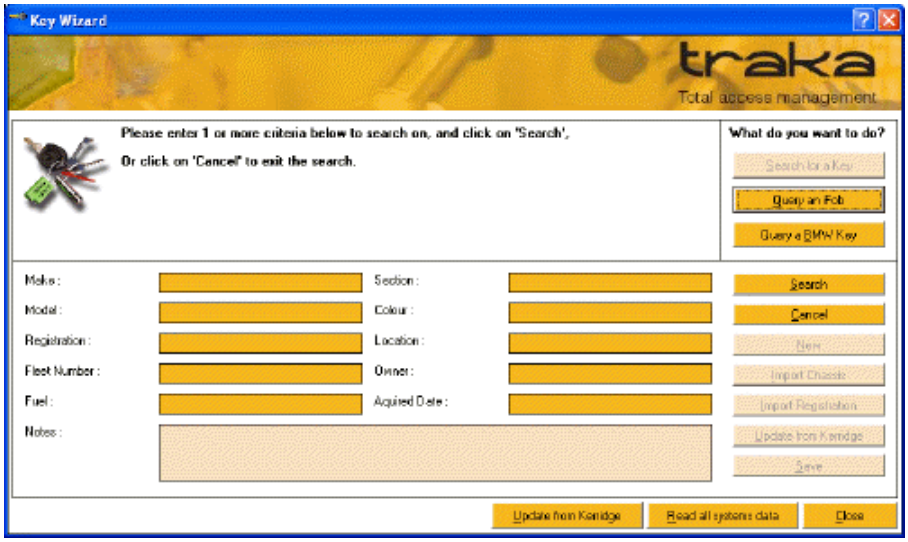
If you have configured the Key Wizard to open automatically when the application starts, and you need to get to other areas of the Traka32 software, simply hold down the **F9** key and click on **Close**.

Update from Kerridge

The update from Kerridge utility will check each key record in the Traka32 database can compare it with Kerridge. If there are any differences the Traka32 database will be updated accordingly.

4.19.21.3 SEARCH FOR A KEY

If you do not have an iFob or BMW Key to hand, it is possible to search for a Key in the Traka Database.



1. Click on **Search for a Key**
2. Type in a 1 or more search criteria and click on **Search**
3. If no keys were found, you can do the following...
    a. Click on **New** to manually add a new key record.

    Simply type in the new details and click on **Save** to save the new record or **Cancel** to discard the new key record.

    b. Click on **Import Chassis** to import a key record from Kerridge based upon a Chassis Number.

    Simply confirm the chassis number and click on OK.

    Traka32 will attempt to find a match in Kerridge.

    If a match was found then click on **Save** to save the new record or **Cancel** to discard the new key record.

    c. Click on **Import Registration** to import a key record from Kerridge based upon a Registration Number.

    Simply confirm the chassis number and click on OK.

    Traka32 will attempt to find a match in Kerridge.

    If a match was found then click on **Save** to save the new record or **Cancel** to discard the new key record.
4. If the key was found, you can do the following...
    a. Insert an iFob into the Traka Desktop iFob Programmer and click on **Allocate Key to iFob** to allocate the key to an iFob.

    If there is no Traka Desktop iFob Programmer, select and iFob and click on **Allocate Key to iFob**.

    b. Insert an iFob into the Traka Desktop iFob Programmer (if available) and click on **Remove Key from iFob** to de-allocate the key to an iFob.

    c. Click on **Edit Key Record** to edit the key record.

    Simply amend details and click on **Save** to save the changes or **Cancel** to discard the changes.

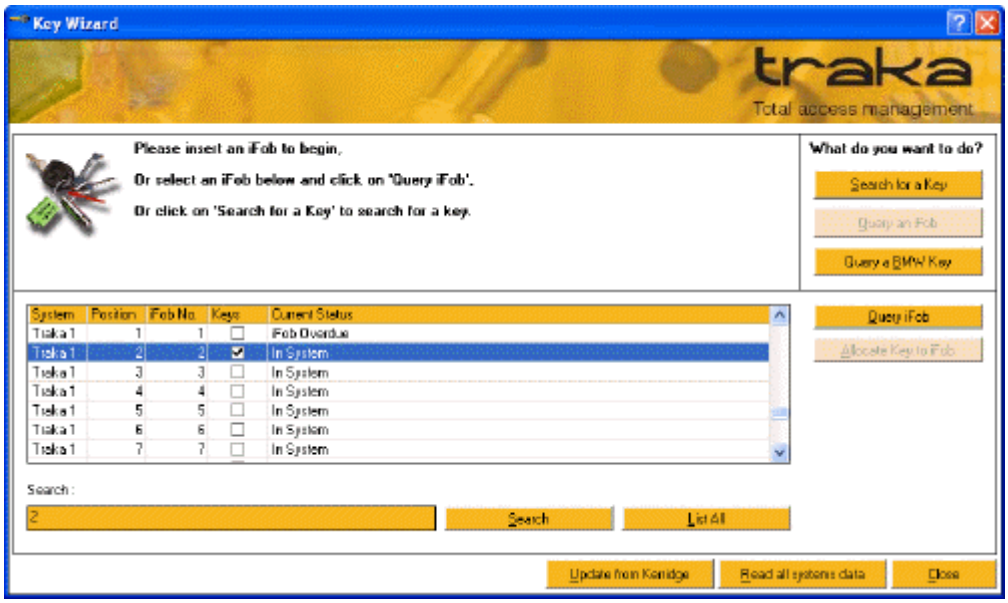
d. When editing a Key Record it is also possible to update the details from Kerridge by clicking on the **Update from Kerridge** button. This will cross reference the Kerridge database via the Chassis or Registration and update all the mapped Key Record fields.

5. To clear the search criteria simply click on **Clear.**

6. To cancel any changes simply click on **Cancel.**

4.19.21.4 QUERY AN IFOB

It is possible to search for a Key in the Traka Database using the Traka iFob.



1. Click on **Query an iFob**

2. Insert an iFob into the Traka Desktop iFob Programmer.

3. If there is no Traka Desktop iFob Programmer or you do not have the iFob to hand, either...

   a. Enter a Search detail such as System, Position or iFob No. into the search field and click on **Search**. If a match is found, select and iFob and click on **Query iFob.**

   b. Click on **List All**, select and iFob and click on **Query iFob**.

4. If no keys were found, you can do the following...

   a. Click on **Search for a Key** or **Query a BMW Key** to search for a key record.

5. If the key was found, you can do the following...

   a. Insert an iFob into the Traka Desktop iFob Programmer (if available) and click on **Remove Key from iFob** to

de-allocate the key to an iFob.

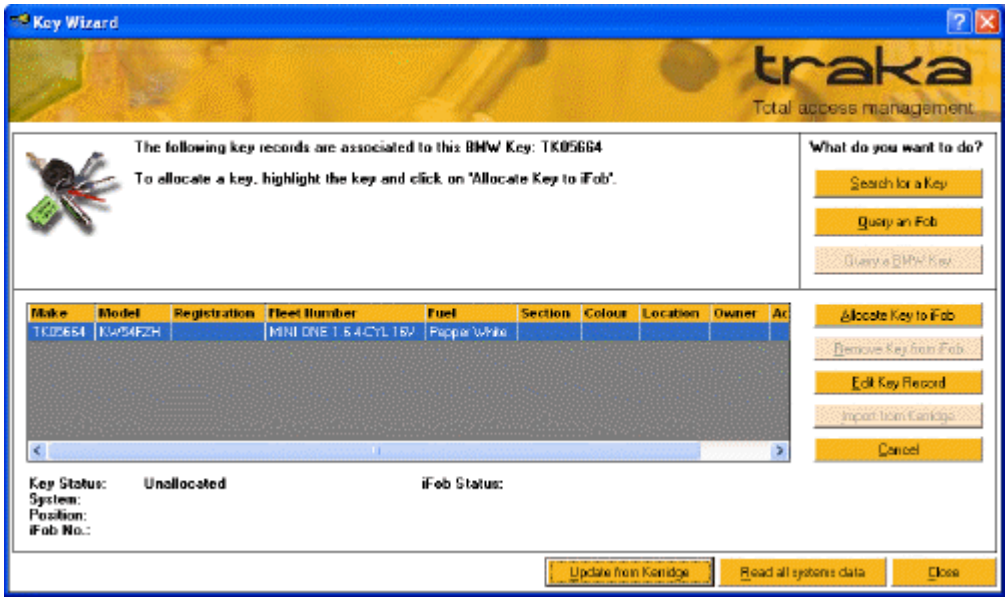
   b. Click on **Edit Key Record** to edit the key record.

Simply amend details and click on **Save** to save the new record or **Cancel** to discard the new key record.

6. To clear the search, simply remove the iFob from the Traka Desktop iFob Programmer or click on **Cancel**.

4.19.21.5 QUERY A BMW KEY

It is possible to search for a Key in the Traka Database using the BMW Key Reader.



1. Click on **Query a BMW Key**
2. Insert a BMW or Mini Key into the BMW Key Reader.
3. If no keys were found, you can do the following...
    a. Click on **Search for a Key** or **Query a iFob** to search for a key record.
    b. Click on **Import from Kerridge** to import a key record from Kerridge based upon a BMW Key's Chassis Number.

    Simply confirm the chassis number and click on OK.

    Traka32 will attempt to find a match in Kerridge.

    If a match was found then click on **Save** to save the new record or **Cancel** to discard the new key record.
4. If the key was found, you can do the following...
    a. Insert an iFob into the Traka Desktop iFob Programmer and click on **Allocate Key to iFob** to allocate the key to an iFob.

    If there is no Traka Desktop iFob Programmer, select and iFob and click on **Allocate Key to iFob**.
    b. Insert an iFob into the Traka Desktop iFob Programmer (if available) and click on **Remove Key from iFob** to de-allocate the key to an iFob.
    c. Click on **Edit Key Record** to edit the key record.

    Simply amend details and click on **Save** to save the new record or **Cancel** to discard the new key record.

4.19.21.6 ALLOCATE KEY TO IFOB

1. First of all search for an iFob record by clicking on **Search for a Key** or **Query a BMW Key**. Please refer to the relevant sections of this guide.
2. Once the key record has been found, insert an iFob into the Traka Desktop iFob Programmer and click on **Allocate Key to iFob** to allocate the key to an iFob.

   If there is no Traka Desktop iFob Programmer, select an iFob and click on **Allocate Key to iFob**.

   NOTE: Inserting the iFob in the Traka Desktop iFob Programmer will ensure the description is written to the iFobs memory for searching.
3. The key record data will get written to the iFob for searching at the Traka Cabinets.

4.19.21.7 REMOVE KEY FROM IFOB

1. First of all click on **Query an iFob**
2. Insert an iFob into the Traka Desktop iFob Programmer (if available).

   NOTE: Inserting the iFob in the Traka Desktop iFob Programmer will ensure the description will be removed from the iFobs memory.
3. Highlight the key record that you wish to remove from the iFob and click on **Remove Key for iFob**.
4. The key record data will get removed from the iFob freeing it up for re-use.

4.19.22 LOCATION STORING

Location Storing or Bay Logging as it's also referred to, allows users to record the current location of a vehicle or item.

Every time a user returns an iFob they will be prompted for a location. The user can use the keypad to enter letters and numbers to make up a location description.

The location can be looked up at any time using the Lookup Facility.

NOTE: Bay Logging will only be available if the firmware of the selected system has Bay Logging enabled. If the Bay Logging option is enabled in the firmware, it is also possible to enable / disable the option on an iFob per iFob basis from the iFob Details window.

Removing an iFob

When a user removes an iFob from the 16bit system, the screen will display the last location of the vehicle or item for that particular slot.

Returning an iFob

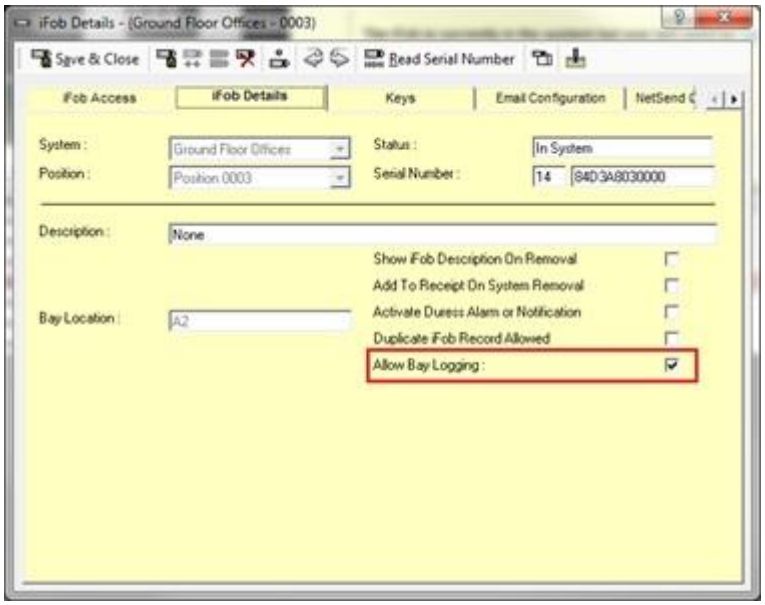
When a User returns an iFob to the 16bit system, they will be required to enter details of the vehicles current location followed by pressing the **#** key.

If a user fails to enter a location, a 'Location not entered' event is generated in Traka32. These events can also be seen in reports.

The location entered is also displayed in the information panel in the system viewer window.

Enabling/Disabling the option on a per iFob basis

The option can be enabled/disabled per iFob from the iFob details window. Right click on the chosen iFob and select **Edit iFob Details**, and then select the **iFob Details** tab.



By default all iFobs will have the bay logging (location storing) option switched on. To switch off for a particular iFob simply uncheck the box and click **Save & Close**.

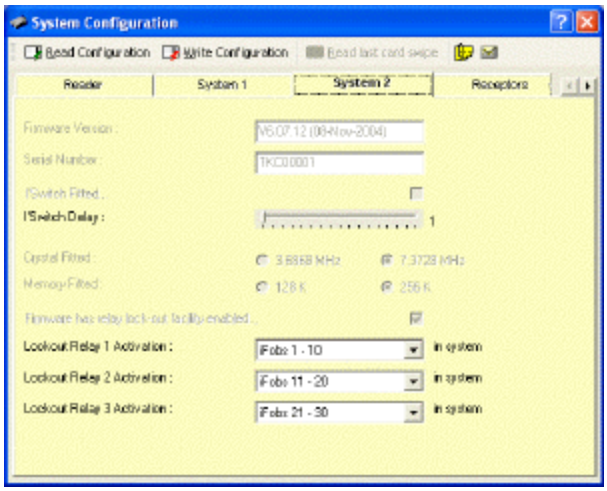
4.19.23 LOCKOUT FACILITY

4.19.23.1 RECEPTOR STRIP LOCKOUT FACILITY OVERVIEW

The Receptor Strip Lockout Facility enables the control of the three relays fitted to the Control PCB. The relays can be programmed to activate / de-activate depending on the status of the iFobs within certain receptor strips. This can be used as a safety lockout facility.

For example, if Relay 1 is assigned to the top receptor strip (I.e. slots 1 to 10). If one or more of the iFobs in the top receptor strip (iFobs 1 to 10) are out of the system then Relay 1 will deactivate. When all the iFobs in the top receptor strip are in place then the Relay 1 will activate.

The relays can be assigned to the relevant receptor strips using the Configure Firmware utility.



The default setup is...

- Slots 1 to 10 = Relay 1
- Slots 11 to 20 = Relay 2
- Slots 21 to 30 = Relay 3

NOTE: When this option is enabled, the relays cannot be configured to operate in any of the alarm conditions.

4.19.23.2 SYSTEM LOCKOUT FACILITY OVERVIEW

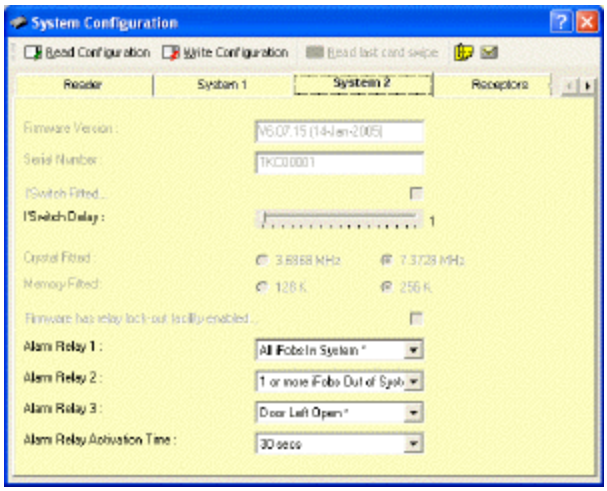
The System Lockout Facility enables the control of the three relays fitted to the Control PCB. The relays can be programmed to activate / de-activate depending on the status of all the iFobs within the system. This can be used as a safety lockout facility.

For example...

- If Relay 1 is assigned to the **1 or more iFobs Out Of System**, if one or more of the iFobs are out of the system then Relay 1 will activate. If all the iFobs are in the system then Relay 1 will deactivate.

- If Relay 1 is assigned to the **All iFobs In System**, if all the iFobs are in the system then Relay 1 will activate. If one or more of the iFobs are out of the system then Relay 1 will deactivate.

The relays can be assigned to the relevant receptor strips using the Configure Firmware utility.



4.19.24 MICRO TRAKA

4.19.24.1 MICRO TRAKA OVERVIEW

Micro Traka is an extension to Traka that places the keys in separate units that are located close to each door that the system provides access to, rather than having the keys attached to each iFob in the cabinet. When a user takes an iFob from the cabinet, it is programmed with their profile that determines which Micro Traka units they have access to. To access the key held in the Micro Traka unit, the user places their iFob in to the appropriate slot and, if the permissions match, the user can extract the iFob with the key attached. When the user returns the key, history information is written in to the user's iFob that is downloaded to Traka32 when the user eventually returns the iFob to the cabinet. A history for each user is then built up, showing to which units and at what times the user has been.

When integration with Micro Traka is enabled in the software, a global Site Code, Office Code and Building Code are specified, together with the Emergency Sequence to release the iFobs from the unit. These settings are applied to all Micro Traka Units that are programmed by iFobs extracted from the cabinet. For a user to be granted access to the key in the Micro Traka Unit, the Site Code, Office Code and Building Code must match.

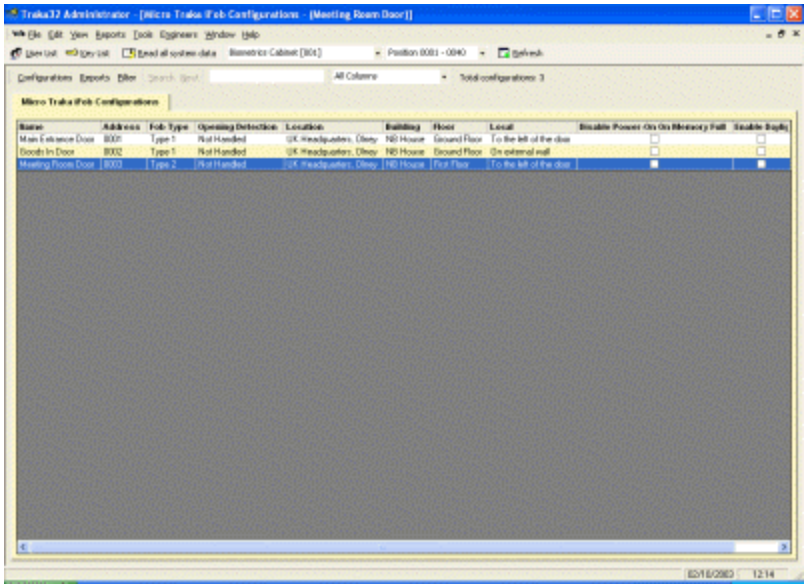
Each Micro Traka unit is then programmed with an Address and, optionally, a Type. This allows fine control over which keys a user may have access to.

Using the Micro Traka System

- To enable Integration with Micro Traka, use the System Details window.
- To create a Micro Traka Unit configuration iFob, use the Micro Traka iFob Configurations window.

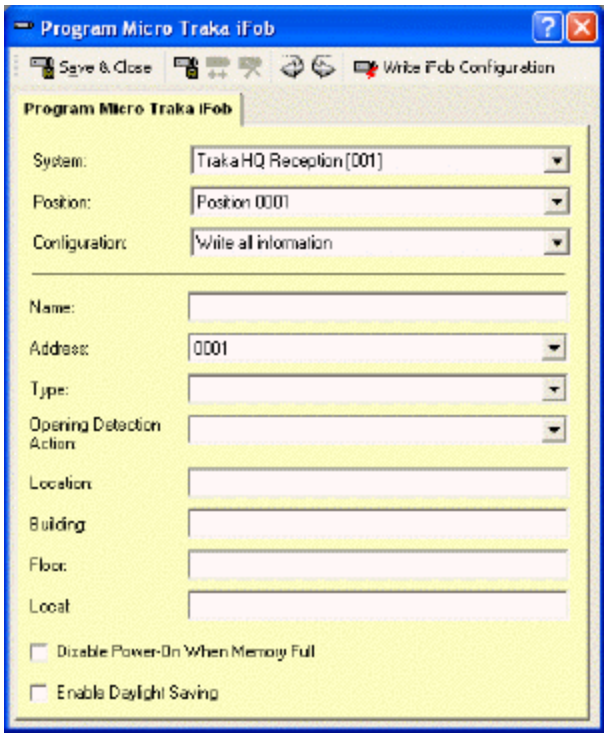
4.19.24.2 MICRO TRAKA IFOB CONFIGURATIONS

From the main screen click **View**, **Micro Traka iFob Configurations** and a list of the currently defined configurations will be displayed.



- To create a new configuration click **Configurations, Add New** and the Program Micro Traka iFob dialog will be opened with blank settings.
- To edit an existing configuration, select the configuration in the list and click **Configurations, Edit Configurations**. The Program Micro Traka iFob dialog will be opened with the settings of the selected configuration.
- To delete an existing configuration, select the configuration in the list and click **Configurations, Delete**.

4.19.24.3 PROGRAM MICRO TRAKA IFOB



System

Select the system in which the iFob to be programmed resides.

Position

Select the position in which the iFob to be programmed resides.

Configuration

Select the type of configuration to be written to the iFob:

- **Write all information;** All configuration information for the unit is written to the iFob.
- **Write configuration without date or address;** All configuration information for the unit except the date and address is written to the iFob.
- **Write configuration without date;** All configuration information for the unit except the date is written to the iFob.
- **Write date only;** Only writes the current date/time to the iFob.

Name

Enter the name of the configuration.

Address

Select the address of the configuration.

Note: An address can only be associated with one configuration.

Type

Select the type of the Micro Traka unit.

Opening Detection Action

Select the action that will be taken when the door of the unit is opened.

Location, Building, Floor and Local

Labels associated with the configuration to describe the location of the Micro Traka unit.

Disable Power-On When Memory Full

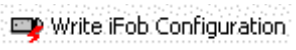
Check to enable the 'Disable Power-On When Memory Full' option.

Enable Daylight Saving

Check to the enable Daylight Saving.

To save the configuration, click  or 

.

To write the configuration to the selected iFob (defined by **System** and **Position**), click 

.

4.19.24.4 SPECIAL IFOBS

There are five special types of iFobs available for management of the Micro Traka system. These are programmed via the iFob menu on the System Viewer window:

- **Priority;** allows an administrator access to any Micro Traka unit, ignoring the address, type and validity dates.
- **Service;** allows an administrator to configure a new key iFob in a Micro Traka unit.
- **Blacklist;** defines the list of blacklisted iFobs which cannot be used in a Micro Traka unit. The list of iFobs is generated from the 60 most recently deleted iFobs.
- **Date/Time;** programs the current date/time in a Micro Traka unit
- **History;** used for diagnostics, allows the history of a Micro Traka unit to be downloaded to an XML file.

4.19.25 MILEAGE LOGGING

4.19.25.1 MILEAGE LOGGING OVERVIEW

Mileage Logging as its name suggests allows a user to record the current mileage of a vehicle or hour's usage in the case of a forklift truck.

Every time a user returns an iFob they will be prompted for the vehicles mileage. The mileage must be a number between 0 and 999,999.

Traka will know what the value of the previous mileage entered and will not allow a user to enter a value lower than the current mileage. However mistakes can be made and this value can be edited through the Traka32 software within the iFob Details window.

When the user has entered the mileage Traka will confirm the value and ask the user to confirm. The user then has the change to confirm the mileage or go back and change the value.

See also the Trip Mileage section.

NOTE: Mileage Logging will only be available if the firmware of the selected system has Mileage Logging enabled. If the Mileage Logging option is enabled in the firmware, it is also possible to enable / disable the option on an iFob per iFob basis from the iFob Details window.

4.19.25.2 TRIP MILEAGE OVERVIEW

A new feature of Mileage Logging is the Trip Mileage which is the distance travelled for each journey. A simple calculation is made by simply subtracting the previously entered mileage with the newly entered mileage to give the trip mileage.

The Trip Mileage is shown on all the usual transaction and event reports. If you have upgraded from previous version of Traka32 (version 02.04.0001 or earlier) the Trip mileage values will not have been previously calculated. To calculate the previous Trip Mileage vales simply follow these steps...

1. Click on **View**, **iFob List** from the main menu and the iFob List will open.
2. Click on the **iFobs** menu followed by **Re-process the Trip Mileage values**.
3. All the Trip Mileage values will be calculated automatically.

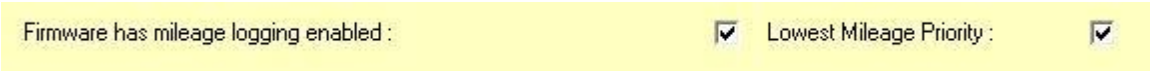
NOTE: Trip Mileage will only be available if the firmware of the selected system has Mileage Logging enabled. If the Mileage Logging option is enabled in the firmware, it is also possible to enable / disable the option on an iFob per iFob basis from the iFob Details window.

4.19.25.3 LOWEST MILEAGE LOGGING PRIORITY

Lowest Mileage Logging is an 'add on' feature to the original Mileage Logging. When a user authenticates themselves at the system, the appropriate LED will illuminate and release the vehicle key that has the lowest mileage out of other vehicles within same access level.

For example if there are 10 Cars setup with Access Level 1 and 10 Vans with Access Level 2 and a user logs in that has access to Cars and a Vans (the users has access levels 1 & 2), the system will give them access to only 1 Car and 1 Van each with the lowest mileage of that access level.

Your Traka system must consist of IRS (Intelligent Receptor Strips). This is clearly show which iFob/s can or cannot be removed once the user has gained access the system. The Lowest Mileage Logging option requires both 'Mileage Logging' and 'Lowest Mileage Priority' to be enabled within the firmware.



User Procedure

1. The user identifies his/herself at the cabinet.
2. Depending on what access levels the user currently has, one or more LED's will illuminate Green (for keys that the user can't take the LED will illuminate Red).
3. The position solenoid will release allowing the user to remove the key/s with the lowest mileage.
4. When the user returns the key they will need to enter the vehicles new mileage number and press hash (#).

iFob Allowance Per Access Level

Lowest Mileage Logging can be very effective when used in conjunction with iFob Allowance Per Access Level. If a user has an iFob Allowance of 0 (unlimited), and takes a key to a vehicle with the lowest reading, the system will re-calculate the next available iFob with lowest reading and then grant access to that iFob. Therefore allowing the user to continuously remove iFobs. However if a user has an iFob Allowance of 1, when they remove a key to a vehicle with the lowest reading, they will not be able to take any further keys.

4.19.26 REASON CODE LOGGING

4.19.26.1 REASON CODE LOGGING OVERVIEW

Reason Code Logging simply allows a user to log a reason for taking an iFob from the Traka System.

Every time a user returns an iFob they will be prompted for a reason code. The reason code is simply a number between 0 and 15...

Once the value has been entered the user simply presses # to confirm the value or * to edit the value.

Each reason code will appear in the Traka32 software against each iFob and Key transaction.

NOTE: Reason Code Logging will only be available if the firmware of the selected system has Reason Code Logging enabled. If the Reason Code Logging option is enabled in the firmware, it is also possible to enable / disable the option on an iFob per iFob basis from the iFob Details window.

4.19.27 RANDOM RETURN

4.19.27.1 FIXED / RANDOM RETURN OVERVIEW

Fixed Return to a Single System (FRSS) allows an iFob to be assigned to a specific slot in a specific system.

Random Return to a Single System (RRSS) allows an iFob to be assigned to any slot in a specific system.

Random Return to Multiple Systems (RRMS) allows an iFob to be assigned to any slot in any system.

Fixed & Random return within the same Database

Traka32 is now able to have a combination of Fixed & Random return cabinets within the same database from software version v02.09.0000 and above. For this to work you will require this option to be enabled within the firmware on the fixed return cabinet/s within the database.

4.19.27.2 SINGLE SYSTEM

4.19.27.2.1 RANDOM RETURN TO A SINGLE SYSTEM OVERVIEW

Random Return to a Single System (RRSS) allows iFobs to be returned to any slot within a single system.

The iFobs can then be taken and returned to any slot within that system.

The iFobs will not be recognised if placed into another system as with fixed return systems.

Random Return to Single Systems Setup

The iFobs are referenced in Traka32 with the Index Number.

The iFobs are configured in the same manner as fixed return. When the iFobs are configured they are allocated an 'iFob Index Number' which is a number of equal value to the slot the iFob was in when configured.

NOTE: This index number is based upon each system so if you have two RRSS system there will be more than one iFob with the same Index Number.

4.19.27.3 MULTIPLE SYSTEMS

4.19.27.3.1 RANDOM RETURN TO MULTIPLE SYSTEMS OVERVIEW

Random Return to Multiple Systems (RRMS) allows any iFobs to be returned to any slot within any RRMS system.

The system will accept any iFob that is returned to the system. Access levels, access times, curfews and iFob pairs still apply but are all set to a default when a new iFob is returned (The default gives all access at all times).

When an iFob is taken, the system will clear all information from its internal memory about the iFob that was the slot freeing up for the next iFob. The event data is not cleared and will be available for download.

What's different in Traka32?

Other than the way in which iFobs are set up and referenced by the iFob Index number, not much else has changed. Users and Keys are configured in the normal manner.

Some functions in the software will not be available such as some reports, the key tree and certain iFob options such as iFob Pairing and iFob curfews (although these options may be re-added in the future).

What's different on the Traka Systems?

The RRMS systems will work in much the same way as RRSS systems but you can put any iFob into a system.

The keypad can be used to look up the last users of an iFob and other option information such as Current Fault Status, Location and/or Mileage but you must use the iFob Index number to reference the iFob and not the slot number as with FRSS systems.

A new optional feature has also been added so that you can store a description in the iFob. With the door closed you can press the * key on the keypad and type in all or part of an iFobs description to search for its location within that system. If the iFob is not in the system the iFob cannot be located with this method and the Traka32 software should be used.

What options will not work with RRMS systems?

The following options will **not** work with RRMS...

NOTE: This is based upon firmware version 6.07.10. Newer version may have more functionality.

- iFob Curfews
- iFob Pairing
- Micro Traka
- Traka Immobilisor
- Siemens Fire Control
- Vehicle Cost Logging

All other options will work as normal.

4.19.27.3.2 RANDOM RETURN TO MULTIPLE SYSTEMS SETUP

Overview

The only difference in setting up the Traka system with RRMS is in the iFobs. In a FRSS or RRSS system, you would normally have to synchronise the iFobs. In RRMS, the systems will accept any iFob automatically.

If the iFob has memory (Data 32 or Data 512) then the system will read the contents of the iFobs memory.

If the iFob has been pre-programmed, the system will use this information to determine the iFobs Access Level, Access Times and optionally Current Fault Status, Description and/or Mileage.

If the iFob has not yet been programmed, the system will program the iFob with a default set of access being Access Level 1 and 24 Hour Access.

If the iFob does not have memory (Standard iFob) then the system will reject the iFob.

To make the iFob records appear in the Traka32 software all you have to do is Read All System Data. The Traka32 software will automatically check if the database has a record for that iFob, if not it will create one.

When an iFob with memory has been programmed with the default information, this information can then be altered with the relevant access levels and access time etc. You can edit the iFob in the normal way and save the changes.
NOTE: The iFob must be in the location shown the iFob Details window for the information to be written to the iFob.

If you reset a system or synchronise a system you will hear the system beep x times, once for each iFob. When the system is reset, no information will be available on the iFobs status and the system will automatically book them in. This is normal.

When an iFob is put into the system for the first time and the Read All System Data is performed, the new record in the database will be assigned an iFob Index number. This number can then be used to look up information on the iFob from the Traka32 software and from the system's keypad.

NOTE: We would normally recommend that you attached a tag to each iFob displaying the iFob's Tag number for easy reference. Please refer to the next section for details on how to assign the iFob tags.

Setting up the systems

In order for the system to assign the iFob Index numbers in a logical order the following procedure should be followed:

1. Install Traka32 as normal.

   NOTE: Ensure you are starting with a blank database.

2. Configure each system as normal. See Configuring Systems.

   NOTE: If you are using the Remote Host function, ensure this is switched off at this point.

3. Ensure all the iFobs are in the systems.

4. From the Traka32 software's System Viewer, right click over the picture of the system click the **Engineers** tab and then click **Reset All Data iFobs**.

5. Repeat step 4 for each system.

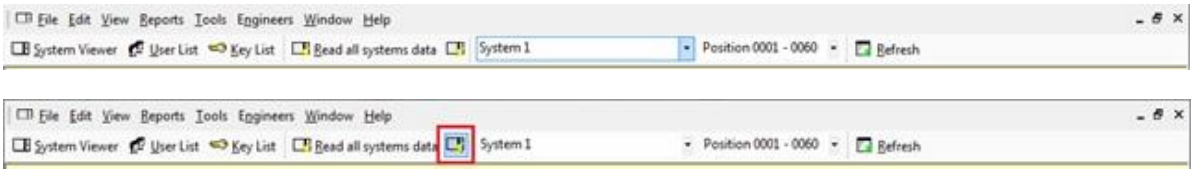
   NOTE: Do NOT click Read All System Data at this stage.

6. From the Traka32 software's System Viewer, right click over the picture of the system and click on **Synchronise System**. Say **No** to the first message and **Yes** to the second. You will hear the system beep x time, once for each iFob.

7. Repeat step 6 for each system.

   NOTE: Do NOT click Read All System Data at this stage.

8. When you have synchronised each system, select the first system from the system dropdown and then click the Read Selected System Data button as highlighted below.



9. Repeat step 8 for each system **in order**.

   NOTE: It is very important that you read the system data in the order in which the iFob Tags are allocated.

10. From the Traka32 software's System Viewer, right click over the picture of the system and click on **Engineers>Synchronise iFobs**. This will write the assigned iFob Indexes into the Data iFobs memory which can then be used for iFob Searching.

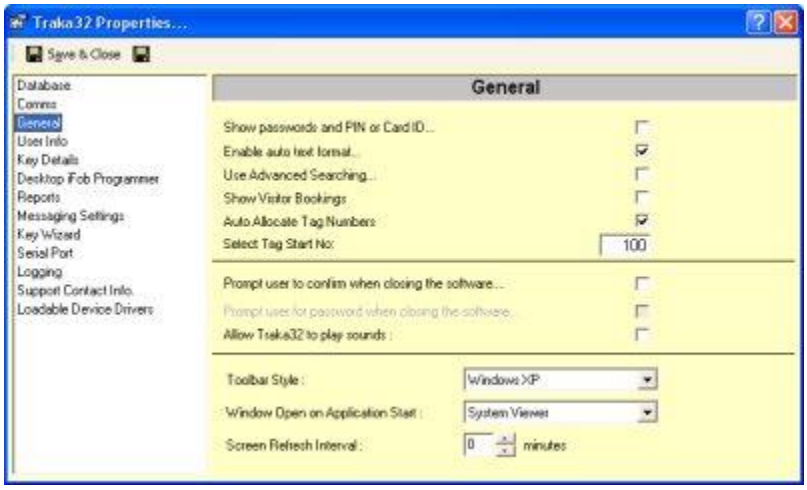
11. Repeat step 10 for each system.

12. Once assigned, we would normally recommend that you attached a tag to each iFob displaying the iFob's Index number for easy reference. Please refer to the next sections for details on how to assign the iFob tags.

Automatic Tag Numbering (Optional)

IF you wish to have tag numbers you can auto allocate them within the software. This option allows the tag number to be allocated automatically when they are added to the system. For example, if you have 10 iFobs in your system with tag numbers 1-10 and you delete iFob 2 (along with its tag number) and replace it with another iFob, when you assign that new iFob to the system accordingly, it will be given tag number 2 automatically. This option is particularly beneficial to customers who already have RRMS and wish to add another system without manually selecting the new tag numbers. This feature is compatible with 8bit & 16bit.

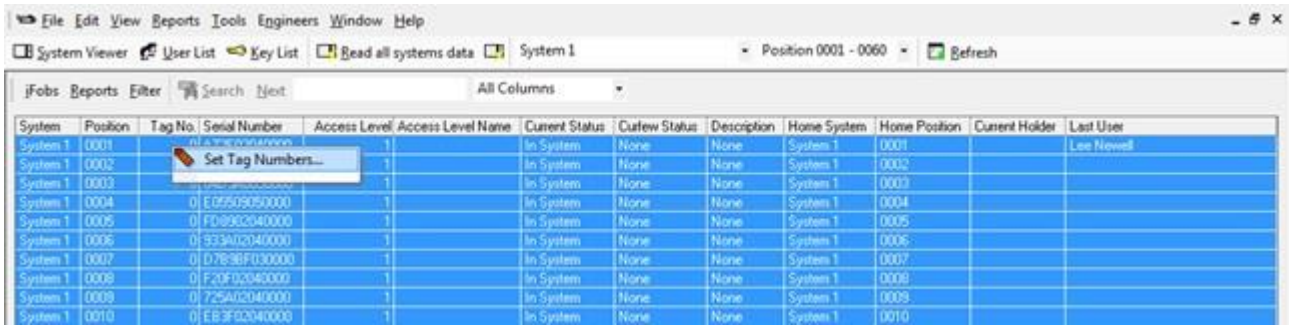
To enable this option click **File>Properties** and select the **General** tab. You will see a small box named **Auto Allocate Tag Numbers**, tick this box. You will also notice there is a **Select Tag Start Number** section, this allows you to select a specific number your tags will start from. If you leave this section blank the tag numbers will start at 1 by default. After choosing the appropriate settings you can **Save and Close**.



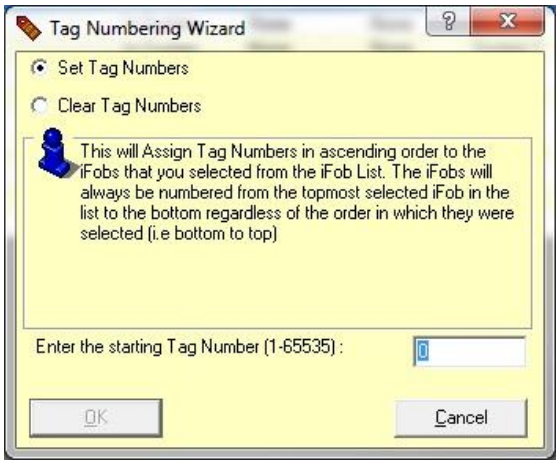
Manual Tag Numbering (Optional)

Manual tag numbering can be done at any stage after the iFobs have been Reset or synchronised to the system, whether or not the system is RRMS, RRSS or a standard Fixed return. For Example, if you require a RRMS then you will need to follow the procedure below for resetting the iFobs and synchronising the system before you can manually select iFob tag numbers. However if you are using standard system then you will need to synchronise the iFobs as normal before being able to manually selecting iFob numbers.

If you would prefer to tag you iFobs manually then you can do this via the 'Tag Numbering Wizard'. If you navigate to the iFob list by clicking **View>iFob List,** you will be confronted by a list of all the iFobs in the database whether the iFob is in or out of the system/s. Highlight all the iFobs you wish to assign tag numbers to (click and hold down the left mouse button on the first iFob you wish to tag and scroll down to the last iFob you wish to tag) then right click over the highlighted section and select the 'Set Tag Numbers...'.



The 'Tag Numbering Wizard' will appear and you will be able to select the desired number you wish to start the tag numbers at.



4.19.27.3.3 REPLACING IFOBS IN RANDOM RETURN TO MULTIPLE SYSTEMS

This procedure should be followed when replacing an iFob in a Random Return to Multiple Systems system and transferring the iFob tag across to the new iFob.

1. Insert the new iFob into a vacant position.
2. Select the correct system from the drop down menu in the main toolbar.
3. Click on the  button and a new iFob record will be created with a new tag number.
4. Click on **View**, **iFob List**.
5. Search for the iFob record of the iFob that is to be replaced.
6. Delete the iFob record. This will free up the iFob Tag No. so that it can be re-allocated to the new iFob.
7. Search for the iFob record of the new iFob.
8. Edit the iFob record and change the iFob Tag No. to that of the old iFob.
9. To **Save** your changes, simply click on  or 

.
10. Add the new tag to the iFob.

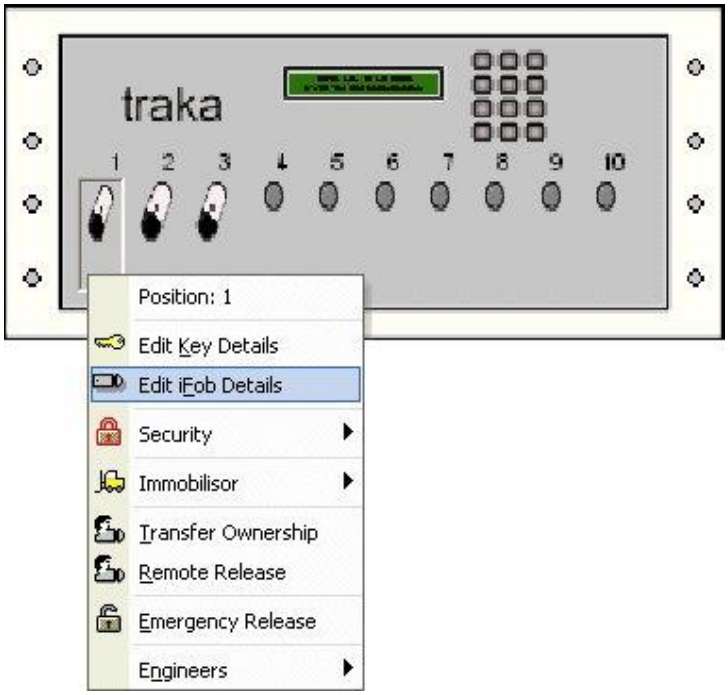
4.19.27.3.4 FIXED RETURN TO MULTIPLE SYSTEMS

Fixed Return to Multiple Systems (FRMS) allows any iFob from one system to be used in another fixed return system within the same database. The desired iFob must have a specific position assigned to it within the second system as well as the first system, this is done by allowing a duplication of the iFob record. The position you assign the iFob in the first system does not have to be the same in the second system. For example the iFob in slot 1 from system one can be allocated to slot 10 in system two if desired.

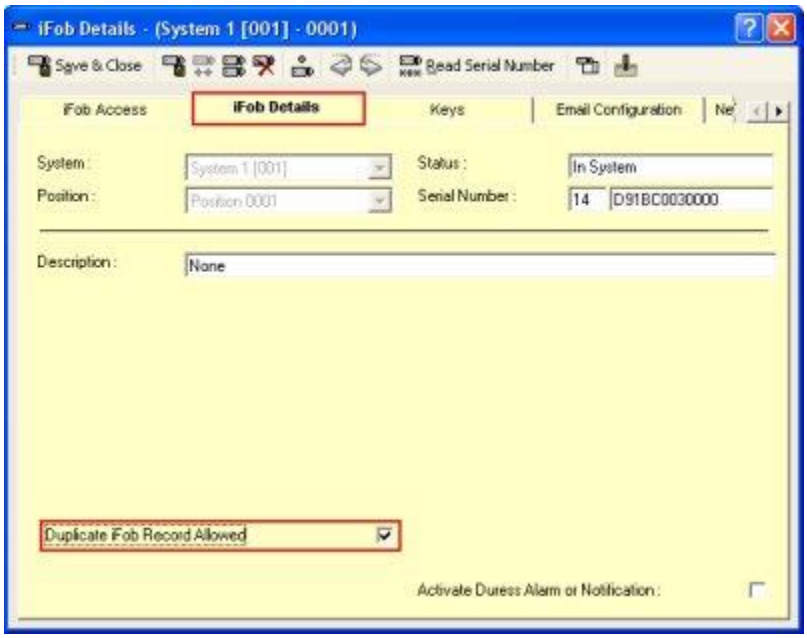
Setting up Fixed Return to Multiple Systems

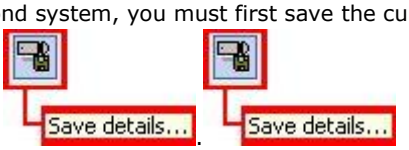
NOTE: This guide does not cover how to set up and configure a cabinet(s) on Traka32. See the Configuring Systems section for more details.

Assuming you already have two or more fixed return systems set up, assign at least one iFob to a blank slot on your first system. Right click the iFob and select' Edit iFob Details'.



Once the iFob Details window has opened select the second tab at the top of the screen named 'iFob Details'. At the bottom of the newly selected tab will be a box that needs to be ticked called 'Duplicate iFob Record Allowed'.

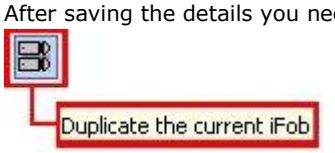


Before assigning the iFob a specific slot in the second system, you must first save the current details by clicking the small save button at the top of the Details window 

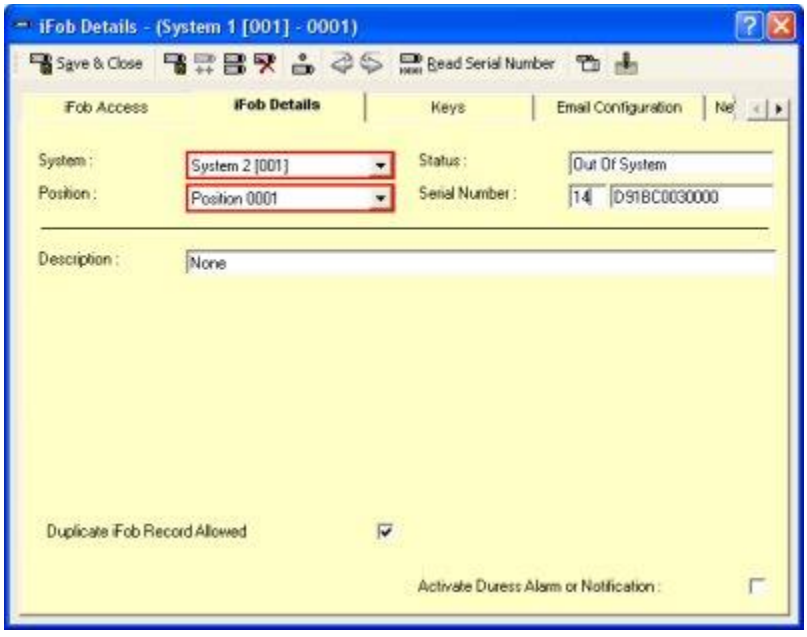
.

NOTE: If you don't save details before you click the Duplicate iFob button you will get a small message pop up telling you that changes have been made you must save details (See below).

After saving the details you need to duplicate the iFob details by clicking the button at the top of the Details window



The previously greyed out 'System' and 'Position' drop down boxes at the top of the Details window will now be selectable.



The System tab allows you to select which system you want to place the iFob in. If you have only two systems it will automatically select the second system for you, however if you have more than two this tab lets you manually select the desired system. The Position tab allows you to assign the iFob to a specific slot for any another system within the database.

NOTE: You can assign any ifob from the first system into any other free slot in the second system, however once the duplicate iFob has been dedicated to a specific position in the second system the iFob cannot be used in another position until it has first been removed from its current position in Traka32

After selecting the appropriate settings in the Details window click the 'Save & Close' button.

Using Fixed Return to Multiple Systems

Now that the iFob record has been duplicated and Traka32 knows the iFob can be used at both cabinets, view the second system within Traka32 and you will notice that there will be a greyed out iFob in the position that you selected to host your duplicate iFob. Traka32 now recognizes that there should be an iFob in that position but it is currently out of the system.

Take the iFob from your first cabinet and place it in the newly assigned position in the second cabinet, Read all System Data and the iFob will appear in that slot. Traka32 and the cabinets will function as normal.

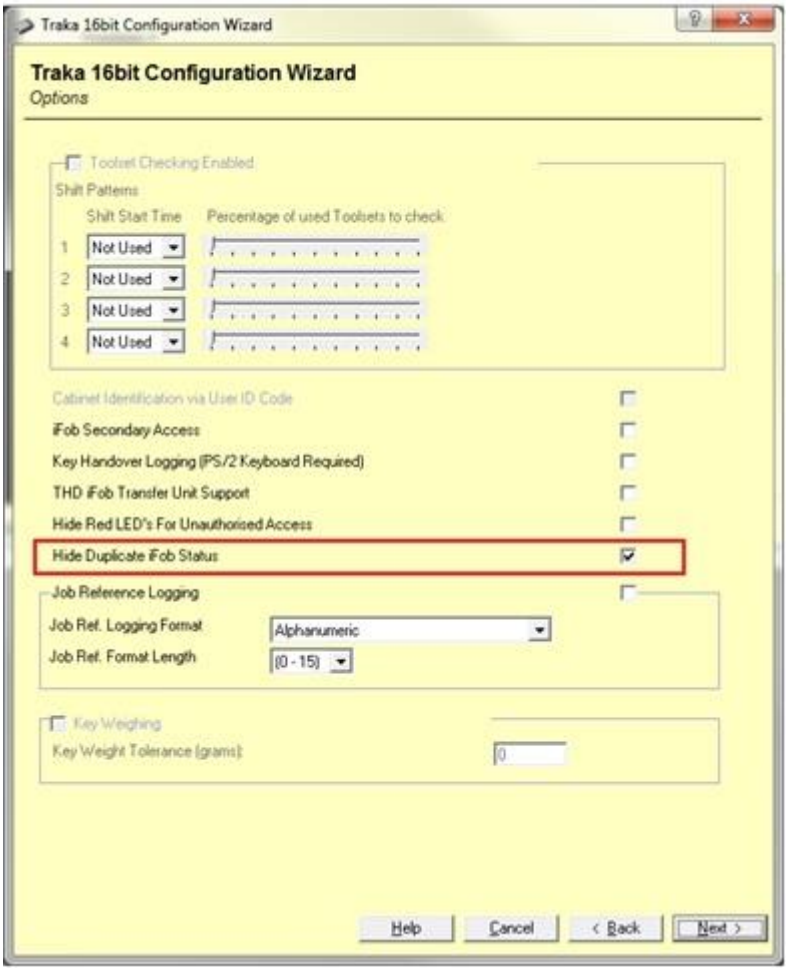
Hide Duplicate iFob Status

When iFobs are removed from a system with LEDs, the LED for that position will illuminate orange to show that the logged in user currently has the iFob. However, when using Fixed Return To Multiple Systems the iFob could be removed from System 1 and placed in System 2. The LED will still illuminate orange when the user logs in to System 1 when in actual fact they no longer have the iFob in their possession.

To overcome this, an option to Hide Duplicate iFob Status is available from the Configure Firmware menu. This option will hide the 'Held' status LED (orange) of duplicated iFob positions only. LEDs will function as normal on all non-duplicated positions.

1. From the System Viewer page right click the Control Pod and select **Configure Firmware**.

2. Click **Next** through the pages until you reach the page shown below. The option for Hide Duplicate iFob Status is highlighted.



3. Select this option and click **Next** until you reach the final page, then click **Apply**. The change will be applied to the system. Repeat this process for each of the systems.

4.19.28 REDUCED USER SECURITY

4.19.28.1 REDUCED USER SECURITY OVERVIEW

Full Reduced User Security Overview

Full Reduced User Security has been developed for customers that do not take advantage of the advanced security settings available within Traka but require the System to work with more users. This only applies to 8bit systems.

When the option is switched on the only visible difference that can be seen is in the User Details and Security Group windows where the following features will **not be visible**...

- Permit Expiry date (user details only).
- Active and Expiry dates (user details only).
- Shift A and B access days and times.
- iFob Allowance.
- Access levels 9 to 200.
- Maximum Primary ID Length of 10.
- Maximum User Name Length of 10.
- User Curfew.
- Access Group.
- Key Not Taken Curfew.

Half Reduced User Security Overview

Half Reduced User Security has been developed for customers that do not take advantage of the advanced security settings available within Traka but require the System to work with more users. This only applies to 8bit systems.

When the option is switched on the only visible difference that can be seen is in the User Details and Security Group windows where the following features will **not be visible**...

- Permit Expiry date (user details only).
- Active and Expiry dates (user details only).
- Shift A and B access days and times.
- Access levels 9 to 200.
- Maximum Primary ID Length of 10.
- Maximum User Name Length of 10.
- User Curfew.
- Access Group.
- Key Not Taken Curfew.

4.19.29 REDUCED IFOB SECURITY

4.19.29.1 FULL REDUCED IFOB SECURITY OVERVIEW

Full Reduced iFob Security has been developed for customers that do not take advantage of the advanced security settings available within Traka but require the System to work with more iFobs (up to 2,560 iFobs per system).

When the option is switched on the only visible difference that can be seen is in the iFob Details window where the following features will **not be visible**...

- iFob Curfew
- iFob Pair
- Access days and times

When the option is switched on the following options will **not be available**...

- iFob Options
- X iFob Authorisers
- iFob Description
- Immobilisor iFob per Person
- Micro Traka
- Bay Logging
- Random Return
- Fuel Level Logging
- Mileage Logging
- Fault Logging

4.19.29.2 HALF REDUCED IFOB SECURITY OVERVIEW

Half Reduced iFob Security has been developed for customers that do not take advantage of the extra features available within Traka but require the System to work with more iFobs (up to 1,280 iFobs per system).

When the option is switched on the following options will **not be available**...

- iFob Options
- X iFob Authorisers
- iFob Description
- Immobilisor iFob per Person
- Micro Traka
- Bay Logging
- Random Return
- Fuel Level Logging
- Mileage Logging

4.19.30 REMOTE SYSTEM LOCKDOWN

4.19.30.1 REMOTE SYSTEM LOCKDOWN

Remote System Lockdown has been developed to keep all users locally locked out of the system whilst the option is enabled and third party hardware is connected. When switched on, Remote System Lockdown will not allow any user to login to the system or access iFobs, keys or items by any means. Remote System Lockdown is a cost option and is also for 16bit systems only.

Connecting the third party system to the Traka Hardware

To connect the third party hardware to the Traka 16bit PCB you will need to gain access to the system electronics.

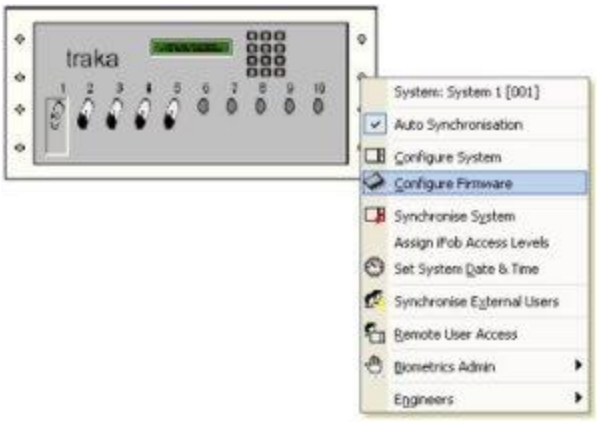
1. Insert the master override key into the CAM lock on the control panel and turn 90° clockwise.
2. Connect the desired hardware to the following location on the 16bit PCB shown below. The relay from the third party hardware must be closed before you can enter your PIN-code on the Traka cabinet.

   For further information on the 16bit hardware please refer to the relevant sections 16bit Control PCB - 16bit I/O PCB.

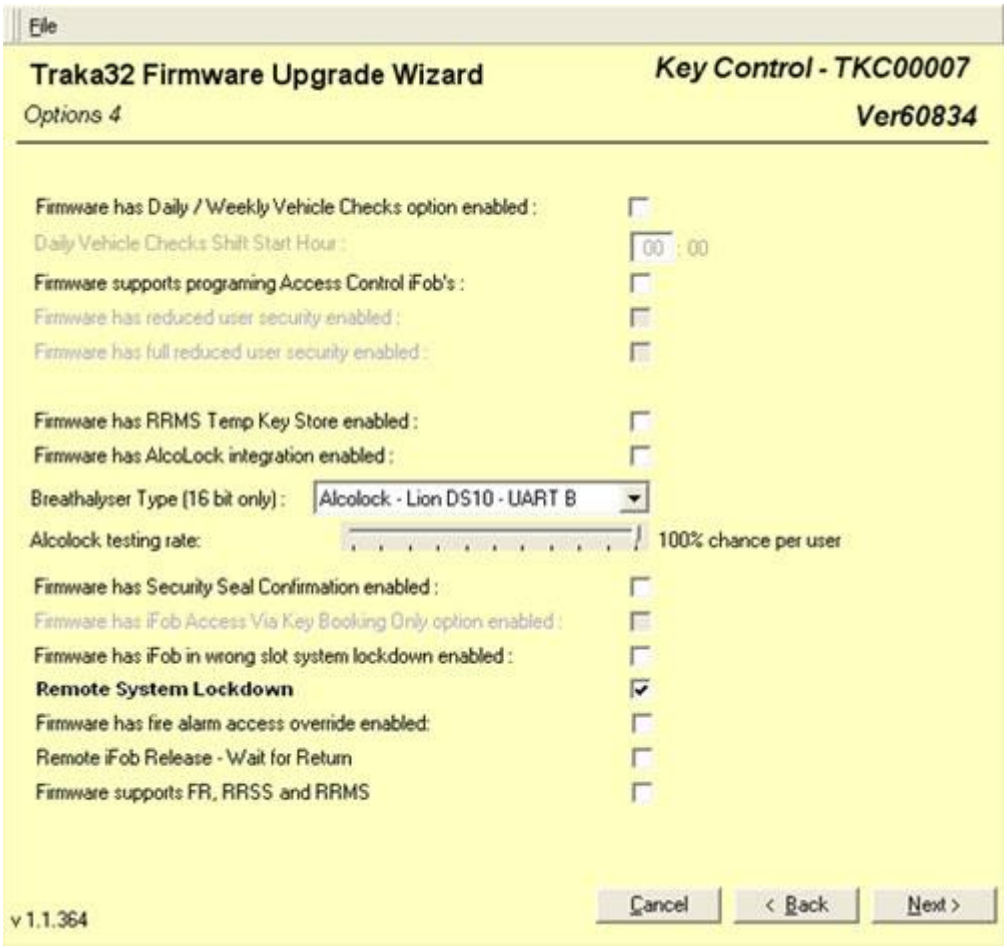
3. Close the control panel and lock it using the master override key.

Applying the Remote System Lockdown Feature

1. Right click the pod of the cabinet/locker from the system viewer and select Configure Firmware.



2. When the 16bit Configuration Wizard appears navigate to the forth options page and select the Remote System Lockdown tick option.



3. Continue to click Next and then finally Finish to communicate and apply the changes to the system.

4. The system now has Remote System Lockdown activated. When a user tries to access the system by pressing a key or swiping a card the LCD will display the message 'System Lockdown' and an error beep will be sounded. After the 5 second period the display will return to the previous scrolling status. This only exception to this is if the user presses the '*' key to access the search menu.

5. To remove the deactivate Remote System Lockdown, access the firmware wizard and deselect the option. Then apply the changes to the system as described in the steps above.

4.19.31 SECONDARY ACCESS LEVELS

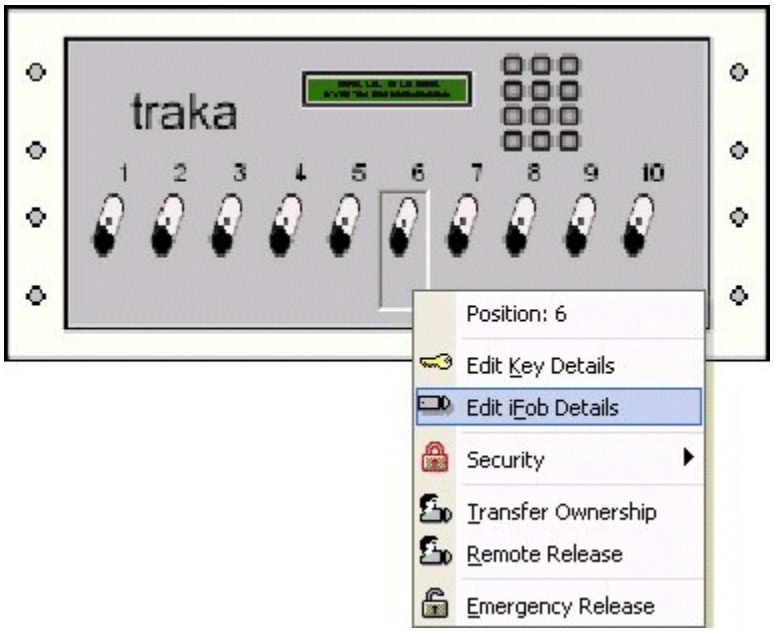
4.19.31.1 SECONDARY ACCESS LEVEL OVERVIEW

Enabling Secondary Access Levels allows a user to take an iFob which primarily has an access level they do not have. Enabling an iFob with a Secondary Access level means a user will be able to remove that iFob once all other iFobs with the user's primary access level have been removed from the cabinet. This option forces the user to remove certain iFobs before being allowed to take others. For example, if you have a cabinet with 10 iFobs and 1-5 are access level 1 and 6-10 have an access level of 2 but also have a secondary access level of 1 (and the user entering the cabinet only has access level 1) when iFobs 1-5 have been removed from the cabinet by other users, upon accessing the cabinet positions 6-10 will drop down to access level 1 allowing the user to take the iFob.

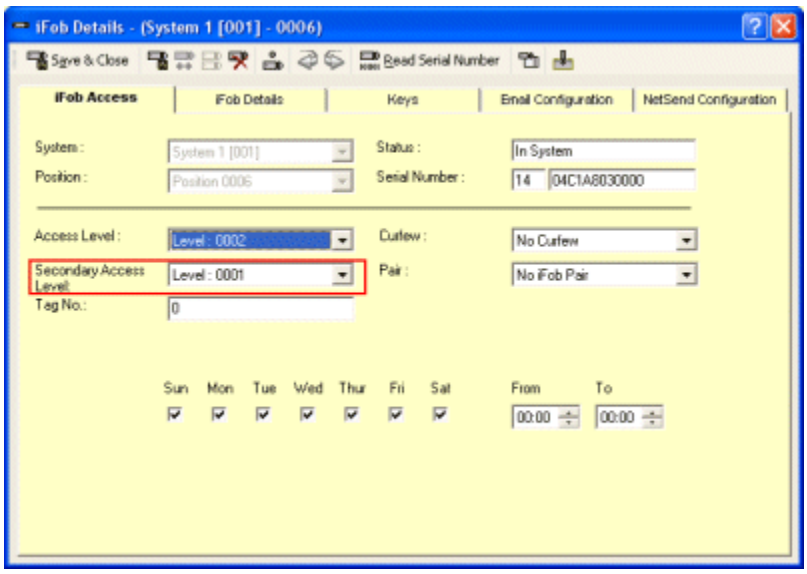
NOTE: Secondary Access Level option is only compatible with 16bit and Intelligent Receptor Strips

How to Set up Secondary Access Levels

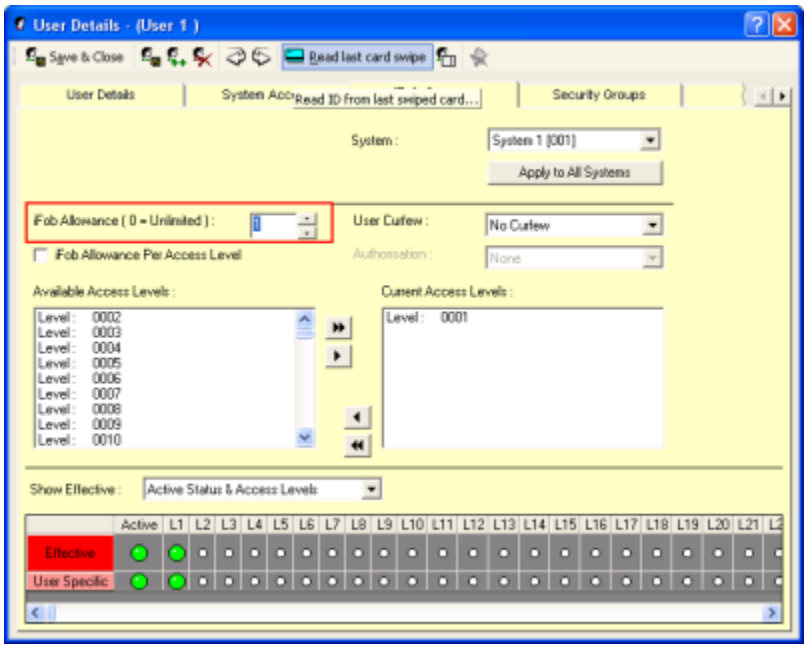
The Secondary Access level is an option that needs to be enabled within the firmware in order to work. Right click over an iFob you wish to assign a secondary access level to and select **Edit iFob Details.**



In the iFob Details window click the iFob Access tab and select a primary access level to assign to the iFob as you normally would, but also select the secondary access level as desired.



Next, open the Details window for the desired User and select the iFob Access tab then Set the iFob allowance to 1. This restricts the number of iFobs a user can take. Without limiting their iFob allowance to 1 a user could take the last iFob with their assigned access level and then at the same time remove iFobs that have secondary access levels, allowing the user to choose another iFob as opposed to being assigned one.



NOTE: For this example positions 1-5 will have access level 1 and 6-10 will have access level 2 and a secondary access level of 1, also the user has access level 1.

When the user gains access to the cabinet the LED's on the Intelligent receptor strip will show you the iFobs you are authorised to take.

In this case the user will be allowed to take iFobs 1-5 because the iFob has access level 1 as does the user, the red LED's symbolise iFobs that the user does not have access to at this point.

If a user accesses the cabinet to take an iFob and finds iFobs 1-5 have been removed by other users, the Secondary Access Levels on the iFobs will activate and the user can now access iFobs 6-10, the LED's will now turn green (see Below).

When the user takes their desired iFob, the other iFobs (if any) will display a red LED because the user has exceeded their iFob limit, the amber LED symbolises the iFob the user has just removed (see below).

4.19.32 SECURITY SEAL CONFIRMATION

4.19.32.1 SECURITY SEAL CONFIRMATION OVERVIEW

The Security Seal Confirmation option prompts a user when removing an iFob from the cabinet to check and verify the security seal no. attached to the iFob. If the security seal no. is different to that of which is stored in Traka, then the iFob and related key may have been tampered with. It is the responsibility of the user removing the iFob to verify if the security seal is correct or different. If the user verifies the seal no. is different, Traka records a "Security Seal Different Please Check!" event in its database. See Security Seal Confirmation Operation for more information.

NOTE: It is the responsibility of the user removing the iFob to verify whether the security seal no. is correct or different.

4.19.32.2 SECURITY SEAL CONFIRMATION OPERATION

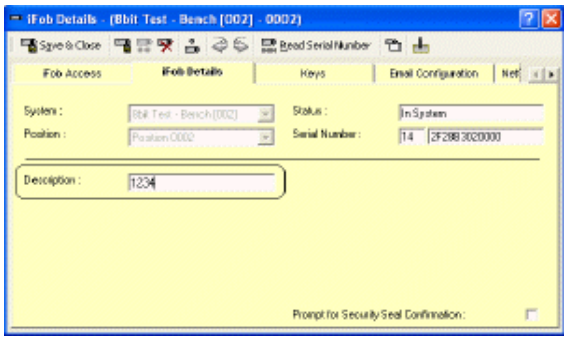
To setup an iFob to Prompt for Security Seal Confirmation:

1. From the Traka 32 system viewer right click over an iFob and click **Edit iFob Details**

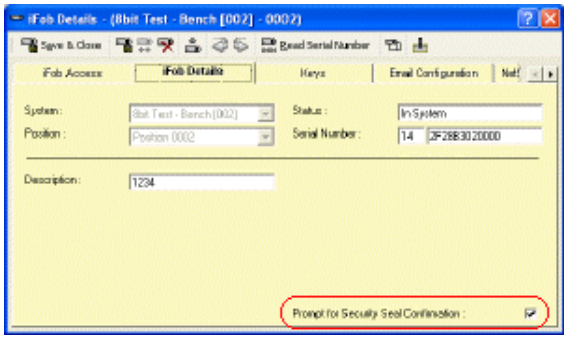
2. Click the **iFob Details** tab.

3. Ensure the System and iFob selected is correct.

4. **Enter the Security Seal No.** in the iFob Description field.



5. Click **Prompt For Security Seal Confirmation** to Enable.



6. Click **Save and Close**, the system will be updated.

7. When a User tries to remove an iFob with Prompt For Security Seal Confirmation enabled, the Traka cabinet LCD will display:

8. The user must then check the security seal no. on the iFob and compare it to the LCD before pressing *** for different** or **# for correct** from the keypad.

   a. If # is pressed, the system will release the iFob.

   b. If * is pressed, the system will not release the iFob and the LCD will display:

A **"Security Seal Different Please Check!" event** is recorded in the database viewable from Traka 32 reports.

NOTE: If the User confirms the security seal no. is different, the system will NOT permanently lock the iFob in place until the condition is resolved. Any user with authorization can still take the iFob. This feature is designed to notify only by logging a "Security Seal Different Please Check!" event in the Traka database!

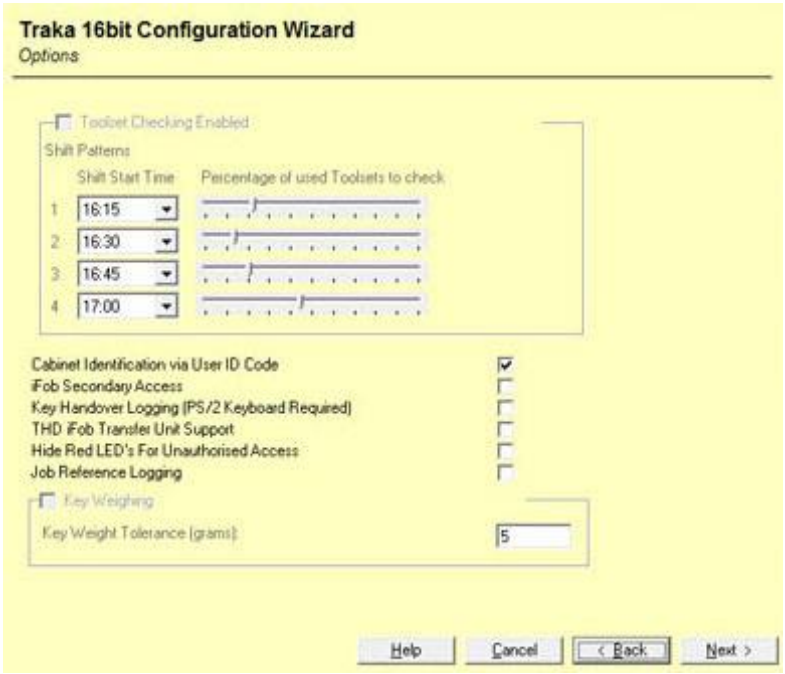
NOTE: It is the responsibility of the user removing the iFob to verify whether the security seal no. is correct or different.

4.19.33 USER IDENTIFICATION NUMBER

The User Identification Number was developed to allow users to securely assign themselves a PIN on the keypad at the system. This eliminates the administrator who is adding the user profiles to Traka32 knowing the PIN codes and ID card numbers of the users. How the feature works is each user is given a unique 'Identification Number' (commonly referred to as a NIP code) that they then enter at the system, which will allow them to swipe their ID card and assign themselves a PIN via the keypad. The following procedure will explain how to setup and use the User Identification Number option.

System Setup

1. Before a user can begin the process of entering their own PIN, the system must have the 'User Identification via User ID Code' option enabled in the firmware. This is a cost option that must be switched on at Traka. If you have an existing system and would like to add this option, please contact Traka for details on receiving an up to date configuration file.



2. The users must already exist in the database before they use the system. An administrator with the appropriate permissions will need to create users and fill in the required details. When adding the details it is important that the primary and secondary PIN fields are left blank, these are later automatically populated when the user assigns themselves a PIN at the system.

3. When all the standard details have been entered, navigate to the advanced tab. At the bottom of the window you will see an empty field called 'User Identification Number'. Enter a number that is at least five digits long and different to the other users ID numbers.

User Process

The user is given the ID number and approaches the system.

1. Press **#** on the keypad. The user will then be prompted to enter the User Identification Number they have been provided.

2. If the ID number is correct the system will then prompt the user to swipe their ID card.

   NOTE: At this point the card number is stored in the system against the user profile as the primary PIN. This information will be read back to Traka32 once the data has been read from the system.

3. Once the card number has been read and stored, the user can enter their own PIN followed by the **#** key.

   NOTE: At this point the PIN is stored in the system against the user profile as the secondary PIN. This information will be read back to Traka32 once the data has been read from the system.

4. The process is now complete and you will receive a message on the LCD stating that the enrolment was successful.

   Now the user has completed this process, when they swipe their ID card and enter their PIN they can access the system and remove keys/iFobs in the usual fashion.

4.19.34 VEHICLE COST LOGGING

4.19.34.1 VEHICLE COST LOGGING OVERVIEW

The Vehicle Cost logging option enables a user of a vehicle to enter certain data about the vehicle when returning the iFob / keys. The information that can currently be recorded is...

- Fuel Quantity Used (Litres)
- Oil Quantity Used (Litres)
- Vehicle Wash Cost (£,€ or $)
- Tyres Quantity Replaced

These values will be logged against each transaction.

NOTE: Vehicle Cost Logging will only be available if the firmware of the selected system has Vehicle Cost Logging enabled. If the Vehicle Cost Logging option is enabled in the firmware, it is also possible to enable / disable the option on an iFob per iFob basis from the iFob Details window.

4.19.35 VISITOR BOOKING

4.19.35.1 VISITOR BOOKING OVERVIEW

Visitor Booking as its name suggests, allows a user to pre-book an iFob / key for a visitor who would normally not have access to the Traka System.

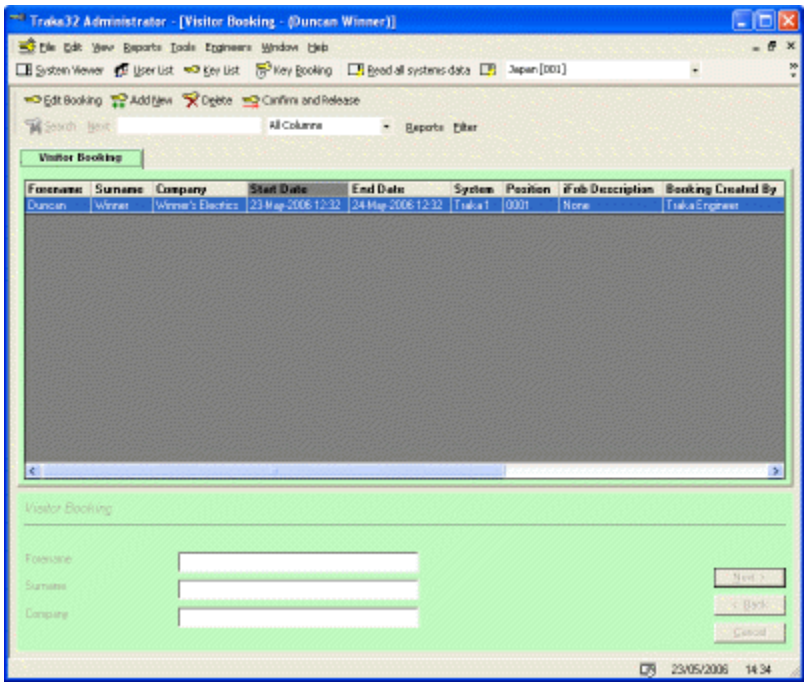
The visitor booking wizard is used to create and edit visitor booking records.

When a visitor has pre-booked a visit and the visitor arrives on site and requests a key, the operative of Traka32 can open the visitor booking list and search for the relevant visit. Once the visit booking record has been found the booking can be confirmed and the related key released from the Traka System.

4.19.35.2 VISITOR BOOKING LIST

The Visitor Booking List allows you to view the current visitor bookings that have been made. From this list you can add and edit the bookings via the easy to use wizard or simply delete bookings.

To view the visitor booking list, click on **View**, **Visitor Booking** from the main menu.



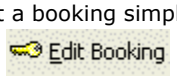
NOTE: If the Visitor Booking option is not visible, this may be because the option has not been enable. To enable the Visitor Booking option...

1. Click on **File**, **Properties** and the Properties window will open.
2. Click on the **General** section.
3. Select the **Show Visitor Bookings** option.
4. Click on **Save & Close**.

4.19.35.3 VISITOR BOOKING WIZARD

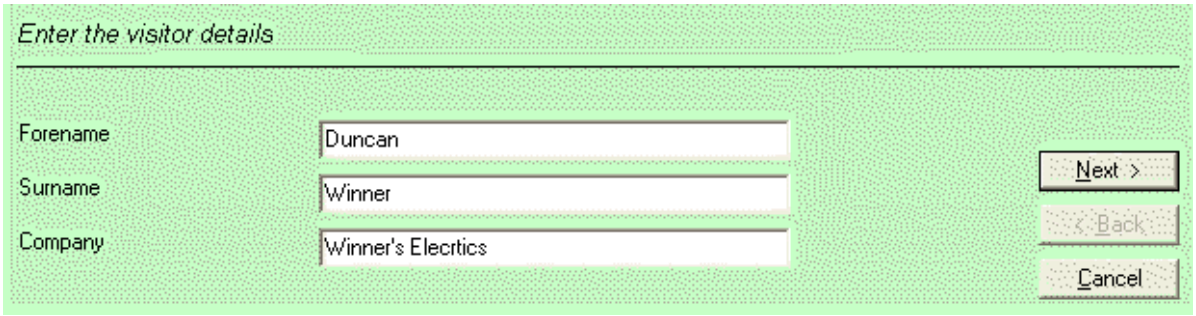
The visitor booking wizard is used to create and edit visitor booking records.

1. To view the visitor booking list, click on **View**, **Visitor Booking** from the main menu.
2. To add a booking simply click on 

the button.
3. To edit a booking simply **double click** on the booking record you wish to edit or select the booking and click on the 

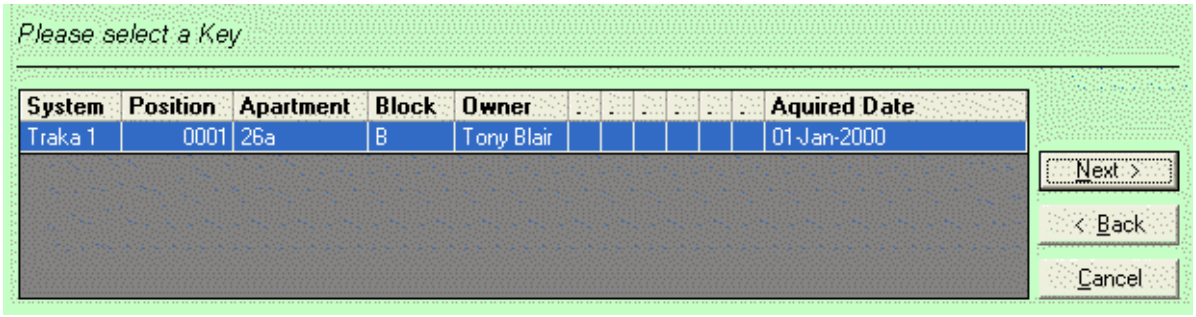
button.
4. **Step 1 - Enter a User:**

   Enter the visitors **Forename**, **Surname** and **Company** name then click on **Next**.



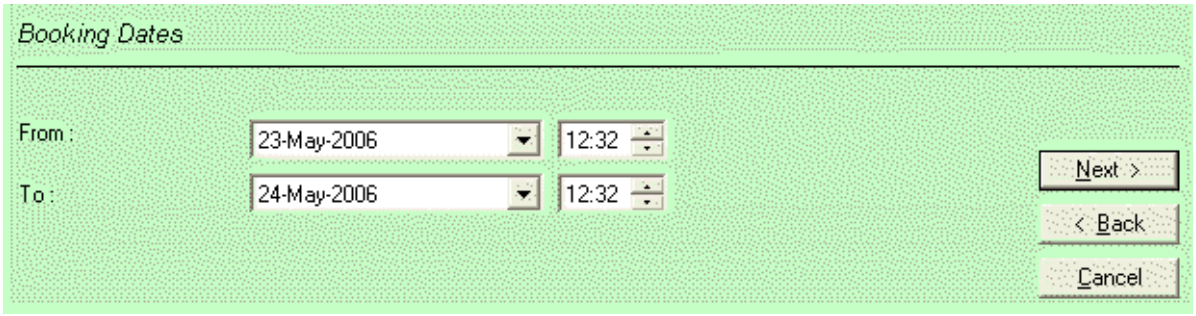
5. **Step 2 – Select a Key:**

   Select an iFob or key from the list and click on **Next**.



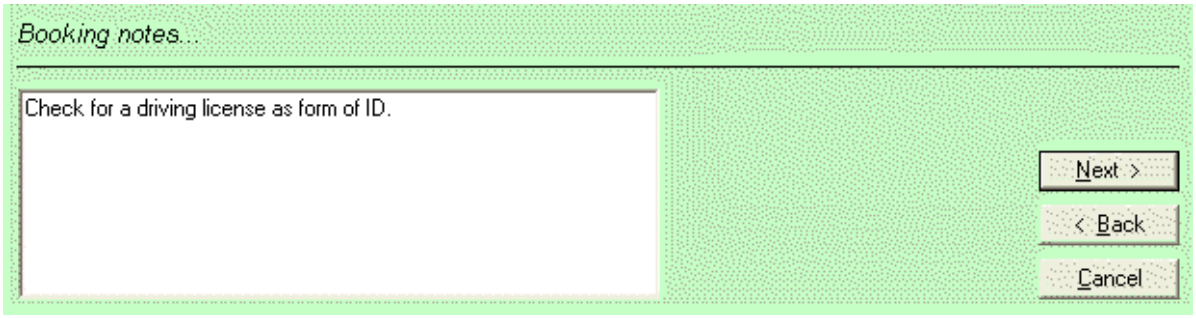
6. **Step 3 – Select the Booking Times:**

   Select a start and end time for the booking and click on **Next**.



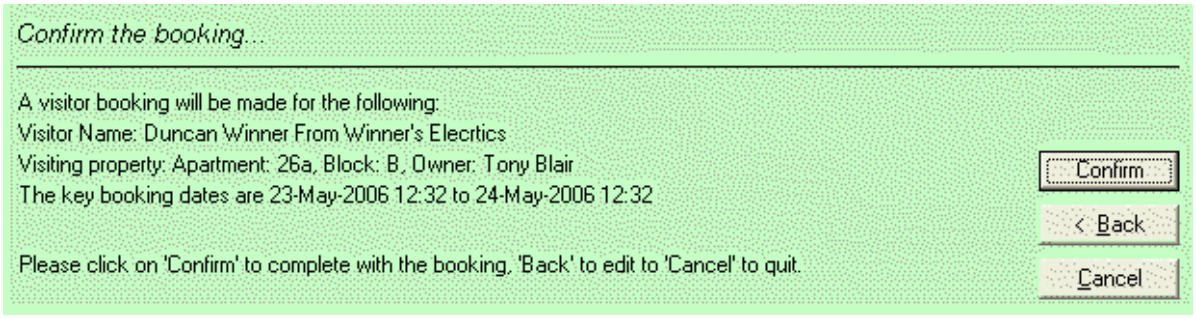
7. **Step 4 – Booking Notes:**

Enter and notes that you want relating to the booking and click on **Next**.



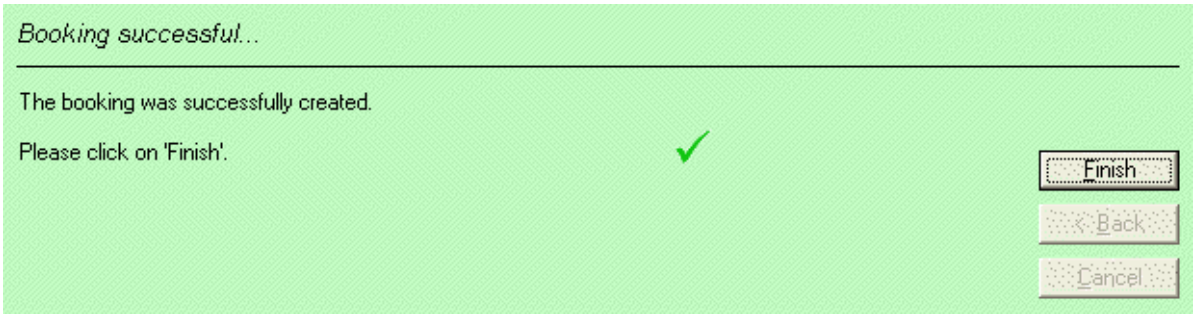
8. **Step 5 – Confirm the booking:**

Confirm the booking details, if you are happy and want to save the booking click on **Confirm** or if you want to change the details click on **Back** or to discard the booking click on **Cancel**.



9. **Step 6 – Finish the booking:**

Click on **Finish** to complete the booking.

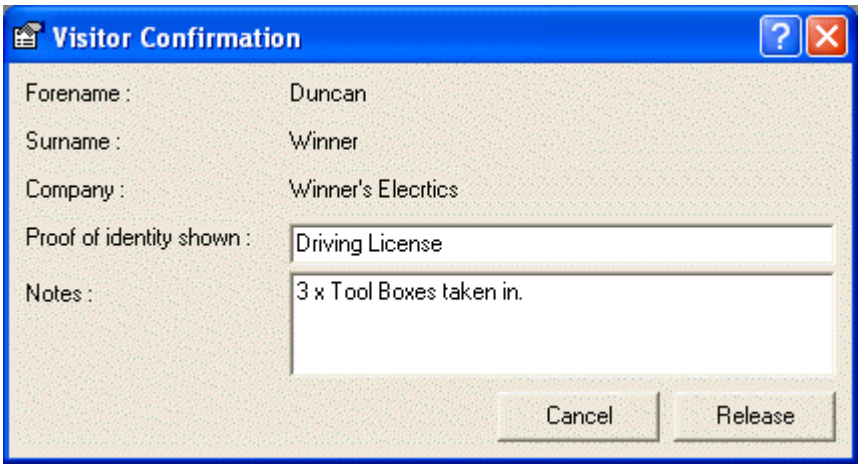


4.19.35.4 CONFIRM AND RELEASE

When a visitor has pre-booked a visit and the visitor arrives on site and requests a key, the operative of Traka32 can open the visitor booking list and search for the relevant visit. Once the visit booking record has been found the booking can be confirmed and the related key released from the Traka System.

1. To view the visitor booking list, click on **View**, **Visitor Booking** from the main menu.
2. Select the booking record and click on the 

button and the **Visitor Confirmation** window will open.
3. Enter the **Proof of identity shown** in order to determine the visitor's identity. For example: passport or driving license.
4. Enter any **Notes** relevant to the visitor booking.



5. Click on **Release** to release the related key from the Traka system.
6. Click on **Cancel** to cancel the Visitor Confirmation.

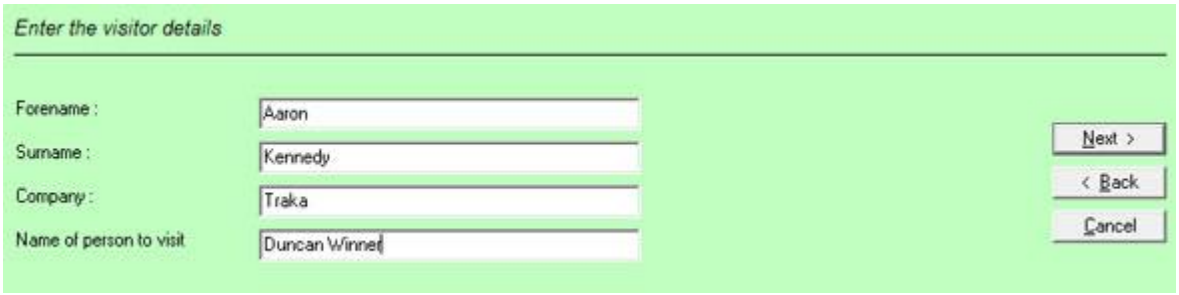
4.19.35.5 VISITOR BOOKING IMMEDIATE RELEASE

Visitor Booking Immediate Release is a second version of the pre-existing option Visitor Booking. This second edition streamlines the original process and slightly alters the key release method to achieve a faster method of booking keys to visitors.

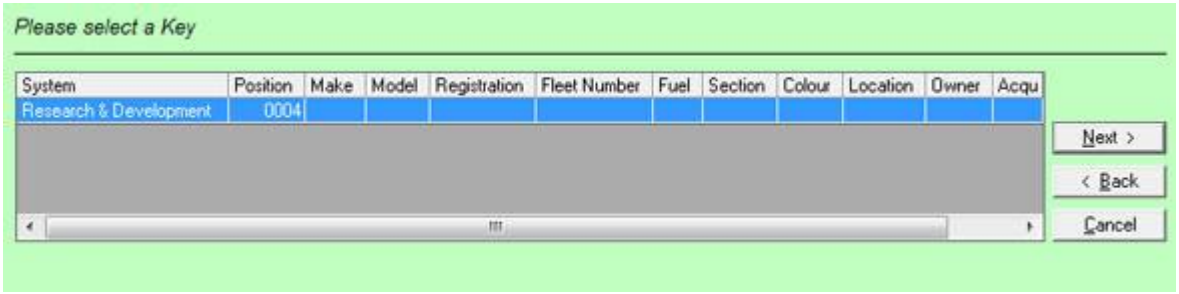
To enable this option you must contact Traka as a Project Manager or Engineer is required to facilitate the upgrade.

Immediate Release Booking Process

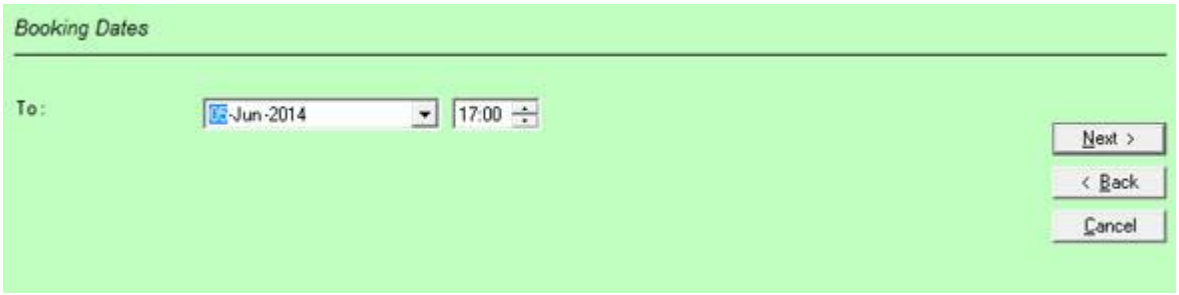
1. From the top of Traka32, click on **View**, **Visitor Booking**.
2. You will be presented with the Visitor Booking List. Here you can Add, Edit or Delete a Visitor Booking. Click Add New.
3. The detail fields at the bottom of the page will become editable. Enter the Forename, Surname and Company of the visitor along with the person they are visiting. After entering the desired details click next.



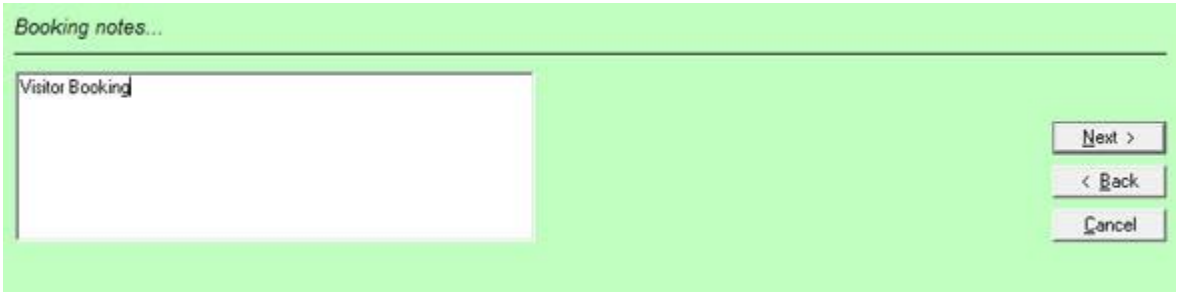
4. Next, select the key you wish to book to the visitor from the list available, then click next.



5. Select the date in which the key must be returned to the system. By default it is set to 17:00 the same day the booking is made, this can be manually changed. When you have selected a date and time, click next.



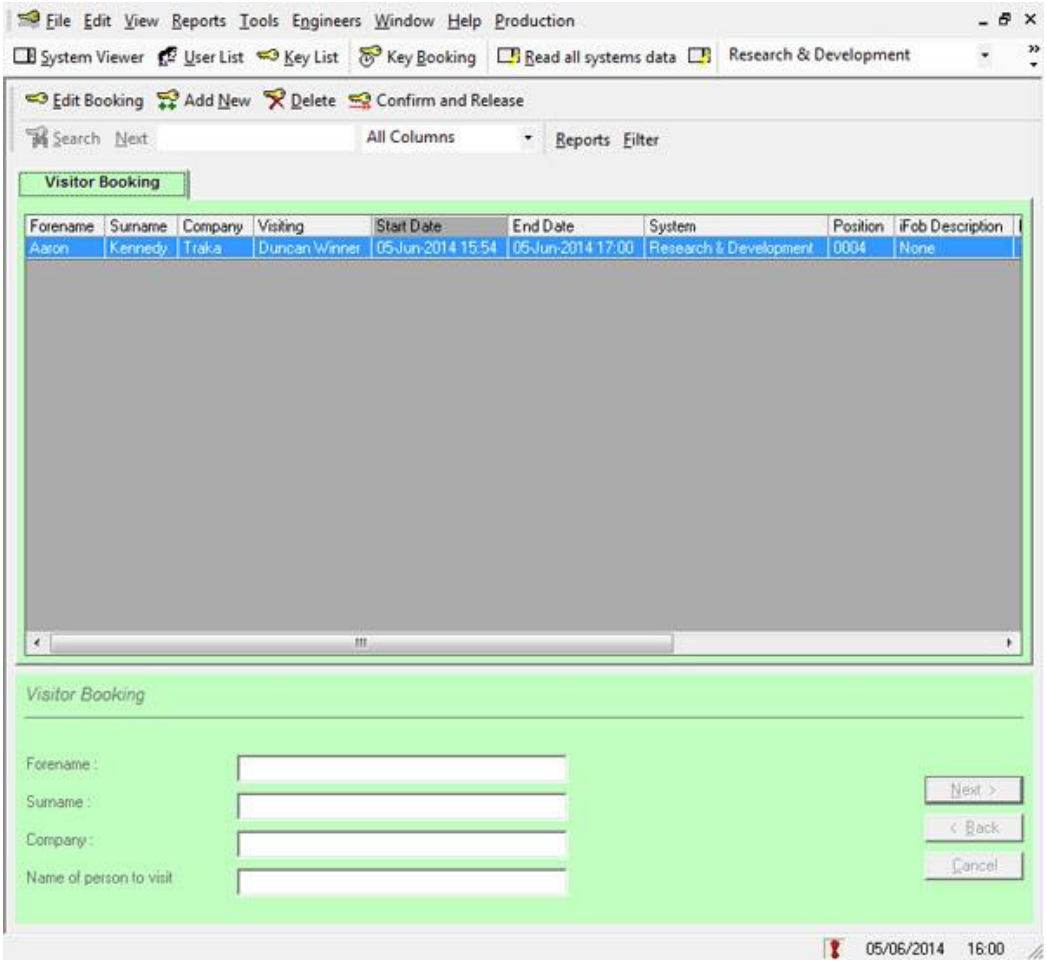
6. Enter any notes you want to make against the booking and click next.



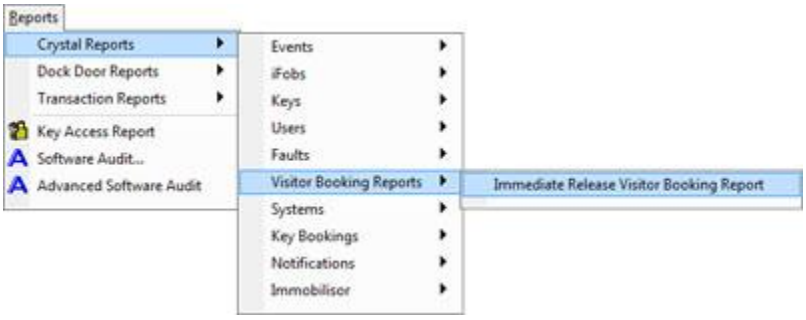
7. This page will display the details of the booking you are creating, if you are happy everything is correct click the Confirm button to complete the booking.

8. Once you click the Confirm button, the system door will then automatically open and release the iFob for you to take.

9. The booking is then displayed in the Visitor Booking List. As the key is released the booking becomes completed therefore you cannot edit or delete the booking.



10. You can run a crystal report to show the completed bookings. From the top of Traka32 select **Reports, Crystal Reports, Visitor Booing Reports, Immediate Release Visitor Booking Report.**



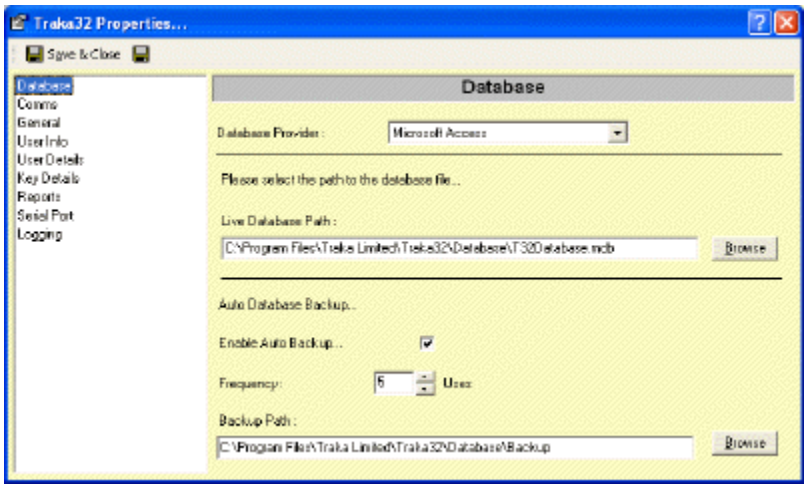
4.20 GENERAL

4.20.1 AUTO DATABASE BACKUP

If you are using a Microsoft Access Database, the Auto Database Backup automatically prompts the backup of the database to a chosen location set in the Properties window.

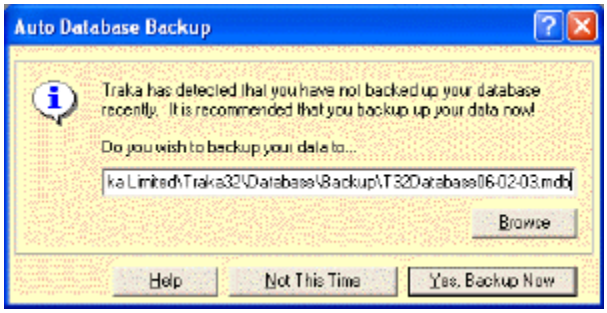
NOTE: It is strongly recommended that you back up your database as regularly as possible.

To enable the Automatic Database Backup reminder click on **File**, **Properties**...



1. In the Database section, check the **Enable Auto Backup** option.
2. Set the **Frequency** to the desired number of uses. This is the number of times the software has to be closed before the auto backup utility will prompt you to back up the database.
3. Select the **Backup Path** to where you would like the database to be backed up to. This could be a directory on your network or a floppy drive.
4. Click on **Save & Close**.

When you have used the software x times (x = Frequency), when you close the software the following prompt will appear...



- Click on **Not This Time** to skip the backup and exit the software.
- Click on **Yes, Backup Now** to back up the database to your chosen location.

  Ensure the backup path is correct (and if required the PC is connected to the network or a floppy disk is inserted etc.).

  If you wish to temporarily alter the backup path or file name, alter the path or click on Browse to pick a new path and click on **Yes, Backup Now**.

  If you wish to permanently change the backup path, click on **File**, **Properties** and from the **Database** section, change the settings.

4.20.2 SETTING UP AUTO COMMS

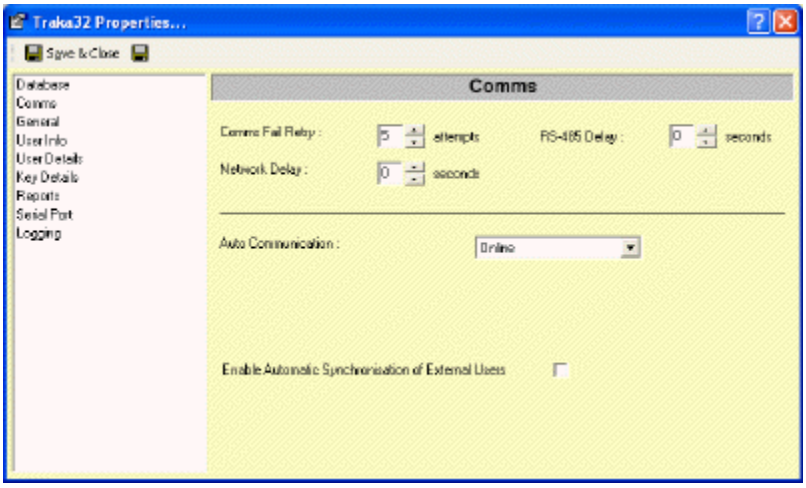
This allows the automatic communication between the Traka system and the supporting Traka32 software. By automatically communicating you ensure that the transactions recorded by the Traka system are always backed up to the PC.

For automatic communication it is of course essential that the Traka32 software is running. In most applications only one PC should be setup as online and this should be a PC that is not commonly used or switched off.

Traka also supports Traka 32 as a Windows Service (TAAS) which provides a means of running Traka32 in the background as a Windows Service on an (unattended) PC. TAAS requires no User interface and keeps running even if no-one logs on to the PC.

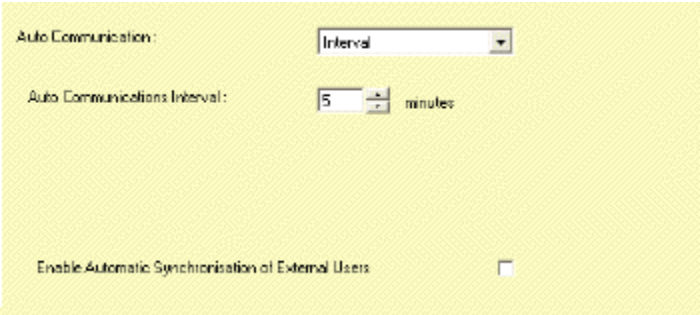
NOTE: Auto Comms in Traka32 will not work if Traka as a Service is installed on the same PC, even if the service is not running. Auto Comms will only work again once the service is uninstalled.

1. Click on File, **Properties**.
2. From the Properties window, click on the **Comms** section.



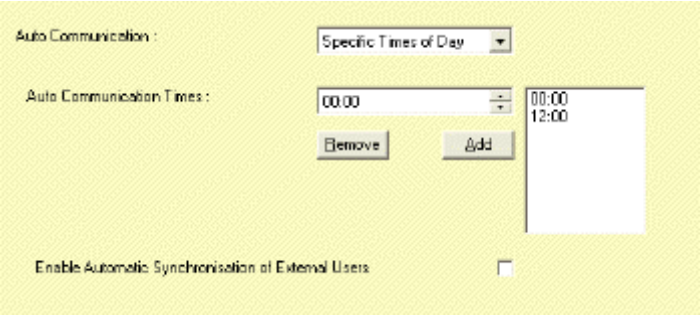
3. Set the **Auto Communication** to **Interval**, **Specific Times of Day**, **Online** or **Remote Host**.
4. Configure the related options...

- **Interval**
  By selecting interval you may specify how frequently, in minutes, that Traka32 should communicate with the systems.



- **Specific Time of Day**

  By selecting specific time of the day you may specify exact times of each day that Traka32 should communicate with the systems.

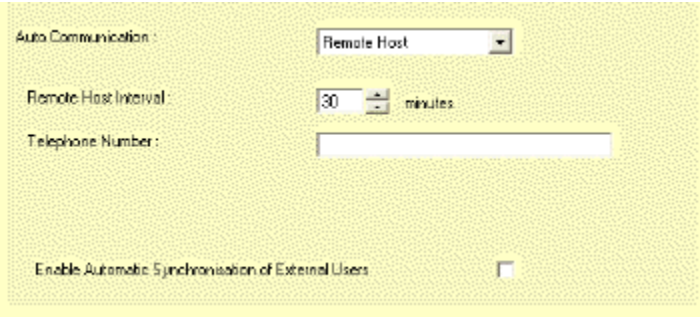


  To add a time, enter the required time and click on Add. The time will appear in the list opposite.

  To remove a time, select the time to remove from the list and click on Remove.

- **Online**
  By selecting online, each selected system will automatically switch online when the Traka32 software is loaded.

- **Remote Host**
  By selecting remote host, Traka32 will add a host entry into each Traka System and will then listen for remote connections from the Traka System every time an event occurs. For further information, please refer to the XPort Remote Host section.

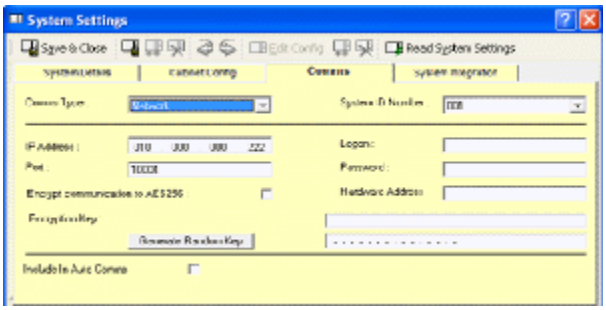


  The **Remote Host Interval** can be set to specify how frequently, in minutes, that Traka32 should communicate with the systems. This is in addition to the Remote Host communications but can be disabled by setting to 0.

  The **Telephone Number** field is available for using the remote host option with a Modem but this option is not yet available.

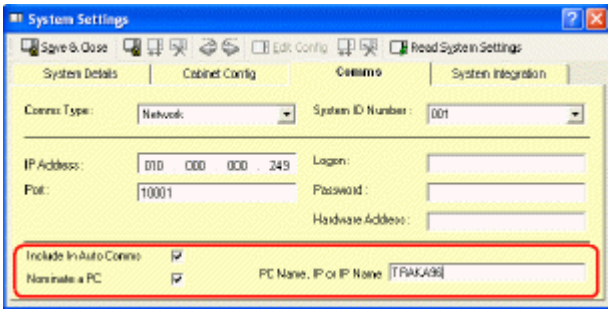
5. Click on **Save & Close**.
6. Click on Tools, **Configure Systems**.
7. Edit each system that you wish to include in the Auto Communications by double clicking on the records.
8. From the System Settings window, click on the **Comms** section.

9. Set the **Auto Communication** to **Include In Auto Comms**.



Nominate a PC

This option allows a PC or a Server of your choice to communicate with your Traka system. Tick this option and nominate a PC or Server to Auto Communicate with the desired system, then enter the PC Name, IP or IP Name. Only the nominated PC will attempt to Auto Communicate with the selected System.



If nominate a PC is left un-ticked, then any copy of Traka 32 set for auto-communications will attempt to communicate with the selected system.

10. Click on **Save & Close**.

4.20.3 RELAYING ON MICROSOFT EXCHANGE SERVER

This is a guide to configuring Microsoft Exchange Server for relaying so that Traka32 can send e-mails to the outside world. In Traka32 we are not able to access a Microsoft Exchange Server E-Mail account directly to send e-mails and so we use the SMTP capabilities of Microsoft Exchange Server (or any SMTP Server) to send e-mails.

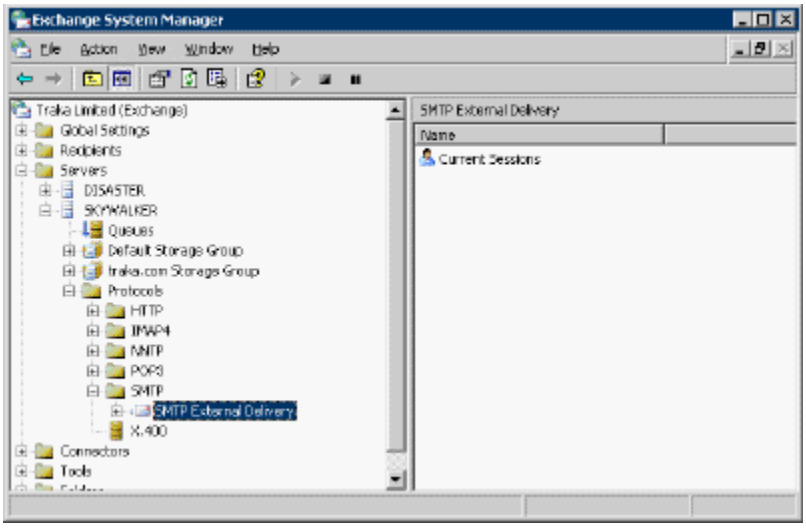
Traka32 simply uses TCP/IP to connect to an SMTP server to send e-mails. Traka32 can have problems sending e-mails if the SMTP Server cannot authenticate who the sender of the e-mail is. The SMTP server will block the e-mail from being sent and an error will occur in Traka32. To overcome this problem you simply need to configure the SMTP to allow relaying from either your internal network or from the specific IP address of the PC running Traka32.

Relaying is the use of a server to accept and then resend mail to recipients on another server.

NOTE: It is very important to be aware that you should not enable your SMPT Server to allow relaying from just anywhere otherwise this could be abused. If you narrow down the relaying to the individual PC's that run Traka32 there is no risk. This configuration should only be carried out by a qualified Microsoft Exchange Server administrator.

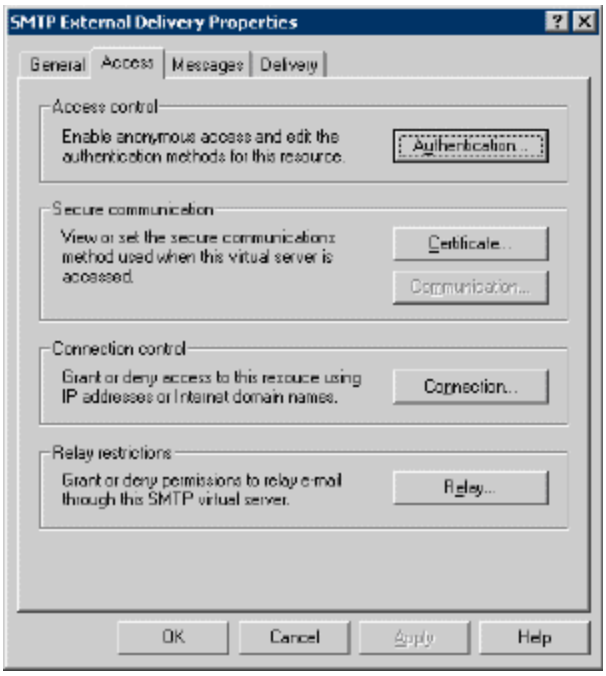
The guide below is based up Microsoft Exchange Sever 2003 and shows how to enable e-mail relaying safely for Traka32...

1. Click on **Start**, **All Programs**, **Microsoft Exchange**, **System Manager**.
2. From the System Manager, expand the **Servers**, **<Server Name>**, **Protocols**, **SMTP** tree.

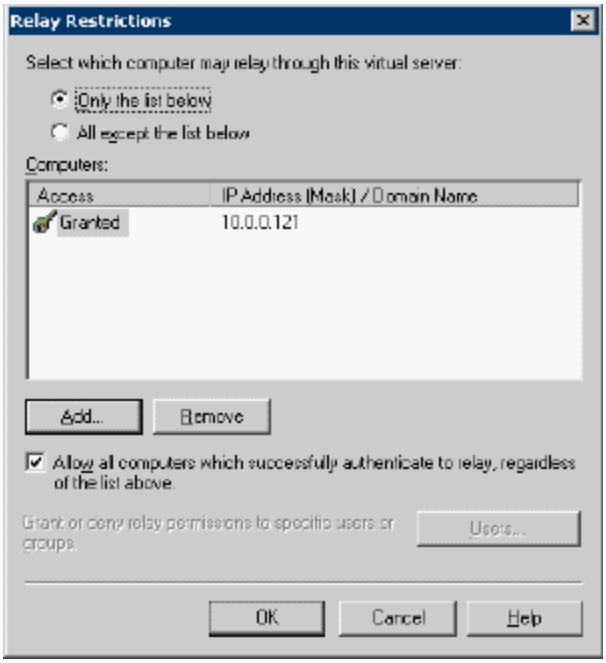


3. Right click over **SMTP External Delivery** and click on **Properties**.

4. From the SMTP External Delivery Properties window, click on the **Access** tab.



5. In the **Relay Restrictions** section, click on **Relay...**



6. From the Relay Restrictions window, select the **Only the list below option** and **Add** in an entry for either the domain or for the specific PC that is running Traka32.

4.20.4 MESSENGER ON MICROSOFT WINDOWS

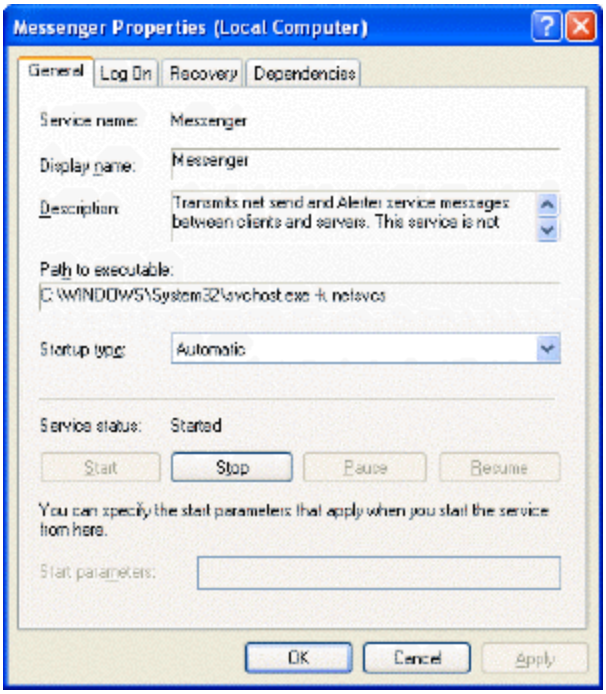
This is a guide to enabling the Microsoft Messenger Service to allow Traka32 to send NetSend messages across a domain.

NetSend is only available on NT based operating system such as Windows ME, 2000, NT and XP. NetSend will not work on Windows 95 or 98.

The Messenger Service must be enabled on all workstations that wish to receive the messages as well as the workstation running Traka32.

To enabled the Messenger Service...

1. Click on **Start**, **Control Panel**.
2. Double click on **Administrative Tools**.
3. Double click on **Services**.
4. In the list of services, look up the **Messenger Service** and double click on it. The Messenger Properties window will open.



5. Set the **Start-up Type** to **Automatic**.
6. Click on the **Start** button and wait for the service to start.
7. Click on the **OK** button.

4.20.5 ALARM & EVENT TYPES

Alarm Types

1. **Triple Primary PIN:** Occurs when a user enters their PIN incorrectly three times or when an unrecognised card is swiped three times.
2. **Door Left Open:** Occurs when a user accesses the system and does no close the door when finished.
3. **Power Fail:** Occurs when the Traka System's mains power fails and Traka runs on its battery backup.
4. **Unauthorised Item Taken:** Occurs when an item is removed from the system by an unauthorised user. This generally can only occur in a non-locking system.
5. **Reserved Item Taken:** This alarm type is not currently used.
6. **Item Undetectable:** Occurs when an Item is removed from the system when the door appears to be closed. This type of alarm can occur when a Traka System is having difficulty reading an Item, in which case the Item is booked out and back in very quickly.
7. **No Transaction Took Place:** Occurs when a user accesses the system but does not take or return any iFobs.
8. **Overdue :** Occurs when an Item goes out under a curfew and is not returned within the time limit set.
9. **iFob Emergency Release:** Occurs whenever an iFob is released using the Emergency Release utility from the iFob Menu of the System Viewer.
10. **System Has Been Reset:** Occurs whenever a hardware or software reset is performed.
11. **User's Quota Exceeded:** Occurs when a user takes more Item than their quota allows.
12. **Door Opened Manually:** Occurs when the door is opened without a user swiping their card or entering their PIN. This would typically occur if the Master Key is used to open the door or if the door has not been closed properly or the door has been forced open.
13. **Alarm Table is Full:** Occurs when the alarm memory within the Traka System has become full. When the alarm memory becomes full, it will start to overwrite the oldest alarms in order to keep the most recent information.
14. **Transaction Table is Full:** Occurs when the transaction memory within the Traka System has become full. When the transaction memory becomes full, it will start to overwrite the oldest transactions in order to keep the most recent information.
15. **Data iFob CRC Failure:** Occurs when the Traka System detects corrupt data when reading data from a Data32 or Data512 iFob used with the Traka Immobilisor.
16. **Immobilisor CRC Failure:** Occurs when the Traka Immobilisor System detects corrupt data when reading or writing data from or to a Data32 or Data512 iFob.
17. **Item Returned to Wrong Location:** Occurs when a user return an Item to the incorrect location.
18. **Unrecognised Item Returned:** Occurs when a user returns an Item that has not been configured for that system.
19. **Triple Secondary PIN:** Occurs when a user enters their secondary PIN incorrectly three times.
20. **Data iFob Read Error:** Occurs when the Traka System was unable to read data from a Data32 or Data512 iFob.
21. **Data iFob Write Error:** Occurs when the Traka System was unable to write data to a Data32 or Data512 iFob.
22. **Date & Time Before Set:** Occurs before the data and time of the system is changed to record the previous date & time. This alarm type on not currently implemented.

23. **Date & Time After Set:** Occurs after the data and time of the system is changed to record the new date & time. This alarm type on not currently implemented.

24. **Remote Item Release via SMS:** Occurs when an Item is released from the system via SMS.

25. **All Item In System:** This alarm does not get recorded but is used in conjunction with the alarm relays to indicate when all the Item are in the system.

26. **Items Out of System:** This alarm does not get recorded but is used in conjunction with the alarm relays to indicate when1 or more Items are out of the system.

27. **Item Removed from wrong location:** Occurs when an incorrectly replaced item has been removed to show who the user was that took it.

28. **Fault code not entered:** Occurs when a user returns an iFob and walks away without entering a fault code.

29. **Location not entered:** Occurs when a user returns an iFob and walks away without entering a location.

30. **Mileage not entered:** Occurs when a user returns an iFob and walks away without entering a mileage.

31. **Fuel level not entered:** Occurs when a user returns an iFob and walks away without entering a fuel level.

32. **Reason code not entered:** Occurs when a user returns an iFob and walks away without entering a reason code.

33. **Vehicle fuel quantity not entered:** Occurs when a user returns an iFob and walks away without entering a vehicle fuel quantity.

34. **Vehicle oil quantity not entered:** Occurs when a user returns an iFob and walks away without entering a vehicle oil quantity.

35. **Vehicle wash cost not entered:** Occurs when a user returns an iFob and walks away without entering a vehicle wash cost value.

36. **Vehicle tyre quantity not entered:** Occurs when a user returns an iFob and walks away without entering a vehicle tyre quantity.

37. **Door Closed Manually:** Reserved for special projects.

38. **Remote Item Release:** Occurs when an Item is released from the Traka32 software using the Remote Item Release utility.

39. **User Has Returned All Item:** Occurs when a user has returned all Item that were previously booked out to them. No audit is recorded for this event; the event is only available for activating the Alarm Output relays on the Control PCB.

40. **User Has 1 Or More Item Out:** Occurs when a user has 1 or more Items booked out to them. No audit is recorded for this event; the event is only available for activating the Alarm Output relays on the Control PCB.

41. **Key Booking Completed:** Occurs when a key booking has been completed. This event only applied to Random Return to Multiple System.

42. **Door Open Authorised:** Occurs when there is an authorised opening of the Traka System door. No audit is recorded for this event; the event is only available for activating the Alarm Output relays on the Control PCB. This event can be used for triggering CCTV systems etc.

43. **Transfer Item Ownership:** Occurs when the ownership of an Item is transferred from one user to another.

44. **Item Returned without Data Entry:** Occurs when a user returns an Item without entering the required data. This event is only recorded with the iFob Return Prompt option.

45. **Item Returned without Data Entry Now Removed:** Occurs when an Item was returned without the required data being entered and has been removed to show who the user was that took it. This event is only recorded with the iFob Return Prompt option.

46. **Lockout Status Cleared:** Occurs when a lockout status has been cleared. This event is only recorded with the Maintenance Lockout Facility option.

47. **Daily vehicle checks not entered:** Occurs when the daily vehicle checks have not been entered at the cabinet. This event is only recorded with the Daily/ Weekly Vehicle checks option.

48. **Weekly Vehicle checks not entered:** Occurs when the weekly vehicle checks have not been entered at the cabinet. This event is only recorded with the Daily/ Weekly Vehicle checks option.

49. **User iFob Expired:** Occurs when a User iFob has expired.

50. Active User Accessed System

51. **Receptor Solenoid Activated:** Occurs when a receptor solenoid has become activated. No audit is recorded for this event; the event is only available for activating the Alarm Output relays on the Control PCB.

52. **Fault Cleared:** Occurs when a fault has been cleared by a User at the cabinet. This event is only recorded with the Fault Logging option.

53. **Low External Battery (16bit Only):** Occurs when the Traka system backup battery is low.

54. **Breath Test Passed:** Occurs when a User has PASSED the alcohol toxicity breath test. This event is only recorded when the firmware has Alcolock integration enabled.

55. **Breath Test Failed:** Occurs when a User has FAILED the alcohol toxicity breath test. This event is only recorded when the firmware has Alcolock integration enabled.

56. **Item Re-detectable:** Occurs when an Item has been redetected by the cabinet after previously being marked as undetectable.

57. **Fingerprint Verification Fail:** Occurs when the Biometrics reader fails to verify a Users fingerprint.

58. **Security Seal Confirmation not entered:** Occurs when a User does not enter the Security Seal I.D after being prompted to do so by the cabinet. This event is only recorded when the firmware has Security Seal Confirmation enabled.

59. **Security Seal different, please check:** Occurs when a User has entered a Security Seal I.D that does not match the I.D stored against the iFob.

60. **Fire Alarm Activated:** Occurs when the system detects that a Fire Alarm has been activated which in turn overrides the access rights to the iFobs.

61. **Fire Alarm Ended:** Occurs when the system detects that the Fire Alarm has ended in which case the access rights to the iFobs are returned to normal.

62. **Item not taken:** Occurs when a User has **not** taken 1 or more Items by a particular time as set by the 'key not taken' curfew in the User Details section of Traka 32.

63. **Breath Test Sample Not Given:** Occurs when a user fails to provide an adequate breath sample within the 20 seconds allowed. This event is only recorded when the firmware has Alcolock integration enabled.

64. **Fire Alarm Emergency Release:**

65. **Unauthorised Item Returned:** Occurs when an item has been returned without authorisation.

66. **Unauthorised Item Returned Now Removed:** Occurs when an item has been returned without authorisation and then been removed again.

67. **User Has Not Taken An Item:** Occurs when an item has a curfew or booking logged against it for a certain period of time and the item has not been removed.

68. **User Has Not Returned All Items:** Occurs when an item has a curfew or booking logged against for a certain period of time, the item is then removed but not returned before the curfew or booking.

69. **Toolset Check Incomplete:** Occurs when a user fails to check their toolset

70. **Toolset Checked Incomplete:** Occurs when a user doesn't fully complete a toolset check
71. **Toolset Not Checked:** Occurs when a user doesn't check their toolset
72. **Allowance Reached:** Occurs when a user has taken their predefined allowance of items.
73. **User Duress Alarm:** Occurs when a user activates the user duress alarm.
74. **Item Returned by a Different Person:** Occurs when a user removes an item from the system but another user returns it.
75. **CC TV Trigger:** When enabled this alarm will trigger for 1 second when the following events occur: User logged into cabinet, iFob returned to wrong slot, The user is not logged into the cabinet (e.g. No door system) and they return an iFob.
76. **Job Reference Not Entered**
77. **Dock Door Override Activated**
78. **Dock Door Override Deactivated**
79. **Dock Door Opened Via Override**
80. **Dock Door Opened**
81. **Unrecognised Item Removed**
82. **Keys Not Weighed**
83. **Key Weight Out Of Range**
84. **Key Booking Overdue:** Occurs when a key is not returned within the booking period
85. **Key Booking Overridden:** Occurs when an iFob has been booked to a user but a different user takes the iFob using the override access level of 195.
86. **Illegal Key Release:** Occurs when an iFob has gone undetectable whilst a user is logged in.

Event Types

127. **SFC Alarm Cleared:** Occurs when a Siemens Fire Control alarm is cleared.
128. **Item Removed:** Occurs when an item is removed from the system.
129. **Item Returned:** Occurs when an item is returned to a system.
130. **Locker Opened:** Occurs when a locker door is opened.
131. **Item Returned for Data Entry:** Occurs when data is entered prior to an items return. This event is only recorded with the iFob Return Prompt option.
132. **Access via Biometrics Reader:** Occurs when a user gains access to the system by using a biometrics reader.
133. **Access via iFob Reader:** Occurs when a user gains access to the system using the iFob Reader.
134. **iFob Per Person Data Buffer:**
135. **Booked Item Removed:** Occurs when an item is removed from the system via a booking. This event is only recorded with the Key Booking option.
136. **Immobilisor iFob Per Person Assigned:**
137. **Breath Test Passed:** Occurs when a user attempts to remove an asset and passes the breath test.
138. **Toolset Check Initiated:** Occurs when a tool set check is underway.

139. **Toolset Check Completed:** Occurs when a toolset check is completed.

140. **Toolset Allocated For Checking:** Occurs when a toolset is automatically allocated to a user ready for checking.

141. **Toolset Checked And Complete:** Occurs when a user has fully checked and completed their toolset.

142. **Overdue Item Returned:** Occurs when an item is returned after the booking/curfew time has expired.

143. **User Enrolled:** Occurs when a user has successfully enrolled.

144. **Key Handover Part 1:** Occurs when a user has had a key handed over to them.

145. **Key Handover Part 2:** Occurs when a user hands a key back to the user who handed it to them.

146. **Job Reference Logging:** Occurs when a user enters their job reference code into the system.

147. **Locker Occupied:**

148. **Locker Unoccupied:**

149. **Dock Door Opened via iFob:**

150. **Dock Door Closed:**

151. **Key Weight OK:**

152. **User Logged In:**

153. **User Logged Out:**

154. **iFob Recharge:**

4.20.6 ACCESS LEVELS

Each iFob must be assigned with an access level. The access level is a number between 1 - 200 for 8bit systems and 1 - 2560 for 16bit systems and does not relate to the position of the iFob.

For a user to be able to take an iFob with a specific access level, you simply need to allocate that access level to the users Current Access Levels list.

To add meaningful descriptions to each access level, please refer to the Access Level Name section.

Access levels can also be used for other purposes depending if the system has been configured with certain optional features...

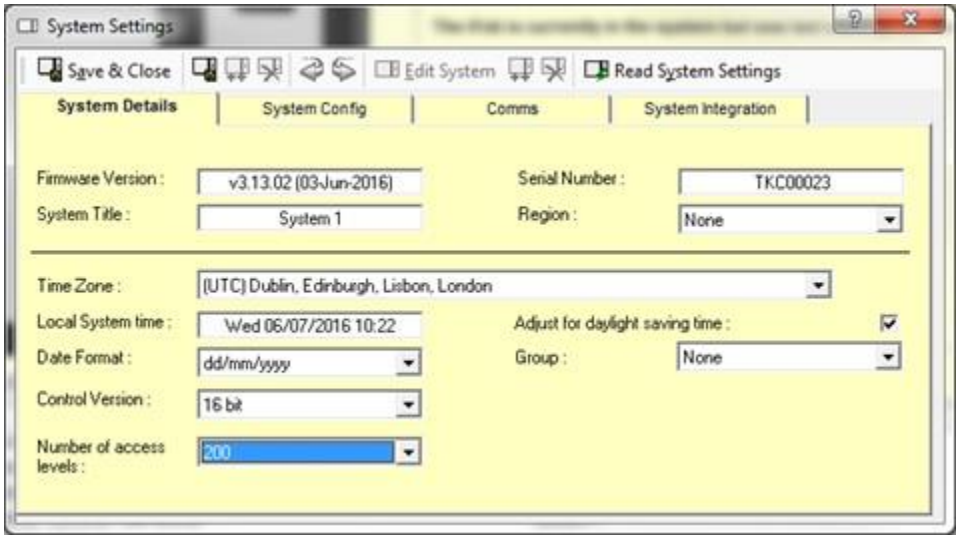
Access Levels		Feature	Purpose
Normal	Reduced User Security 8bit ONLY		
200	8	Fault Logging	If a critical fault is logged when an iFob is returned, only users that have this access level in addition to the access level of the iFob can take the iFob until the fault is cleared. Also if the additional Fault Logging option 'Allow Faults to be Logged at Cabinet' is enabled, users with access level 200 can clear the fault at the cabinet.
200	8	RRMS & Temp Key Store	Access Level 200 is used as an override to remove any iFob/Key. Usually when this system is used any user with access to the cabinet can put any iFob into any available slot, and only the user who inserts the iFob(s) can then remove it/them. With Access Level 200, a user can remove all iFobs that are present in the cabinet.
200	8	Authorisers	Having Access Level 200 will override Access Level 199 for the Deny Single Authoriser option. This will allow a particular user to access all 'Deny Single Authoriser' iFobs without requiring authorisation themselves.
199	7	Authorised Access	Used with either System or iFob authorisers with the 'Force Access Level 199 to Authorise' feature, it allows a user to authorise other users and also self-authorise.
198	6	iFob Access Times	If you assign a user with this access level, this will override the iFob Access Times allowing that user 24 hour access to the restricted iFobs.
197	5	Fire Control	This access level identifies a user who can respond to the fire control alarms.
196	4	Immobilisor	This access level identifies a user who can remove a Program, Service, Test and Debug iFob.
195	3	Key Booking, System Lockdown	This access level identifies a user who can override a key booking and remove an iFob during the booking period. It also identifies a user who can remove an iFob in Wrong Slot during System Lockdown.
194	This option does not function on 8bit systems	Tool Set Checking	This access level (Random Toolset Checker) when enabled defines a user who must be prompted to check/audit randomly selected toolsets.
193	This option does not function on 8bit systems	Authorised Access	Much like access level 199, used with either System or iFob authorisers with the 'Force Access Level 193 to Authorise' feature, it allows a user to authorise another user but not self-authorise.

User Definable Number of Access Levels Per Cabinet

Each system can have the number of usable access levels defined. The default number of access levels is show below:

System Type	Number of Access Levels
16bit systems - Key Cabinets	2560
16bit systems - Locker Systems	200
8bit Key Cabinets and Locker Systems	200
8bit with Half Reduced User Security	8
8bit with Full Reduced User Security	8

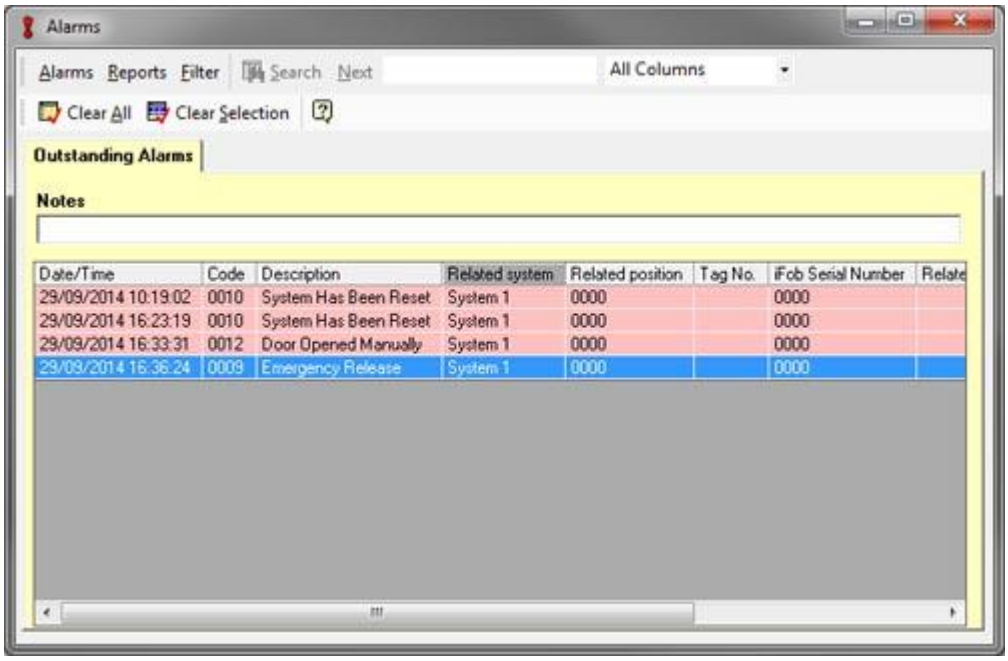
In the System Settings screen for a cabinet, you can select the number of access levels that you want to use (up to the maximum allowed for the cabinet configuration), the benefit of doing this is that it reduces that amount of time in all the calculations and the form load time anywhere where the access levels are displayed. E.g. iFob Details, User Details, Access Grid etc.



4.20.7 ALARM NOTIFICATION

When Traka32 downloads one or more alarm type events, the following symbol will appear in the status bar . Optionally Traka32 will play a notification sound if the **Allow Traka32 to play sounds** property is enabled. For further details on enabling sounds, please refer to the Properties section.

When a notification occurs, double click on the symbol.



To clear the alarms...

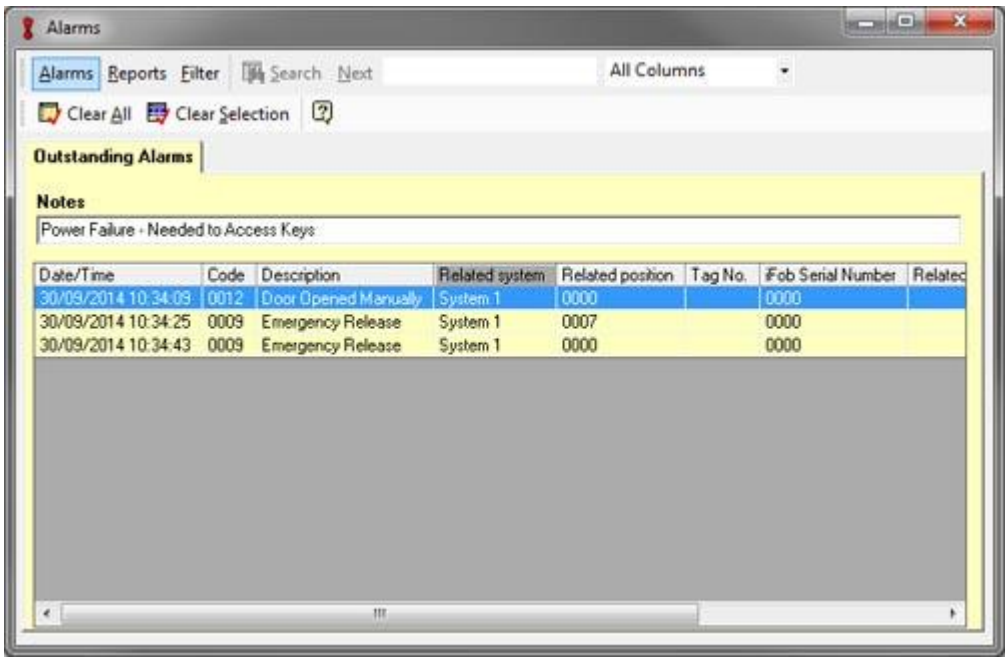
- Click on **Clear All** to clear all current alarms or
- Highlight the alarms that you wish to clear and click on **Clear Selection**.

  To highlight a group of alarms, click on the first alarm, hold down the **Shift** key and click on the last alarm in the group.

  To highlight several individual alarms hold down the **Ctrl** key and click on the alarms in the group.

Entering Notes

You can enter a note against each alarm that is cleared. Simply highlight the desired alarm/s, enter a note into the provided field and select the **Clear Selection/Clear All** button. The notes field is limited to 255 characters.



Reports

When alarms are cleared an audit is kept of when the alarms were cleared and who by. You can view this information by running the Reports > Crystal Report > Events > Alarm History report. Notes are logged against the single or multiple alarms (depending on what was selected) and a list of the associated alarms underneath.

Alarm History Report

Alarm Notes: iFob Became Undetectable

Date/Time	Code	Description	Related system	Related position	Tag No.
30/09/2014 10:34:43	9	Emergency Release	System 1	0	0
30/09/2014 10:34:25	9	Emergency Release	System 1	7	0

Alarm Notes: Power Failure - Needed to Access Keys

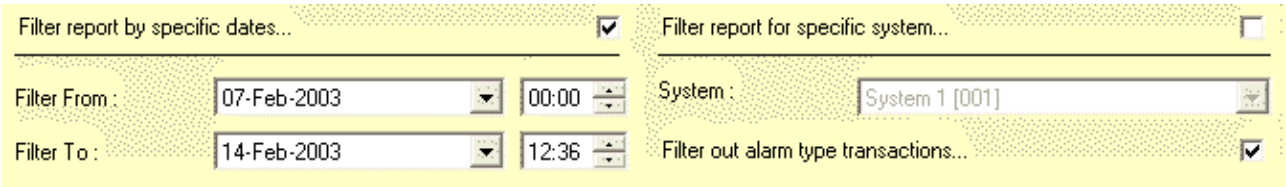
Date/Time	Code	Description	Related system	Related position	Tag No.
30/09/2014 10:34:09	12	Door Opened Manually	System 1	0	0

NOTE: Alarm notification will only work when firmware version 6.07.31 or above is used.

4.20.8 LISTS & REPORTS

4.20.8.1 FILTERING REPORTS

The reports filter can be used to filer the any of the reports between certain date and times and between systems.



Filtering Dates

To view all the transactions that have ever occurred, clear the 'Filter report by specific dates' checkbox.

To view transactions between certain dates, check the 'Filter report by specific dates' checkbox and specify the **From** and **To** date and time.

Filtering Systems

To view the transactions for all systems, clear the 'Filter report for specific systems' checkbox.

To view the transactions for a specific system, check the Filter report for specific systems' checkbox and select the system from the **System** drop down menu.

Filter out alarm type transactions

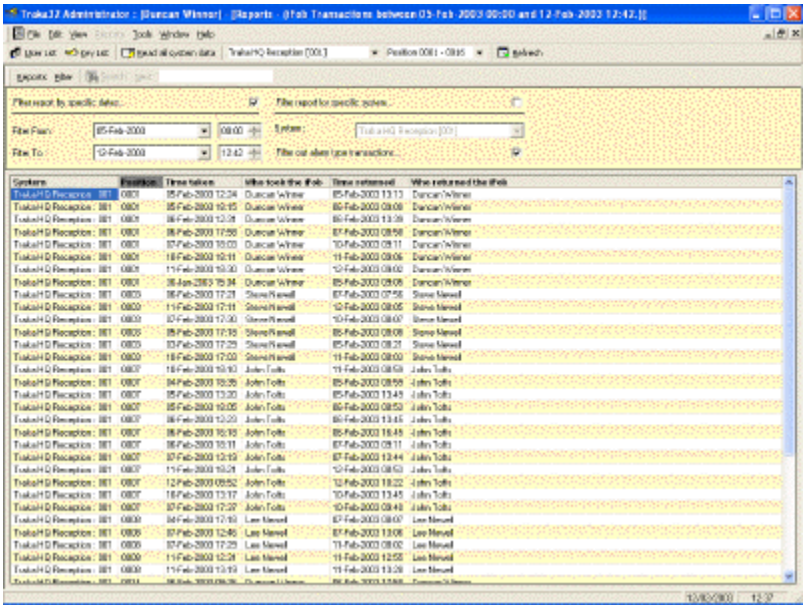
Check the box to filter out transactions that start and end within the same minute. These types of transactions can occur when a Traka System is having difficulty reading an iFob, in which case the iFob is booked out and back in very quickly. Traka records these transactions so not to compromise on accuracy but can make it difficult to see valid transactions.

4.20.8.2 SORTING LISTS AND REPORTS

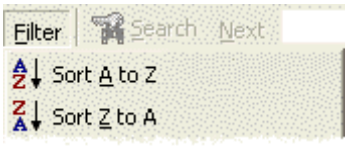
All the lists and reports within the Traka32 software can be sorted in the same way.

1. Simply highlight the top of the column that you wish to sort by.

   For example I want to sort by the Position column...



2. At the top of each list or report there is a **Filter** menu. Simply click on **Sort A to Z** to sort the column in ascending order or **Sort Z to A** to sort the column in descending order.



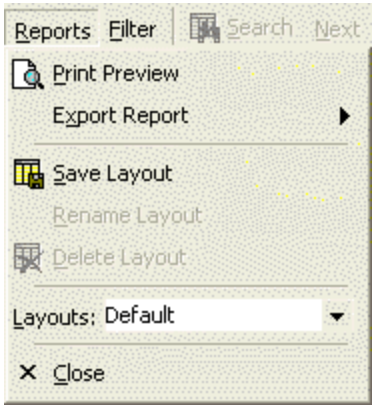
4.20.8.3 CUSTOMISING LISTS AND REPORTS

All the lists and reports within the Traka32 software can be customised in the same way.

General

- Each column may be moved by clicking over the column and dragging it to the required location.
- By clicking with the right mouse button over the report the **Show column** menu will appear. By checking or un-checking the options the report will display the relevant columns.

Reports Menu



Print Preview

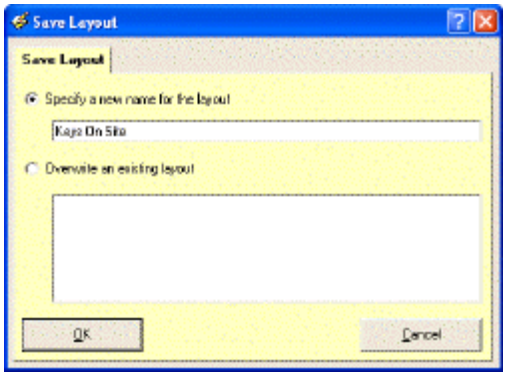
Click on Print Preview to view and print the selected list or report.

Export Report

Reports may be exported to Microsoft Excel. You will be asked the name and destination of the report.

Save Layout

Once you have modified a report layout you may save the layout with a name.



Specify a new name for the layout

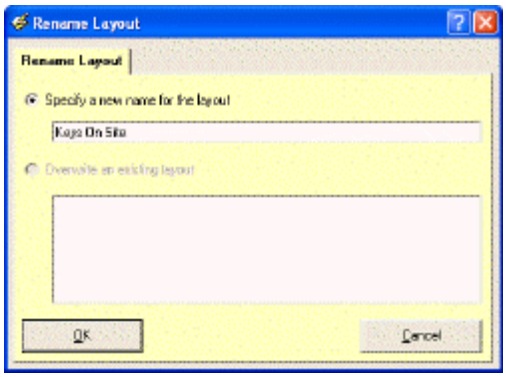
Enter the name of the new layout and click OK. **Note:** You cannot have more than one layout with the same name.

Overwrite an existing layout

If you wish to overwrite an existing layout, select the overwrite option, select the layout from the list and click OK.

Rename Layout

To rename a saved layout simply select the layout that you want to rename from the Layout List and click on Rename Layout. Specify a new layout name and click on OK to rename.



Specify a new name for the layout

Enter a new name for the layout and click OK. **Note:** You cannot have more than one layout with the same name.

Delete Layout

To delete a saved layout simply select the layout that you want to delete from the Layout List and click on Delete Layout.

Layout List

To load a saved layout, simply select the layout required from the drop down Layout list.

NOTE: Whenever you open a new window, the Default layout is automatically selected.

4.20.8.4 SEARCHING

4.20.8.4.1 STANDARD SEARCHING

All the lists and reports within the Traka32 software can be searched upon all in the same way.

1. At the top of each list or report there is a search menu...

2. If you wish to search on a specific column simply select the column title from the drop down list. To search all the visible columns select **All Columns**.

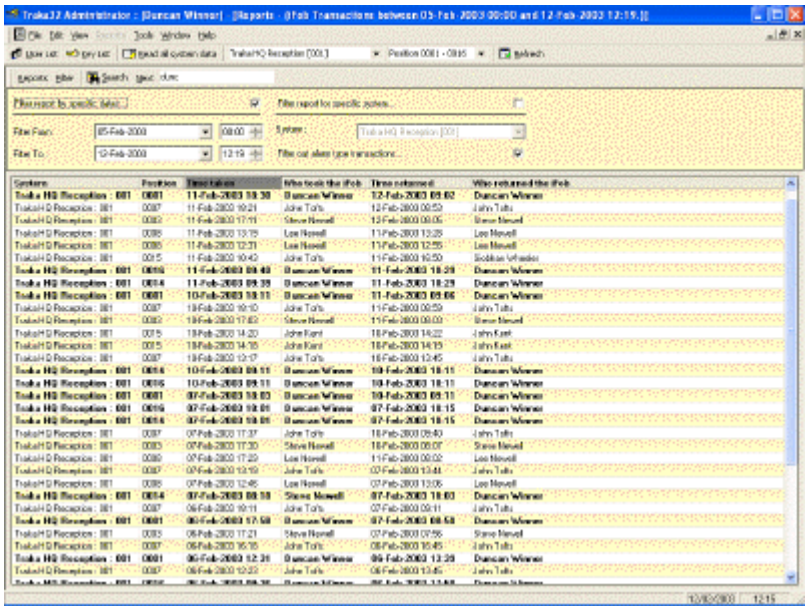
NOTE: Traka32 versions 01.05.0003 or before does not allow you to search by specific columns.

3. To search simply **type in all or part of a word or number** that you want to search on and press **Enter** or click on the **Search** button.

   For example if I want to search for Duncan...

4. All of the data that is visible in the list or report will be searched.

   - If one or more matches are found the records will be highlighted in the list or report. To move to the next record found in the search simply click on **Next**.



   - If no matches are found the following message will be displayed...

4.20.8.4.2 ADVANCED SEARCHING

Advanced Searching is similar to Standard Searching but allows you to search on more than one criterion and also filters the list so that only records that have matching criteria are visible.

To enable the Advanced Searching feature, check the Use Advanced Searching option in the Properties window.

All the lists and reports within the Traka32 software can be searched upon all in the same way.

1. At the top of each list or report there is a search menu...

2. If you wish to search on a specific column simply select the column title from the drop down list. To search all the visible columns select All Columns.

NOTE: When using the option 'Advanced Search' you will not be able to select 'All Columns' when searching for a user or a key.

3. To search simply type in all or part of a word or number that you want to search on and press Enter or click on the Search button.

   For example if I want to search for Duncan...

   All of the data that is visible in the list or report will be searched.

4. If one or more matches are found the only the records with matching criteria will be visible.

5. If no matches are found the following message will be displayed...

6. Repeat step 3 to search on additional criteria. The search criteria are listed in the search menu.

7. To clear the search, click on the Clear button.

4.20.9 FIRMWARE UPGRADES

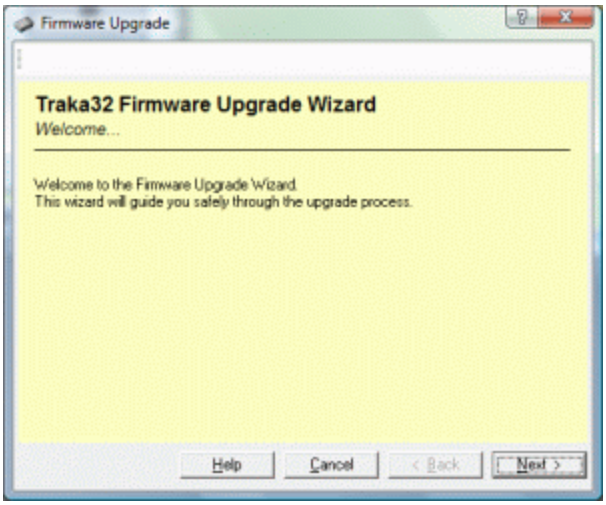
4.20.9.1 8BIT FIRMWARE UPGRADE

If you are upgrading the Traka32 software and firmware, please ensure you upgrade the Traka32 software before upgrading the firmware.

Upgrading the firmware will take approximately 5 minutes per Traka system to complete. Please ensure that any important keys are removed from the systems prior to the upgrade, as it may be difficult to obtain the keys during the upgrade.

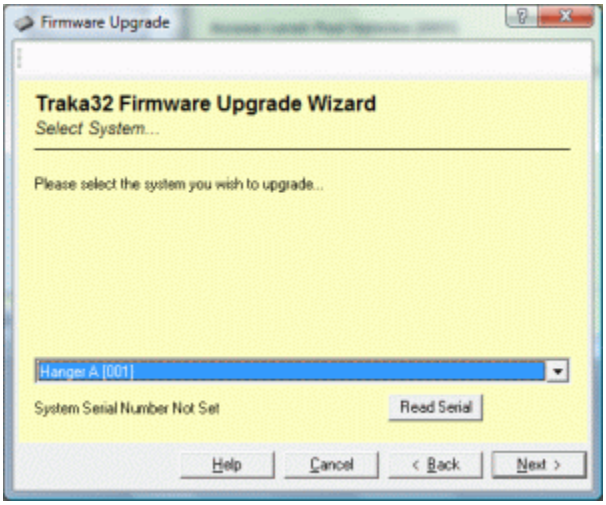
Please ensure you have the correct upgrade file for your system! Using an incorrect file may stop your system from working. If in doubt, please contact your supplier.

1. Click on **Tools** followed by **Upgrade Firmware** from the main menu.



2. Click on **Next.**

3. Select the system that you wish to upgrade.



If you see '**System Serial Number Not Set**', click on the either:

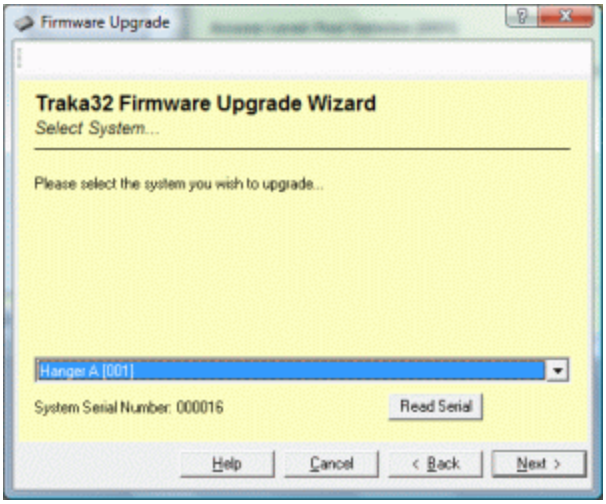
- **Enter Serial**

  For older systems (firmware version 6.06.01 and above), enter the serial number of the system. This can be located on the inside of the Pod.

- **Read Serial**

  For newer systems (firmware version 6.06.02 and above), this will read the serial number from the firmware of the system.

4. When you have selected the system and confirmed the serial number is correct, click on **Next**.



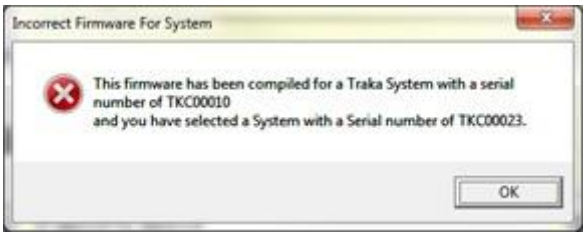
5. Select the path to the upgrade file. To search for the upgrade file simply click on the **Browse** button.

   NOTE: If you have more than one Traka System to upgrade and depending on the configuration there maybe a separate T6_xxxxx.s1f files for each Traka System. The xxxxx part of the file name should match the 5 digits of the system's serial number.

   NOTE: If your firmware file is stored on a USB drive, to ensure reliability we do ask that you copy the T6_xxxxx.s1f file from the USB drive to your hard disk drive.

6. When you have selected the path to the upgrade file, click on **Next**.

   If the '**Incorrect Firmware For System**' message appears the firmware upgrade file you have selected is not meant for the selected system. Click **Back** to review your system and file selections.



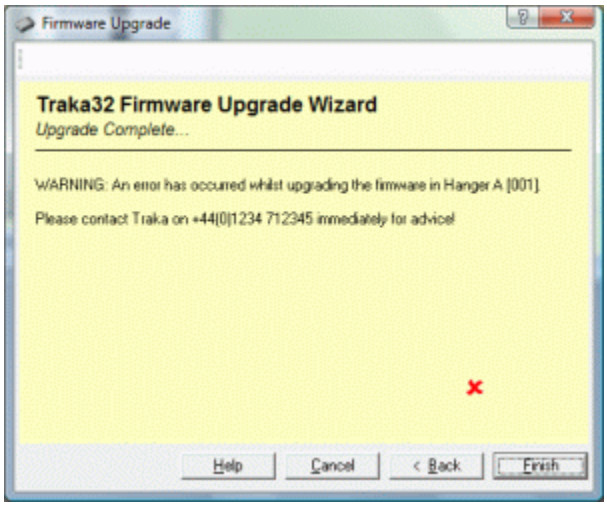
7. Make sure the **Upgrade Firmware Only** checkbox is **NOT** checked (if visible). This option is for use by Traka Engineers only.

8. When you are happy click on **Upgrade.**

The Traka32 software will back up all the data from the selected Traka System, upgrade the firmware and restore all the backed up data.

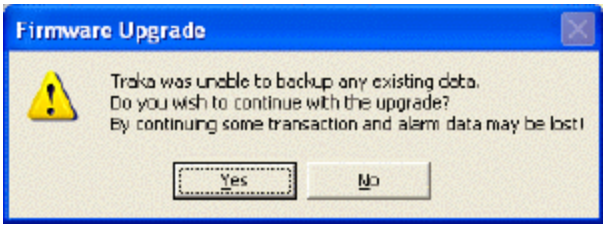
9. Provided the upgrade completed successfully, click on **Finish**

What if the upgrade goes wrong?

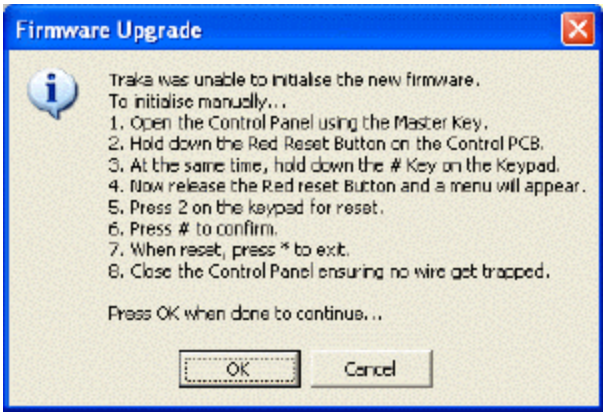


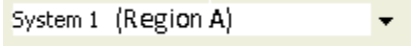
If the upgrade did not complete successfully, click on **Back** and then click on **Upgrade** again to retry.

- If you see the following message during the upgrade, the upgrade wizard was not able to back up the data from the system. If you are not worried about losing some of the transaction or alarm data then click **Yes**. If you do not want to lose any data then click **No** and contact you supplier for further details.



- If you see the following message during the upgrade, the upgrade wizard was unable to detect if the vector was swapped correctly. Follow the instruction on the message and click **OK** when completed to complete the upgrade. If you are in any doubt contact you supplier for further help.



If this still does not clear the problem, click on **Cancel** and then click on **Finish**. From the main screen select the system you have just upgraded 

and from the system viewer right click over the picture of the pod and click on **Synchronise System**. Click **No** to the first message and then **Yes** to the second message and this will complete the upgrade manually.

- If an error has occurred during the upgrade that is not covered, please contact one of our engineers on + 44 (0) 1234 712345 immediately for advice.

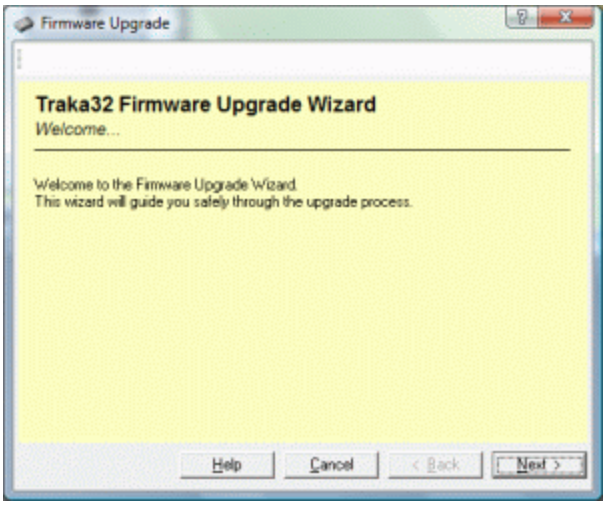
4.20.9.2 16BIT FIRMWARE UPGRADE

If you are upgrading the Traka32 software and firmware, please ensure you upgrade the Traka32 software before upgrading the firmware.

Upgrading the firmware will take approximately 5 minutes per Traka system to complete. Please ensure that any important keys are removed from the systems prior to the upgrade, as it may be difficult to obtain the keys during the upgrade.

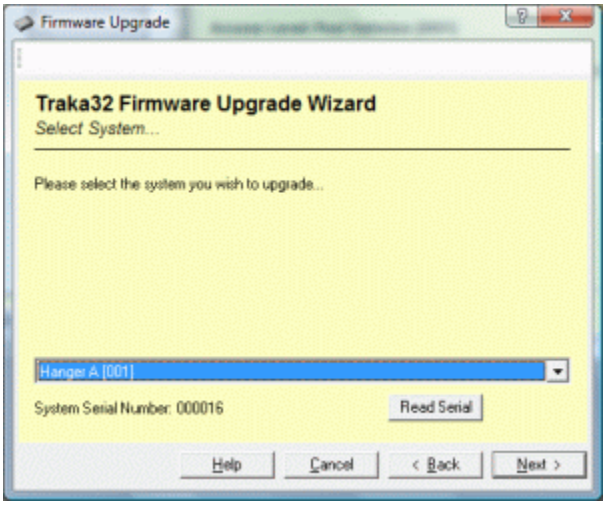
Please ensure you have the correct upgrade file for your system! Using an incorrect file may stop your system from working. If in doubt, please contact your supplier.

1. Click on **Tools** followed by **Upgrade Firmware** from the main menu.



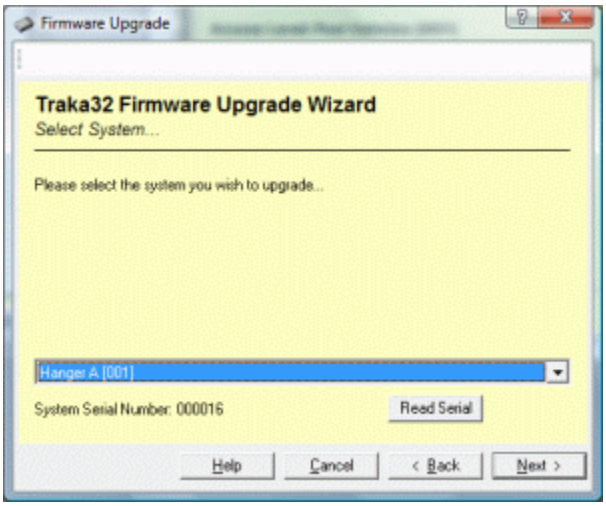
2. Click on **Next.**

3. Select the system that you wish to upgrade.



If you see '**System Serial Number Not Set**', click **Read Serial.** This will read the serial number from the firmware of the system.

4. When you have selected the system and confirmed the serial number is correct, click on **Next**.



5. Select the path to the upgrade file. To search for the upgrade file simply click on the **Browse** button.

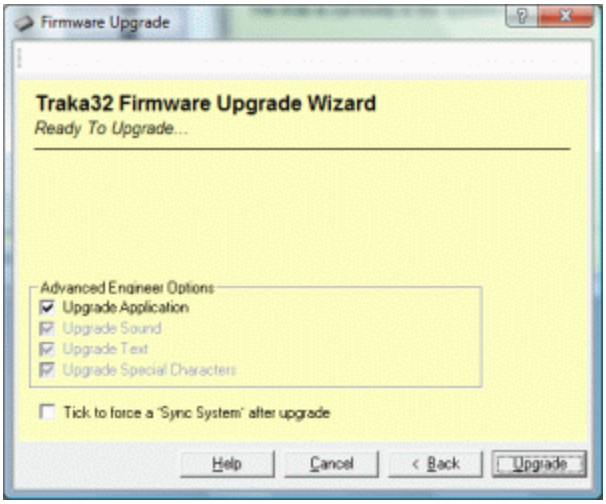
   The firmware upgrade file name will be formatted as follows **TKCvNNNNN-DDDDDD.MOT** where the **NNNNN** part is the version and the **DDDDDD** part is the release date.

   NOTE: If you have the firmware upgrade file on disk USB drive, to ensure reliability we do ask that you copy the .MOT to your hard disk drive!

6. When you have selected the path to the upgrade file, click on **Next**.

   Make sure the following **Advanced Engineers Option** check boxes are **checked** (if visible).
   These options are for use by Traka Engineers only.

   Upgrade Application
   Upgrade Sound
   Upgrade Text
   Upgrade Special Characters



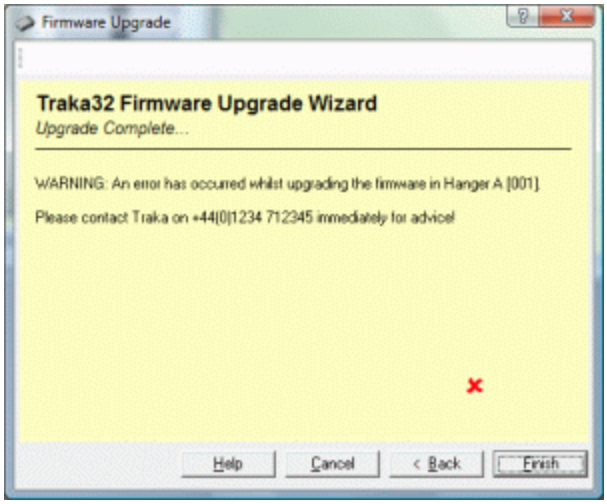
   The firmware upgrade wizard will automatically determine if a Synchronise System is required after the upgrade but this can be forced by checking the **Tick to force a 'Sync System' after upgrade** check box. Ticking this box will not affect the upgrade however it may take slightly longer.

7. When you are happy click on **Upgrade**

The Traka32 software will back up all the data from the selected Traka System, upgrade the firmware and restore all the backed up data.

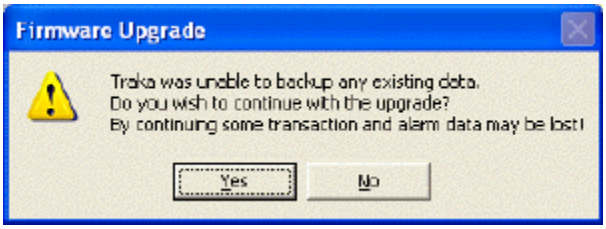
8. Provided the upgrade completed successfully, click on **Finish**.

What if the upgrade goes wrong?

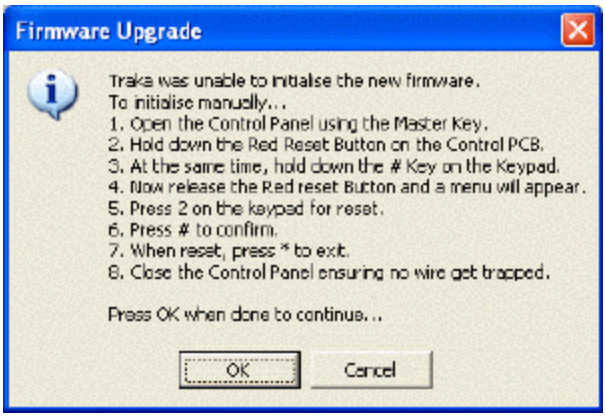


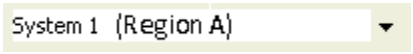
If the upgrade did not complete successfully, click on Back and then click on Upgrade again to retry.

- If you see the following message during the upgrade, the upgrade wizard was not able to back up the data from the system. If you are not worried about losing some of the transaction or alarm data then click on **Yes**. If you do not want to lose any data then click on **No** and contact you supplier for further details.



- If you see the following message during the upgrade, the upgrade wizard was unable to detect if the vector was swapped correctly. Follow the instruction on the message and click **OK** when completed to complete the upgrade. If you are in any doubt contact you supplier for further help.



If this still does not clear the problem, click on **Cancel** and then click on **Finish**. From the main screen select the system you have just upgraded 

and from the system viewer right click over the picture of the pod and click on **Synchronise System**. Click **No** to the first message and then **Yes** to the second message and this will complete the upgrade manually.

- If an error has occurred during the upgrade that is not covered, please contact one of our engineers on + 44 (0) 1234 712345 immediately for advice.

4.20.10 CONFIGURE FIRMWARE

The System Configuration window allows you to view and edit the current configuration of the selected Traka System.

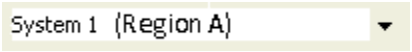
On a 16bit Traka System, the Configure Firmware wizard is also used to register the hardware to the database. This is required before Traka32 will fully communicate with the hardware.

Please refer to the relevant 8bit Configure Firmware or 16bit Configure Firmware Wizard sections for assistance with configuring the firmware.

4.20.10.1 8BIT CONFIGURE FIRMWARE

The 8bit System Configuration window allows you to view the various options that are enabled on the selected Traka System. It is also possible to make minor adjustments to specific parts of the configuration such as the number of receptor strips and reader settings.

The System Configuration window also has Print and Email toolbar buttons that allow you print or email the current configuration in an html format. This is very useful for assisting when requesting upgrade to Traka Systems as this will clarify what options are currently in use.

To open the System Configuration window, from the main screen select the system 

and from the system viewer right click over the picture of the relevant position and click on **Configure Firmware**.

For details on the various settings, please refer to the Firmware Options & Settings section.

Read Configuration

Click on Read Configuration to read the current configuration of the firmware in to the System Configuration window.

Write Configuration

When you are happy with the configuration changes, click on Write Configuration to write the configuration to the Traka Systems firmware.

Read Last Card Swipe

The Read Last card Swipe button reads the last card swiped or PIN entered into the Traka System. This button is useful for testing the card reader settings of the firmware.

Print

Clicking the print button will print a report of the firmware configuration. This can be faxed to Traka on +44 (0)1234 713366 in order to request a new firmware.

Email

Clicking the email button will email a report of the current firmware configuration to support@traka.com. This can be used in order to request a new firmware version.

NOTE: This will only create an email if you have Microsoft Outlook or Outlook Express installed and configured on the local PC.

4.20.10.2 FIRMWARE OPTIONS & SETTINGS

Below is a list of firmware options and settings for the 8bit and 16bit Traka Systems:

Reader

NOTE: The card reader section should not be altered from the factory settings. If you are experiencing problems with the setup of your ID Card, please contact Traka as they will be able to discuss the problems with you and suggest alternate settings which can be altered below.

Main Access Settings

Reader Type

This field shows the current reader configuration compiled into the firmware. The current options are as follows…

- Clock & Data
- Wiegand
- HandKey Wiegand
- Wiegand Interrupt
- RS-232
- RS232 UARTB
- Barcode
- Touch Memory
- Keypad Only
- Biometrics (TSSI)
- NEDAP Access Control
- TriScan
- Sagem MorphoSmart CBM

To alter the choice of reader, please contact Traka with details as a firmware upgrade will be required.

Human Interface Type

Select the Human Interface Device (HID) Type used for access. For example an RFID card or tag would be placed within "proximity" of the reader and a magstripe card would be "swiped" through the reader.

NOTE: This settings has no effect on how the data is decoded; it simply updates the LCD scrolling text accordingly.

Number of bits / bytes to process

Enter the number of bits to process for a **Wiegand** reader or enter the number of bytes to decode for the either an **RS-232**, **Barcode** or **NEDAP Access Control** reader.

For example, for a Wiegand 26bit card you would be 26 bits.

Number of bits / bytes to decode

Enter the number of bytes to decode for either an **RS-232** or **NEDAP Access Control** reader or enter the number of digits required for the PIN on a **Keypad Only** or **Biometrics (TSSI)** reader.

Card Section Count

Select the number of sections of data to decode from a **Clock & Data**, **Wiegand** or **Barcode** reader. The selected number of sections (1 to 4) will enable the relevant number of section settings below.

Wiegand Buffer Base (bits)

This field shows the maximum base size of the Wiegand buffer. This value can be used for calculating the Card Section Starts.

Card Section Start

Enter the start bit or byte for this section.

Card Section Length

Enter the number of bits or bytes within this section to decode.

Card Section Offset

Enter the number of characters to offset the result by.

Card Reader Code

The card reader code can be used with a **Wiegand** reader to display the current configuration in a string.

- * = Ignore this bit
- 1 to 4 = Decode this as the entered section number

For example, for a Wiegand 26bit card the string would read *22222222111111111111111*

The **Encode** button can be used to convert the Card Reader Code into the relevant Card Section Numbers above and likewise the **Decode** button can convert the Card Section Numbers into a Card Reader Code.

End Sentinel

Enter the end sentient character for a **Clock & Data** card. This is the character that tells Traka to stop reading data from the card. The industry standard for the end sentinel is a ’r;**?**’.

RS232 Settings

Enter a decimal value according to the required settings…

0 = 7 Data Bits, No Parity

1 = 8 Data Bits, No Parity

2 = 7 data Bits, Even Parity

3 = 8 data Bits, Even Parity

6 = 7 data Bits, Odd Parity

7 = 8 data Bits, Odd Parity

Please do not enter any other value than specified above.

EOR Check

Check this box if Traka should perform an Exclusive OR (EOR) check to verify the data being read from a **Clock & Data** card.

Parity Check

Check this box if Traka should perform a Parity check to verify the data being read from a **Clock & Data** card.

Invert Section Start

Check this box if Traka should invert the way the card sections are read for a **Clock & Data** card.

Hexadecimal Conversion

Check this box if Traka should convert the decoded card data into Hexadecimal (HEX) rather than decimal for a **Wiegand** card.

2nd Card Format (Wiegand Only)

The requirement for a 2nd Wiegand format can apply if an organisation are using 2 different Wiegand formats for their access control system, e.g 26 bit *and* 37 bit.

Support second card format (Wiegand only)

This box will be checked if the firmware has been configured to support a second Wiegand card format.

The remaining options on this view are a **copy** of the Wiegand options listed under the **Reader Type** section, please see above.

Options

Reader and/or PIN

If this option is available, there are four different ways a user can access a system depending on how you configure a user. Please refer to the User Details section for more information.

Anti Pass back

This box will be checked if the firmware has the Anti Pass back option enabled.

System 1

Product Type

This field shows the related product type, for example, Key Control, Remote Key Box and Lockers etc.

System ID Number

The System ID Number can be altered from 1 to 255.

NOTE: If you alter this setting you will need to alter the System ID Number within the System Details window otherwise the Traka32 software will not be able to communicate with the Traka System if the ID's do not match.

Comms Delay

Slide the Comms Delay control to alter the comms delay between 0 and 255. This value should not be altered from 0 but is made available for bust RS485 network adjustment.

NOTE: If you alter this setting you will need to alter the RS485 Delay within the Properties, Comms window otherwise communication problems could occur.

System Title

Enter a System Title to represent the system you are adding for example Reception or Basement.

LCD Scroll Speed

Slide the LCD Scroll Speed between 1 and 45 to alter the speed at which the LCD text scrolls. 1 is the slowest and 45 is the fastest. The default is **35**.

Language

This field shows the current language setting of the firmware. Please view the Languages topic to see what languages are currently available. To alter the language, please contact Traka for a firmware upgrade.

Date Format

Select the date format that is display on the LCD. You can choose between the following depending on your regional date format.

- mm/dd/yy
- dd/mm/yy
- yy/mm/dd

NOTE: When you click on Set System Date & Time, the current date format of the local PC is written to the selected Traka System.

Automatically adjust clock for daylight saving changes

Selecting this option will automatically adjust the clock on the Traka System for daylight saving time (DST).

NOTE: If the Date Format is set to 'mm/dd/yy' the clock will automatically adjust according to 'Pacific Daylight Saving' rules. If the Date Format is set to 'dd/mm/yy' the clock will automatically adjust according to 'GMT Daylight Saving' rules. If the Date Format is set to 'yy/mm/dd' then no clock adjustment will be made.

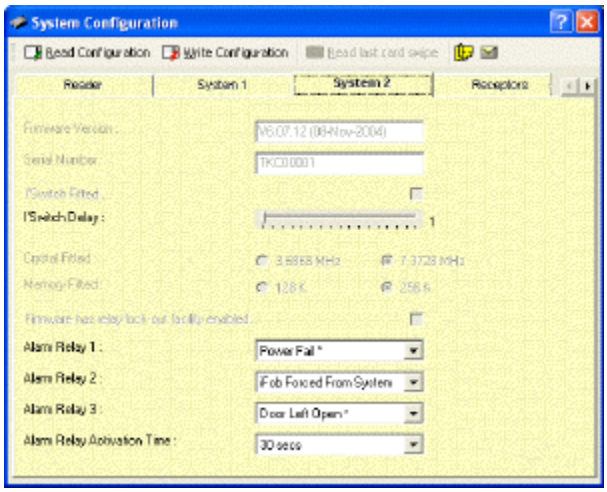
Modem Setup Included

This box will be checked if the firmware has the Modem Setup utility included.

LCD Resynchronisation

Only to be switched on with the advice of Traka R&D. Corrects a display issue only present in certain environments. 16bit only.

System 2



Firmware Version

This field shows the current version of the firmware.

Serial Number

This field shows the serial number of the system.

I'Switch Fitted

This box will be checked if the firmware has the I'Switch Delay utility included.

The Traka I'Switch is a device that allows two set of keypads, LCD's and readers to be connected to a Traka Control PCB. A switch is provided on the I'Switch to toggle between the two set of controls.

I'Switch Delay

The Traka I'Switch is a device that allows two set of keypads, LCD's and readers to be connected to a Traka Control PCB. A switch is provided on the I'Switch to toggle between the two set of controls.

The delay can be adjusted to ensure the smooth scrolling of the LCD display and the accuracy of the keypad response times depending on the distance the controls are from the Control PCB.

Crystal Fitted

This field shows the current crystal speed the firmware has been complied for.

NOTE: The firmware crystal setting must be used with the correct crystal fitted to the Control PCB otherwise errors will occur.

Memory Fitted

This field shows the current memory capacity the firmware has been complied for.

NOTE: The firmware memory setting must be used with the correct memory fitted to the Control PCB otherwise errors will occur.

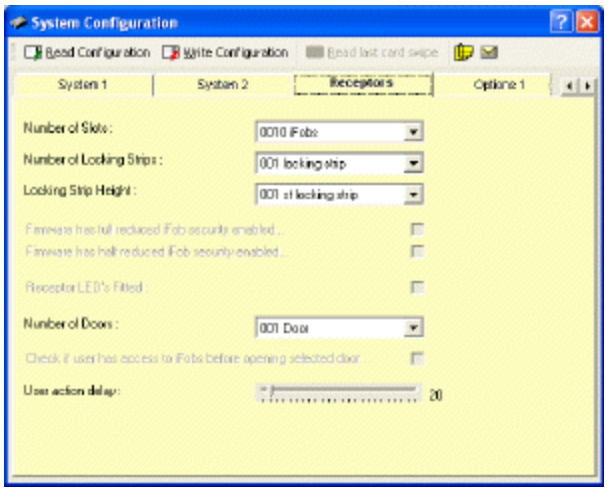
Firmware has relay lock-out facility enabled

This box will be checked if the firmware has the relay Lockout Facility enabled.

Alarm Relay 1 to 3

There are three Alarm Relays fitted to the Traka Control PCB which can be configured to activate under certain circumstances. Simply select the alarm type that you wish to associate with the required relay. The alarms that are marked with a * are conditional alarms which only deactivate when the alarm condition has cleared. All other alarms will activate for a specified period which is defined by the **Alarm Relay Activation Time**.

Receptors



Number of Slots

Select the total number of positions the selected system has.

NOTE: If you alter this setting you will need to alter the Cabinet Configuration settings within the System Details window otherwise the errors could occur.

Number of Locking Strips

Select the total number of locking receptor strips the selected system has.

For example, if you had a 60 way locking system, this would have 6 locking strips.

Locking Strip Height

Select the height of the first locking receptor strip within the selected system starting at 1 for the top strip.

Firmware has full reduced iFob security enabled

This box will be checked if the firmware has full reduced iFob security enabled.

Firmware has half reduced iFob security enabled

This box will be checked if the firmware has half reduced iFob security enabled.

Receptor LED's Fitted

This box will be checked if the firmware has the extra functionality enabled for receptors strips fitted with LED's, such as highlight the iFobs the user has access too and highlighting the correct slot if a user returns an iFob to the wrong slot.

Number of Doors

Select the total number of doors that the selected system has.

NOTE: If you system has no doors, you must keep this setting to No Doors otherwise the system will just display Please Close The Door all the time and you will not be able to communicate without placing a link across the door connector contacts on the Control PCB!

Check if a user has access to iFobs before opening selected door

Selecting this option will only allow a user to open a door if they have access to one or more iFobs behind that door.

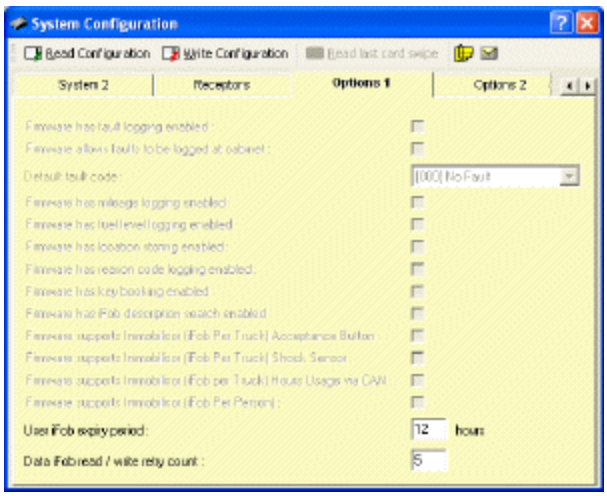
NOTE: This option is only available if the selected Traka System is a Fixed Return system and has more than one door.

User Action Delay

Slide the User Action Delay between 10 and 240 seconds to alter the amount of time a user has to take and return iFobs. The default is **20** seconds.

Options 1

NOTE: The following options are available within the firmware upon request from Traka. If you would like to add or remove any of these features, please contact Traka with the details and Traka will supply you with a firmware upgrade file with the relevant options enabled.



Firmware has fault logging enabled

This box will be checked if the firmware has fault logging enabled.

Firmware allows faults to be logged at cabinet

This box will be checked if the firmware has the ability to log faults from the keypad.

Default fault code

The drop down list allows a default fault code to be selected. When an iFob is returned, the defined fault code will automatically be selected unless changed by the user. This option is only available if the firmware allows faults to be logged at the cabinet.

Firmware has mileage logging enabled

This box will be checked if the firmware has mileage logging enabled.

Firmware has fuel level logging enabled

This box will be checked if the firmware has fuel level logging enabled.

Firmware has location storing enabled

This box will be checked if the firmware has location storing enabled. This is also referred to a Bay Logging.

Firmware has reason code logging enabled

This box will be checked if the firmware has reason code logging enabled.

Firmware has key booking enabled

This box will be checked if the firmware has the key booking utility enabled.

Firmware has iFob description search enabled

This box will be checked if the firmware has the iFob description search facility enabled.

Firmware supports Immobilisor (iFob per Truck) Acceptance Button

This box will be checked if the firmware has immobilisor acceptance button logging enabled.

Firmware supports Immobilisor (iFob per Truck) Shock Sensor

This box will be checked if the firmware has immobilisor shock counter logging enabled.

Enable CRC Check

This option is only available for use with the Traka Immobilisor firmware version 1.4.2 and later. Check this box to enable the CRC checking to ensure reliable data return.

Firmware supports immobilisor (iFob per Truck) Hours Usage via CAN

This option is only available for use with the immobilisor hours usage via CAN option enabled.

Firmware supports immobilisor (iFob per Person)

This box will be checked if the firmware has immobilisor iFob per Person enabled.

User iFob expiry period

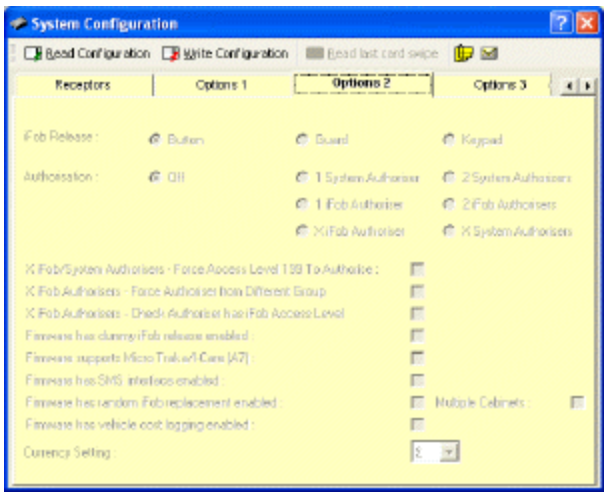
This option is used in conjunction with the Traka Immobilisor (iFob per Person) option. Enter the number of hours the iFob will remain active from the time the iFob is taken. The iFob will no longer work after the time unless returned to the cabinet where it can be re-charged.

Data iFob read / write retry count

Enter the retry count for reading and writing to and from the Data32 and Data512 iFobs. The default is **5**. This value should be increased if you are seeing a large number of **Data iFob Read Error** and/or **Data iFob Read Error** alarms being generated by the Traka System.

Options 2

NOTE: The following options are available within the firmware upon request from Traka. If you would like to add or remove any of these features, please contact Traka with the details and Traka will supply you with a firmware upgrade file with the relevant options enabled.



iFob Release

This field shows the current iFob release method the firmware has been complied for.

- **Receptor Strip** – The user presses the button adjacent to the iFob to request an iFob.
- **Guard** – The user enters the position number of the iFob they require. If authorised the door will open releasing the iFob to a guard who will then issue the iFob to the user. If not authorised or the iFob is already out, a message will be displayed on the LCD allowing the user to pick another iFob. To remove another iFob the guard must close the door and the user must repeat the process. To return the iFob the user simply presses the # key on the keypad, the door will open, the user will pass the iFob to the guard allowing the guard to return the iFob.
- **Keypad** – The user enters the position number of the iFob they require. If authorised the door will open releasing the iFob to the user. If not authorised or the iFob is already out, a message will be displayed on the LCD allowing the user to pick another iFob. To remove another iFob the user must close the door repeat the process. To return the iFob the user simply presses the # key on the keypad, the door will open allowing the user to return the iFob.

Authorisation

1 System Authoriser

This option will be selected if the firmware has the 1 System Authoriser option enabled.

2 System Authorisers

This option will be selected if the firmware has the 2 System Authorisers option enabled.

1 iFob Authoriser

This option will be selected if the firmware has the 1 iFob Authoriser option enabled.

2 iFob Authorisers

This option will be selected if the firmware has the 2 iFob Authorisers option enabled.

X System Authorisers

This option will be selected if the firmware has the X System Authorisers option enabled.

X iFob Authorisers

This option will be selected if the firmware has the X iFob Authorisers option enabled.

X iFob/System Authorisers – Force Access Level 199 To Authorise

This option will be selected if the firmware has either X System Authorisers or X iFob Authorisers options enabled and the authoriser is required to have access level 199. If this option is enabled and the authorisers do not have access level 199 then they will not be able to authorise.

X iFob Authorisers – Force Authoriser from Different Group

This option will be selected if the firmware has X iFob Authorisers option enabled and forces each user to be from a different User Group.

X iFob Authorisers – Check Authoriser has iFob Access Level

This option will be selected if the firmware has X iFob Authorisers option enabled and check to make sure the Authoriser also has the corresponding access level of the iFob that has been requested. This adds an extra level of security where required.

Firmware has dummy iFob release enabled

This box will be checked if the firmware has dummy iFob release enabled.

Firmware has data logging enabled

This box will be checked if the firmware has immobilisor data logging enabled.

Firmware has fire control integration enabled

This box will be checked if the firmware has fire control integration enabled.

Firmware has half reduced user security enabled

This box will be checked if the firmware has half reduced user security enabled.

Firmware has SMS interface enabled

This box will be checked if the firmware has the SMS interface enabled. An external SMS interface module can be added to the Traka system so that iFobs can be remotely released by sending an SMS message via a mobile phone or GSM modem etc. More functionality is planned for the SMS interface. For the latest information, please contact your supplier.

Firmware has random iFob replacement enabled

This box will be checked if the firmware has random iFob replacement to a single cabinet enabled.

Multiple Cabinets

This box will be checked if the firmware has random iFob replacement to multiple cabinets enabled.

Firmware has vehicle cost logging enabled

This box will be checked if the firmware has vehicle cost logging enabled.

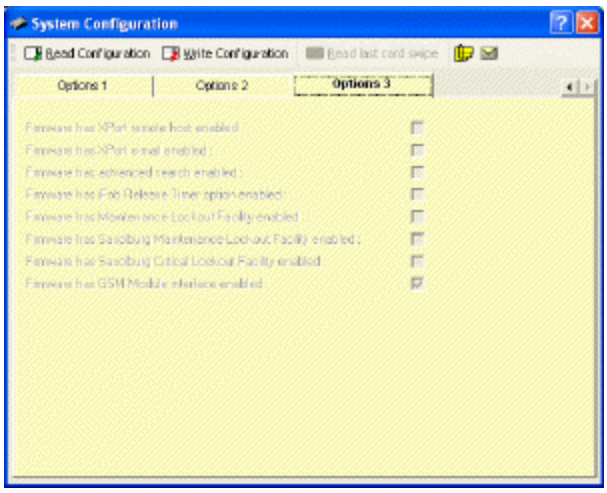
Currency Setting

This field shows the selected currency setting of the firmware. The following currencies are currently available. To alter the currency, please contact Traka for a firmware upgrade.

- £
- €
- $

Options 3

NOTE: The following options are available within the firmware upon request from Traka. If you would like to add or remove any of these features, please contact Traka with the details and Traka will supply you with a firmware upgrade file with the relevant options enabled.



Firmware has XPort remote host enabled

This box will be checked if the firmware has XPort remote host enabled.

Firmware has XPort e-mail enabled

This box will be checked if the firmware has XPort e-mail enabled.

Firmware has advanced search enabled

This box will be checked if the firmware has the advanced iFob search option enabled. This only applies to firmware version 6.07.23 and above.

Firmware has iFob release timer enabled

This box will be checked if the firmware has the iFob release timer option enabled.

Firmware has Sasol Secunda turbo facility enabled

This box will be checked if the firmware has the Sasol Secunda turbo facility enabled. For more details, please refer to the maintenance lockout facility section.

Firmware has Sasol Sasolburg turbo enabled

This box will be checked if the firmware has the Sasol Sasolburg turbo facility enabled. For more details, please refer to the maintenance lockout facility section.

Firmware has Sasol Sasolburg critical lockout facility enabled

This box will be checked if the firmware has the Sasol Sasolburg critical lockout facility enabled. For more details, please refer to the maintenance lockout facility section.

Firmware has Sasol Secunda catalyst enabled

This box will be checked if the firmware has the Sasol Secunda catalyst option enabled. For more details, please refer to the maintenance lockout facility section.

Firmware has Sasol Secunda oil enabled

This box will be checked if the firmware has the Sasol Secunda oil option enabled. For more details, please refer to the maintenance lockout facility section.

Firmware has GSM Module interface enabled

This box will be checked if the firmware has the GSM Module interface enabled. This option is only available with firmware version 6.07.33 and above.

Firmware has iFob return prompt enabled

This box will be checked if the firmware has the iFob return prompt option enabled.

Firmware has key booking by ref. enabled

This box will be checked if the firmware has the key booking by reference option enabled.

Firmware has Daily / Weekly Vehicle Check option enabled

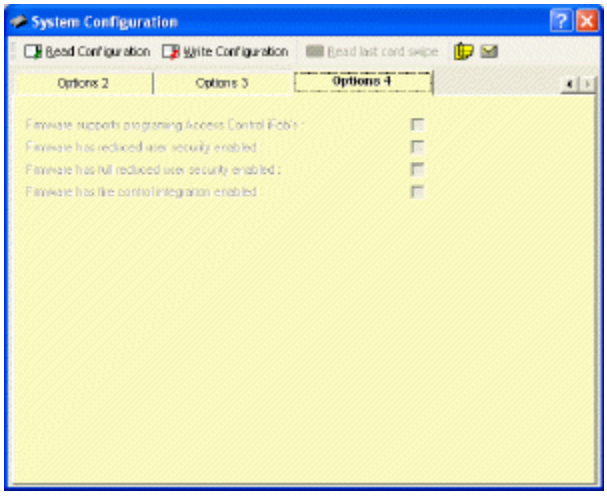
This box will be checked if the firmware has the daily / weekly vehicle check option enabled.

Daily Vehicle Check Shift Start Hours

This field shows the selected shift start time for the daily vehicle check option.

Options 4

NOTE: The following options are available within the firmware upon request from Traka. If you would like to add or remove any of these features, please contact Traka with the details and Traka will supply you with a firmware upgrade file with the relevant options enabled.



Firmware supports programming Access Control iFob's

This box will be checked if the firmware has the capability of programming iFobs for use with the Traka Access Control System.

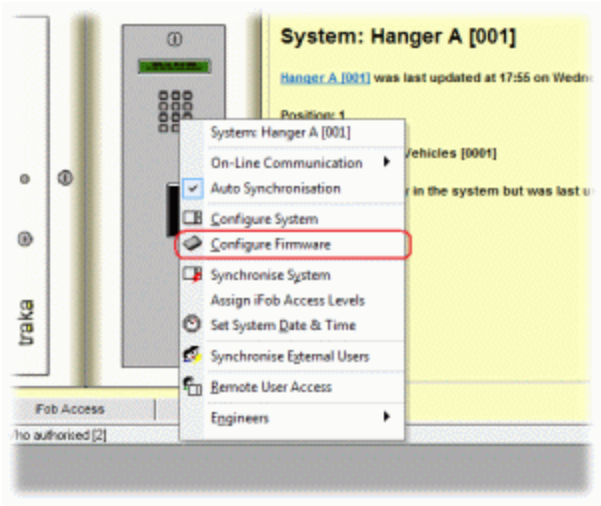
Firmware has full reduced user security enabled

This box will be checked if the firmware has full reduced user security enabled.

4.20.10.3 16BIT CONFIGURE FIRMWARE

4.20.10.3.1 16BIT CONFIGURE FIRMWARE WIZARD

The **16bit Configure Firmware Wizard** can be manually launched by **right** clicking over the Traka system pod on the System Viewer and selecting **Configure Firmware** from the System Menu.



The 16bit Configure Firmware Wizard allows you to:-

- View the various options that are enabled on the selected Traka System.
- Make adjustments to specific parts of the configuration for example editing the number of receptor strips, changing the door configuration, amending card reader settings as well as globally turning on and off options that have already been unlocked in the configuration file.

  Please note options that are not available to edit (greyed out) are not unlocked. To unlock a specific option, a new configuration file will have to be obtained from Traka or your local distributor. Please view the configuration file section under the topic 16bit System File Types for more information.
- Load a configuration file. View Changing Firmware Settings for information on how to apply a new configuration file to your Traka system.

The 16bit Configuration Wizard can also be launched automatically if you are adding a new system to the database or if Traka32 detects a change in the hardware such as the 16bit Control PCB. If Traka32 has detected a change in the hardware then a new configuration file will need to be obtained from Traka in order for the communications to continue permanently. If you are adding a new system, please view the section Adding a New 16bit System.

4.20.10.3.2 CHANGING 16BIT CONTROL HARDWARE

When changing the 16bit Control hardware, the replacement hardware must be re-configured for the new system.

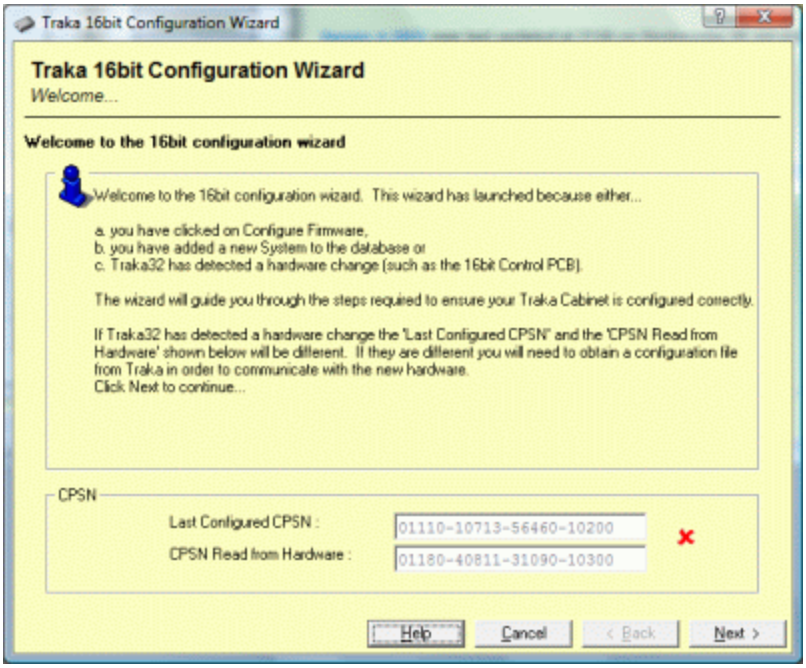
Because the 16bit application firmware is generic and not customer specific (like the 8bit firmware), a configuration file is required to customise the firmware for each system. The configuration file contains the configurable parts to the system such as the number of receptor strips and card reader settings as well as the cost options.

Without a configuration file, a Traka System can be used as normal, however no cost options will be enabled and the card reader settings will remain as they were last programmed into the Control PCB.

The communications between Traka32 and the Traka System will also be possible for up to 30 days, but every time communications is initiated, Traka32 will prompt for a configuration file first.

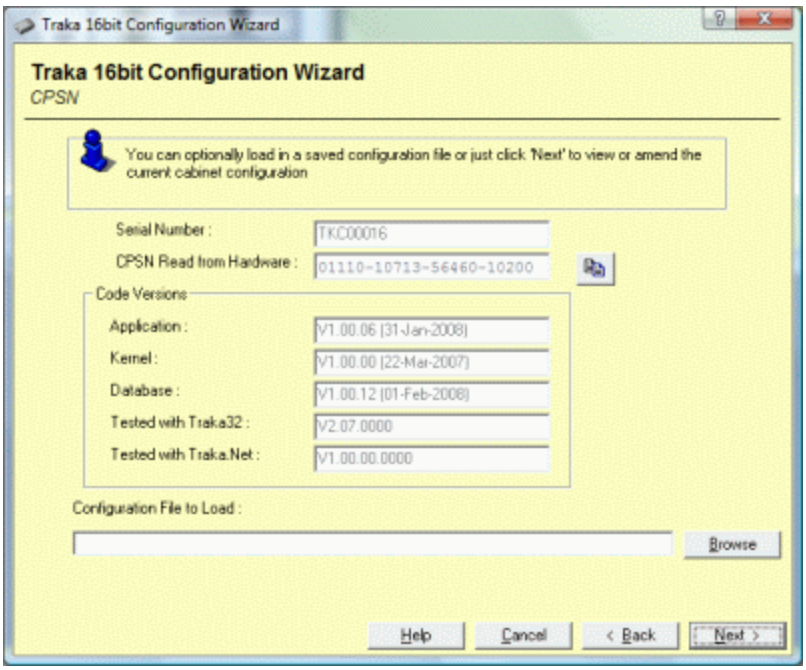
When changing the 16bit Hardware

1. After changing the hardware and communicating for the first time, the16bit Configuration Wizard will be displayed.



2. Click on **Next**.

3. The CPSN window is displayed confirming the Serial Number, CPSN Read from Hardware, the Hardware and Code versions and in addition the Traka32 version the firmware was tested with.



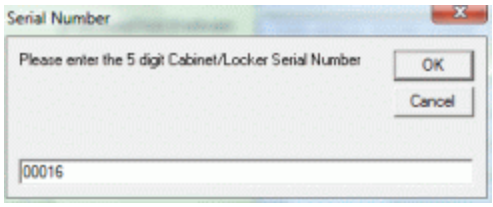
You will need to contact your distributor quoting the **CPSN Read from Hardware**. The distributor will them be able to e-mail you with a configuration file for your hardware.

TIP: Click the  button to **copy** the CPSN to the clipboard for pasting into a file or email.

4. Once you have obtained the configuration file from Traka or your distributor, **save** it to the machine from which you wish to load it.

5. Click **browse** to search for the configuration file.

    a. Enter the **5 digit serial number** of the Traka system (excluding TKC,TIL etc).



    b. Click OK and browse to the location the configuration file was saved to. Only configuration files matching that of the entered serial number will be available for selection.

    NOTE: The configuration file name is structured as follows...

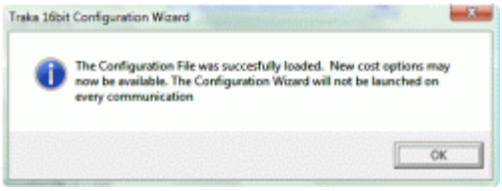
    <Serial Number> - <CPSN Number> - <Firmware Version>.TKCcfg

    For example, for a system with a serial number TKC12345, a CPSN of 01041006164704010200 and a firmware version of 1.00.00, the following file is required:

    12345 - 01041006164704010200 - 010000.TKCcfg

6. When you have selected the path to the configuration file, click on **Next**.

    If the configuration file was correct a message will be displayed indicating the hardware will be licensed to the database and any cost options will become available. A message is displayed indicating the file has been successfully loaded.



NOTE: This indicates it has been loaded into the Traka32 database only at this stage and not yet applied to the cabinet.

If the configuration file was incorrect, check that you have the correct file via the file name and try again. An incorrect file may be may be because…

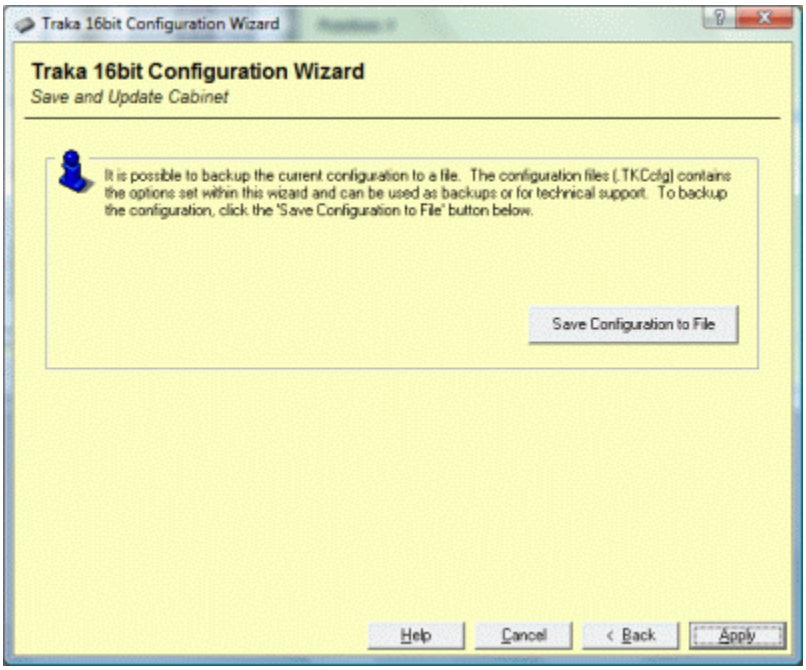
a. The CPSN did not match,

b. The Hardware Key did not match or,

c. The Firmware Version did not match.

7. Follow the wizard through, checking ALL the settings and amend as required. For details on the various settings, please refer to the Firmware Options & Settings section.

8. Finally click on **Apply** to load the configuration into the cabinet.



If you wish you may also save the current configuration (with any changes) to a File. Click on 

to do so and provide a suitable name for the file perhaps indicating any specific options that it contains.

9. Now that the new 16bit Control PCB's CPSN has been registered, you will be able to communicate as normal.

Also View:-

16bit System File Types

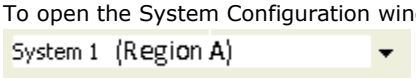
16bit Configure Firmware Wizard

Changing Hardware

Changing Firmware Settings

4.20.10.3.3 CHANGING 16BIT FIRMWARE SETTINGS

The 16bit Configuration Wizard can also be used to make changes to the current system settings and also to unlock new cost options via a configuration file.

1. To open the System Configuration window, from the main screen select the system 

and from the system viewer right click over the picture of the relevant position and click on **Configure Firmware**.

2. Click on **Next**.

3. If you have a new configuration file to unlock new cost options, select the path to the configuration file. To search for the configuration file simply click on the **Browse** button.

   NOTE: The configuration file name is structured as follows...

   <Serial Number> - <CPSN Number> - <Firmware Version>.TKCcfg

   For example, for a system with a serial number TKC12345, a CPSN of 01041006164704010200 and a firmware version of 1.00.00, the following file will be required:

   12345 - 01041006164704010200 - 010000.TKCcfg

4. When you have selected the path to the configuration file, click on **Next**.

   If the configuration file was correct the hardware will be licensed to the database and any cost options will become available.

   If the configuration file was incorrect, check that you have the correct file via the file name and try again. An incorrect file may be may be because…

   a. The CPSN did not match,

   b. The Hardware Key did not match or,

   c. The Firmware Version did not match.

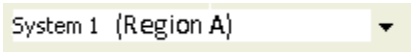
5. Follow the wizard through, checking ALL the settings and amend as required. For details on the various settings, please refer to the Firmware Options & Settings section.

6. Finally click on **Finish** to save any changes.

4.20.10.3.4 LOADING A 16BIT CONFIGURATION FILE

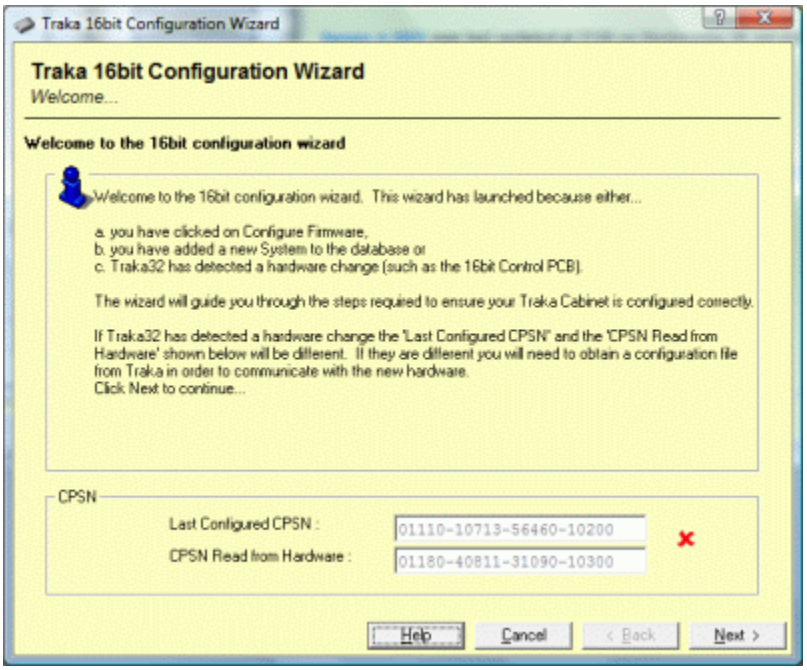
Because the 16bit application firmware is generic and not customer specific (like the 8bit firmware), a configuration file is required to customise the firmware for each system. The configuration file contains the configurable parts to the system such as the number of receptor strips and card reader settings as well as the cost options.

1. From the top of Traka32 select the appropriate system from the drop down selection box



2. From the system viewer right click over the picture of the control panel and click on **Configure Firmware**.

3. A small communication window will appear for a few seconds followed by the configuration wizard. Click on **Next.**



4. The CPSN window is displayed confirming the Serial Number, CPSN Read from Hardware, the Hardware and Code versions and in addition the Traka32 version the firmware was tested with. You will need to contact your distributor quoting the CPSN Read from Hardware. The distributor will then be able to e-mail you with a configuration file for your hardware.

   NOTE: You will need to save the config file somewhere memorable and easy to access.

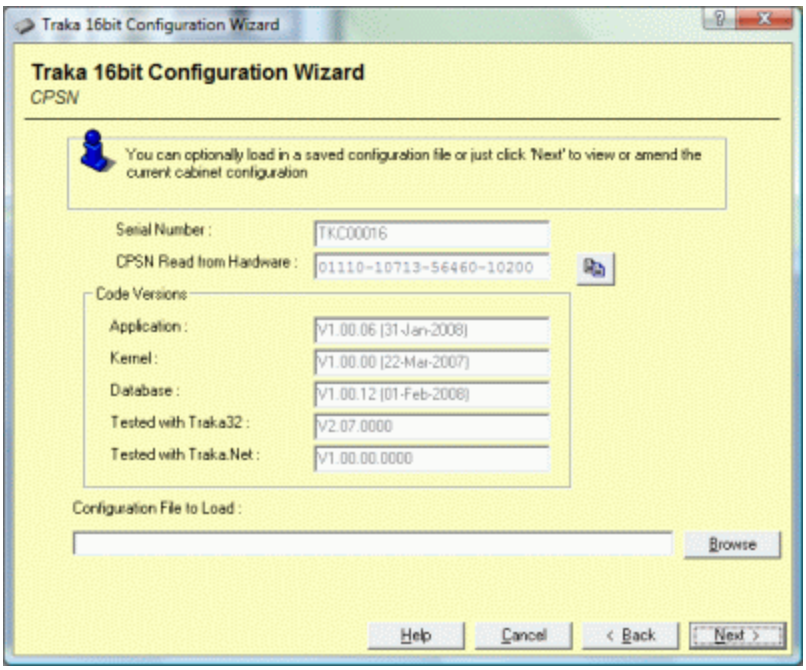
5. Click on **Browse** and locate the config file that was sent to you.

   The configuration file name is structured as follows…

   <Serial Number> - <CPSN Number> - <Firmware Version>.TKCcfg

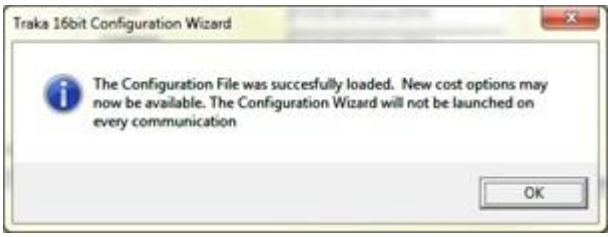
   For example, for a system with a serial number **TKC12345**, a CPSN of **01041006164704010200** and a firmware version of **1.00.00**, the following file will be required:

   12345 - 01041006164704010200 - 010000.TKCcfg



6. When you have selected the path to the configuration file, click on **Next**.

7. If the configuration file was correct a message will be displayed indicating the hardware will be licensed to the database and any cost options will become available. A message is displayed indicating the file has been successfully loaded.



NOTE: This indicates it has been loaded into the Traka32 database only at this stage and not yet applied to the cabinet.

If the configuration file was incorrect, check that you have the correct file via the file name and try again. An incorrect file may be because:

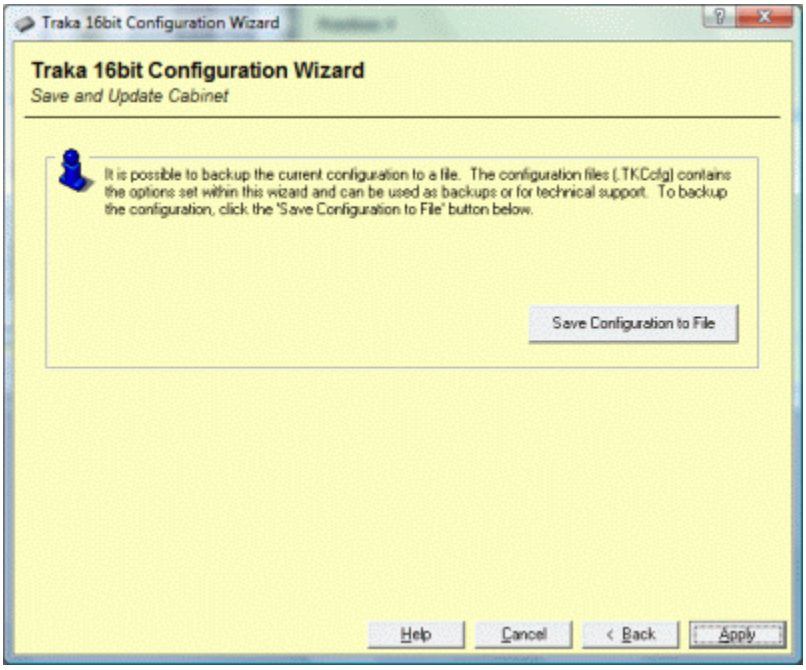
   a. The CPSN did not match,

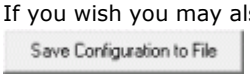
   b. The Hardware Key did not match or,

   c. The Firmware Version did not match.

8. Follow the wizard through, checking ALL the settings and amend as required. For details on the various settings, please refer to the Firmware Options & Settings section.

9. Finally click on **Apply** to load the configuration into the cabinet.



If you wish you may also save the current configuration (with any changes) to a File. Click on  to do so and provide a suitable name for the file perhaps indicating any specific options that it contains.

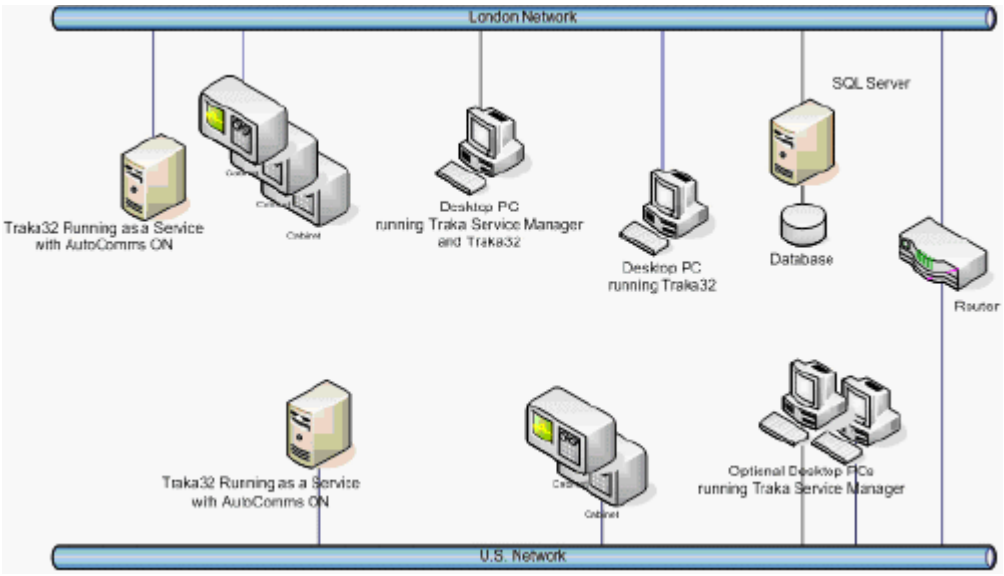
Now that the new 16bit Control PCB's CPSN has been registered, you will be able to communicate as normal.

4.21 TRAKA32 AS A WINDOWS SERVICE

4.21.1 TRAKA32 AS A WINDOWS SERVICE (TAAS) OVERVIEW

Traka 32 as a Service (TAAS) provides a means of running Traka32 in the background as a Windows Service on a PC or Server. TAAS requires no User interface and keeps running even if no-one logs on to the PC / Server. This has major benefits for organisations that require functionality such as Auto Communications without the need to run Traka32 as a Client (TAAC) on a PC or Server. TAAS can be monitored remotely from a PC running Traka Service Manager.

Example:



The Acme (UK) Server on the Acme HQ Network in London runs Traka32 as a Service (TAAS) which Auto Communicates and reads the events from all three London cabinets and stores them in the Traka database on the Corporate SQL Server which is also happens to be in London. They make changes to the Traka database using a desktop PC running a standard copy of Traka32.

The Acme (U.S) Server also runs a copy of TAAS and Auto Communicates with the two cabinets attached to their U.S LAN.

Their Global System Administrator is based in the UK and runs two copies of Traka Service Manager on one of his management/monitoring PCs and can see the Service and Auto Communications status of both servers.

4.21.2 TRAKA AS A SERVICE INSTALLATION PREREQUISITES

The PC or Server that **Traka as a Service** is to operate on, must be running Windows NT 4.0 SP6 or later (i.e NT, 2000,2003, XP or Vista). Please note that **Windows 95 and Windows 98 are not supported**.

Other requirements are as per Traka32 Minimum PC Requirements. The user **must** have administrative rights to the machine(s) where services are to be installed or controlled.

4.21.3 TRAKA AS A SERVICE INSTALLATION

All of the functionality to install and uninstall Traka32 as a Windows Service is contained within the Traka32 program itself providing **Install Traka32 as a Service** was selected from the **Custom Setup** window during installation. Please view Traka32 Installation for how to install the Traka32 software.

Installing Traka32 as a Service

Once Traka32 is installed, **register Traka32 as a Service** with Windows using any of the following methods:-

1. **Double click** the **shortcut** on the Desktop.

or

2. From the **Windows Run** dialog box.

   a. **Open** the **Windows Run** dialog using **Start > Run**

   b. **Browse** to the **ServiceInstall.bat** file located in the Traka32 installation directory or type the path directly into field for example:-

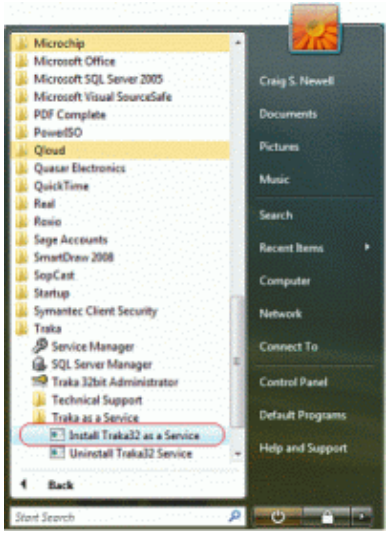
   C:\Program Files\Traka Limited\Traka32 /serviceinstall

   NOTE: Please note the 'space' and 'forward slash' after Traka32

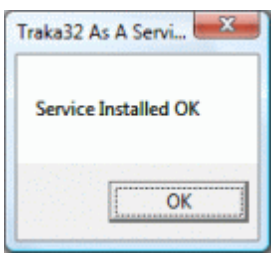
3. From the Windows Start Menu.

   a. Click the **Start** button

   b. Select **All Programs > Traka > Traka as a Service > Install Traka as a Service**



4. For each method, if installation is successful, you will see:



4.21.4 SETTING UP TRAKA32 AS A WINDOWS SERVICE

The procedure for setting up Traka32 as a Windows Service is as Follows:

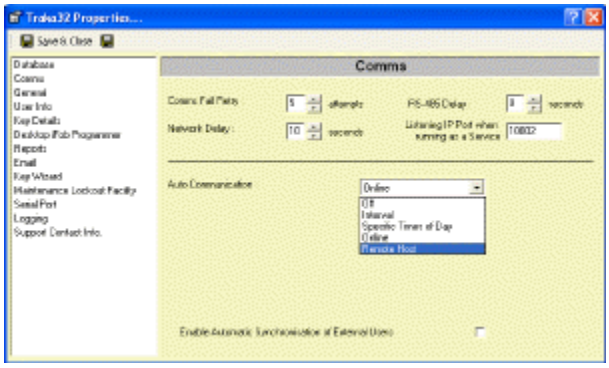
1. Install Traka32 including Service Manager on the Target PC / Server that is required to run Traka32 as a Service.

2. **Deploy** Service Manager on any further PCs as required by the application.

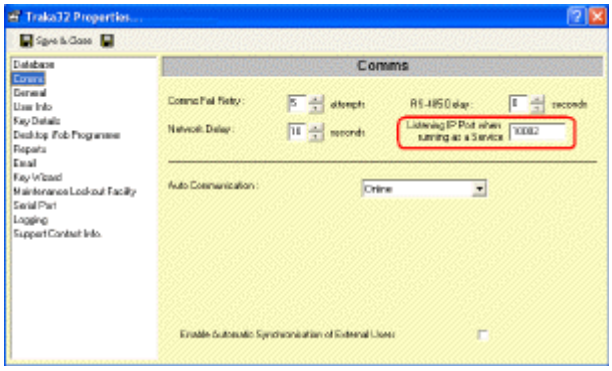
3. **Install** Traka32 as a Service on the Target PC / Server as required by the application.

4. **Run** Traka32 as a Client on the Target PC / Server.

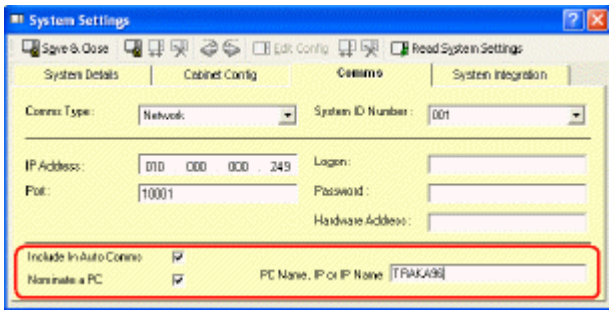
5. **Switch on** Auto Communications in File >Properties under the Comms window and configure as required by the application.



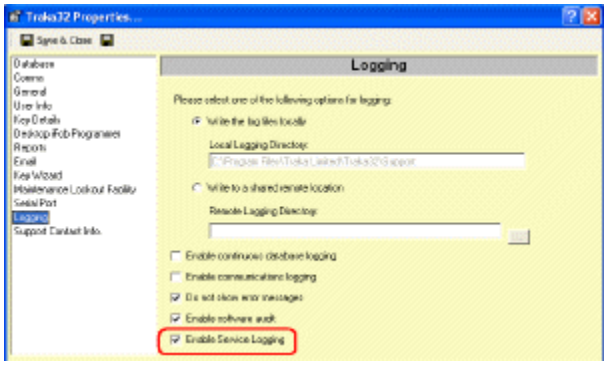
6. **Enter the Listening IP Port Number** in File->Properties under the Comms window.



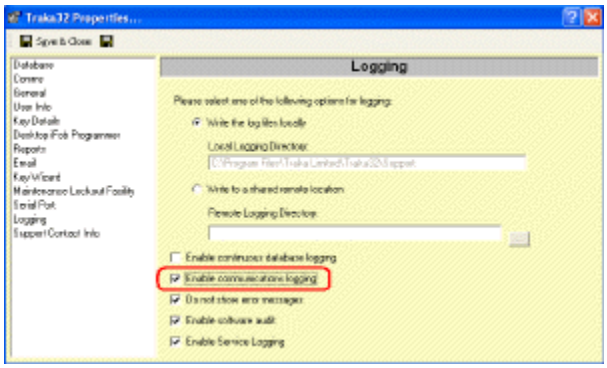
7. **For each Traka System** that the Target PC / Server will Auto Communicate with, tick **Nominate a PC** and **Set the Nominated PC Name** under the **Comms** tab in the System Details window. Note that if **Nominate a PC** is left not ticked, then all Traka32 clients will attempt to communicate with the selected system.



8. **Switch on Service Logging** in File->Properties under the Logging tab.



9. It is recommended that **Comms Logging** should also be switched on during testing of the application. Communications messages between the Traka systems and Traka32 will then be shown in the Service Manager Details panel.



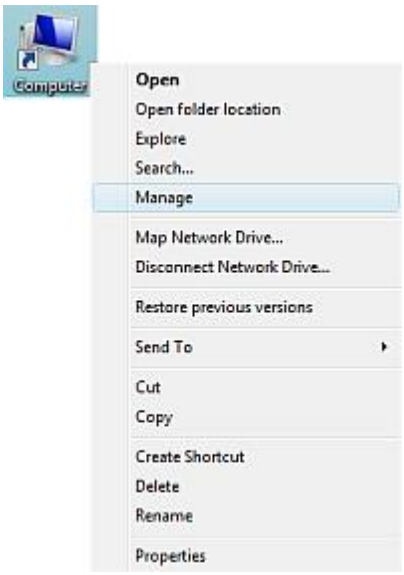
NOTE: Recommended for testing purposes only.

10. Please refer to Starting the Service for how to start, pause and stop Traka32 as a Service.

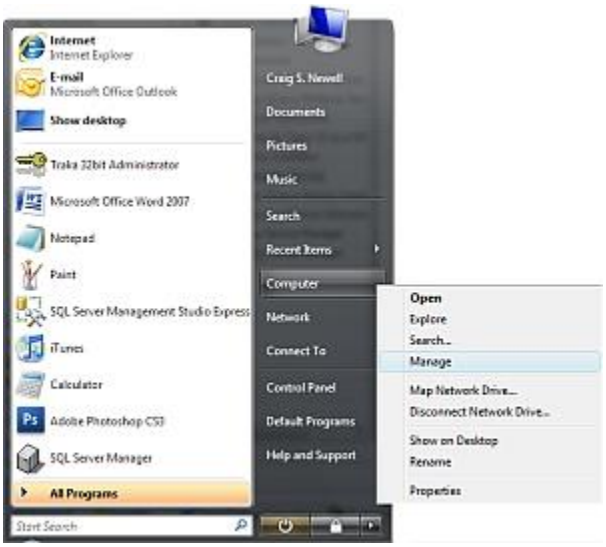
4.21.5 STARTING AND STOPPING THE SERVICE

To Start, Pause, Continue, Restart or Stop the service under XP, you should use the Windows' Computer Management tool. This is available by:

1. Right-clicking the **My Computer** icon.

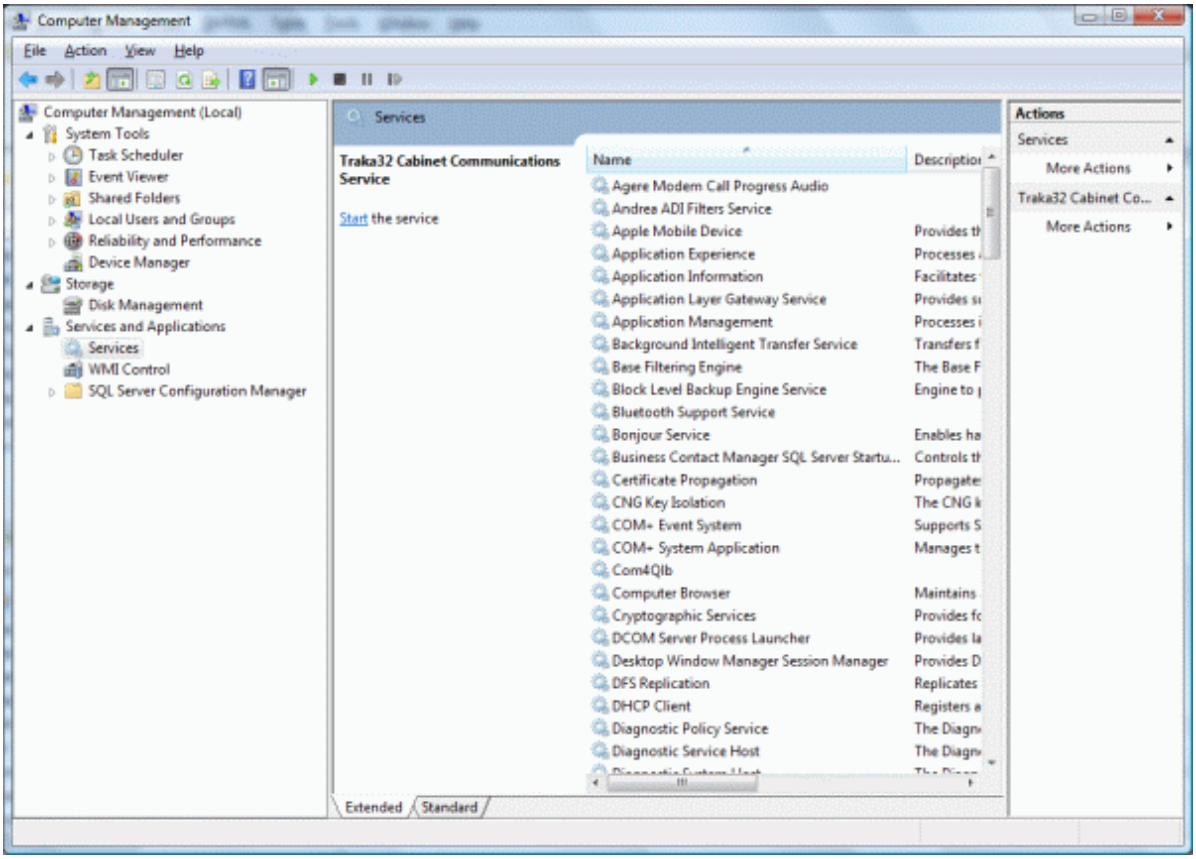


or right-clicking **any** link to **My Computer**.

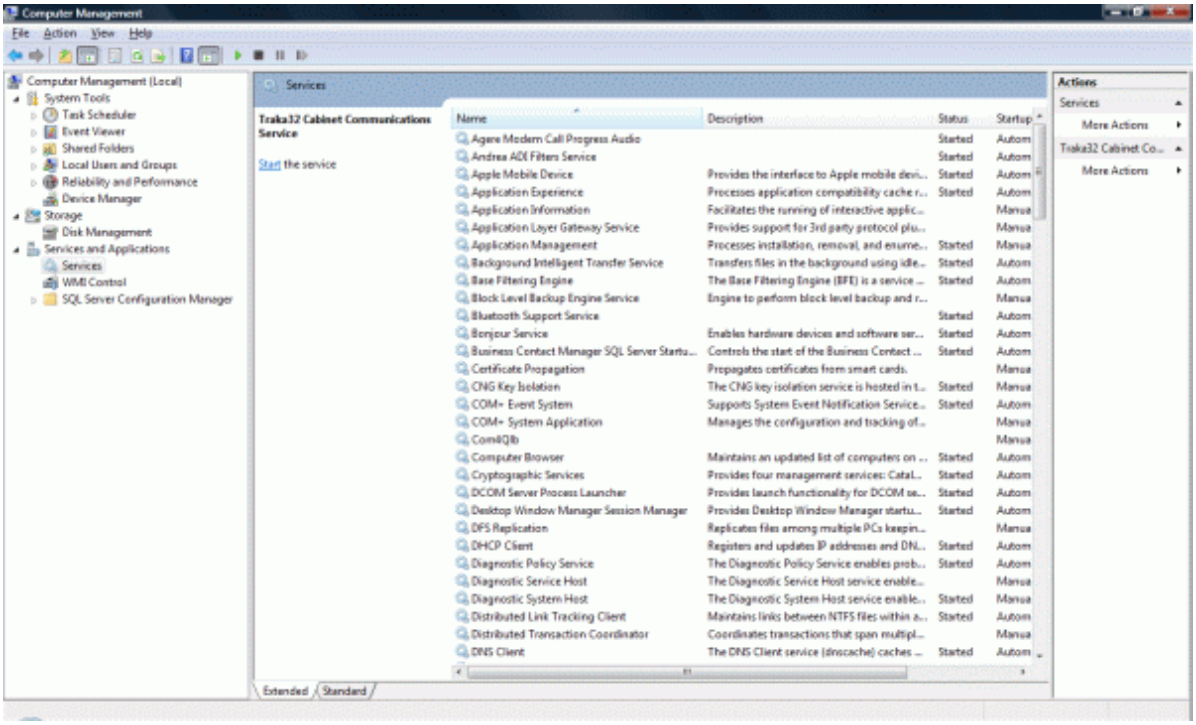


2. Choose **Manage** from the context menu.

   This will load the Computer Management program:

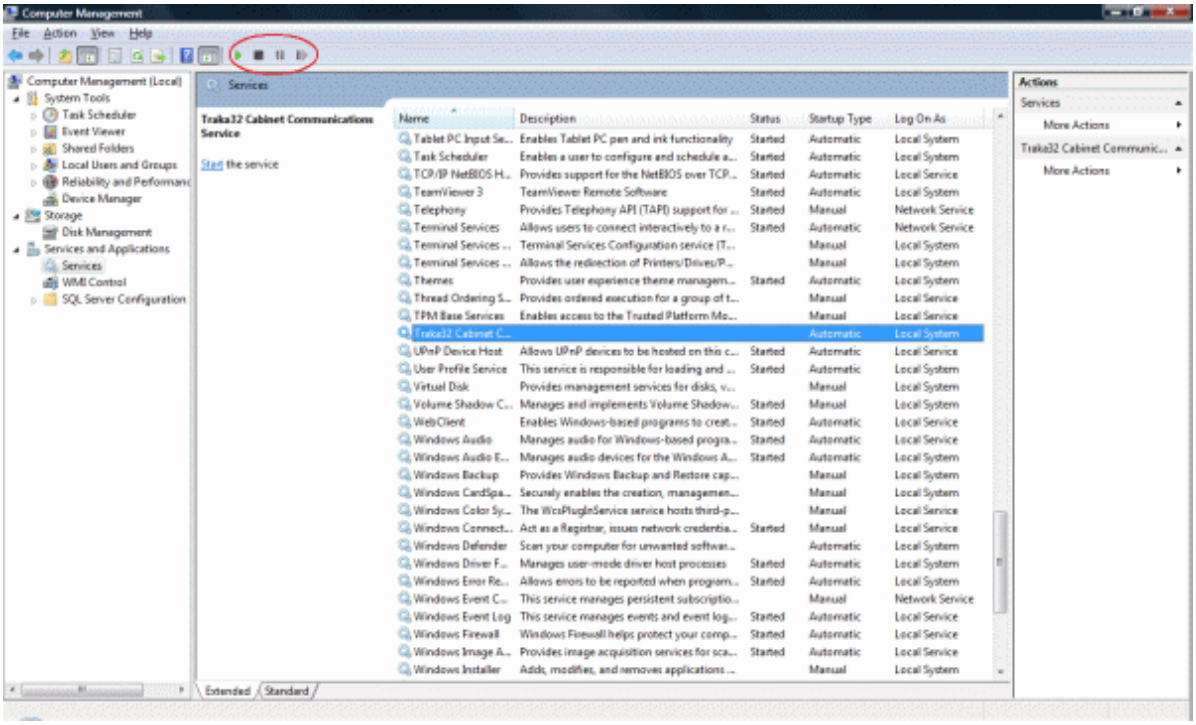


3. Expand **Services and Applications**, then single-click **Services**, you should see a complete list of Windows Services.



4. Scroll down until you see **Traka32 Cabinet Communications Service**, then single-click the line to select it. If it's not there, the service is not installed.

5. To start or stop the service, use the **Play**, **Stop**, **Pause** and **Restart** icon buttons in the top toolbar.



NOTE: Under Windows NT 4.0, use the 'Service applet' in Control Panel.

Refer to Service on Windows NT 4.0 Consideration for important information on running the Service on this operating system.

4.21.6 FIRMWARE AND SOFTWARE UPGRADES (TAAS)

When upgrading the Traka32 software and/or database, or executing a firmware upgrade on a Traka system, the Service **must** be in a **Stopped** (not paused) state. Please view Starting the Service which illustrates how to use the Windows Computer Management tool to start, pause and stop the service.

After a Traka32 software upgrade, use the Traka32 Client to perform any database integrity checks before restarting the service. Unless the location of Traka32.EXE changes, there is no need to reinstall the Service.

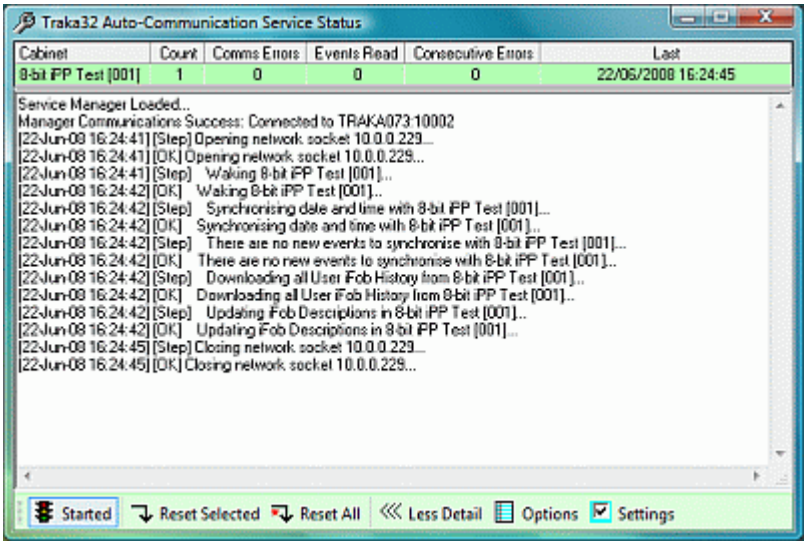
4.21.7 TRAKA SERVICE MANAGER

The Traka Service Manager program has been designed to continuously monitor a Traka32 Service running on a remote PC.

The Service Manager operates by periodically sending status requests over the network to a copy of Traka32 running as a service and displaying the returned information in an easy to see, colour-coded fashion.

Service Manager continuously displays the status of:

1. Whether Service Manager can communicate with the Service.
2. The status of the Service on the remote PC (Started, Paused etc).
3. The detailed statistics of that Services' communication with the Traka systems.



Service Manager Prerequisites

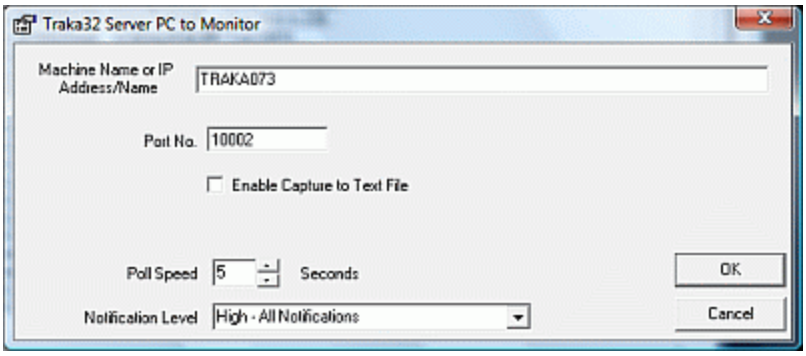
Client PCs running Service Manager can have any Operating System supported by Traka32 Minimum PC Requirements. The user **must** have administrative rights to the machine(s) where services are to be installed or controlled.

Service Manager Installation

When installing Traka32, select **Install Service Manager** from the **Custom Setup** window during the install shield wizard. See Traka32 Installation for how to install Traka32.

Service Manager Options

Click Options to adjust the Service Manager parameters:



Machine Name or IP Address/Name

Enter the Machine Name or IP Address of the target PC / Server running the Service to be monitored.

Port No.

Enter the TCP/IP Port No. used to communicate with the Service. **10002 is the default** however when using **Remote Host** communications where each Traka system must use a unique Port No, ensure the Service Port No. does not clash with that of a Traka system.

For example where three Traka systems are communicating using **Remote Host**, the TCP/IP Ports may be configured as follows:-

Network Device	TCP/IP Port
Traka System 1	10001
Traka System 2	10002
Traka System 3	10003
Traka Windows Service	10004

Enable Capture to Text File

Tick to output the communications to a text file, selecting a file name and location.

Poll Speed

Set how frequently (in seconds) the Service Manager will poll the Service for information. 5 seconds is the default and adequate for the majority of applications.

4.21.8 OTHER SERVICE INFO

4.21.8.1 WHAT TO DO IF SERVICE IS UNRESPONSIVE

In the unlikely event that the Traka32 Service becomes unresponsive, try the following in this order:

1. Try stopping the Service with Windows Computer Management tool. Refer to Starting the Service.
2. Otherwise try stopping the Service using Windows Task Manager.

4.21.8.2 WHICH MACHINE IS THE SERVICE RUNNING ON?

If you only have access to a Traka32 workstation PC and need to find out which machine the TAAS is running on, there are two methods depending on which database type is used:

1. **Access**: Open the T32Database.LCK file with notepad and you should be able to see the Computer names of any PCs that have the Database open.
2. **SQL Server**: Use the SQL Server management tools to determine who has the Database open.

4.21.8.3 SERVICE AND CLIENT ON SAME MACHINE

Normally, only a single copy of Traka32 can be run at a time on a single machine. This restriction is lifted once Traka32 is installed as a Windows Service in order to be able to run both the Traka32 Service and Traka32 Client at the same time on the same machine. This means that you can (unintentionally) run two or more copies of the Traka32 Client simultaneously.

4.21.8.4 SERVICE AUDIT TRAIL

Audit trails for the Service (install, start, stop events etc) are written to both **Support\T32Service.txt** (assuming that Service Logging is switched on in Traka32) and the Windows Application and System Event logs. Note also that as **T32Service.txt** grows larger than 3Mb, it is automatically archived into **T32ServiceArchive.txt.**

4.21.8.5 SERVICE ADVANCED TIPS

Tip 1.

To manage the services on a PC other than the one you are at, right click **Computer Management** (Local) at the top then select **Connect to another computer**.

Tip 2.

The service can be started and stopped from a Command Prompt or batch file by typing:

NET START "Traka32 Cabinet Communications Service"

or

NET STOP "Traka32 Cabinet Communications Service"

Advanced:

By default, the Service is installed as **Startup**:*Automatic* and '**Log on as Local System Account**'. This means that the Service will start when Windows starts and run it as 'SYSTEM'. These can be changed (with care) using the Properties dialog.

4.21.8.6 SERVICE ON UNSUPPORTED WINDOWS VERSION

Attempting to install Traka32 as a windows service on an unsupported version of Windows (such as Win98SE) will result in any command line (*/serviceinstall*) being ignored.

See Service Prerequisites for information on supported Operating Systems.

4.21.8.7 SERVICE ON WINDOWS NT 4.0 CONSIDERATION

When manually starting the service on NT 4.0 using an Access Database, the Service can take over 40 seconds to start. This will cause Windows Service Control Manager to show an error message after 30 seconds:

'The Service failed to start or respond to a control message in a timely manner'.

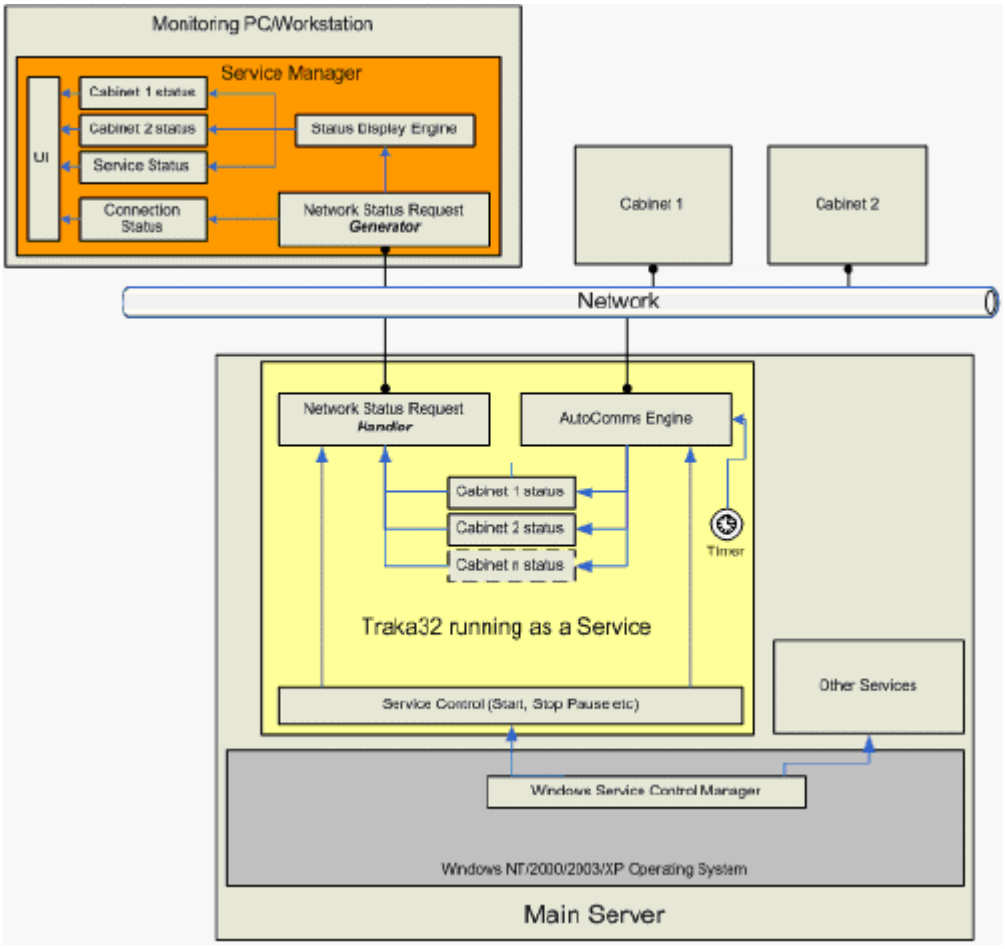
This can be ignored as the Service will continue starting. You should reopen the Services applet in order to show the correct 'Stop' and 'Continue' buttons.

4.21.8.8 SERVICE MESSAGE BOX DIALOG HANDLING

Message box dialogs that are presented during the course of operation of Traka32 As A Service (including questions, confirmations and operational errors) will be suppressed, written to the **T32Service.txt** log file and 'OK' will be automatically supplied to the dialog to allow the service to continue without waiting for a user response.

4.21.8.9 SYSTEM BLOCK DIAGRAM

The block diagram shows the relationship between the Server PC that Traka as a Service runs on, the Traka Systems and the PC that the Service Manager runs on.



4.22 TRAKA SQL SERVER MANAGER

4.22.1.1.1 TRAKA SQL SERVER MANAGER OVERVIEW

The Traka SQL Server Manager is a utility for managing the most common tasks required to support a Traka database in SQL Server.

The installation for managing SQL Server does not have to be located on the same machine as SQL Server itself however the Traka SQL Server Manager requires the SQL DMO Object Library to work.

To install Traka32 with the SQL Server options on any PC you need either of the following two things:

1. Full Microsoft SQL Server installed on the PC
2. Or the DMO Object Library installed on the PC

The DMO object library is a free download and can be downloaded from the following link:

http://www.microsoft.com/downloads/details.aspx?FamilyID=d09c1d60-a13c-4479-9b91-9e8b9d835cdc&displaylang=en

This download is called the 'Feature Pack for Microsoft SQL Server 2005 - November 2005' and it contains several files however the item that you will need is:

Microsoft SQL Server 2005 Backward Compatibility Components

The SQL Server Backward Compatibility package includes the latest versions of Data Transformation Services 2000 runtime (DTS), SQL Distributed Management Objects (SQL-DMO), Decision Support Objects (DSO), and SQL Virtual Device Interface (SQLVDI). These versions have been updated for compatibility with SQL Server 2005 and include all fixes shipped through SQL Server 2000 SP4.

Audience(s): **Customer, Partner, Developer**

X86 Package (SQLServer2005_BC.msi) - 11222 KB

X64 Package (SQLServer2005_BC_x64.msi) - 18516 KB

IA64 Package (SQLServer2005_BC_ia64.msi) - 23453 KB

You only need to install this component and then you will be able to create SQL databases from a remote PC.

For more in depth information on the Traka SQL Server Manager, please contact your supplier.

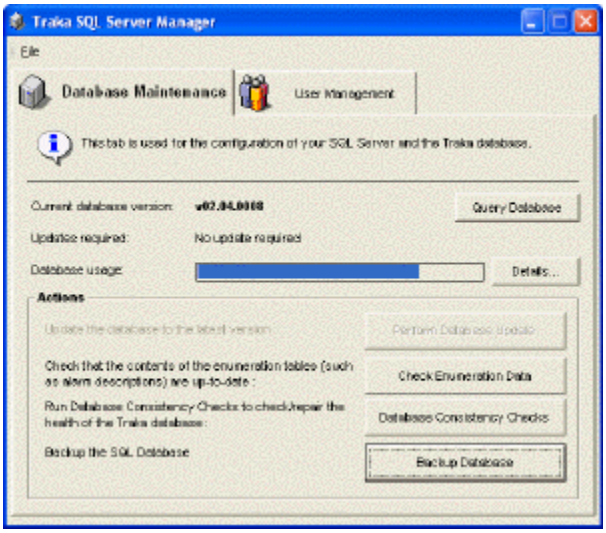
4.22.2 SQL DATABASE BACKUP

It is extremely important to take regular backups of the Traka database in case of disk or file corruption or hardware failure. Unlike with an Access database, the SQL Server backup process currently cannot be automated and so a regular manual backup must be taken.

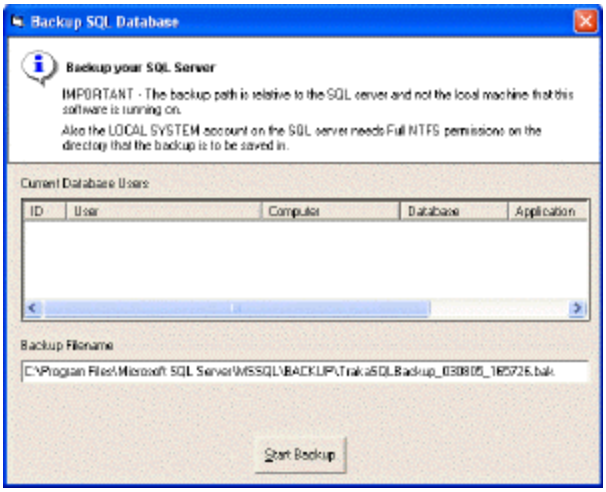
It is strongly recommended that you incorporate Traka into your disaster recovery plans in case the worst happens.

The Traka SQL Server Manager can be used to make a backup of the selected Traka database...

1. Click **SQL Server Manager** from the **Traka** program group in the **Start** menu to open the Traka SQL Server Manager:



2. Click on **Backup Database**.



3. Check the **Backup Filename** is correct and alter if required.

   NOTE: The backup path is relative to the SQL Server and NOT the local machine that the Traka SQL Server Manager is running on. Also the local system account on the SQL Server needs full NTFS permissions on the directory that the backup is to be saved to.

4. Click on **Start Backup**.

5. When the backup has completed a message will show, click on **OK**.

6. Click on **Close**.

4.22.3 SQL UPDATES

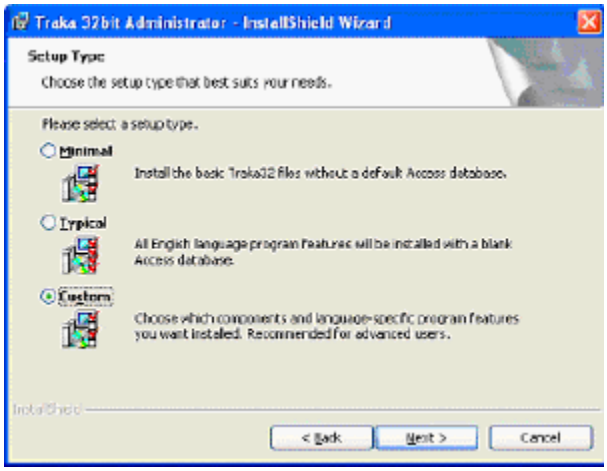
This section provides a guide for upgrading an existing installation of Traka32 for use with SQL Server. It assumes the reader is already familiar with the Traka32 software, SQL Server Enterprise Manager and SQL Server security.

NOTES:

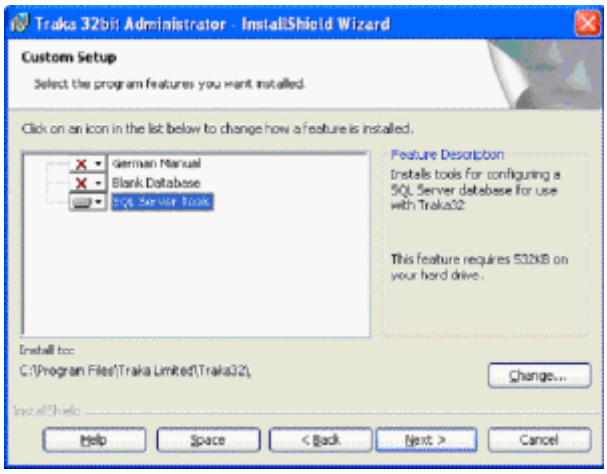
- Before upgrading the database structure, it is important to make a full backup of the database prior to upgrading.
- Once the database has been upgraded, old copies of the Traka32 software will no longer work with the new database structure.
- If you are heavy users of Traka32 please plan the upgrade with all those who will be affected.

NOTE: This section assumes you have an existing installation of Traka32 and the Traka SQL Server Manager software and you are familiar with both.

1. Using Enterprise Manager or the Traka SQL Server Manager, make a full backup of the Traka database.
2. Upgrade the copy of Traka32 and the SQL Server Tools that you use to administer the database...
    a. Run the Traka32 installation as usual.
    b. At the **Setup Type** dialog, select the **Custom option**:



    c. Remove the **Blank Database** from the setup and include SQL Server Tools:

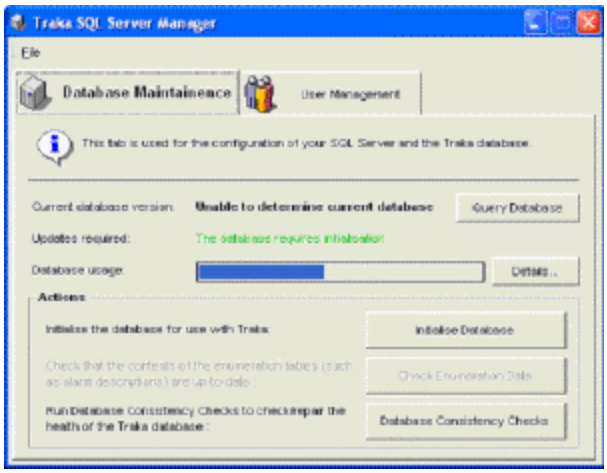


d. Complete the set-up as usual. When the installation finished, uncheck the **Launch application now checkbox** and click on **Finish**.

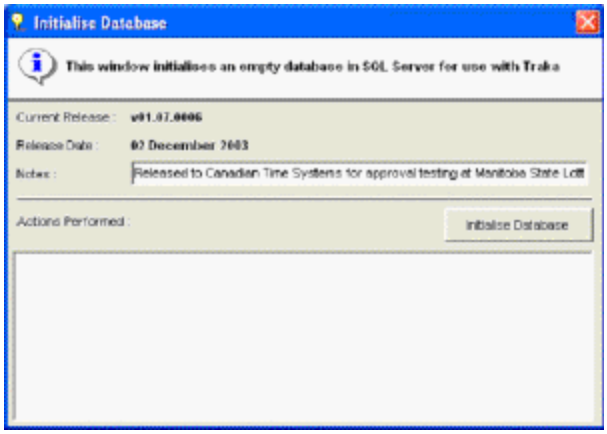
3. Update the Database using the SQL Server Manager...

a. Click **SQL Server Manager** from the **Traka** program group in the **Start** menu to open the Traka SQL Server Manager:

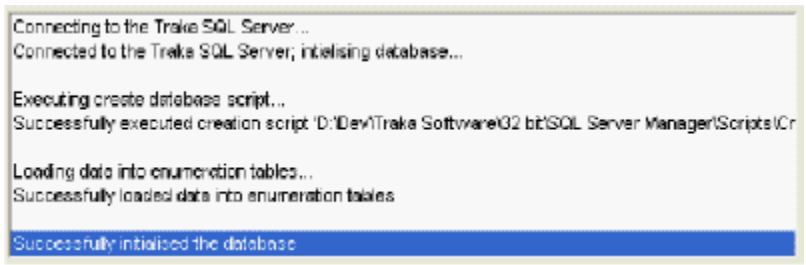
b. Click **Query Database** to check the current state of the database.



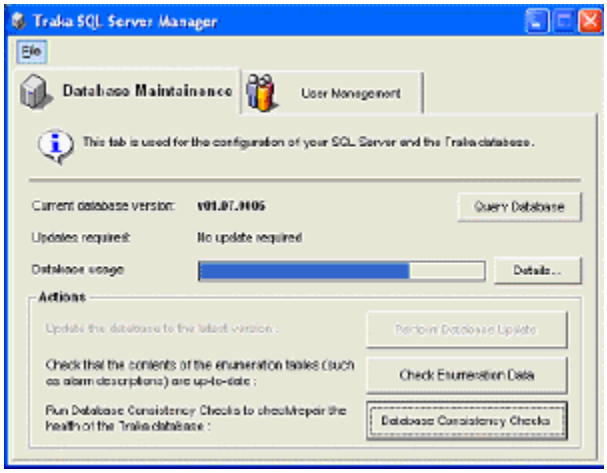
c. Click the **Perform Database Updates** button:



d. Confirm the **Current Release** is correct and click **the Initialise Database** button. The actions performed should be displayed as follows:



e. Close this dialog and the main window should appear as follows:



4. The initialisation is now completed and the database is ready for use with Traka.

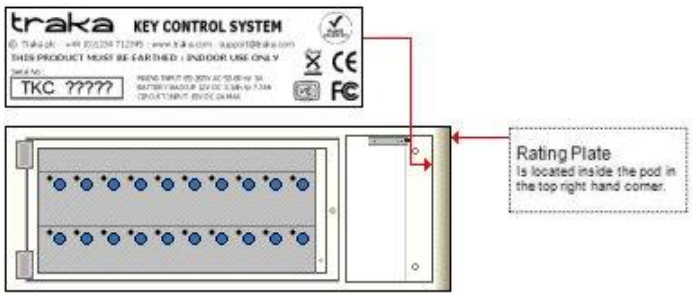
5. Upgrade all the remaining copies of Traka32 to the latest version.

5 TRAKA SYSTEMS

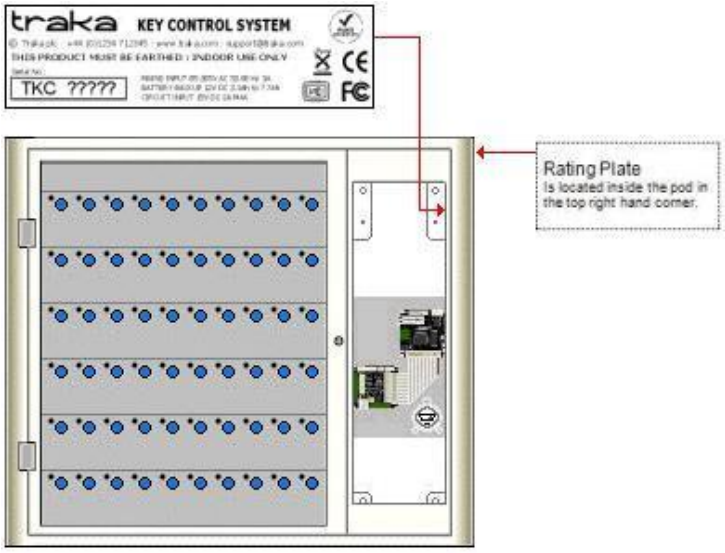
5.1 SERIAL NUMBER / RATING PLATE

All Traka Systems are fitted with a Serial Number / Rating Plate. This can be found in the following location...

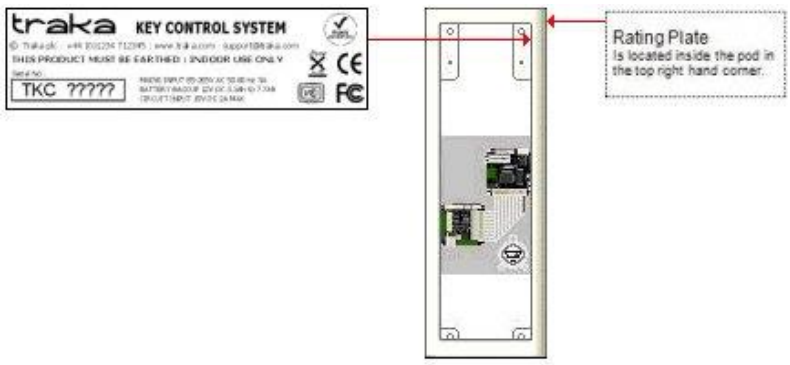
For the Traka **M-Series** the Rating Plate is located on the inside, you will need to remove the control panel in order to view the Rating Plate. Additionally there will be another label on the outside of the S-Series on the right hand side stating were you can find the Rating Plate.



For the Traka **S-Series** the Rating Plate is located on the inside, you will need to remove the control panel in order to view the Rating Plate. Additionally there will be another label on the outside of the S-Series on the right hand side stating were you can find the Rating Plate.



For Traka Products such as the **L-Series, Lockers and Access control Pods**, the Rating Plate is located inside the Pod. You will need to remove the control panel in order to view the Rating Plate. Additionally there will be another label on the outside of the Pod on the right hand side stating were you can find the Rating Plate.



5.2 BATTERY CONNECTION DETAILS

WARNING: All Traka Systems have two power sources, mains and battery. Before installing or servicing a Traka System, please ensure both mains and battery power sources are disconnected from the system.

This section will explain how to disconnect the battery from 8bit and 16bit systems.

Battery Disconnection

1. Open the control pod/panel of the system using the master key.
2. Locate the battery. Usually placed at the bottom of the control pod.
3. Disconnect the battery cable from the terminals as shown below.

5.3 HOW TO ACCESS THE SYSTEM

1. First access the Traka System.
    - For a Keypad entry Traka System, press **#** and enter the Primary Personal Identification Number (PIN) followed by **#**.

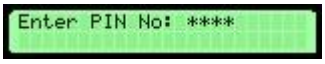
      

    - For a Card entry Traka System, swipe your card.
    - For Fingerprint entry, simply press **#** and place your finger on the reader.

      NOTE: If the LCD displays ID Not recognised then the card or PIN has not been configured. Please refer to the User Details section.

2. If you have a **Secondary PIN** set then type in the secondary PIN followed by **#**.

3. If your card and secondary PIN (if set up) are recognised the door will open (if fitted).

   If you have more than one cabinet attached to your system you will be asked to select which door you want to open, simply enter the door number on the keypad.

4. The display will show the users name and any iFobs the user may already have.

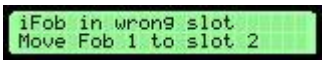
   

5.4 HOW TO RETURN AN IFOB

Button Release System

1. First access the Traka System. Please refer to the 'How to access the system' section.
2. To return an iFob simply return the iFob to the correct slot.

   NOTE: If you do not return the iFob to the correct slot the LCD will display iFob in wrong slot, Move iFob X to slot Y. Simply remove the iFob (you do NOT need to push the button on a locking system) and place it in the correct slot.

3. If you have any of the optional features such as fault, bay, mileage and/or fuel logging, you will be prompted to enter the relevant information.
4. The LCD will clear the position number of the iFob you have returned.

5. Repeat these steps for each iFob you want to return.

   NOTE: If you have a no door system, you do not have to access the system before returning an iFob, but the system will not record who returned the iFob, only the time it was returned.

Keypad Release System

1. Access the Traka System. Please refer to the 'How to access the system' section.
2. Press **#**.
3. The door will open allowing the user to return the iFob(s).

   NOTE: If you do not return the iFob to the correct slot the LCD will display iFob in wrong slot, Move iFob X to slot Y. Simply remove the iFob (you do NOT need to push the button on a locking system) and place it in the correct slot.

4. If you have any of the optional features such as fault, bay, mileage and / or fuel logging, you will be prompted to enter the relevant information.

Traka32

In Traka32 the previous user of an iFob is the user who returned the iFob to the system, not the user who removed it.

5.5 8-BIT CONFIGURATION MENU

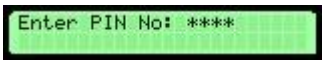
The Configuration Menu of the Traka System allows you to configure certain settings, reset the system and allows you to toggle to the Loader Program for firmware upgrades.

1. Using the **Master Key**, unlock the **Pod Lock**. The **Control Panel** is hooked in at the bottom and locked at the top. Carefully begin to open the **Control Panel**.

2. Hold down the **#** key on the keypad. At the same time press and release the **Reset** button on the Control PCB.

3. Close the **Control Panel** carefully into the **Pod** and lock with the **Master Key**. The Control Panel should fit easily, if not check that no wires have become caught or trapped between the Control Panel and the Pod.

4. The LCD will now be displaying the following, at this point you will need to enter the last 4 digits of the cabinet/system serial number and press **#**. For example if the cabinet serial number was TKC12345 you will need to enter 2345 then press #



5. After entering your PIN you will be at the LCD Configuration menu pictured below. Use the keypad to navigate through the menu.

- **Press 1** to enter the setup menu. From here you can setup the Net ID. For RS-232, Modem and Ethernet applications the System ID Number can be set to 1. For RS-485 applications each Traka System on the network must have its own unique ID.

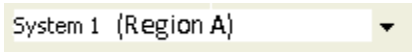
  

  To change the Sys ID, press the ***** key to delete the existing setting, type in the new Sys ID (1, 01, 001 are all acceptable) and press **#** to store the settings**.**

- **Press 2** to reset the systems memory. This utility should only be used under guidance from a Traka Engineer. To reset, press the **#** key or to cancel press the ***** key.

  NOTE: This option should be used with great caution! It deletes the information held with the system and resets the Traka system memory.

  To ensure no loss of data, load the Traka32 software, select a system from the 

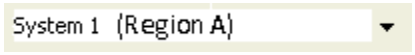
  drop down menu and click on the  button to backup all the data from the system. After resetting from the System Viewer, right click over the picture of the system and click on Synchronise System to restore all the data.

  NOTE: Traka will not be held responsible for the loss of data if you do not read the system data before resetting.

- **Press 3** to swap from the Main Program to the Loader Program. This utility should only be used under guidance from a Traka Engineer. To swap, the vector press the **#** key or to cancel press the ***** key.

  NOTE: This option should be used with great caution! It toggles the program from the main program to the loader program that can be used to upgrade the firmware.

To ensure no loss of data, load the Traka32 software, select a system from the 

drop down menu and click on the  button to backup all the data from the system. After swapping the vector a firmware upgrade can then be performed, please refer to the Upgrade Firmware section for more details.

NOTE: Traka will not be held responsible for the loss of data if you do not read the system data before swapping the vector.

- **Press *** to escape from the configuration menu.

5.6 16BIT CONFIGURATION MENU

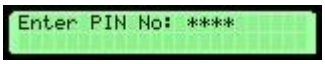
The Configuration Menu of the 16bit Traka System allows you to configure certain settings, such as reset the system, change the CPSN number and restore the Default Configuration.

1. Using the **Master Key**, unlock the **CAM Lock**. The **Control Panel** is hooked in at the bottom and locked at the top. Carefully begin to open the **Control Panel**.

2. Hold down the # key on the keypad. At the same time press and release the **Reset** button on the 16bit Control PCB.

3. Close the **Control Panel** carefully into the **Pod** and lock with the **Master Key**. The Control Panel should fit easily, if not check that no wires have become caught or trapped between the Control Panel and the Pod.

4. The LCD will now be displaying the following, at this point you will need to enter the last 4 digits of the cabinet/system serial number and press #. For example if the cabinet serial number was TKC12345 you will need to enter 2345 then press the # key.



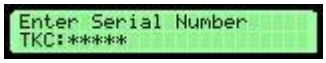
After entering your PIN the LCD Configuration menu will appear. There are two main options to the configuration menu, **System** and **Utilities.**

System

Press the 1 key from the main configuration menu to enter the System menu. From here you can alter the Serial Number, change the CPSN Number or edit the communication of the selected cabinet. Because there are four options to the system menu, you will need to use the # key to scroll down to select the other two options.

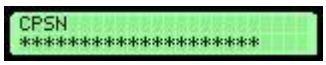
Serial Number

Press 1 at the System menu to enter the **Serial Number** section. To change the Serial Number press the * key to delete the current number and enter the appropriate number via the Traka keypad and press #.



CPSN

Press 2 at the System menu to enter the **CPSN** section. To change the CPSN Number press the * key to delete the current number and enter the appropriate number via the Traka keypad and press #.



Comms

Press 3 at the System menu to enter the **Comms** section. The Comms section consists of the following sub options...

Press 1 at the Comms menu to enter the **System ID** section. To change the System ID Number press the * key to delete the current number and enter the appropriate number via the Traka keypad and press #.

Press 2 at the Comms menu to enter the UartA Baudrate section. To change the baudrate select Key 1,2 or 3 depending on what you wish to change it to.

Press 3 at the Comms menu to enter the UartB Baudrate section. To change the baudrate select Key 1,2 or 3 depending on what you wish to change it to.

Press 4 at the Comms menu to enter the X-Port setup section. This allows you to configure your X-Port, for more details please refer to the X-Port Config section.

Press 5 tat the Comms menu to enter the GSM Setup section. The change the GSM interface select Key 1,2 or 3 depending on what you wish to change it too.

KeyDock

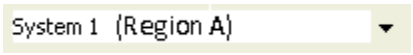
Press 4 at the system menu to enter the **KeyDock** section. This will allow you to set the KeyDock back to its default settings.

Utilities

Press the 2 key from the main configuration menu to enter the Utilities menu. From here you can Reset the control board and Set Default Config.

Press 1 to select the Reset option. Press * to Abandon the Reset or # to Confirm the Reset.

NOTE: This option should be used with great caution! It deletes the information held with the system and resets the Traka system memory.

To ensure no loss of data, load the Traka32 software, select the desired system from the 

drop down menu and click on the  button to backup all the data from the system. After resetting from the System Viewer, right click over the picture of the system and click on Synchronise System to restore all the data.

NOTE: Traka will not be held responsible for the loss of data if you do not read the system data before resetting.

Press 2 to select the Set Default Config section. Press * to Abandon the Default Config or # to Confirm the Default Config.

5.7 16-BIT SYSTEM FILE TYPES

The 16-bit control system firmware uses 3 files for operation. A summary of these are given in the table below.

File	Functional Description	When do I need it?
Configuration (<Serial Number> - <CPSN Number> - <Firmware Version>**.TKCcfg**)	Contains the system configuration i.e number of receptor strips, door configuration, card reader settings etc. In addition it allows cost options to be unlocked; cost options include Fault Logging, Key Booking, X-iFob Authorisers etc. There is no limit (aside from where certain options would conflict) to the number of cost options that can be enabled at a single time. View Firmware Options & Settings for the various options available. Each Traka system must have its own dedicated configuration file and be registered to the Traka32 database. The file contains a CPSN (Control PCB Serial Number) that must match the CPSN stored in the 16-bit Control PCB hardware for operation.	The configuration file **will** be required when commissioning a new system. This is because It needs to be registered to the new Traka32 Database even if the system was shipped with a configuration file in. View Adding a New System for more information on this. An updated version of the configuration file will be required to enable new cost options. Please provide Traka (U.K) or your distributor (outside U.K) with the System Serial Number along with a **Purchase Order No.** for the options required. A new configuration file will be emailed to you. Distributors can also download .cfg files from http://www.traka.com/support. The configuration file is easily loaded using the 16bit Configure Firmware Wizard. View Changing Firmware Settings for more information on this.
Application Firmware (<Version> - <Date>**.MOT**)	Generic file that contains the program code that operates the Traka system. Note that unlike the 8-bit system, all of the program code for the cost options is contained within this single file. This then allows the cost options to be 'unlocked' using the small configuration file.	The application firmware file will only be needed to upgrade the application to include a brand new feature or bug fix. For a list of new features and any bug fixes please visit http://www.traka.com/support
Bootloader a. (<Version> - <Date> .em0 b. (<Version> - <Date> .rom)	Basic input/output operating system providing an interface for the firmware application file.	The bootloader should never need to be changed unless there is a major change to the basic input/output operating system. In which case it is perhaps more likely that the 16-bit Control PCB would be changed instead of a field upgrade of the bootloader.

Also View...

16bit Configure Firmware Wizard

Adding a New System

Changing Firmware Settings

Firmware Options & Settings

16bit Control PCB Overview

5.8 IFOB SEARCH FACILITY

5.8.1 SIMPLE IFOB SEARCH

NOTE: The simple iFob search facility is standard in firmware versions 6.07.16 and below. For firmware versions 6.07.17 and 6.07.22 only the Advanced iFob Search option is available. For firmware versions 6.07.23 and above the simple iFob search is standard and the advanced iFob search is optional.

If an iFob / key is currently out of the system and a user wants to know who's got the iFob / key or if an iFob / key is in the system and a user wants to know who the last user of the key was, they can do this using the lookup facility.

1. Using the keypad, press the ***** key then type in the position number of the iFob in question followed by the **#** key.
2. If the iFob is currently out of the system the **Current Holders** name will be displayed.

3. Pressing **#** again will display the **User Before** name.

4. If the iFob is currently in the system the **Last Users** name will be shown.

5. To exit press **#** again.

NOTE: If any of the optional features are installed other information can also be accessed from the lookup facility such as...

- Random iFob Location
- iFob Curfew
- Fault Codes
- Bay Location
- Mileage
- Fuel Level

5.8.2 ADVANCED IFOB SEARCH

5.8.2.1 ADVANCED IFOB SEARCH OVERVIEW

NOTE: The Simple iFob Search facility is standard in firmware versions 6.07.16 and below. For firmware versions 6.07.17 and 6.07.22 only the advanced iFob search option is available. For firmware versions 6.07.23 and above the simple iFob search is standard and the advanced iFob search is optional.

If a user wants to know who's currently in possession of an iFob / key or if an iFob / key is in the system and a user wants to know who the last user of the key was, they can do this using the advanced search facility.

1. From the Traka System, press the * key on the keypad.

   Fixed Return Systems:

   Random Return Systems:

2. Select the required search option and follow the on screen instructions.
3. For more details on the options available please refer to the following sections...
   - Search by Position
   - Search by iFob Tag
   - Search by iFob Description

5.8.2.2 IFOB POSITION SEARCH

The iFob position search enables a user to search by a physical position within the system. This search is useful if there is an unlabelled iFob / key in a position and you need to find out more information.

Using the position search facility

1. From the Traka System, press the * key on the keypad.

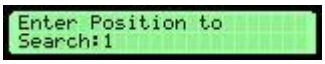
   Fixed Return Systems:

   Random Return Systems:

2. Select the Position option by pressing 1 on the keypad.

3. Using the alphanumeric keys, type in a position e.g. 1.

   NOTE: Use the * key to delete mistakes.

4. When you are ready, press the # key to search.

5. If a match on the position is made, the current iFob status will be shown.

   iFob In System:

   iFob Out of System:

6. Press the # key to view more details about the iFob. This will first show information such as the description, active curfew, current fault code, current location, mileage and fuel level.

7. Press the # key again to view recent events such as who has recently taken and returned the iFob.

   iFob Taken:

   iFob Returned:

   NOTE: The number to the left of the user name is the related iFob Tag Number and will only show if the firmware has Random Return enabled.

5.8.2.3 IFOB TAG SEARCH

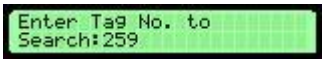
NOTE: The iFob tag search will only be available if the firmware has Random Return enabled.

The iFob tag search enables a user to search by an iFob tag number. This search is useful if there is an unlabeled iFob / key in a position and you need to find out more information or if you are searching for an iFob / key.

Using the tag search facility

1. From the Traka System, press the * key on the keypad.

2. Select the Tag option by pressing 2 on the keypad.



3. Using the alphanumeric keys, type in a position e.g. 259.

   NOTE: Use the * key to delete mistakes.

4. When you are ready, press the # key to search.

5. If a match on the iFob tag is made, the current iFob status / position will be shown.

   iFob In System:

   iFob Out of System:

6. Press the # key to view more details about the iFob. This will first show information such as the description, active curfew, current fault code, current location, mileage and fuel level.

7. Press the # key again to view recent events such as who has recently taken and returned the iFob.

   iFob Taken:

   iFob Returned:

   NOTE: The number to the left of the user name is the related Position Number within the system.

   NOTE: This search facility will not search across systems however this is planned for the future. Please contact your supplier for more details.

5.8.2.4 IFOB DESCRIPTION SEARCH

With this option enabled, it is possible to search on the description of an iFob using the alphanumeric keypad on the Traka system. For example, details such as vehicle registrations or chassis numbers could be searched upon to locate the keys within the cabinet.

Configuration

1. Using the Traka32 software, click on **File**, **Properties**.
2. Click on the **Key Details**, **Use as iFob Description** tab.
3. Select one of the Key Description fields to be used.

   As there are 10 fields for each key record, to simplify the searching only 1 field can be searched upon. Select one of the Key Detail description fields to be written to the Traka systems for searching.

   If there is more than one key attached to the iFob, the first key in the list will be selected.

Using the description search facility

1. From the Traka System, press the * key on the keypad.

   Fixed Return Systems:

   Random Return Systems:

2. Select the Description option by pressing 2 or 3 on the keypad.

3. Using the alphanumeric keys, type in all or part of a description e.g. XYZ.

   NOTES:

   - The search is not case sensitive.
   - Use the * key to delete mistakes.

4. When you are ready, press the # key to search.
5. If a match on the description is made, the location of the iFob will be shown.

   To view more details about the iFob, press the 0 key. This will first show information such as the description, active curfew, current fault code, current location, mileage and fuel level followed by recent events such as who has recently taken and returned the iFob.

   If there is more than one occurrence, press the # key to see all matches.

The system will display if no further matches are found.

6. The system will display if no matches are found at all.

NOTE: This search facility will not search across systems however this is planned for the future. Please contact your supplier for more details.

5.9 EMERGENCY IFOB RELEASE

5.9.1 EMERGENCY IFOB RELEASE

The Emergency iFob Release utility is available to release all the iFobs from a system one at a time.

1. Using the **Master Key**, unlock the **Pod Lock**. The **Control Panel** is hooked in at the bottom and locked at the top. Carefully begin to open the **Control Panel**.

2. Hold down the * key on the keypad. At the same time press and release the **Reset** button on the Control PCB.

NOTE: If you are running v6.06.12 or below of the firmware you will not get a menu and the system will open the door (if fitted) and start to release each iFob one at a time for 5 seconds starting at position 1 and will continue to do so until the door is closed. Empty slots will be skipped.

3. Close the **Control Panel** carefully into the **Pod** and lock with the **Master Key**.

   The Control Panel should fit easily, if not check that no wires have become caught or trapped between the Control Panel and the Pod.

4. Use the keypad to navigate through the menus...

   - **Press 1** to release all the iFobs.

     The door will open (if fitted).

     If you have more than one cabinet attached to your system you will be asked to select which door you want to open, simply enter the door number on the keypad.

     The Traka System will release each iFob one at a time for 5 seconds starting at position **1** and will continue to do so until the door is closed. Empty slots will be skipped.

   - **Press 2** to release a specific iFob.

     You will be prompted to enter the position number of the iFob that you wish to release. Using the keypad, enter the position number followed by **#**.

     If you have a fixed return system, the appropriate door will open automatically. If you have a Random Return system with more than one cabinet you will be asked to select which door you want to open, simply enter the door number on the keypad.

     The Traka System will release the specified iFob until the door is close or the system times out.

     To release another iFob, simply close the door and repeat step 4.

   - **Press *** to exit.

5. Simply remove the iFob from the position; you do not need to press the black button next to the iFob.

6. When you have finished simply close the door.

5.9.2 TOTAL SYSTEM FAILURE

In the event of total system failure you have two choices...

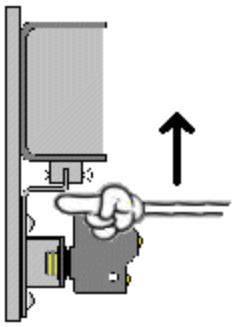
If you need to gain access to the keys **quickly** or you have a **Mini Traka System** the best way is to cut the security seals that hold the keys to the iFobs.

Tools required...

- Heavy duty wire cutters.

1. Using the **Master Key** release the door (if fitted) using the **Door Release Lock**.

   On a Mini Traka System you will need to use the **Master Key** to unlock the **Pod Lock**. The **Control Panel** is hooked in at the bottom and locked at the top. Carefully begin to open the **Control Panel**. You will see the lock at the bottom of the panel, using you finger release the **Catch** that hold the door shut.



2. Using a heavy duty pair for **wire cutters**, cut the security seals that hold the keys to the iFobs.

3. Please contact your supplier to have your Traka System repaired and tested.

If you have more time you will need to remove various parts of the Traka System to gain access to the iFobs / Keys. Please refer to the Manual iFob Release Guide section for the relevant systems.

5.9.3 MANUAL IFOB RELEASE

5.9.3.1 M-SERIES MANUAL IFOB RELEASE

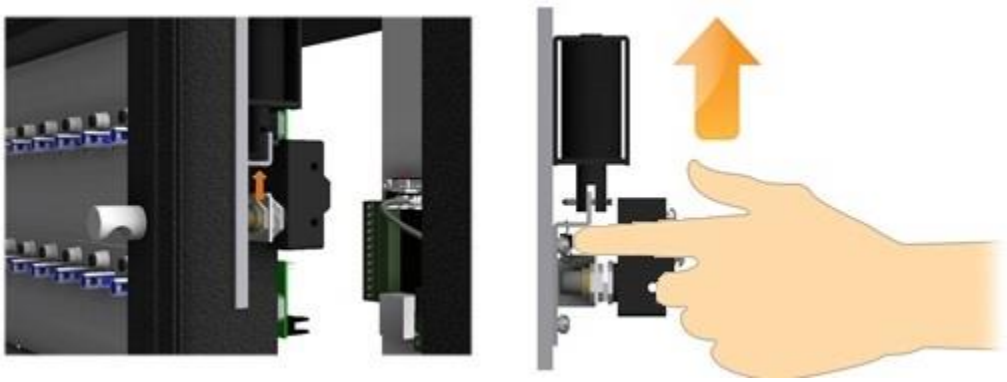
In the event of total system failure you will need to remove various parts of the M-Series Traka System to gain access to the iFobs / Keys.

Tools required...

- Large flat blade screwdriver
- Small flat blade screwdriver
- 4mm Allen Key

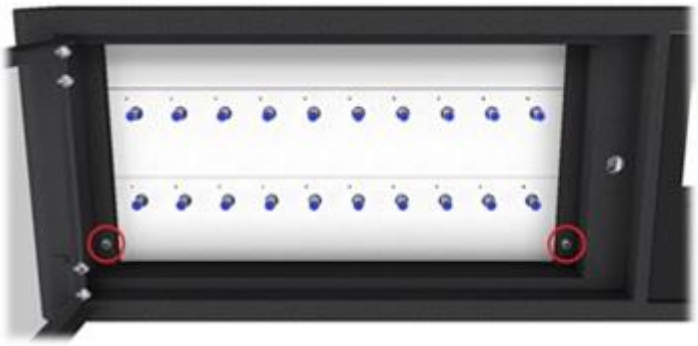
1. Switch off the mains power to the unit by removing the fuse from the fused spur or unplugging from the mains.
2. The Control Panel is hooked in at the bottom and locked at the top. Using the Master Key, unlock the Cam Lock.
3. Lean the Control Panel forward and set the On/Off switch on the Control PCB to **Off**.

4. Reach inside and open the door manually by moving the door lock catch up.

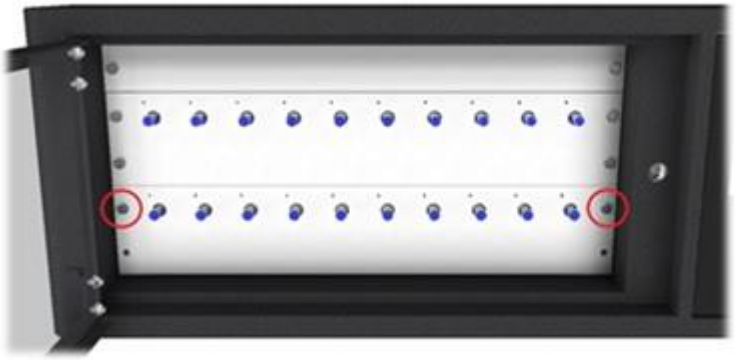


5. Carefully close the Control Panel.

6. Using a 4mm Allen Key, remove the cover panel screws one at a time and remove the cover panels.



7. Using a large flat bladed screwdriver, remove the screws from the receptor strip you wish to release the iFobs from. Remove the strip, carefully disconnecting the receptor ribbon cable.



8. Using a small flat blade screwdriver, you will be able to pull back the small solenoid blade that holds the iFob in place and remove the iFob.

9. Repeat steps 9 to 11 for each receptor strip you wish to remove the iFobs from.

10. When you have released the iFobs you require, replace all the receptor strips, reconnecting the receptor ribbon cable. Using a large flat bladed screwdriver secure the receptor strips in place with the fixings and spacers removed earlier.

    NOTE: It is essential that the receptor strips are replaced in the same location from which they were removed otherwise the system will not function correctly.

11. Using a 4mm Allen Key, replace the cover panels one at a time. Once the cover panels have been replaced then close the door (if fitted).

5.9.3.2 S-SERIES MANUAL IFOB RELEASE

In the event of total system failure you will need to remove various parts of the S-Series Traka System to gain access to the iFobs / Keys.

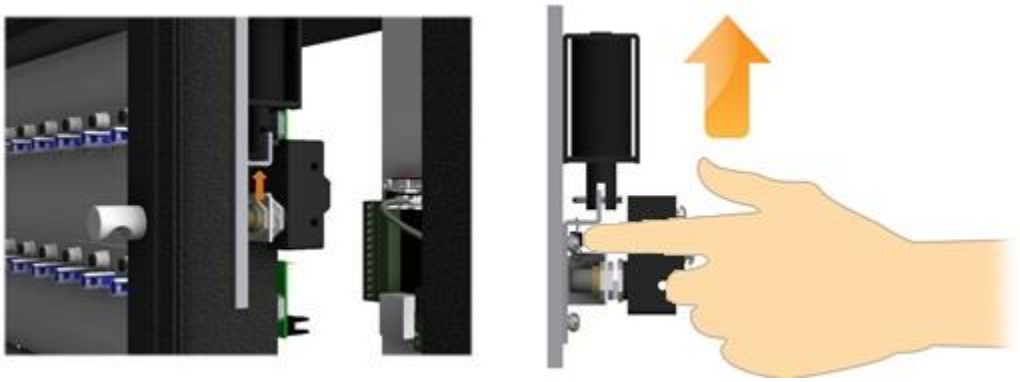
Tools required...

- Large flat blade screwdriver.
- Small flat blade screwdriver
- 2.5mm Allen Key
- Receptor Frame Hinge.

1. Switch off the mains power to the unit by removing the fuse from the fused spur or unplugging from the mains.
2. The Control Panel is hooked in at the bottom and locked at the top. Using the Master Key, unlock the Control Panel Cam Lock.

3. Lean the Control Panel forward and set the On/Off switch on the Control PCB to **Off**.

4. Tilt the Control Panel forward and reach inside and open the door manually by moving the door lock catch up.



5. Undo the plastic Wing Bolt then close and lock the Control Panel. You will now be able to swing open the Control Panel Door.

6. Fit the Receptor Frame Hinge into the locating slots at the top and bottom of the cabinet by inserting the top first and then the bottom.

7. Using a 2.5mm Allen Key, remove the bolts holding the receptor frame in place.

8. Carefully slide the frame to the right aligning the holes in the Receptor Frame Hinge with those in the Frame itself.

9. Fit two plastic Wing Bolts attaching the Receptor Frame Hinge to the Receptor Frame.
10. Slowly open the Receptor Frame.
11. Using a small flat blade screwdriver, you will be able to pull back the small solenoid blade that holds the iFob in place and remove the iFob.

5.9.3.3 L-SERIES MANUAL IFOB RELEASE

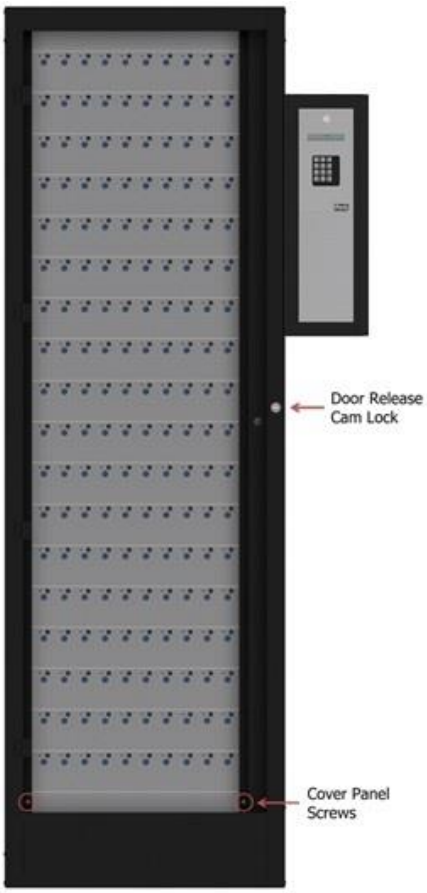
In the event of total system failure you will need to remove various parts of the L-Series Traka System to gain access to the iFobs / Keys.

Tools required...

- 10mm Socket/Nut Spinner
- Small flat blade screwdriver
- 4mm Allen Key

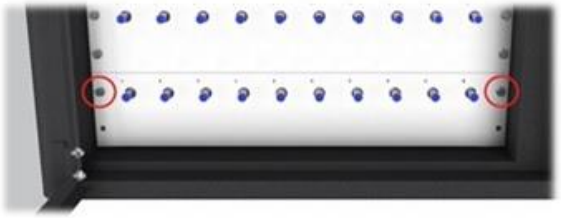
1. Switch off the mains power to the unit by removing the fuse from the fused spur or unplugging from the mains.
2. The Control Panel is hooked in at the bottom and locked at the top. Using the Master Key, unlock the Cam Lock.
3. Lean the Control Panel forward and set the On/Off switch on the Control PCB to **Off**.

4. Using the Master Key open the door (if fitted) using the Door Release CAM Lock.



5. Using a 4mm Allen Key, remove the Cover Panel Screws one at a time and remove the cover panels.

6. Using a 10mm nut spinner, remove the nuts from the receptor strip you wish to release the iFobs from. Remove the strip, carefully disconnecting the receptor ribbon cable.



7. Using a small flat blade screwdriver, you will be able to pull back the small solenoid blade that holds the iFob in place and remove the iFob.

5.9.3.4 MINI 16 MANUAL IFOB RELEASE

In the event of total system failure you will need to remove various parts of the Mini 16 Traka System to gain access to the iFobs / Keys.

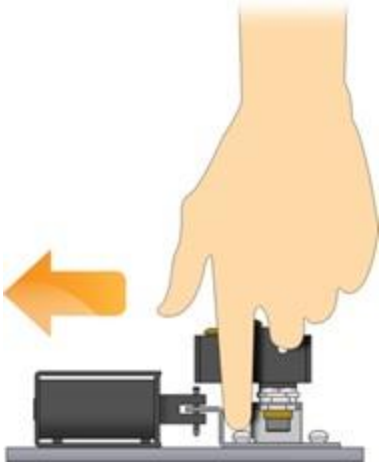
NOTE: On a Mini 16 system it is not possible to manually remove an iFob without removing PCBs and various other components. Therefore this process describes how to access the keys and manually remove them from the iFobs.

Tools required...

- Heavy duty wire cutters.

1. Switch off the mains power to the unit by removing the fuse from the fused spur or unplugging from the mains.

2. Use the Master Key to unlock the Cam Lock. The Control Panel is hooked in at the bottom and locked at the top. Carefully begin to open the Control Panel. You will see the lock at the bottom of the panel, using your finger release the Catch that holds the door shut.



3. Using a heavy duty pair of wire cutters, cut the security seals that hold the keys to the iFobs.

4. Please contact your supplier to have your Traka System repaired and tested.

5.9.3.5 STANDARD TRAKA MANUAL IFOB RELEASE

In the event of total system failure you will need to remove various parts of the Standard Traka System to gain access to the iFobs / Keys.

Tools required...

- Large flat blade screwdriver.
- Small flat blade screwdriver.

2. Switch off the mains power to the unit by removing the fuse from the fused spur or unplugging from the mains.
3. Using the Master Key, unlock the Pod Lock. The Control Panel is hooked in at the bottom and locked at the top. Carefully begin to open the Control Panel.
4. You will see that there are several wires connected to the Printed Circuit Board (PCB) that are attached to the control panel. Determine which version of the Control PCB you have using the Control PCB Diagrams.
5. If you have **V2.20** of the Control PCB then...

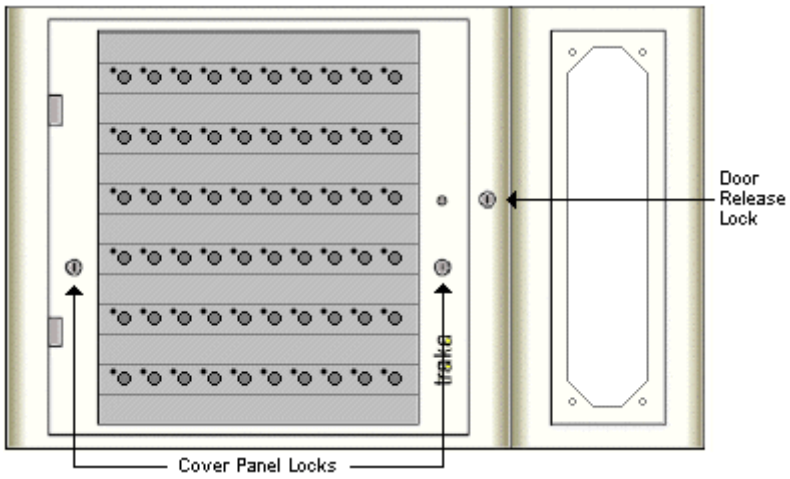
3.

   a. Disconnect the Battery.
   b. Disconnect the Power Supply.

4. If you have **V2.30.01 or above** of the Control PCB then...

   a. Set the On/Off switch to Off.

5. Carefully close the Control Panel.
6. Using the Master Key release the door (if fitted) using the Door Release Lock.



7. Using the master key again, unlock the Cover Panel Locks one at a time and remove cover panels.
8. Using a large flat bladed screwdriver, carefully remove the screws from the blank receptor strip above the receptor strip you wish to release the iFobs from. Remove the strip and spacers and place to one side.
9. Again using a large flat bladed screwdriver, carefully remove the screws from the receptor strip you wish to release the iFobs from. Remove the strip carefully disconnecting the receptor ribbon cable.
10. Using a small flat blade screwdriver, you will be able to pull back the small solenoid blade that holds the iFob in place and remove the iFob.

11. Repeat steps 9 to 11 for each receptor strip you wish to remove the iFobs from.

    NOTE: It is essential that the receptor strips are replaced in the same location from which they were removed otherwise the system will not function correctly.

12. When you have released the iFobs replace all the receptor strips reconnecting the receptor ribbon cable. Using a large flat bladed screwdriver secure the receptor strips in place with the fixings and spacers removed earlier.

13. Using the Master Key, replace and lock the Cover Panels one at a time. Note the cover panels are handed. Once the cover panels have been replaced and locked securely in place then close the door (if fitted).

14. Please contact your supplier to have your Traka System repaired and tested.

5.9.3.6 LARGE TRAKA MANUAL IFOB RELEASE

In the event of total system failure you will need to remove various parts of the Large Traka System to gain access to the iFobs / Keys.

Tools required...

- Large flat blade screwdriver.
- Small flat blade screwdriver.
- 4mm Allen Key

2. Switch off the mains power to the unit by removing the fuse from the fused spur or unplugging from the mains.
3. Using the Master Key, unlock the Pod Lock. The Control Panel is hooked in at the bottom and locked at the top. Carefully begin to open the Control Panel.
4. You will see that there are several wires connected to the Printed Circuit Board (PCB) that are attached to the control panel. Determine which version of the Control PCB you have using the Control PCB Diagrams.
5. If you have **V2.20** of the **Control PCB** then...

3.

   a. Disconnect the Battery.

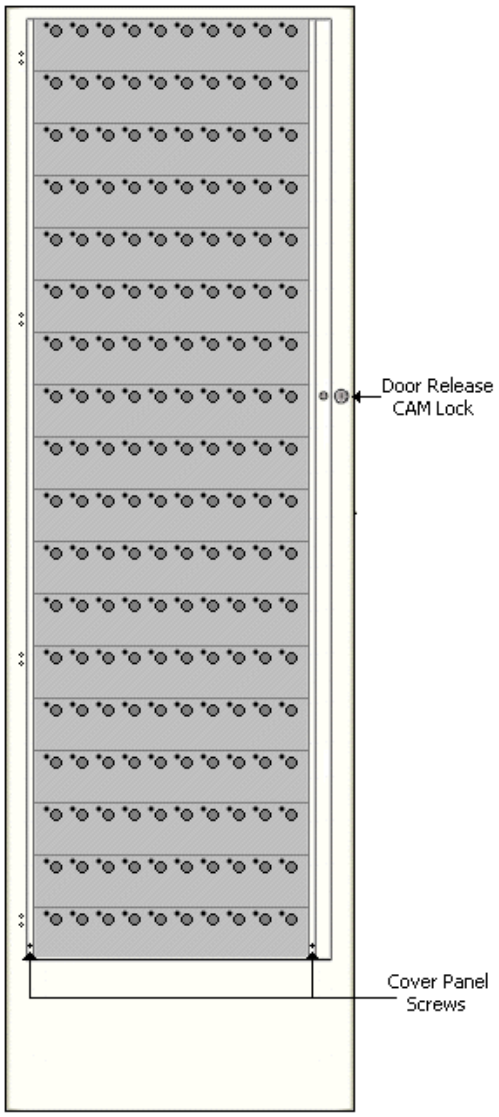
   b. Disconnect the Power Supply.

4. If you have **V2.30.01 or above** of the **Control PCB** then...

   a. Set the On/Off switch to Off.

5. Carefully close the Control Panel.

6. Using the Master Key release the door (if fitted) using the Door Release Lock.



7. Using a 4mm Allen Key, remove the cover panel screws one at a time and remove the cover panels.

8. Using a large flat bladed screwdriver, carefully remove the screws from the blank receptor strip above the receptor strip you wish to release the iFobs from. Remove the strip and spacers and place to one side.

9. Again using a large flat bladed screwdriver, carefully remove the screws from the receptor strip you wish to release the iFobs from. Remove the strip carefully disconnecting the receptor ribbon cable.

10. Using a small flat blade screwdriver, you will be able to pull back the small solenoid blade that holds the iFob in place and remove the iFob.

11. Repeat steps 9 to 11 for each receptor strip you wish to remove the iFobs from.

    NOTE: It is essential that the receptor strips are replaced in the same location from which they were removed otherwise the system will not function correctly.

12. When you have released the iFobs replace all the receptor strips reconnecting the receptor ribbon cable. Using a large flat bladed screwdriver secure the receptor strips in place with the fixings and spacers removed earlier.

13. Using a 4mm Allen Key, replace the cover panels one at a time. Note the cover panels are handed. Once the cover panels have been replaced then close the door (if fitted).

14. Please contact your supplier to have your Traka System repaired and tested.

5.10 IFOB UNDETECTABLE

5.10.1 IFOB UNDETECTABLE OVERVIEW

The Traka cabinet continuously scans the iFobs to ensure they remain present and correct. If the system fails to detect the iFob whilst no authorised user is logged in then it is flagged as undetectable and an 'iFob Undetectable' event is recorded. It is important to note that an 'iFob Removed' event is not recorded in this instance.

The system continues to scan the iFobs and if an iFob previously marked as undetectable is re-detected, an 'iFob Re-detectable event' is recorded.

View also...

Causes of iFob Undetectable

Solenoid Vibration

What happened to iFob Forced from System

Intelligent Receptor Features (helping to cure iFob Undetectable issues)

Alarm and Event Types

5.10.2 CAUSES OF IFOB UNDETECTABLE

The main reason for an iFob becoming undetectable is a loss of contact between the iFob and the receptor slot contacts. This can be happen due to a number of reason...

1. In order for the Traka Cabinet to communicate to an iFob there must be a good contact between the iFob and the Receptor Socket Contacts. A poor connection can occur and prevent the Traka Cabinet from detecting the iFob if...

    a. the **Contacts** inside the Receptor Socket are dirty, worn, bent, damaged or

    b. the **iFob** is dirty, worn, or damaged.

2. On a Locking receptor strip, the black push button is wired' in series' with the iFob. If there is a large bunch of keys pressing against the black push button whilst the door is closed then the iFob is 'open circuit' and the Traka Cabinet will no longer be able to detect the iFob.

NOTE: The new Intelligent Receptor Strip resolves this problem because the black push button switch is wired independently of the iFob. See Intelligent Receptor Features for more details.

3. If an iFob is not fully inserted into the Receptor Socket then again a poor connection can occur.

Where regular 'iFob un(re-)detectable' events are being recorded against a single position it is a good idea to inspect the iFob and receptor slot for signs of wear or damage. To determine if the problem is with the receptor slot or the iFob, try replacing the iFob with a new iFob and monitoring over a short period.

View also...

iFob Undetectable

Solenoid Vibration

What happened to iFob Forced from System

Intelligent Receptor Features (helping to cure iFob Undetectable issues)

Alarm and Event Types

5.10.3 SOLENOID VIBRATION

When an iFob is marked as 'iFob Undetectable', the system vibrates the receptor solenoid in an attempt to move the iFob slightly so as it establishes contact again. therefore you should not be alarmed upon hearing a vibrating sound every so often from the Traka system. However Traka would recommend you check the event reports in Traka32 as it could an indication of a faulty iFob.

View also...

iFob Undetectable

Causes of iFob Undetectable

What happened to iFob Forced from System

Intelligent Receptor Features (helping to cure iFob Undetectable issues)

Alarm and Event Types

5.10.4 WHAT HAPPENED TO IFOB FORCED FROM SYSTEM?

In older firmware versions, instead of recording an 'iFob Undetectable' event the system would have recorded an 'iFob Forced from System' event in addition to an 'iFob Removed' event (recorded against the last User who accessed the system).

It was viewed that if an iFob went undetected whilst a user was not logged into the system, then it must have been forced. However this understandably led to some confusion because in the vast majority of cases the iFob was not being forcefully removed; the events were being generated due to a momentary loss of contact between the iFob nd receptor slot..

The 'iFob Forced from System' event is no longer recorded.

View also...

iFob Undetectable

Causes of iFob Undetectable

Solenoid Vibration

Intelligent Receptor Features (helping to cure iFob Undetectable issues)

Alarm and Event Types

5.11 TROUBLESHOOTING

5.11.1 BROKEN IFOB IN CABINET

If a Traka System starts displaying the 'Broken iFob In Cabinet' message, there is a broken iFob somewhere within the system.

To find the broken iFob...

1. First access the Traka System. Please refer to the 'How to access the system? ' section
2. Check the LCD...
    - If the LCD is displaying the following message then start at position **1**.

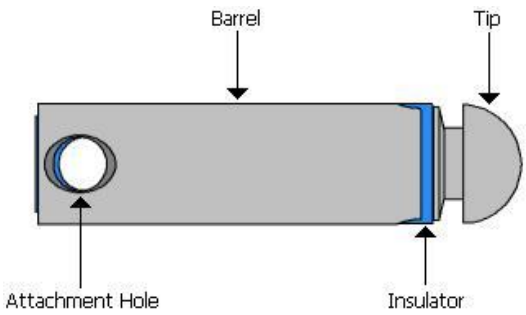
      

    - If the LCD is displaying the following message then start at the left hand position on the receptor strip number displayed.

3. If there is an iFob in the position...
    - If the position is a **Locking** position, press the black button against the iFob.
    - If the position is a **Non-Locking** position, remove the iFob.
4. Check the LCD to see if the 'Broken iFob In Cabinet' has cleared...
    - If the 'Broken iFob In Cabinet' message has cleared, you have found the broken iFob. Discard the iFob and add a new iFob. Please refer to the Adding iFob section.
    - If the 'Broken iFob In Cabinet' message has not cleared, move to the next position and repeat steps 3 and 4 until all positions have been checked.
    - If the display is showing 'PLEASE CLOSE THE DOOR', close the door and access the system again and carry on from the where you left off.
5. If you have thoroughly checked all the iFobs and the message is still showing, please contact your supplier for further help and assistance.

   NOTE: A broken iFob usually occurs is earlier models of the Traka Systems and iFobs. You can visually check an iFob to see if it needs replacing.

6. Check the **Insulator** to ensure there is no damage. If the insulator is damaged or missing then replace the iFob immediately.
7. Check the **Tip** to ensure that it does not spin by twisting it with your fingers, do use any tools. If the tip does spin, replace the iFob immediately.

5.11.2 ID NOT RECOGNISED

If a user cannot gain access to the Traka System check their user details have been set up correctly from the Traka32 software. Please refer to the User Details section.

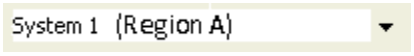
5.11.3 IFOB NOT AUTHORISED

If a user can gain entry to the Traka System but cannot remove an iFob that they should have access too, check the user details have been set up with the appropriate access levels for the iFob in question. Please refer to the User Details section. You can look up the access level of the iFob from the iFob list, click on **View**, **iFob List**.

5.11.4 MEMORY ALMOST FULL

If a Traka System starts displaying the 'Memory Almost Full' message, the alarm and/or transaction memory within the Traka System is nearing maximum capacity.

To clear this message...

1. Load the Traka32 software by double clicking on the  icon.
2. Select the appropriate system from the 

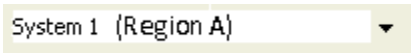
drop down menu.
3. Click on the  button.

NOTE: When the memory becomes full, it will start to overwrite the oldest information in order to keep the most recent information and data may be lost.

5.11.5 WARNING: MEMORY FULL !!

If a Traka System starts displaying the 'WARNING: MEMORY FULL !!' message, the alarm and/or transaction memory within the Traka System has reached maximum capacity.

To clear this message...

1. Load the Traka32 software by double clicking on the  icon.
2. Select the appropriate system from the 

drop down menu.
3. Click on the  button.

NOTE: When the memory becomes full, it will start to overwrite the oldest information in order to keep the most recent information and data may be lost.

5.11.6 CHECK ALARMS

The Check Alarms message will show on the LCD if there are some alarms to download.

Simply open a copy of Traka32 and click on  .

5.11.7 HOW TO TAKE AN IFOB

Button Release System

1. First access the Traka System. Please refer to the 'How to access the system? ' section.
2. To take an iFob...
    - If the position is a **Locking** position, press the black button against the iFob until you hear a beep.

      Release the button, the solenoid that holds the iFob in place will activate and you should be able to remove the iFob.

    - If the position is a **Non-Locking** position, simply remove the iFob and check the LCD displays the correct position number.

      NOTE: The iFob description may be shown on the LCD when a user removes the iFob from the system.

      NOTE: If you do not have access to the iFob the LCD will display iFob NOT Authorised. If you should have access to the iFob then check the access level of the iFob and the current access levels of the user match.

3. The LCD will display the position number of the iFob you have taken.

4. Repeat step 2 and 3 for each iFob you require.

   NOTE: If you have a no door system you will only be able to take one iFob at a time. To take another iFob you will have to access the system again.

Keypad Release System

1. First access the Traka System. Please refer to the 'How to access the system?' section.
2. Type in the position number of the iFob that you wish to take followed by **#**.
3. If the user has access and the iFob is currently in the system, the door will open and the iFob will be released.

NOTE: The Time Due Back for an item/iFob is now calculated when the item is taken during a Key Booking. This information is displayed on the system viewer information panel and can also be seen in the iFob and Key Current Holder Reports.

5.12 DESKTOP IFOB PROGRAMMER

5.12.1 DESKTOP IFOB PROGRAMMER OVERVIEW

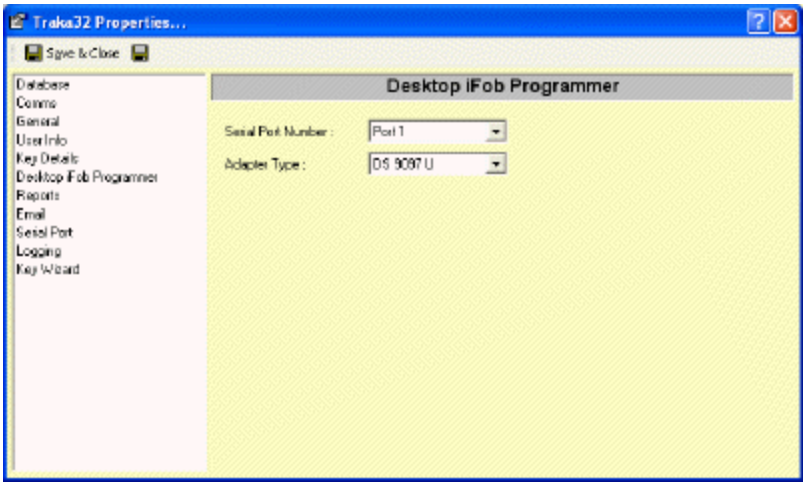
The Traka Desktop iFob Programmer is a single iFob receptor incorporated into a desktop programmer device. The desktop programmer connects to a computer running Traka32 via a spare serial or USB port.

The desktop programmer can be used to configure new iFobs for a cabinet or to program iFobs using the Traka Immobilisor iFob Programmer.

5.12.2 DESKTOP IFOB PROGRAMMER INSTALLATION

Serial Desktop iFob Programmer

1. To install the desktop programmer, simply connect the desktop programmer's serial adaptor to a free serial port on a computer with Traka32 installed. Please make a note of the serial port number for use in step 5.
2. Load the Traka32 software by double clicking on the  icon.
3. Click on **File**, **Properties**.
4. Click on the **Desktop iFob Programmer** section.



5. Select the relevant **Serial Port Number** according to which serial port you have connected the Desktop iFob Programmer to.
6. Set the **Adaptor Type** accordingly. The adaptor type is printed on the serial port connector of the Desktop iFob Programmer.
7. Click on **Save & Close.**

USB Desktop iFob Programmer

To use the USB Desktop iFob Programmer you need to install the appropriate drivers. This can be done two ways, First there is a custom installation option when you are installing Traka32 for the first time, the second way is you can edit the drivers in the add/remove programs folder from the control panel, this option is for anyone who already has Traka32 installed.

Option 1

NOTE: Do not plug the USB Desktop Programmer into your PC until the driver have been successfully installed.

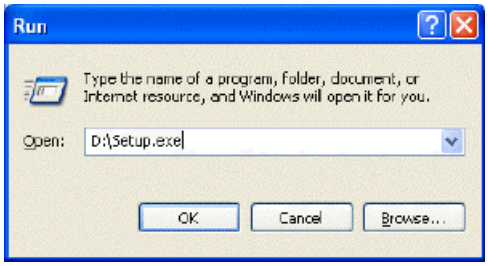
This option is applicable if you are installing Traka32 for the first time.

NOTE: Before installing the Traka32 software, please check that the PC you are going to install the software on meets the minimum requirements otherwise you may face problems during the installation or use of the software. Please refer to the minimum PC requirements section for more details.

1. Insert the Traka32 CD into the CD-ROM drive.

2. After a few seconds the set-up wizard should run automatically.

   If not, click on Start > Run and type D:\Setup.exe followed by Enter
   (replacing the D with the appropriate CD-ROM letter)

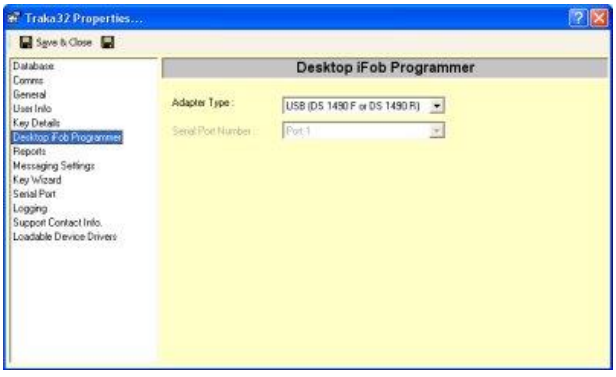


3. The Traka32 Administrator will now appear. At this point you will have the option to choose the location you wish to save Traka32 to by clicking the 'Change' button, if however if you leave this unchanged by clicking 'Next' it will save in a default location. The next screen will ask you what type of install you wish to proceed with, i.e 'Typical', 'Normal' or 'Custom'. Select 'Custom' install and you will be taken to the Custom setup screen where you will see all the drivers and additional features that can be enabled. Expand the 'Drivers' menu, then expand USB Desktop iFob Programmer Driver, and select 'This Feature Will be installed on Local Hard drive'. Click 'Next' then 'Install' and the set-up wizard will guide you through the rest of the installation.

4. When the software has fully installed you will need to find the drivers folder which will be in the following location, unless you chose a different location to save Traka32 at the point of installation. C: > Program Files > Traka Limited > Traka32 > Drivers. Within the Drivers folder will be another folder named 'USB Desktop Programmer' in there will be a file called 'Install_1_wire_drivers' that you need to install. Double click the file and follow the instructions to install the drivers.

5. USB Desktop Programmer is now ready for use. Insert the USB connector into a free port on the required PC and open the TRAKA32 software by double clicking on the  icon on your desktop.

6. Select File/Properties, and then select 'Desktop iFob Programmer'. Now use the drop down box labelled 'Adapter Type', and select 'USB (DS 1490 F or DS 1490 R)', (see below) now save and close. Installation is now complete and you can now begin to use your Desktop Programmer.



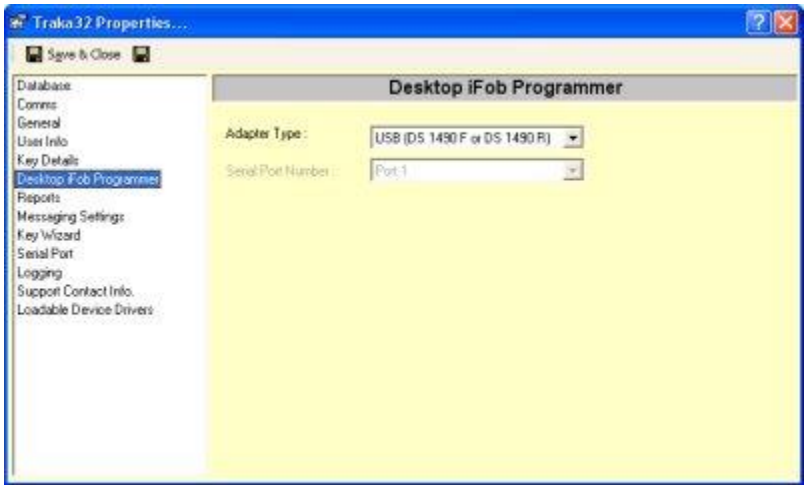
Option 2

NOTE: Do not plug the USB Desktop Programmer into your PC until the driver have been successfully installed.

This option is applicable if you already have Traka32 installed and wish to activate the USB Desktop iFob Programmer Drivers.

- Select... Control Panel\ Add or Remove Programs and select 'Traka32bit Administrator'.
- Select change, then next.
- Check the box for 'Modify' and select next.
- Expand the 'Drivers' menu.
- Expand the 'USB Desktop iFob Programmer Driver', and select 'This Feature Will be installed on Local Hard drive'.

1. Now the Drivers have been enabled, they must be installed the setup file is located in C:\Program Files\Traka Limited\Traka32\Drivers\USB Desktop Programmer\ (This file path may be custom depending on how Traka32 was initially installed). Once you have opened the folder select the 'Install_1_wire_drivers' icon, and follow the instructions of the setup wizard.
2. When the drivers are fully installed the USB Desktop iFob Programmer is ready for use.
3. Insert the USB connector into a free port on the required PC.
4. Open the TRAKA32 software by double clicking on the  icon on your desktop and select File/Properties, then select 'Desktop iFob Programmer'. Now use the drop down box labelled 'Adapter Type', and select 'USB (DS 1490 F or DS 1490 R)', (see below) now save and close. Installation is now complete and you can now begin to use your Desktop Programmer.



5.13 TRAKA HANDHELD IFOB TRANSFER DEVICE

5.13.1 HANDHELD IFOB TRANSFER DEVICE OVERVIEW

The Traka Handheld Device is a universal platform for mobile Traka Applications. This user guide focuses on the iFob Transfer Unit application. The iFob Transfer Unit features an iFob receptor socket and Sagem Morphosmart CBM Biometrics reader. The purpose of this unit is to log the handover of an iFob from one user to another.

Communications between the Traka Handheld Device and Traka32 Software is via a USB connection. Traka32 may be used to set up the device and read back configuration information in a similar way to communicating with a Traka Key Cabinet or Locker System.

NOTE: The 8bit system does not support the Handheld Device.

The Traka Handheld Device hardware is powered from an internal Lithium-Ion rechargeable battery that is recharged through the USB connection to the device.

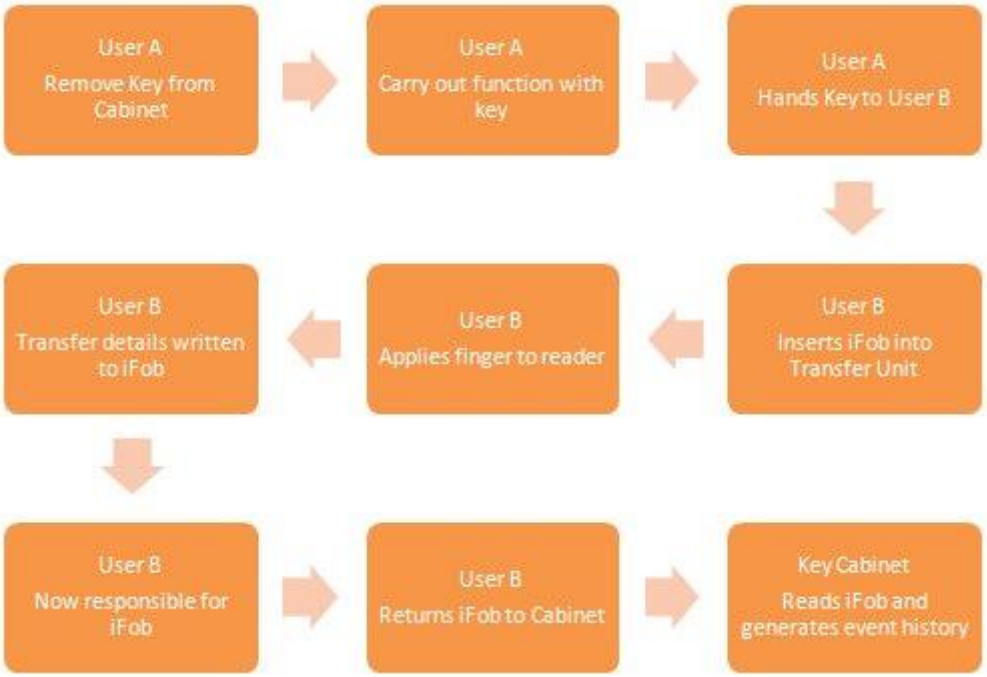
With each Traka Handheld Device, the following items are supplied:

- Mains USB charger with USB A to B cable for charging
- USB A to B cable for PC connection
- CD with documentation, Windows drivers and support software

The Traka Handheld Device is a rugged metal enclosure fitted with a protective rubber boot. The front panel features a 16x2 character display, two illuminated function buttons, a biometrics reader and an iFob receptor socket.

A USB type B (device) socket can be found on the rear of the unit for communication and battery charging.

The iFob Transfer Unit application is used to record the handover of an iFob, with associated keys, from one user to another. This process is summarised below:



5.13.2 HANDHELD DEVICE DRIVER INSTALLATION

The Handheld iFob Transfer Device requires certain drivers be installed before use. You can install these drivers one of two ways see below.

NOTE: Do not connect the Traka Handheld Device until you have installed the drivers.

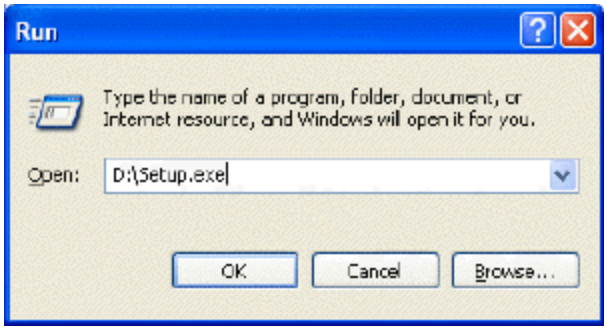
Option 1

This option is applicable if you are installing Traka32 for the first time.

NOTE: Before installing the Traka32 software, please check that the PC you are installing the software on meets the minimum requirements, otherwise you may face problems during the installation or use of the software. Please refer to the minimum PC requirements section for more details.

1. Insert the Traka32 CD into the CD-ROM drive.
2. After a few seconds the set-up wizard should run automatically.

   If not, click on Start > Run and type D:\Setup.exe followed by Enter (replacing the D with the appropriate CD-ROM letter)



3. The Traka32 Administrator will now appear. At this point you will have the option to choose the location you wish to save Traka32 to by clicking the 'Change' button, if however if you leave this unchanged by clicking 'Next' it will save in a default location. The next screen will ask you what type of install you wish to proceed with, i.e 'Typical', 'Normal' or 'Custom'. Select 'Custom' install and you will be taken to the Custom setup screen where you will see all the drivers and additional features that can be enabled. Expand the 'Drivers' menu, then expand Traka Handheld Device Driver, and select 'This Feature Will be installed on Local Hard drive'. Click 'Next' then 'Install'. The set-up wizard will guide you through the rest of the installation.

Option 2

This option is applicable if you are altering your current Traka32 installation.

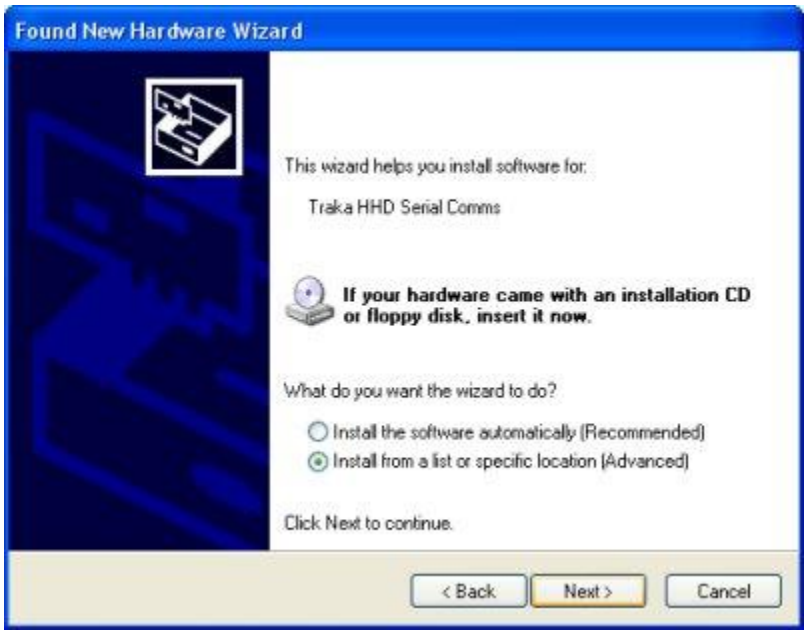
1. Firstly proceed to the control panel and select 'Add or Remove Programs'.
2. When the Program List appears highlight Traka32 and select 'Change'.
3. You will then be confronted by the Traka32 InstallShield. Click 'Next' and 'Modify' you will then be taken to the modification setup screen where you will see all the drivers available and additional features that can be enabled. Expand the 'Drivers' menu, then expand Traka Handheld Device Driver, and select 'This Feature Will be installed on Local Hard drive'. Click 'Next' then 'Install'. The set-up wizard will guide you through the rest of the modification.

After you have finished modifying or installing Traka32 plug in the Handheld Device via your provided USB A to B cable.

Windows should detect and enumerate the device. You may see a status bubble appear at the bottom right hand corner of your taskbar.

Shortly after the device is detected by Windows the 'Found New Hardware Wizard' will appear. Select 'No, not this time' to reject connecting to Windows Update and click next.

Windows will then prompt to help you find the driver automatically. For this driver installation we are going to browse directly to the drivers. Select 'Install from a list or specific location (advanced)' then click next.



Next Windows will prompt for a location to search for the drivers. Ensure 'Search for the best driver in these locations' is selected, and the tick box for 'Include this location in the search'. Then click browse to locate the drivers. Providing the installation/modification of Traka32 was successful, you will need to browse to the following location an then click 'Next'.

C:\Program Files\Traka Limited\Traka32\Drivers\Traka Handheld Device

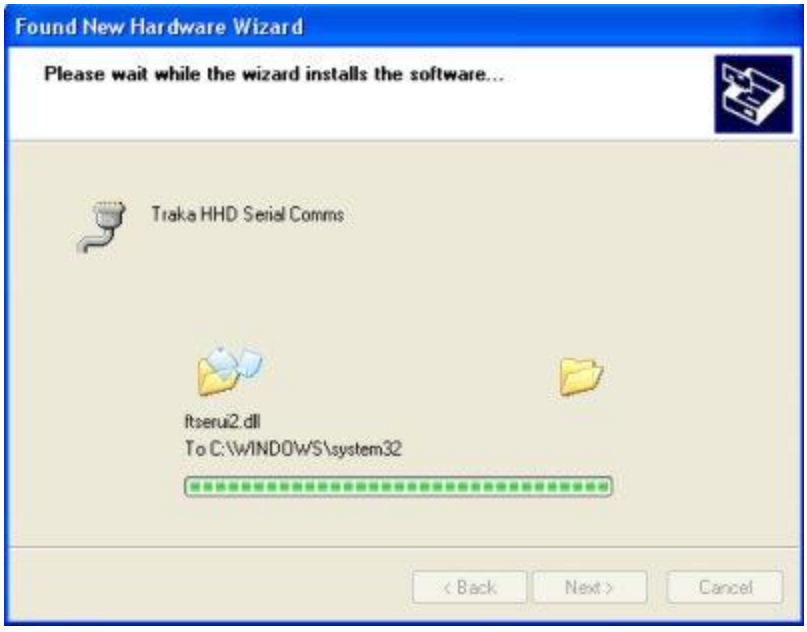
Windows will then attempt to install the drivers. The Traka Drivers are a modified version of driver source supplied by the USB interface IC vendor. The modification is to add a unique product ID for the Traka Handheld Device. This modification voids the Windows Certification of the drivers, and as such the following window will appear. The drivers are safe to install click 'Continue Anyway'.

Windows will then ask you to select the appropriate .sys file. Depending on what processor your PC has affects which .sys file is needed. Click 'Browse'.

Browse to the following location. C:\Program Files\Traka Limited\Traka32\Drivers\Traka Handheld Device

There are two folders within the Traka Handheld Device folder, the first is amd64 and the second is i386. If you PC processor is an amd64 open this folder and select the .sys file. If your PC has anything other than a amd64 processor then select the .sys file within the i386 folder. After selecting the appropriate file you will then be taken back to the 'Files Needed' window above, click 'OK'.

Windows will then install the drivers for the Handheld Device.



At the end of the installation the following Window will be displayed.

NOTE: Windows will then detect the Handheld Device once more and require a second driver installing. Follow the same procedure for the second driver installation.

After completing this procedure the Handheld Device is now installed and ready to use. It will behave as a serial port to the PC so that serial communication can take place between Traka32 and the Handheld Device.

5.13.3 USING THE HANDHELD DEVICE

Powering The Handheld Device

The iFob Transfer Unit application firmware that runs inside the Traka Handheld Device automatically puts the unit into a low power standby mode if there is no user interaction for a preset period of time. The factory default setting for this timeout is 20 seconds.

In the standby state the unit is switched into power save mode turning off the reader and LCD and putting the on-board microcontroller to sleep. To wake the unit, press Function Button 1, the left hand button looking at the front of the unit. The unit will wake from standby and display the following message on the LCD as it boots up:

If during the boot-up sequence the battery level is found to be below the low battery threshold, then the unit will emit a warning tone and the display will show the following message:

If during the boot-up sequence the biometrics reader cannot be initialised then the display will show the following message:

NOTE: The unit will also boot up from sleep mode when a live USB cable is inserted or removed. After the timeout period the device will go back to sleep however the charging status LED will remain lit.

Charging the Handheld Device

The Traka Handheld Device can be charged through a standard USB port. It may also be charged using in-car USB accessory leads or mains-to-USB power supply devices (supplied).

NOTE: The unit cannot be charged from passive USB hubs (i.e. hubs that take their power directly from the bus). Connect either directly to a PC or to hub that uses an external power supply.

The Traka Handheld Device has a standby battery lifetime of 280 hours. The battery life in use will depend on how frequently the unit is operated.

The LED inside Function Button 1 is used to show the battery status. The table below summarises the different LED statuses possible:

LED 1 Status	Description
Off	Charge Suspended
Flashing Green	Pre-Charge Conditioning the Battery
Red	Charging
Green	Charge Complete
Blinking Red	Battery Low

The battery level can be checked by pressing Function Button 2 when on the idle screen of the iFob Transfer Unit application, and when the unit is not connected via USB. On each successive press of Function Button 2 the device will cycle through the information pages – on one of these pages the battery level is shown as follows:

The second line of the display is a bar chart where the battery level remaining is represented by '>' symbols. If the unit is charging then the battery level screen will show:

If the unit is fully charged but connected via USB then the battery level screen will show:

When the battery level reaches the low battery threshold, the user will be prompted with the following message when waking the unit from sleep:

The idle screen of the iFob Transfer Unit Application will have a '*' symbol in the top right hand corner of the display which signifies that the battery level is low:

When the battery gets to the low state the unit should be charged immediately. Eventually the battery will be discharged to the lock-out threshold where the unit is shut down and cannot be woken using Function Button 1. This is to prevent the battery from deep discharging. At this point the unit must be recharged before further use is possible.

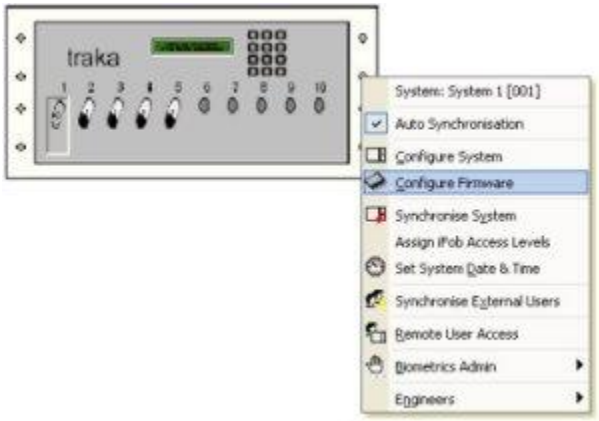
Setting up Traka32

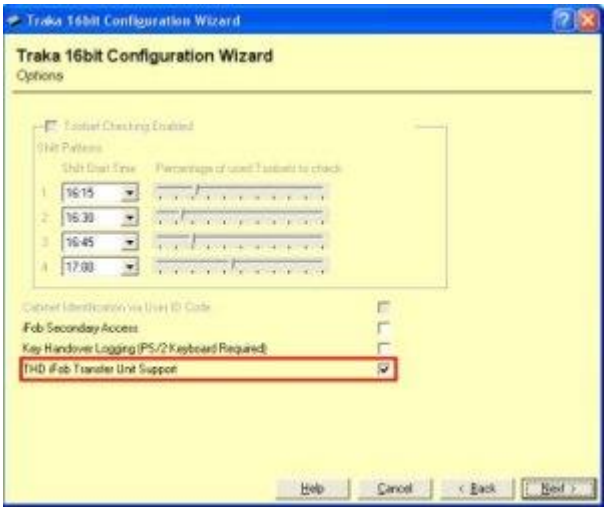
The Traka Handheld Device can be configured through Traka32. The device is set up as if it is any other type of Traka System and therefore has its own System Viewer page.

The cabinet/system that will be used in conjunction with the Handheld Device requires an option to be enabled in the firmware. If you have ordered your Handheld Device along with a Cabinet then this option will be enabled for you, however if you have an existing cabinet you wish to work with the Handheld Device then you need to enable this option manually.

NOTE: The 8bit system does not support the Handheld Device.

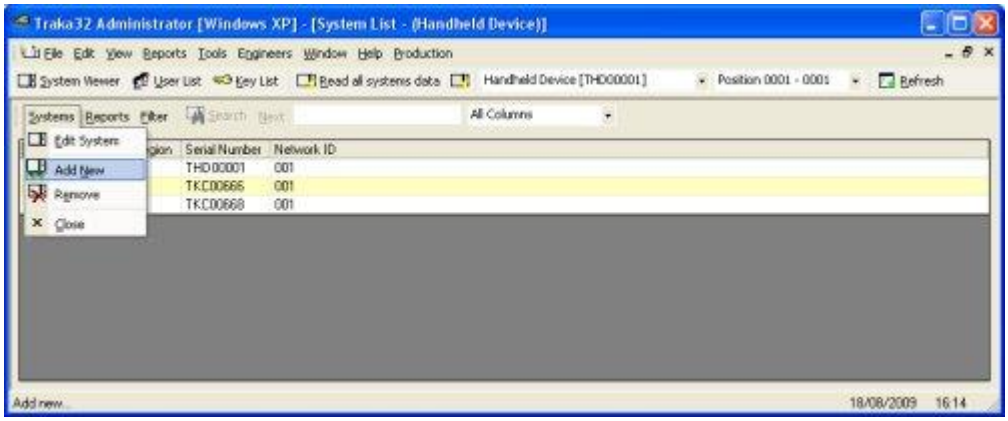
Right click the desired system and select 'Configure Firmware'. Then skip along the option pages until you reach the section which has the 'THD iFob Transfer Unit Support' option. Tick the box then continue and load the configuration file.





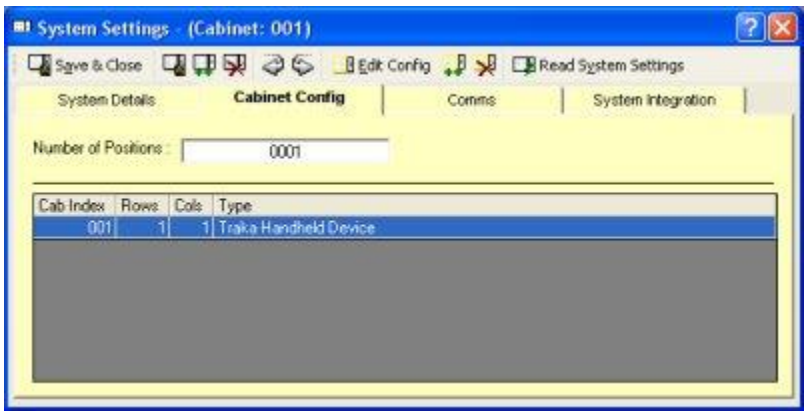
NOTE: Ensure that the Handheld Device is connected to the PC and the USB Drivers are installed before attempting to communicate with the Handheld Device.

The first step to setting up the Handheld Device in Traka32 is to add a new system. From the main menu bar, select 'Tools' then 'Configure Systems'. From the Configure Systems window, select 'Systems' then 'Add New'.

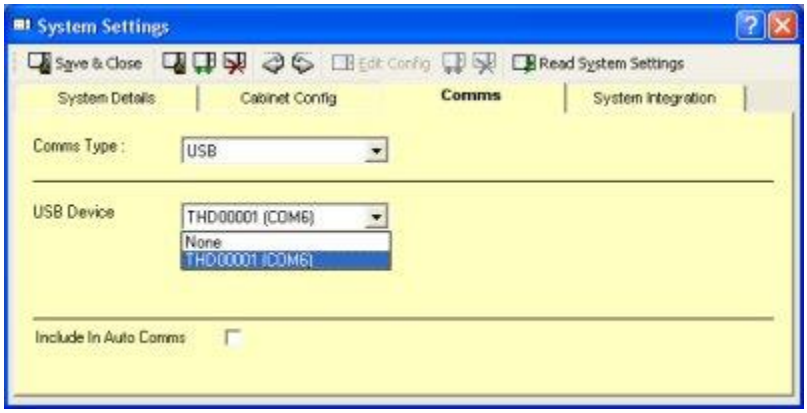


The 'System Settings' window will then appear. Enter the desired system title – i.e. Handheld Device. Select the date format required from the date format drop down box. Select THD (Traka Handheld Device) from the Control Version drop down box.

Next select the 'Cabinet Config' tab. Double click on the Cab Index 001 row in the cabinet setup table and you will be confronted by the cabinet Configuration window. Select 'Traka Handheld Device' from the 'Cabinet Style menu'.



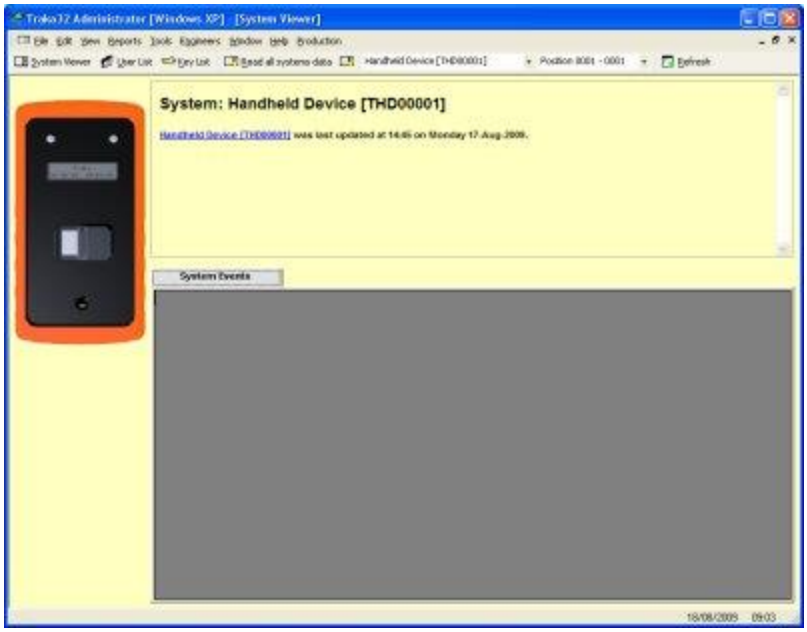
Next select the Comms tab to set up the USB interface. Change the 'Comms Type' box to USB and ensure that the Handheld Device is plugged in to the USB port. The 'USB Device' drop-down box is automatically filled with all of the available Traka Handheld Devices. These are listed by their unique Traka Serial Number. Select the Handheld Device that this system is to be set up for. Then click 'Save and Close'. The unit is now connected and configured for use with Traka32.

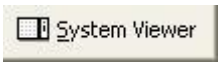


NOTE: When the Traka Handheld Device is connected to a USB port the Serial Number will be displayed on the screen for two seconds. This is to aid identification of the unit for when determining which device is to be selected in Traka32.

System Viewer

The system viewer image for the Handheld Device iFob Transfer Unit is as follows.



This can be viewed by clicking the 

button in the Traka32 toolbar, then select the Handheld Device from the drop-down system box:

NOTE: Each Handheld Device will have its own system viewer page. Ensure you have selected the device that you have connected and wish to communicate with, using the serial number as a reference. This is displayed on the device when first connected.

Right clicking on the image of the device will bring up a context menu with a number of options for setting up and configuring the Handheld Device. First you will need to Set Date and Time. Then hover over the Biometrics Admin tab and select 'Restore Biometrics' to upload all the user fingerprint templates from the database into the Handheld Device.

Below is a description of every selectable command from the context menu

Auto Synchronisation

Select - this option to automatically keep the software and hardware synchronised whenever a change is made in the software to User, iFob or Key details.

Clear - this option if you wish to make changes to the database without synchronisation with the Traka system. This is useful if you have a large number of changes to make or if you are setting up a new database without the Traka System.

This option applies to All Systems and is selected by default whenever Traka32 is loaded.

Configure Systems

Selecting 'Configure System' will open the System Settings window which allows you to change certain settings of the device such as...

- System Name
- Date and Time Format
- Cabinet/System Type
- Communication Settings

Set Date & Time

Selecting this option opens the Date & Time window. From this window you can set the Date & Time of your Device / System by clicking the 'Set Date & Time' button. By clicking the 'Read' button you can obtain the devices current date & time.

Biometrics Admin

This tab breaks down into two options:

1. Reset Biometrics - This command communicates with the Biometrics reader on the Handheld Device and clears out all user templates from the database

2. Restore Templates - This command sends all the user fingerprint templates in the database to the Handheld Device.

Engineers

This tab breaks down into three options:

1. Reset System - This command is not yet supported for the Handheld device.

2. Check Version - This command allows Traka32 to communicate to the device and read back its current firmware version.

3. Check Serial Number - This command allows Traka32 to communicate to the device and read back its Serial Number.

User Process

All users who will be using the Handheld device need to have their fingerprint enrolled and synchronised to the Handheld Device. For more information on how to enroll a user with the Sagem Biometrics reader please refer to the 16bit Sagem Fingerprint section of the user guide. Also the user must have an access level of some kind in order to use the Handheld Device for more information please refer to the User Details section of the user guide.

User A removes a set of keys from a Traka Key Cabinet. The cabinet logs events to record that User A has taken the keys and when they were taken.

User A carries out some function using the keys removed from the cabinet.

User A wishes to hand the keys over to *User B* who will then accept the responsibility for their ownership at some remote location away from the Key Cabinet. This transfer of ownership must be recorded so that reports can be generated to track all key movements.

User B has a Traka Handheld Device running the iFob Transfer Unit Application. The unit is woken up by pressing Function Button 1 and the idle screen is displayed...

User B inserts the iFob into the receptor socket on the Handheld Device. The validity of the iFob is then checked. If the iFob is found to be a valid type then the next step is for User B to identify himself using the biometrics reader. The display will show...

The reader will light up red to show that a request has been made to identify a finger print. User B then places their finger onto the reader. If the fingerprint exists in the database then the display will show...

If User B is identified by the fingerprint reader then the unit will attempt to write his unique user ID and the date and time to the iFob. The display will show...

If the transfer details are successfully written into the iFob then the transfer has completed successfully. The display will show...

The LED in Function Button 2 will turn green to show that the transfer has completed successfully. User B is now responsible for the iFob. When User B has finished with the iFob they return it to the Traka Key Cabinet. The cabinet reads the transfer information from the iFob and generates the necessary events.

NOTE: An iFob can only be transferred once using the iFob Transfer Unit after which it must be returned to a Traka Key Cabinet.

The following iFob events are logged by the Traka Key Cabinet to show this transfer process taking place:

Event	Related	User(s) Description
iFob Removed	User A	Taking key from cabinet
iFob Returned	User A	iFob Transfer Unit Used
iFob Removed	User B	iFob Transfer Unit Used
Transfer iFob Ownership	User A to User B	iFob Transfer Unit Used
iFob Returned	User B	iFob returned to cabinet

NOTE: Any iFob returned event to the cabinet will always be against the user that logged in to put the iFob back. Technically if User B hands the iFob to another user then the final iFob returned event will be against that user.

NOTE: The iFob must remain in the unit until the transfer is complete.

NOTE: The transfer can only be deemed complete when the LED of Function Button 2 lights green and the display shows that the transfer has been completed. If the LED is red then the transfer has failed.

Handheld Device Information Pages

Each press of Function Button 2 from the idle screen of the iFob Transfer Unit application scrolls through the Device Information Pages. These are displayed in the following order...

Firmware Version and Date:

This page shows the version of firmware running in the Handheld Device and the date on which it was released. This information is useful for determining whether a firmware upgrade is available to support new features.

Battery Level:

This page shows the current battery level or power status if connected via USB. See Section 5 for more details.

Serial Number:

This page shows the unique Traka Serial number given to the product. The Handheld Device serial number format consists of three letters and five digits. THD stands for Traka Handheld Device.

Pressing Function Button 2 for the forth time will take you back to the main display.

5.13.4 TRAKA HANDHELD DEVICE TROUBLESHOOTING

When using the Traka Handheld Device you could encounter some common errors or problems, the list below highlights these problems and references the cause.

LCD Error Message	Cause Of Error
	If the Handheld Device does not power up when pressing the 'F1' button then this means the battery is flat and needs to be charged immediately.
	This message will appear if a user has inserted a faulty iFob.
	This message will appear if the iFob that has been inserted is not a Blue or Yellow Traka iFob (i.e. Traka Black iFob or Clock iFob).
 	If the iFob is formatted for another application, i.e. for a Traka Immobilisor function, then the display will cycle between these messages until the iFob is removed. The 'X' will be replaced with the error code or, for more common errors, a text description of the problem.
 	If the iFob has already been transferred from another user, then the display will cycle between these messages until the iFob is removed.
 	If the iFob is found to be a valid type then the next step is for the user to identify themselves using the biometrics reader. The display will show 'Place Finger On Reader'. The reader will light up red to show that a request has been made to identify a finger print. If at this stage there is a problem with the biometrics reader, the display will show 'Reader Error X'. The 'X' will be replaced with the reader error code or, for more common errors, a text description of the problem. The unit will keep retrying to communicate with the biometrics reader for as long as the iFob is left in the unit. If this message persists then contact Traka Technical support quoting the error code or description.
	This message will appear if the user fails to present their finger to the reader before the finger acquisition timeout (default 10 seconds).
	This message will appear is the presented finger is not recognised in the Handheld Device.

	When attempting a transfer, if the iFob is left in the unit then it will automatically retry to acquire a finger print from the user who is accepting the iFob transfer. After three attempts the display will show this message. To attempt the transfer again the iFob should be removed re-inserted into the unit.
	When attempting a transfer, if User is identified by the fingerprint reader then the unit will attempt to write their unique user ID and the date and time to the iFob. If the transfer details are not written successfully to the iFob then the display will show this message.

5.14 TSSI BIOMETRICS READER

5.14.1 TSSI BIOMETRICS OVERVIEW

The Biometrics Reader is used to verify a user identity based upon a 4 digit PIN.

The fingerprint reader is an add-on system to Traka and holds information about the PIN and Fingerprint separately to Traka.

NOTE: When installing, position the cabinet so that users can stand in a comfortable and natural position. Do not position in direct sunlight.

5.14.2 TSSI BIOMETRICS ENROLMENT

To enrol a user on the biometrics readers...

1. Using Traka32, configure a user with a 4 digit Primary PIN.

   Please refer to the User Details section for more details.

2. Using the keypad on the Traka system, press **#** and enter the Primary Personal Identification Number (PIN) followed by **#**.

3. Follow the on screen instructions.

   NOTE: It is very important that you place your finger on the reader in the same location and in the same manner each time, otherwise verification will be difficult. Here are some tips on how to achieve the best enrolment score...

   - Stand in a comfortable & natural position
   - Grab the reader with your hand and do not let go
   - Rock your finger onto the reader
   - When prompted to remove your finger, rock your finger back but do NOT let go of the reader
   - When promoted to place your finger, rock your finger forward onto the reader head again

4. Once completed you will be shown an enrolment score.

   NOTE: If the score is below 8/10 we recommend you remove the user's template and re-enrol. Please refer to the User Details section for more details on removing the user template.

5. If you are having problem with the enrolment, please refer to the tips & tricks section.

Prompt for Security Level when Enrolling

'Prompt for Security Level when Enrolling' is an optional firmware feature for the TSSI Biometrics reader that allows you to choose the security level you wish to enrol at. When the 'Prompt for Security Level when Enrolling' option is enabled, a user with a 4 digit Primary PIN (please refer to the User Details section for more details) who attempts to access the cabinet will be confronted by the following message on the LCD...

Security Levels 1-5

There are five security levels to choose from, the security levels get increasingly harder to enrol with as the numbers ascend (number 1 being the easiest and number 5 being the hardest), however if you enrol with a high security level you are heightening the sensitivity of the reader, this will ensure you get a good quality template. You have to be very accurate with your finger placement when enrolling with a higher security level.

Pin Only

This option is available at the LCD when enrolling and is also configurable as a 'Global Security Level' (see below). When this option is selected and a user enrols with their PIN, they become a 'PIN only' user and they wont be prompted to use place their finger on the reader. To allow the user to use Fingerprint entry again, you will have to reset that particular users fingerprint template in their User Details and enrol again.

Global Security Level

The Global Security Level is effectively a 'shared' security level that is the same for every user who enrols with it. If you configure the global security level to 3 for example, then any user who enrols using the Global Security Level option is enrolling at security level 3. Also all users who enrol using the Global Security Level are affected if it changes, for example, if several users are enrolled with the global Security Level which is 1 and that gets changed to 5, all the those users security levels will change to 5 immediately. The Global Security Level can be configured for any of the five security levels, or there are other options such as 'PIN Only' & 'Any Fingerprint'.

NOTE: If the 'Prompt for Security Level when Enrolling' option is not enabled, every user will be automatically forced to enrol with the default Global Security Level.

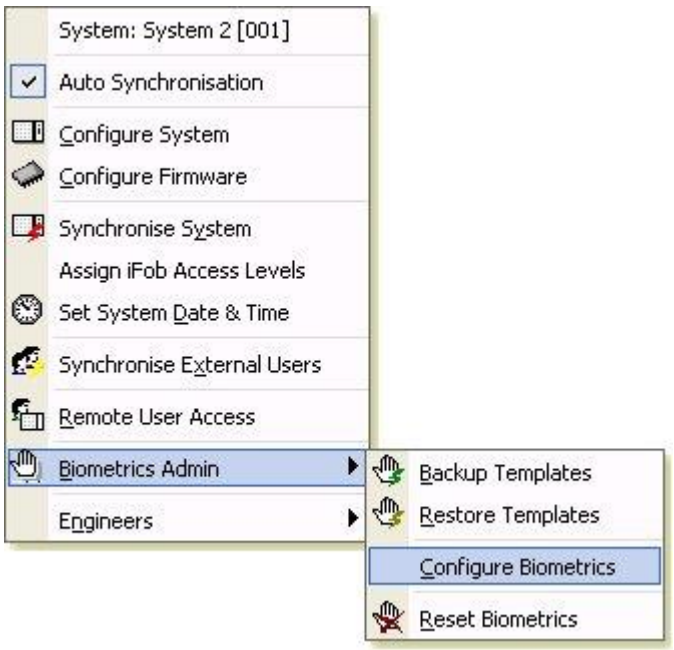
Pin Only

As mentioned above this option is available at the LCD as well as the Global Security Level. When this option is selected and a user enrols with their PIN, they become a 'PIN only' user and they wont be prompted to use place their finger on the reader. To allow the user to use Fingerprint entry again, you will have to reset that particular users fingerprint template in their User Details and enrol again.

Any Fingerprint

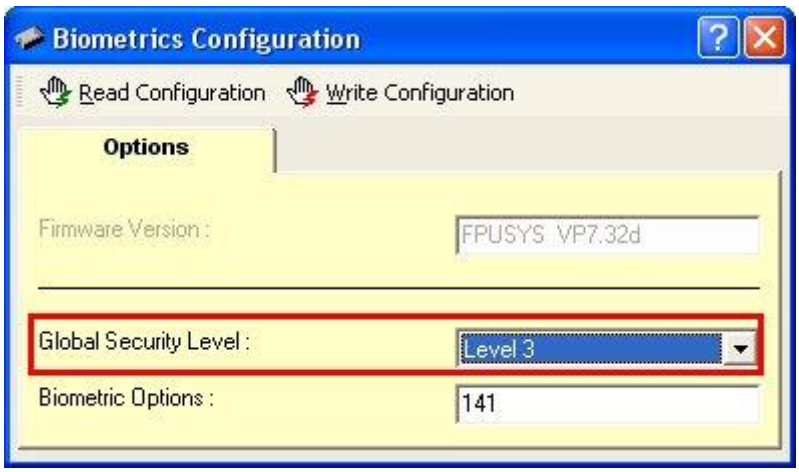
This option is only available as a Global Security Level and allows any users fingerprint to access the system, assuming their PIN number is correct and they have sufficient access to the system. This option is in fact a 'dummy' option used for sites that wish to have the illusion of a fingerprint reader.

To configure the Global Security Level, right click the cabinet/system from the 'System Viewer', scroll down to Biometrics Admin, then select 'Configure Biometrics'.



The Biometrics Configuration window will appear allowing you to change the Global Security Level as desired.

NOTE: the Biometric Options section is always set to number 141 by default, this should NOT be changed unless advised otherwise.



As of firmware versions v6.07.58 (8bit) and v2.00.40 (16bit) upwards, when you backup the reader templates via Traka32 the users security level will be saved along with their individual fingerprint template.

5.14.3 TSSI BIOMETRICS VERIFICATION

To verify a user with the biometrics readers...

1. Using Traka32, configure a user with a 4 digit Primary PIN.

   Please refer to the User Details section for more details.

2. Using the keypad on the Traka system, press **#** and enter the Primary Personal Identification Number (PIN) followed by **#**.

3. Follow the on screen instructions.

   NOTE: It is very important that you place your finger on the reader in the same location and in the same manner as when you enrolled, otherwise verification will be difficult.

4. If you are having problem with the verification, please refer to the tips & tricks section.

5.14.4 TSSI BIOMETRICS READER TIP & TRICKS

If you having problems when enrolling users or with verification then please try the following...

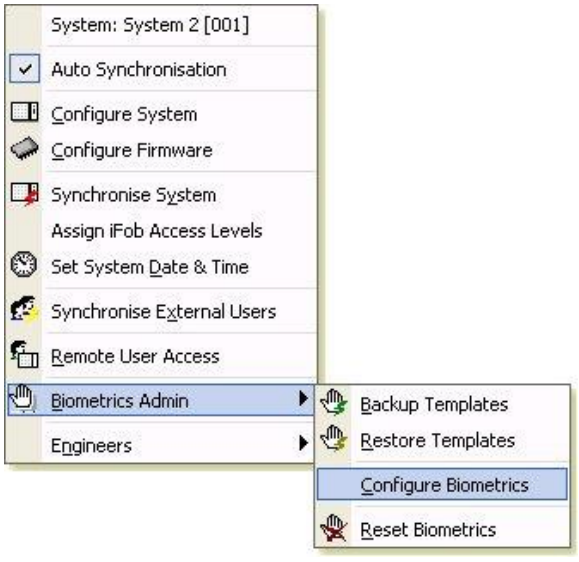
- When enrolling do NOT rush
- Always place your finger in the same location
- Grab the reader with your hand and do not let go
- Rock your finger onto the reader

- Make sure you get at least an 8 out of 10 score when enrolling
- Having dry, wet or very clean fingers can make a difference

  Try wiping your finger on your forehead before enrolling or verifying. This may sound silly but this will put a thin layer of grease on your finger making it much easier for the biometrics reader to read your fingerprint template.

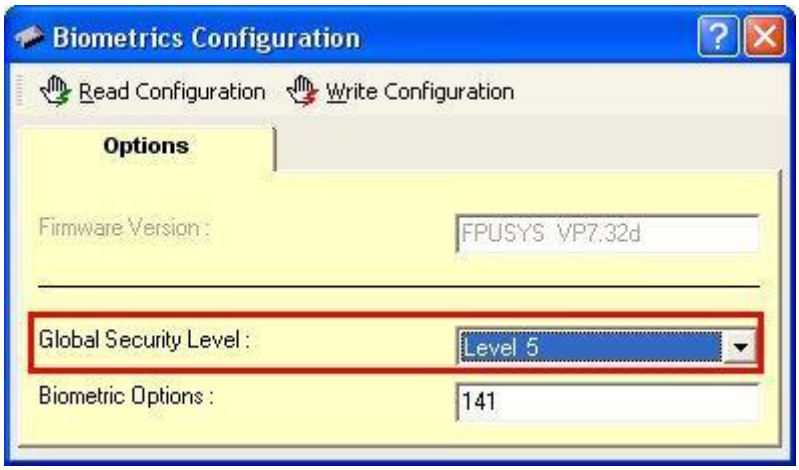
- When enrolling increase the sensitivity. This will ensure you get a good quality template.

To customise the sensitivity Level, right click the cabinet in your 'System Viewer' , scroll down to Biometrics Admin, then select 'Configure Biometrics'.

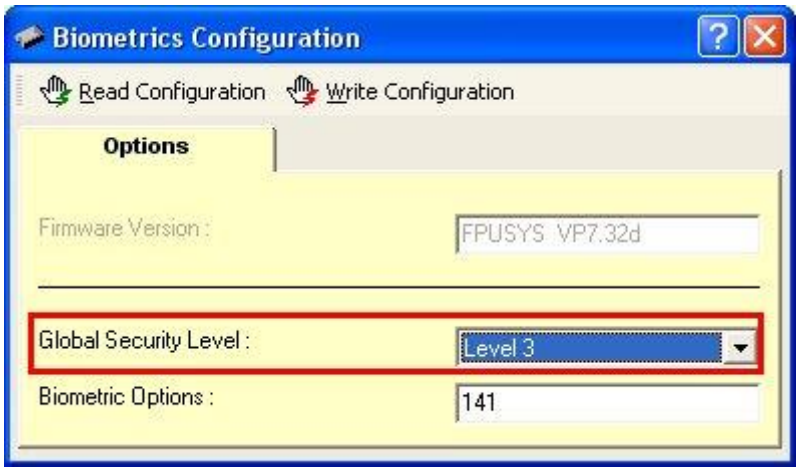


The Biometrics Configuration window will appear allowing you to change the Global Security Level as desired.

NOTE: the Biometric Options section is always set to number 141 by default, this should NOT be changed unless advised otherwise.



When enrolment is complete, reduce the sensitivity. This will make the biometrics reader less fussy about finger placement.

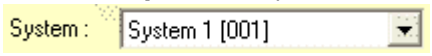


5.14.5 TSSI BIOMETRICS - RESET TEMPLATE

If you have a user enrolled on the biometrics reader and you would like to re-enrol them, simply reset their template and let the user enrol again.

NOTE: When deleting a user, the record is deleted from Traka but NOT from the biometrics reader automatically.

1. From the main screen click on 

and a list of the current users will be shown.
2. From the user list simply **double click** on the user record you wish to edit or select the record and click on the **Users** menu followed by **Edit User**.
3. Click on the **System Details** tab.
4. **Select the system** that you wish to remove the template from using the 

drop down menu.
5. Click on the  toolbar button.
6. Repeat steps 4 and 5 for each system that you wish to reset the template on.

5.14.6 TSSI BIOMETRICS - BACKING UP THE TEMPLATES

When you are have a number of users enrolled on the fingerprint reader it is strongly recommended that a backup of the templates is done as this is not done automatically.

To back up the templates **right click over the picture of the system** and click on **Biometrics Admin**, **Backup Templates**. This will backup all the enrolled templates to the database.

5.15 GSM MODULE

5.15.1 GSM MODULE OVERVIEW

With the increasing need to administer Traka Cabinet remotely, Traka has decided to take a step forward and implement a simple text message service directly with the Traka Cabinets.

Traka has sourced a low cost Sony Ericsson GSM Module to integrate directly with the Traka Cabinet to allow...

- Remote iFob Release
- Get Event Information from the Traka Cabinet when specific iFobs are taken or returned or certain alarms occur.

5.15.2 CONFIGURING THE GSM MODULE

Before using the GM28 or GM29 module, the module will need configuring using Traka32 and a standard serial cable.

NOTE: If the unit was supplied by Traka, this configuration will already have been done at the factory.

1. Insert a SIM Card into the SIM Holder on the Sony Ericsson GM28 or GM29 module.
2. Connect a standard serial cable from the 9 PIN D-Sub on the Sony Ericsson GM28 or GM29 module to a spare serial port on a PC with Traka32 installed.
3. Connect the Power connector of the Sony Ericsson GM28 or GM29 module to a Traka Control PCB and power up the unit.
4. Load Traka32 (use the 'Traka Engineer' login if required)
5. Click on ***Engineers***, ***Diagnostics*** and the diagnostics window will open.
6. Click on the ***Serial Tab***.
7. Set the ***Serial Port Number*** as required.
8. Set the serial port settings to ***9600,N,8,1***.
9. Click on the ***Traka*** toolbar menu item to toggle it to ***Dumb***.
10. Click on the ***Clear*** toolbar menu item to clear the main screen.
11. Click on ***Connect***.
12. From the main screen type the following...
    a. Type **at+ifc=0,0** followed by **Enter** and you should see **OK** appear.
    b. Type **at+ipr=19200** followed by **Enter** and you should see **OK** appear on the next line.
13. Click on ***Disconnect***.
14. Set the serial port settings to ***19200,N,8,1***.
15. Click on the ***Clear*** toolbar menu item to clear the main screen.
16. Click on ***Connect***.
17. From the main screen type the following...
    a. Type **at+cpin="1234"** followed by **Enter** and you should see **OK** appear.

       NOTE: '1234' is the SIM Card's PIN.
    b. Type **at+cgsms=3** followed by **Enter** and you should see **OK** appear.
    c. Type **at+cmgf=1** followed by **Enter** and you should see **OK** appear.
    d. Type **at+csdh=1** followed by **Enter** and you should see **OK** appear.
    e. Type **at+csdh=1** followed by **Enter** and you should see **OK** appear.
    f. Type **at+csmp=17,167,0,0** followed by **Enter** and you should see **OK** appear.
    g. Type **at+cnmi=3,2,2,1** followed by **Enter** and you should see **OK** appear.
    h. Type **at&w** followed by **Enter** and you should see **OK** appear.
18. Click on ***Disconnect***.
19. Close the ***Diagnostics*** window.

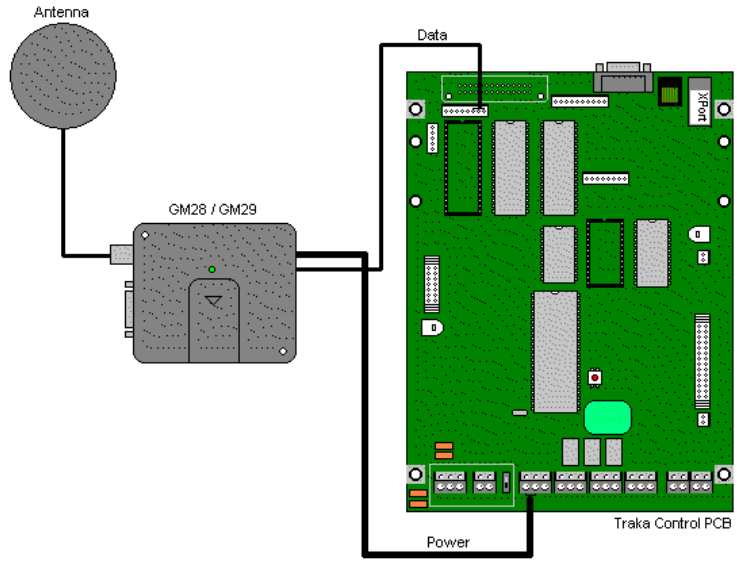
5.15.3 INSTALLING THE GSM MODULE

Connecting to Traka

Connect the Sony Ericsson GM28 or GM29 module as follows:

1. Connect the Power Cable to the Power Output connect of the Traka Control PCB.
2. Connect the Communications Cable to the UARTB connector of the Traka Control PCB.

   NOTE: The communications will not work if the UARTB is connected and a Serial Cable is connected to the 9 Pin D-Sub of the Sony Ericsson GM28 or GM29 module at the same time.



NOTE: To integrate the Sony Ericsson GM28 or GM29 module with the Traka Control PCB v2.30.04, the following modifications are required:

- Add a wire link between Pin 21 of U15 (DUART) and Pin 16 of U1 (Processor)
- Add 10K Ohm resistor to R31

Setup

The Sony Ericsson GM28 or GM29 module will initially need setting up as follows.

To access the GSM Module Setup Menu...

1. Hold down the ***Reset*** button on the Control PCB and the ***5*** key on the Keypad.
2. Release the ***Reset*** button and the following menu will appear.

NOTE: When installing a GSM Module, enter the SIM PIN first (menu item 3, if required), then enter the phone number (menu item 4) and then check the signal strength (menu item 2).

3:PIN

If the SIM Card used in the Sony Ericsson GM28 or GM29 module requires a PIN, press the 3 key on the Keypad.

Enter the 4 digit SIM PIN followed by the # key. If the PIN is accepted, OK will be displayed on the LCD. If the PIN is rejected, ERROR will be displayed on the LCD.

NOTE: If a PIN is required and is not entered, the Sony Ericsson GM28 or GM29 module will not operate.

NOTE: After entering the PIN please wait 5 to 10 seconds before continuing as the module takes a few seconds to talk to the SIM card.

4:Num

When the Traka Cabinet needs to send a message it will do so to the number stored in the first location of the SIM Card's phonebook.

To edit the phonebook entry, press the 4 key on the Keypad.

Enter the up to a 20 digit phone number followed by the # key. If the number is accepted, OK will be displayed on the LCD. If the PIN is rejected, ERROR will be displayed on the LCD.

By holding the 0 key for more than 1 second a + symbol can be entered. This is for international number formats.

For example +441234712345

2: SIG

To check the strength of the signal, press the 2 key on the Keypad. The signal strength will be displayed as +CSQ: 9,99

The first number represents the signal strength in dBm:

00 = -113 dBm, (Weakest)
01 = -111 dBm,
and so on... (Each increment up to 31 subtracts 2 dBm)
30 = - 53 dBm,
31 = - 51 dBm. (Strongest)
99 = Unknown

The second digit represents the channel bit error rate. This is usually 99 when there is a signal. When the module cannot get a lock a value less than 99 will be shown.

Press # to exit the signal check loop.

1:PWR

To power down the Sony Ericsson GM28 or GM29 module press the 1 key on the Keypad. This safely disconnects the module from the Mobile Phone Network.

Operating States / LED

The GSM Module has a green LED, which is used to indicate various operating states. These states are described in the following table:

Operating State	LED Status
After switching on the GSM Module	On after 4 seconds
Switch off (Power down) or power removed	Off
Standby or talk	Flashing
No network, network search, no SIM card, no PIN entered	On

5.15.4 REMOTE IFOB RELEASE VIA SMS

It is possible to remotely release an iFob by sending an SMS Text Message to the Traka Cabinet via the GSM Module as follows:

1. Text the following message to the Traka Cabinet

   GET<Number of iFob e.g. 10>

   For example **GET10**

2. Traka should respond after a short delay and ask you to open the door.
3. Open the door and Traka should ask you to remove the selected iFob E.g. 10.
4. Traka should send a text message back to the predefined phone number if the iFob was taken

   Message from Traka
   (TKC10123)

   iFob Taken: 10

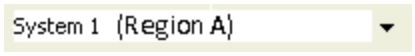
NOTE: The SMS messages will be sent to the phone number that was entered via the setup menu on the Traka Cabinet.

5.15.5 EVENT INFORMATION VIA SMS

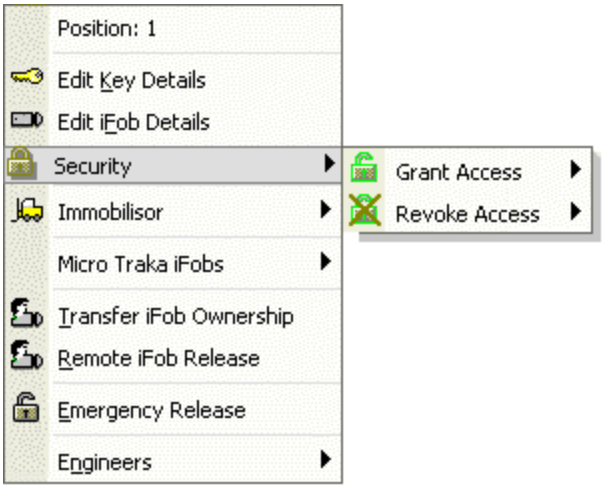
It is possible to get Event Information from the Traka Cabinet when specific iFobs are taken or returned or certain alarms occur. The SMS messages will be sent to the phone number that was entered via the setup menu on the Traka Cabinet.

iFobs Taken or Returned

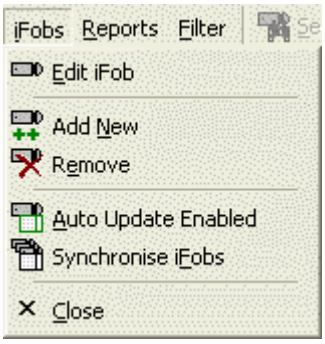
The Traka Cabinet must be configured in order to send SMS Text Messages when specific iFobs are taken or returned.

1. The quickest way to add a new iFob into a system is from the **System Viewer**.
2. From the main screen select the system 

and from the system viewer right click over the picture of the relevant position and click on **Edit iFob Details**.

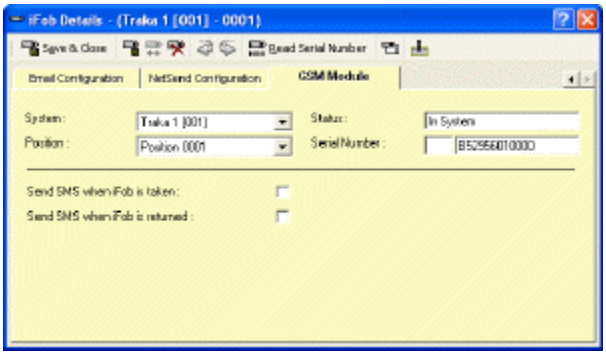


NOTE: You can also access the iFob Details from the iFob List. Click on View, iFob List from the main menu and the iFob List will open. From the iFob list simply double click on the iFob record you wish to edit or click on the iFobs menu followed by Edit iFob.



3. The selected iFob record will open.

4. Click on the **GSM Module** tab.



5. Select the **Send SMS when iFob is taken** option to allow the Traka Cabinet to send a SMS each time the selected iFob is taken from the Cabinet.

6. Select the **Send SMS when iFob is returned** option to allow the Traka Cabinet to send a SMS each time the selected iFob is returned to the Cabinet.

Alarm Events

The Traka Cabinet will also send SMS Text Messages when certain alarm event occurs.

Only the Alarm Code will be displayed. For details on the Event Codes please refer to the Alarm & Event Types section.

NOTE: The following event / alarm codes are NOT sent by the GSM Module:

10. System Has Been Reset

24. Remote iFob Release via SMS

5.16 ALCOLOCK BREATH TEST

5.16.1 ALCOLOCK OVERVIEW

With the increasing need to ensure business employees are not operating vehicles or machinery whilst under the influence of alcohol, Traka has taken steps to integrate an Alcolock device directly with the Traka cabinets.

The Alcolock integration provides the following features:

- The system can be configured to prompt for a breath test when removing and/or returning an iFob.
- A User to be prevented from taking an iFob if they are over a pre-determined alcohol limit or fail to take an adequate sample.
- The breath test result to be recorded in the Traka database.
- A User who has not passed the breath test to be prevented from taking any further iFobs requiring a breath test until a supervisor has reset their user profile in the Traka32 software.
- Random breath testing where the percentage chance per user can be selected from 0 – 100%.

Traka is currently working with different companies to provide an Alcolock solution that is suitable for a wide variety of different markets.

For more information please view the following sections:

Alcolock System Configuration

Alcolock Operation

Alcolock Calibration Requirements

5.16.2 ALCOLOCK SYSTEM CONFIGURATION

The Alcolock device is supported by 8bit cabinet firmware **version 6.07.47** and later. This is a cost option that is compiled upon request only. The minimum required Traka32 version is **02.006.005**. Please inform Traka if you require a firmware or software upgrade.

iFob Setup

Breath Test on iFob Removal

This option forces a user to provide a breath sample when removing an iFob from the system to ensure they have not consumed any alcohol before they operate machinery or drive a vehicle.

1. Setup any **iFobs** that are required to have **Prompt for Breath Test on Removal**:

   The requirement for a breath test is configured on a per iFob basis allowing non-vehicle or machinery related iFobs to be taken without requiring a breath test.

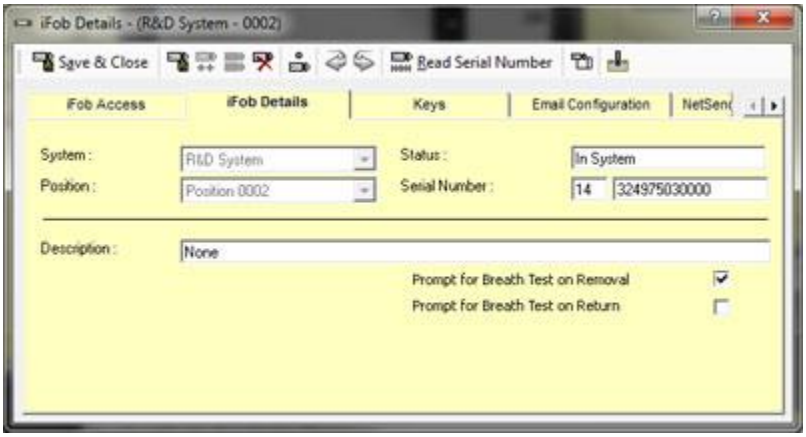
   From the Traka 32 System Viewer for the selected system:

   a. **Right click** over a selected **iFob** that requires a breath test.

   b. Select **Edit iFob Details** from the drop down menu.

   c. Select the iFob Details tab.

   d. Tick **Prompt for Breath Test on Removal** to enable.



NOTE: If you can't see 'Prompt for Breath Test on Removal', it is because the selected Traka system does not have it enabled in the firmware. Please consult Traka for an upgrade.

Breath Test on iFob Return

This option forces a user to provide a breath sample when returning an iFob to the system. This ensures that the user has not been under the influence of alcohol whilst the keys have been out of the system.

1. Setup any **iFobs** that are required to have **Prompt for Breath Test on Return**:

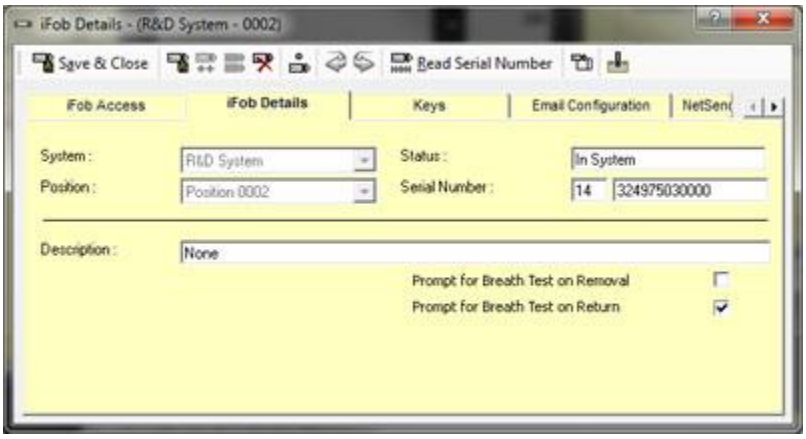
   The requirement for a breath test is configured on a per iFob basis allowing non-vehicle or machinery related iFobs to be taken without requiring a breath test.

   From the Traka 32 System Viewer for the selected system:**Right click** over a selected **iFob** that requires a breath test.

   a. Select **Edit iFob Details** from the drop down menu.

b. Select the iFob Details tab.

c. Tick **Prompt for Breath Test on Return** to enable.



NOTE: If you can't see Prompt for Breath Test on Return, it is because the selected Traka system does not have it enabled in the firmware. Please consult Traka for an upgrade.

System Configuration

Select the **Alcolock Testing Rate** of the system:

The Alcolock Testing Rate is the percentage chance per user that the system will prompt for a breath test upon selecting any iFob that has Prompt for Breath Test enabled. This can be set from 0 to 100% in 10% increments where:

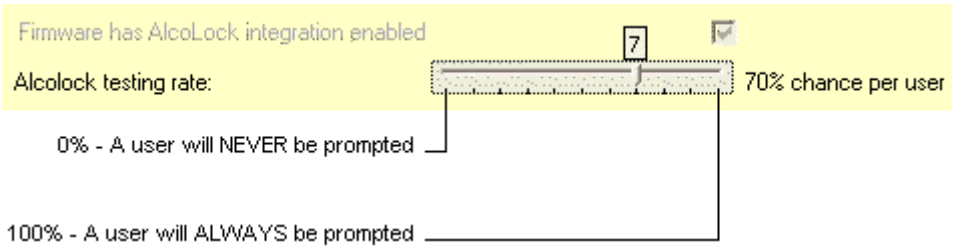
0% means the user will **never** be prompted for a breath test.
...
...
...
...
100% means the user will **always** be prompted for a breath test.

1. From the Traka 32 System Viewer for the selected system:

   a. Right Click over the keypad and select Configure Firmware to display the System Configuration window.

   b. Click the button to scroll along the tabs and select the **Options 4** tab.

   c. Set the **Alcolock Testing rate ba**r to the percentage required.



2. Setup any users who require a **Mandatory Breath Test**:

   You may wish for certain users to ALWAYS have to take a breath test regardless of the Alcolock Testing Rate.

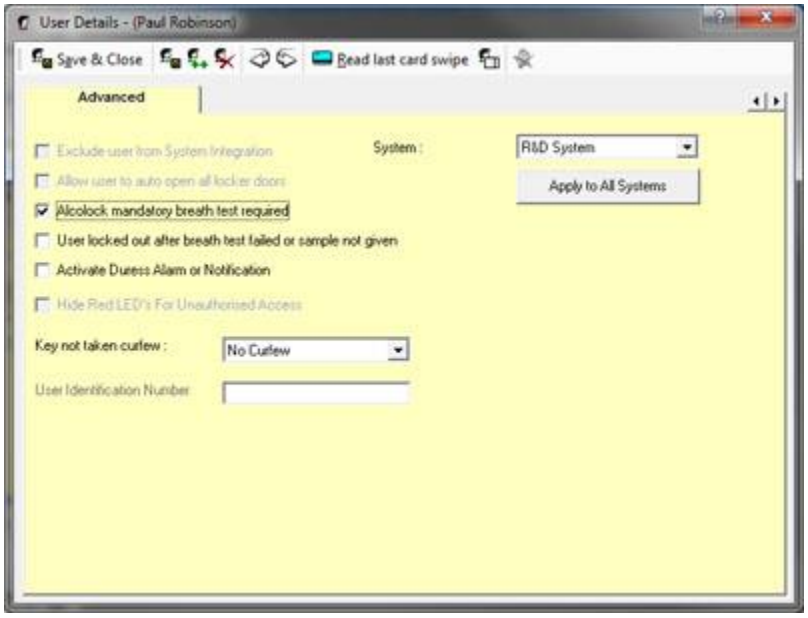
   From the Traka 32 System Viewer for the selected system:

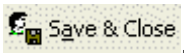
a. Click on User List.

b. Select and open a **User** who should be required to take a mandatory breath test.

c. Click the  button to scroll along the tabs and select the **Advanced** tab.

d. Tick **Alcolock mandatory breath test required** to enable.



e. Click 

.

For more information please view the following sections:

Alcolock Operation

Alcolock Calibration Requirements

5.16.3 ALCOLOCK OPERATION

NOTE: Please refer to the section on Alcolock System Configuration prior to using the Alcolock on the Traka system.

The following section describes how to use the Alcolock device and what happens if a User fails a breath test or does not provide an adequate sample.

Breath Test on iFob Removal

1. **Taking a Breath Test:**

    a. **Authorise** yourself to the Traka system using your card, pin or fingerprint in the usual way.

    b. **Select** an iFob that has been configured to Prompt for a Breath Test.

    If the system requests the User must takes a breath test the LCD will display:

    c. **Lift the Alcolock** and follow the instructions as indicated on the Alcolock device display. In general, all models will inform you to insert the mouthpiece as required and blow continuously into the mouthpiece for approximately 5 seconds.

    NOTE: Depending upon the type of device used, the sampling time period and method may vary slightly.

    NOTE: It can take a little practice to achieve a successful sample at first! If the device informs the user to take a further sample please don't panic, try to relax and re-take the sample as instructed.

    HINT: For the 'Alcometer 500' device, tail off your breath naturally after aprox 5 seconds to achieve a successful sample every time.

    d. Once the sample has been taken the LCD on the Traka system will show one of the following:

    - The breath sample is below the BAC limit set in the device, the user may **remove** the selected iFob.

    - The breath sample is above the BAC limit set in the device, the selected iFob will NOT be released to the user. Do **not** attempt to remove the iFob.

    - 20 seconds has passed and the user has either **Failed to Provide an Adequate Sample** *or* **Not Provided a Sample at all.**

2. **User Lockout – if a User has failed the Breath Test!**

If a User fails the breath test or does not provide an adequate sample the User is "locked out". This means that if a user attempts to remove another iFob that requires a breath test it will not be released to them and the LCD will show:

NOTE: It is important to note the user will still be able to remove another iFob that has the Prompt For Breath Test parameter set without having to give another breath test.

The user must be "unlocked" from within the Traka 32 software. From the Traka 32 System Viewer for the selected system:

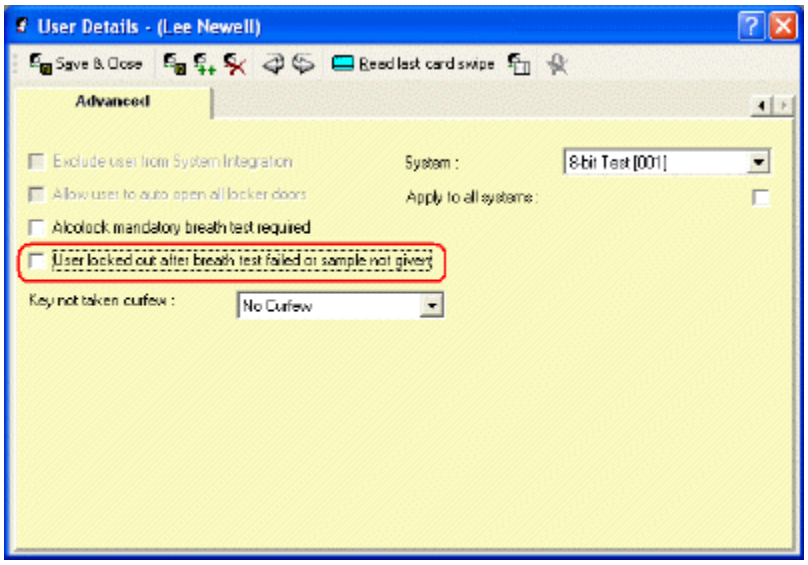
a. Click  **Read All System Data** to ensure the event data has been downloaded from the selected system of which the user has been locked out from.

b. Click on User List.

c. Select and open a **user** who is currently locked out of the system.

d. Click the  button to scroll along the tabs and select the **Advanced** tab.

e. **Uncheck** the "User locked out after breath test failed or sample not given" tick box.



f. Click 

g. The selected system(s) will be updated. The User will now be able to request an iFob with the Prompt for Breath test enabled.

3. **Alcolock Breath Test iFob Events**

The Traka system records 3 iFob events related to the Alcolock system viewable from the Traka 32 software:

- **Breath Test Passed** (code 54)
  Recorded when a user has passed the breath test.

- **Breath Test Failed** (code 55)
  Recorded when a user has failed the breath test.

- **Breath Test Sample Not Given** (code 63)
  Recorded when a user has not provided an adequate sample.

- **Breath Test Sample Not Given** (code 63)
  Recorded when a user has failed to provide any sort of sample. The user will immediately be locked out when they fail to provide a sample.

For details on the all Event Codes please refer to the Alarm & Event Types.

For more information please view the following sections:

Alcolock Calibration Requirements

Breath Test on iFob Return

1. **Taking a Breath Test**:

    a. **Authorise** yourself to the Traka system using your card, pin or fingerprint in the usual way.

    b. **Return** the iFob to the correct position, that has been configured to Prompt for a Breath Test.

    If the system requests the User must takes a breath test the LCD will display:

    c. **Lift the Alcolock** and follow the instructions as indicated on the Alcolock device display. In general, all models will inform you to insert the mouthpiece as required and blow continuously into the mouthpiece for approximately 5 seconds.

    NOTE: Depending upon the type of device used, the sampling time period and method may vary slightly.

    NOTE: It can take a little practice to achieve a successful sample at first! If the device informs the user to take a further sample please don't panic, try to relax and re-take the sample as instructed.

    HINT: For the 'Alcometer 500' device, tail off your breath naturally after aprox 5 seconds to achieve a successful sample every time.

    d. Once the sample has been taken the LCD on the Traka system will show one of the following:

    - The breath sample is below the BAC limit set in the device, the user may close the door and complete the process **or** return another iFob.

    - The breath sample is above the BAC limit set in the device, then a Breath Test Failed event is generated against the iFob.

    - 20 seconds has passed and the user has either **Failed to Provide an Adequate Sample** *or* **Not Provided a Sample at all. If this occurs then a** Breath Test Sample Not Given event is generated.

2. **User Lockout – if a User has failed the Breath Test!**

    If a User fails the breath test or does not provide an adequate sample the User is "locked out". This means that if a user attempts to remove an iFob whilst logged in that requires a breath test it will not be released to them and the LCD will show:

NOTE: It is important to note the user will still be able to return another iFob that has the Prompt For Breath Test parameter set without having to give another breath test whilst the door is open.

The user must be "unlocked" from within the Traka 32 software. From the Traka 32 System Viewer for the selected system:

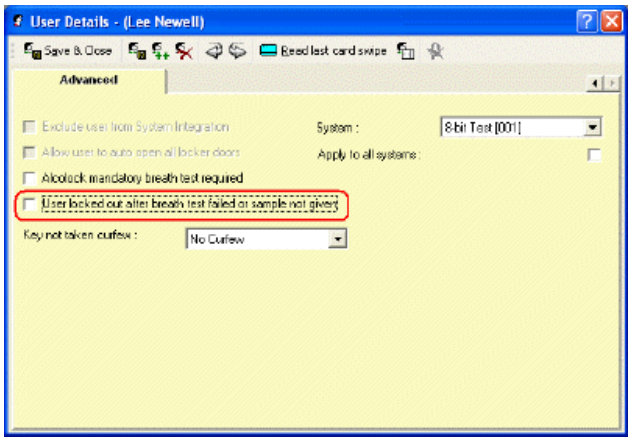
a. Click **Read All System Data** to ensure the event data has been downloaded from the selected system of which the user has been locked out from.

b. Click on User List.

c. Select and open a **user** who is currently locked out of the system.

d. Click the button to scroll along the tabs and select the **Advanced** tab.

e. **Uncheck** the "User locked out after breath test failed or sample not given" tick box.



f. Click Save & Close

g. The selected system(s) will be updated. The User will now be able to request an iFob with the Prompt for Breath test enabled.

3. **Alcolock Breath Test iFob Events**

The Traka system records 3 iFob events related to the Alcolock system viewable from the Traka 32 software:

2.

- **Breath Test Passed** (code 54)
  Recorded when a user has passed the breath test.

- **Breath Test Failed** (code 55)
  Recorded when a user has failed the breath test.

- **Breath Test Sample Not Given** (code 63)
  Recorded when a user has not provided an adequate sample.

- **Breath Test Sample Not Given** (code 63)
  Recorded when a user has failed to provide any sort of sample. The user will immediately be locked out when they fail to provide a sample.

For details on the all Event Codes please refer to the Alarm & Event Types.

For more information please view the following sections:

Alcolock Calibration Requirements

5.16.4 ALCOLOCK CALIBRATION REQUIREMENTS

All Alcolock devices are required to be calibrated every 6 months. Traka can provide the means for this service to be undertaken as part of a Service Contract. The calibration process itself is usually completed using dry gas and takes just a few minutes to complete, however the procedure will vary depending upon the type of Alcolock device being used.

Alcolock Threshold

The Blood Alchohol Content (BAC) threshold level can be set in the Alcolock device to comply with the regulations according to the environment where the system is to be used. An example might be where drivers are monitored to ensure they are not above the legal limit for driving. In the U.K the limit is currently 0.08% BAC which is approximately 2 pints of normal strength beer. However in Sweden the limit is much lower at 0.02% BAC.

5.17 CAN GATEWAY

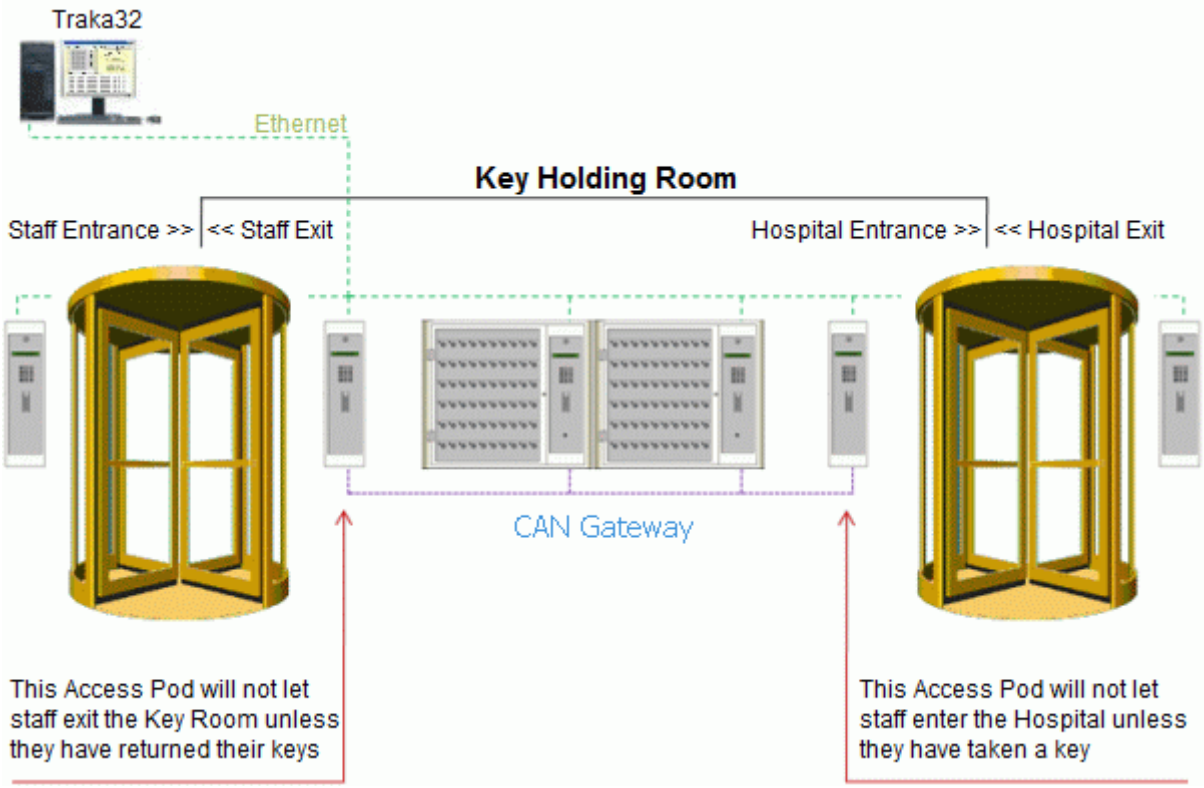
5.17.1 CAN GATEWAY OVERVIEW

CAN Gateway allows Traka Systems (such as Key Cabinets, Locker Systems and Traka Access Control Pods) to be linked together using Controller Area Network (CAN). This "multi-master" protocol enables systems and access pods to communicate instantly with each other without using Traka32.

An example of the need for CAN Gateway is where an Access Pod needs to know if a user is currently holding keys before making a decision as to whether they are allowed to leave a premise or area. One of the main problems organisations face is where a member of staff takes a key off site often by mistake. The cost of this in time and money can be astronomical. CAN Gateway helps solve this problem.

An Access Pod can also be configured such that it only allows a user to enter a premise (e.g. prison) if they have taken a key (or a device from a Locker e.g. a personal attack alarm).

A diagram of a typical application for a hospital follows:-



5.17.2 CAN GATEWAY CONFIGURATION

Firmware Configuration Options

Each system (Key Cabinet and Access Pod) will need *CAN Gateway* to be enabled in the cabinet firmware. Please contact Traka or your distributor for a firmware upgrade or configuration file (16-bit) files as necessary.

You can check to see if your system has the correct firmware options by viewing the system configuration. From the system viewer right click the pod of the selected system, and click Configure Firmware.

Key Cabinet Firmware Options

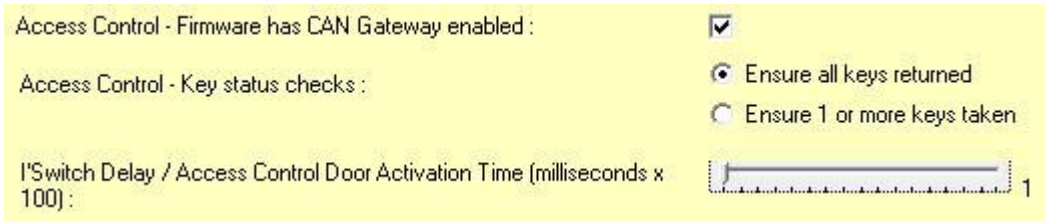
- **Key Cabinet - Firmware has CAN Gateway enabled**

  Required to be ticked for Key Cabinets with CAN Gateway.

- **Enforce iFob Allowance across all cabinets**

  Tick if you wish for the key cabinet to 'ask' the other key cabinets on CAN Gateway how many iFobs the user is currently holding before releasing an iFob. If the users iFob Allowance is exceeded across all cabinets, the iFob will not be released to the user.

Access Pod Firmware Options



- **Access Control - Firmware has CAN Gateway enabled**

  Required to be ticked for Access Pods with CAN Gateway.

- **Access Control - Key status checks**
  - Ensure 1 or more keys taken

    Access pod will check to ensure that 1 or more keys have been taken from any key cabinet before allowing the user access.

  - Ensure all keys returned

    Access pod will check to ensure all keys have been returned to all key cabinets before allowing the user access.

- I'Switch Delay / Access Control Door Activation Time (milliseconds x 100)

  Set the activation period of Alarm Relay ONE. This is used to activate the door or turnstile. It can be configured in 10ths of a second, for example to activate the relay for 5 seconds would require a value of 50. See Control PCB Alarm Outputs for how to connect up the door or turnstile.

Firmware Options Common to Key Cabinets, Lockers and Access Control Pods

- CAN Gateway - Key Cabinet count

  Set the number of key cabinets only (not including access pods) that are on the same CAN Gateway network as the currently selected key cabinet / access pod. For the access pods, this needs to be configured so as it knows how many responses (from each key cabinet) to expect after requesting number of keys held by a user. For the key cabinets this is applicable if enforce iFob Allowance across all systems is enabled.

- CAN Gateway Adaptor Type
  - Clock & Data (Shock Sensor) - 8bit Only

    Select if using the CAN Gateway PCB adaptor to send / receive CAN messages.
  - CAN232

    Select if using the CAN232 adaptor or the CANSG to send / receive CAN messages.

System ID Configuration

Each system on CAN Gateway will require a **unique system ID number**. Please view Setting 8bit System ID or Setting 16bit System ID for how to do this from the Traka system keypad.

Example:-

System Description	System ID
Access Pod Hospital Entrance	001
Access Pod Staff Exit	002
Key Holding Room Cab Blue	003
Key Holding Room Cab Green	004

5.17.3 8BIT CAN GATEWAY HARDWARE AND CONNECTIONS

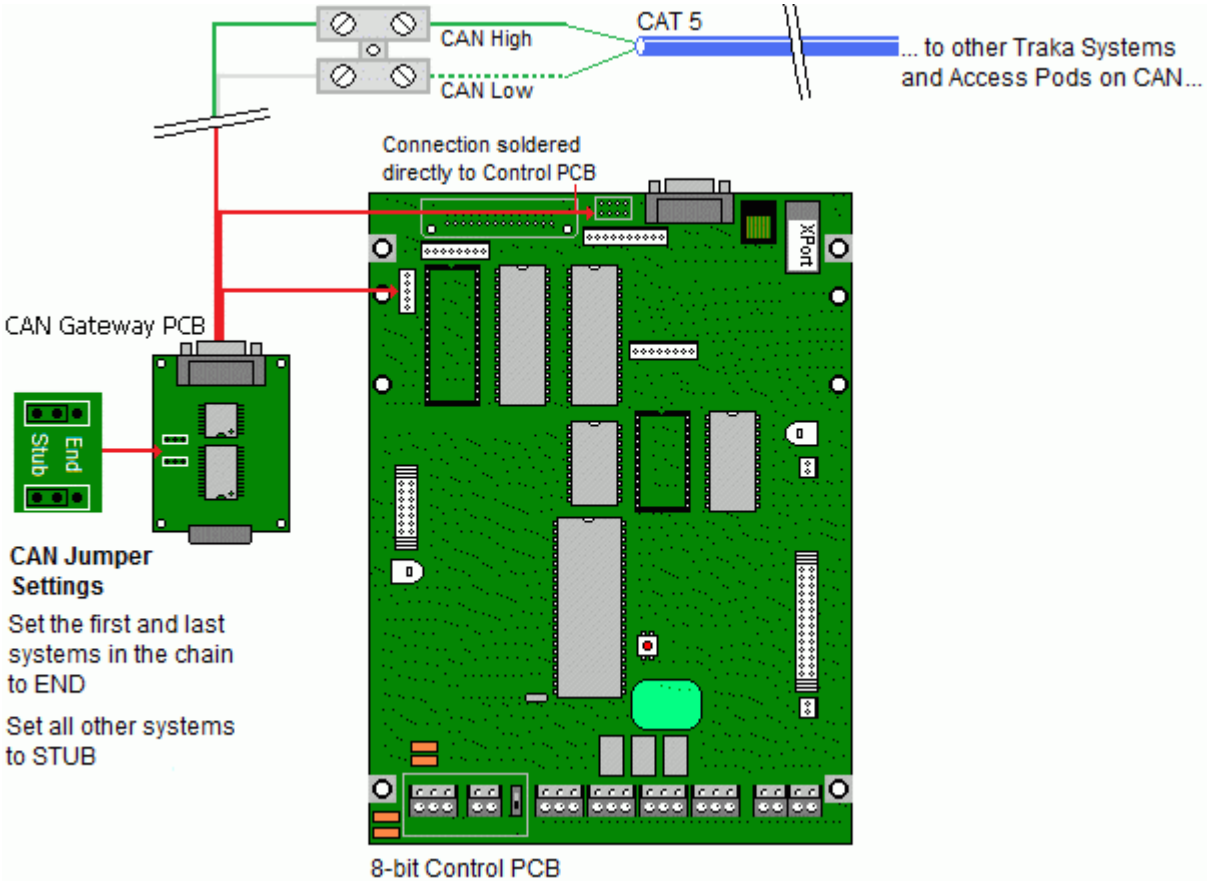
Each Traka Key Management System, Locker or Access Pod requires a CAN Gateway adaptor that converts messages from the Traka Control PCB into Controller Area Network (CAN) messages for sending over CAN.

Traka currently supports **two** different types of CAN Gateway adaptor. The type required depends on the card reader as well as the other peripheral devices the system needs to support. Please contact Traka with your application requirements and the correct device will be specified for your needs.

CAN Gateway PCB Adaptor

The Traka Shock Sensor PCB can be used to send and receive CAN messages. This type of CAN Gateway adaptor is required when the TSSI Biometrics reader is used. This is because the CAN Gateway PCB does not use the UARTB interface (unlike the CAN232 Converter) but instead connects to the Clock and Data card reader interface.

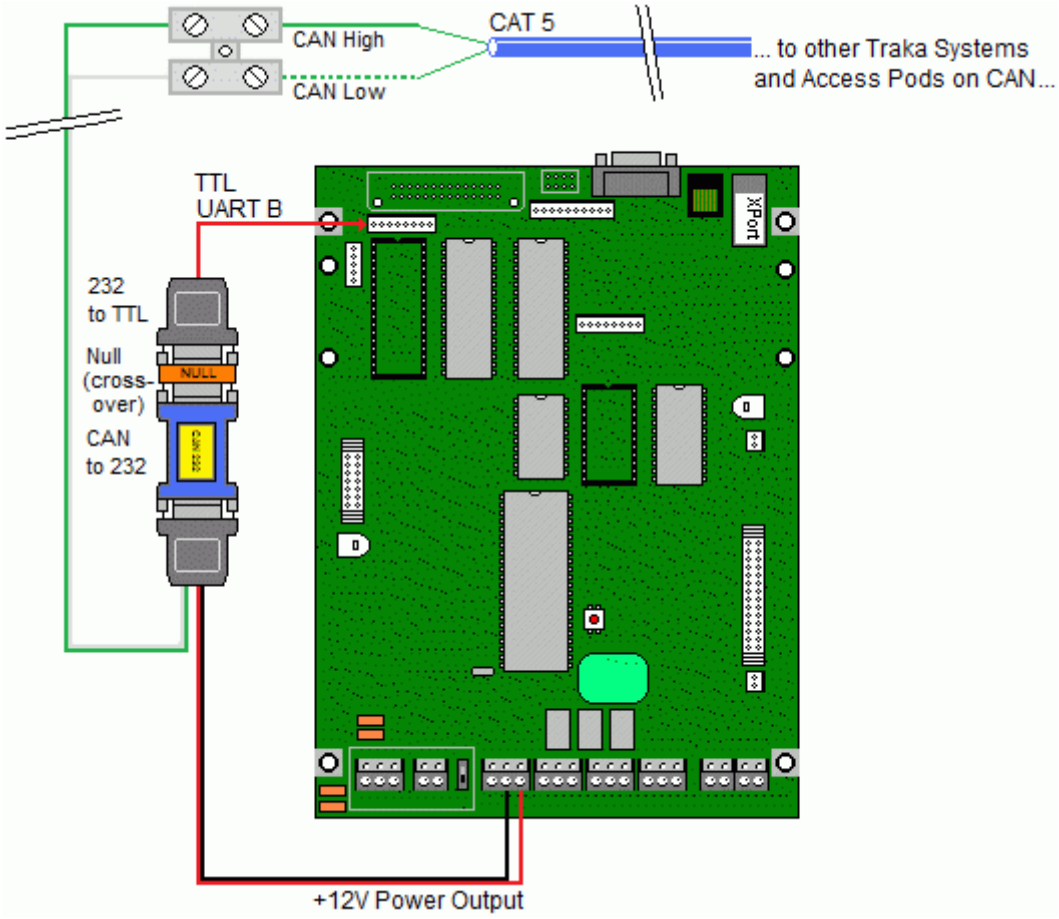
See following CAN Gateway PCB connection diagram:-



CAN232 Adaptor

The CAN232 adaptor (CAN to RS232 converter) can also be used to send and receive CAN messages and connects to the UARTB interface. This also allows the card reader interface to be used as normal for proximity and magstripe readers.

See following CAN232 connection diagram:-

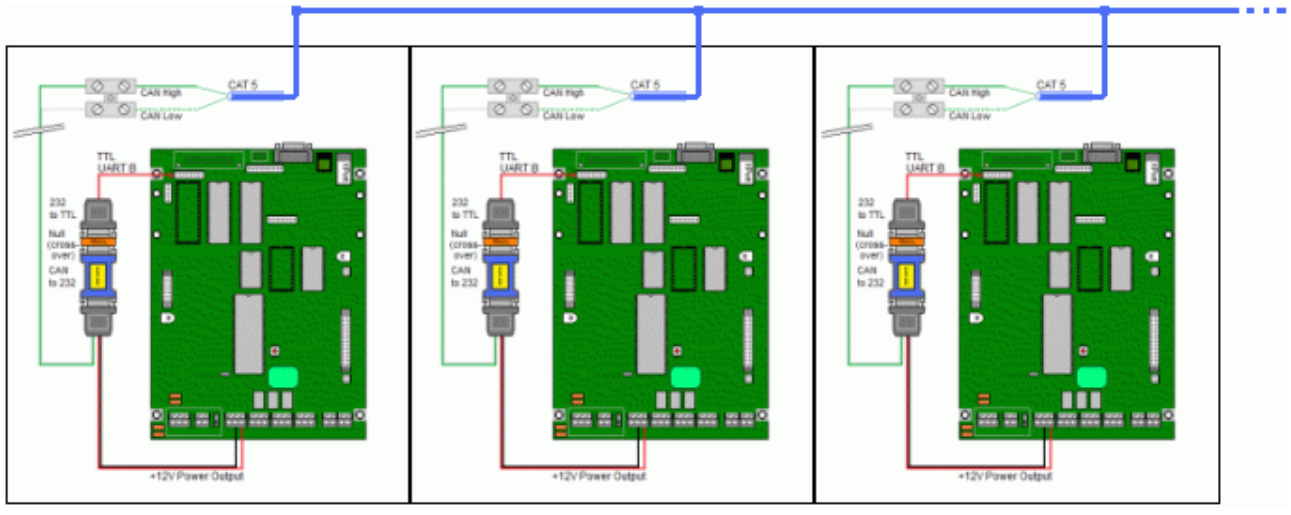


Connecting systems together on CAN

All Traka systems and Access Pods on CAN are connected using only a **single pair (2 wires)** from a standard Category 5 twisted pair network cable. Ideally they should be **daisy chained** together on a **single long bus**.

In some installations it may not be possible to daisy chain all systems together and some maybe "spurred" off the main bus. Contact Traka for advice on the best wiring method in this instance.

Simply select a colour pair and daisy chain together as follows:-



IMPORTANT - Bus Termination Rules

CAN Gateway PCB

The **first** and **last** systems in the chain should have the jumper settings configured to **END** (see diagram above). The systems in the middle of the chain should be set to **STUB**. See CAN Gateway PCB diagram above.

RS232 CAN Converter

The first and last systems in the chain should have a **120 ohm resistor** connected across the 2 pin terminal block (CAN High and CAN Low pins). The systems in the middle of the chain all other systems do not require a resistor.

5.17.4 16BIT CAN GATEWAY HARDWARE AND CONNECTIONS

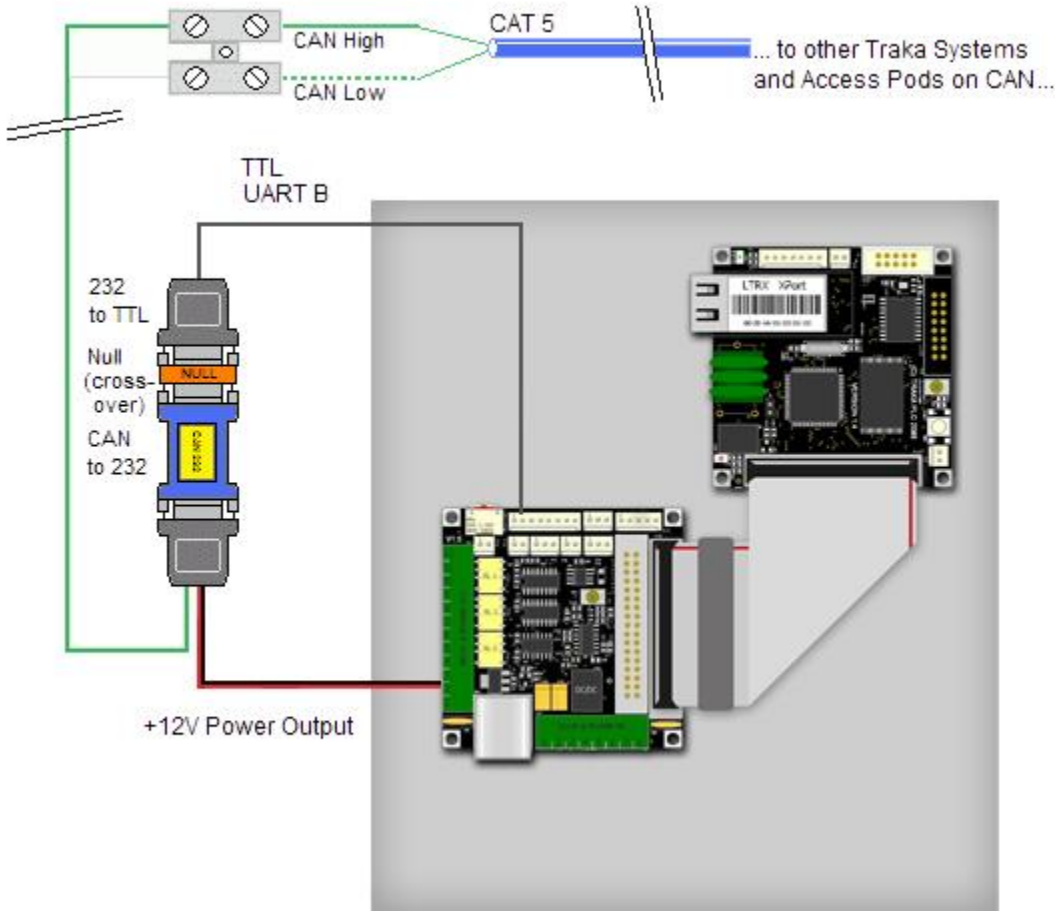
Each Traka Key Management System, Locker or Access Pod requires a CAN Gateway adaptor that converts messages from the Traka Control PCB into Controller Area Network (CAN) messages for sending over CAN.

Traka currently supports **two** different types of CAN Gateway adaptor. The type required depends on the card reader as well as the other peripheral devices the system needs to support. Please contact Traka with your application requirements and the correct device will be specified for your needs.

CAN232 Adaptor

The CAN232 adaptor (CAN to RS232 converter) can also be used to send and receive CAN messages and connects to the UARTB interface. This also allows the card reader interface to be used as normal for proximity and magstripe readers.

See following CAN232 connection diagram:-

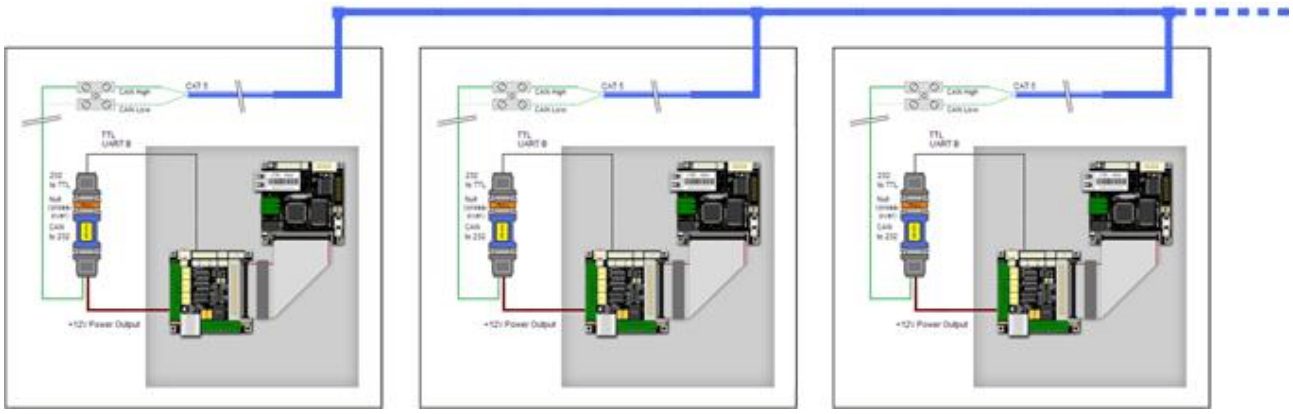


Connecting systems together on CAN

All Traka systems and Access Pods on CAN are connected using only a **single pair (2 wires)** from a standard Category 5 twisted pair network cable. Ideally they should be **daisy chained** together on a **single long bus**.

In some installations it may not be possible to daisy chain all systems together and some maybe "spurred" off the main bus. Contact Traka for advice on the best wiring method in this instance.

Simply select a colour pair and daisy chain together as follows:-



IMPORTANT - Bus Termination Rules

RS232 CAN Converter

The first and last systems in the chain should have a **120 ohm resistor** connected across the 2 pin terminal block (CAN High and CAN Low pins). The systems in the middle of the chain all other systems do not require a resistor.

5.17.5 USING CAN GATEWAY

The users of a CAN Gateway enabled system do not have to do anything differently to that of a normal system. However it is useful to be aware of the following LCD messages that will be displayed during operation.

Access Pod

When a user is identified and verified to the Access Pod, the LCD will momentarily display:-

- Ensure all keys returned
  - User is holding keys

    If the user is holding keys they will not be **denied** access and the LCD will display:-

  - User is not holding keys

    If the user is not holding any keys, they will be granted access and the LCD will display:-

- Ensure 1 or more keys taken
  - User is holding 1 or more keys

    If the user is holding 1 or more keys, they will be granted access and the LCD will display:-

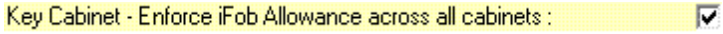
    

  - User is not holding keys

    If the user is not holding any keys, they will be denied access and the LCD will display:-

Key Cabinet



When a user tries to remove an iFob, the LCD will momentarily display:-

If their allowance has been exceeded across all key cabinets, they will be denied access to the iFob and the LCD will display:-

CAN Communication Issue

When an access pod or key cabinet is checking for keys, if the LCD displays **"CAN Error Please Retry"** then retry taking the iFob or identifying yourself on the Access Pod (as applicable). If this continues to be a problem, then double check the Key Cabinet count for this system.

5.18 SAGEM FINGERPRINT READER

5.18.1 SAGEM FINGERPRINT READER OVERVIEW

The Sagem Fingerprint reader is an add-on system to Traka that is used to identify a user before allowing access to a system.

The Sagem reader is similar to the TSSI Biometrics reader however, the Sagem reader is much smaller is provided with a separate module that allows users to enrol at the PC Traka32 is installed on rather than the system the Sagem reader is fixed to.

- You can enrol two fingers per user
- Enrolment is now at the PC in which you have Traka32 installed via a USB enrolment module, rather than the reader itself
- Its faster when communicating to Traka32

The reader and/or PIN option is also available when using a Sagem fingerprint reader. If ticked, this will allow a user to enter the PIN number instead of using their fingerprint to authenticate with the cabinet.

NOTE: When installing, position the cabinet so that users can stand in a comfortable and natural position. Do not position in direct sunlight.

The minimum software and firmware versions required to support the Sagem MorphoSmart reader on the 8bit are as follows.

Software: 02.08.0003

Firmware: v6.07.58

5.18.2 SAGEM FINGERPRINT READER DRIVERS

Installing the Drivers

NOTE: The drivers MUST be installed before plugging in the enrolment module.

To enable the use of the fingerprint USB enrolment module, the drivers must be enabled, for this you will need to be an administrator of the PC you wish to install the module on, also this must be done per PC for every PC you wish to use to enrol users.

If you are installing Traka32 for the first time and wish to install the drives at this point follow **Option 1**, if you already have Traka32 installed and you wish to install the drivers themselves follow **Option 2.**

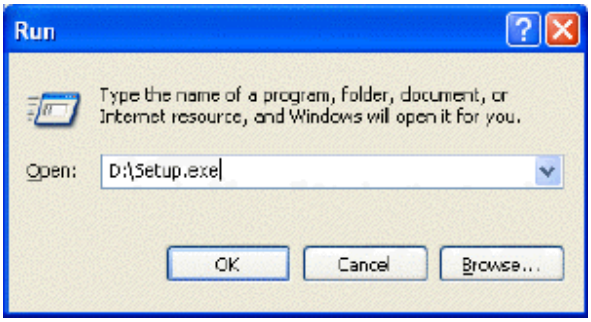
Option1

NOTE: Before installing the Traka32 software, please check that the PC you are going to install the software on meets the minimum requirements otherwise you may face problems during the installation or use of the software. Please refer to the minimum PC requirements section for more details.

1. Insert the Traka32 CD into the CD-ROM drive.

2. After a few seconds the set-up wizard should run automatically.

   If not, click on Start > Run and type D:\Setup.exe followed by Enter
   (replacing the D with the appropriate CD-ROM letter)



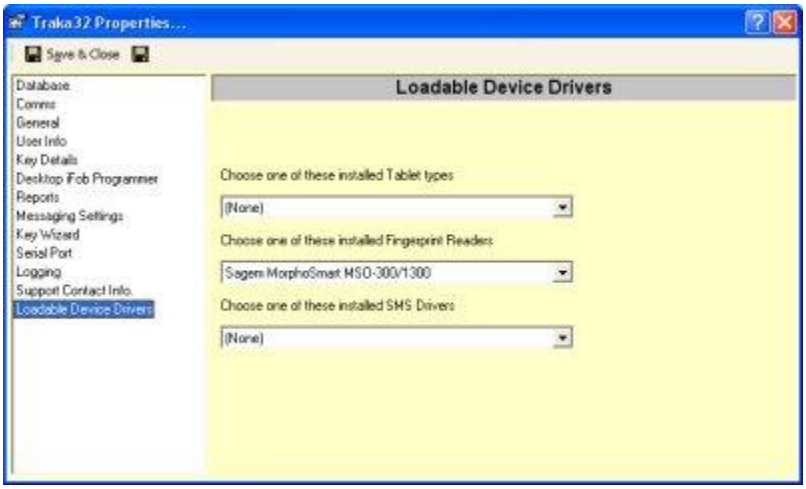
3. The Traka32 Administrator will now appear and will ask you what type of install you wish to proceed with, i.e 'Typical', 'Normal' or 'Custom'. Select 'Custom' install and you will be taken to the Custom setup screen where you will see all the drivers and additional features that can be enabled. Expand the 'Drivers' menu, then expand the Sagem MorphoSmart MSO300 Driver, and select 'This Feature Will be installed on Local Hard drive'. Click 'Next' then 'Install' and the set-up wizard will guide you through the rest of the installation.

   When the drivers are fully installed the USB enrolment module is now ready for use. Insert the Enrolment Module into a USB port on the required PC and open the TRAKA32 software. Select File/Properties, and then select 'Loadable Device Drivers'. Now use the drop down box labelled 'Choose one of these installed Fingerprint Readers', and select 'Sagem MorphoSmart MS0-300/1300', (see below) now save and close.

Option 2

- Select... Control Panel\ Add or Remove Programs and select 'Traka32bit Administrator'.
- Select change, then next.
- Check the box for 'Modify' and select next.
- Expand the 'Drivers' menu.
- Expand the Sagem MorphoSmart MSO300 Driver, and select 'This Feature Will be installed on Local Hard drive'.

1. Now the Drivers have been enabled, they must be installed the setup file is located in C:\Program Files\Traka Limited\Traka32\Drivers\Biometrics\TrakaMSO300Driver. Once you have opened the folder select the 'Setup' icon, and follow the instructions of the setup wizard.
2. When the drivers are fully installed the USB enrolment module is ready for use.
3. Insert the Enrolment Module into a USB port on the required PC.
4. Open the TRAKA32 software and select File/Properties, and select 'Loadable Device Drivers'. Now use the drop down box labelled 'Choose one of these installed Fingerprint Readers'. Select 'Sagem MorphoSmart MS0-300/1300' (see below). Save and close.

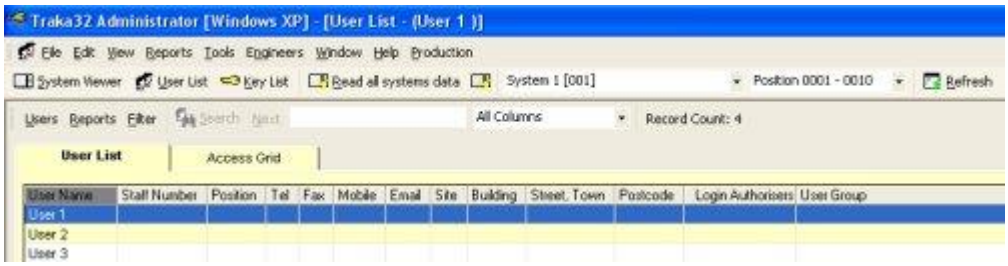


5.18.3 SAGEM FINGERPRINT ENROLMENT

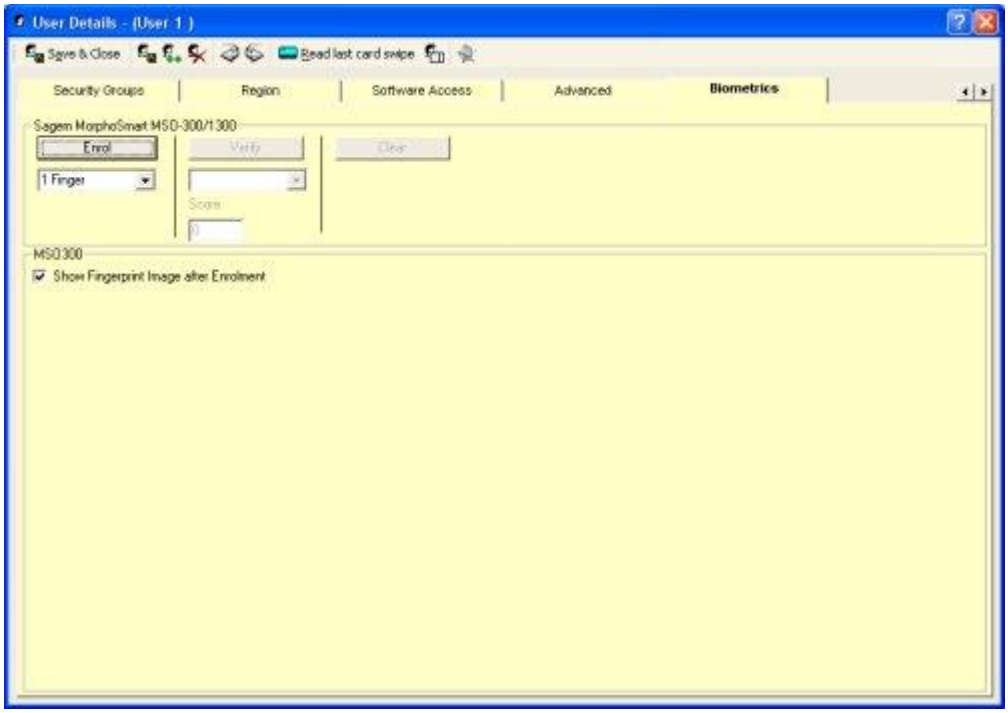
NOTE: At this point all hardware (Sagem Fingerprint Reader, USB Enrolment Module and/or 8bit Interface Board and Traka reader cable) must be plugged into the UART-B. before attempting an upgrade or configuring the system. This also applies when communicating to the system, or if the system is to be changed to PIN only, i.e. if the cabinet firmware includes Sagem MorphoSmart reader settings, the hardware MUST be plugged in at ALL times.

Setup your system and upgrade the firmware as normal (the firmware needs to have 'Sagem Fingerprint MorphoSmart CBM' enabled as the reader interface).

Set date and time, synchronise users and iFobs then open the *User List.*



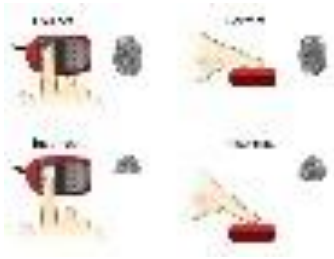
Double click the user you wish to enrol to bring up their User Details. Click along to the tab named 'Biometrics' and click the Enrol button.



The Acquisition window will appear asking you to place your finger on the enrolment module. Present 3 fingerprint samples on the face of the Enrolment Module. The green percentage bar on the right hand side symbolises the quality of each enrolment attempt, and needs to be more than 15% to pass as an accurate template.

When enrolling it is important you align the your finger to the centre of the Enrolment Module and lay you finger flat to receive accurate results (See Below)

- Do not move finger when enrolling
- Do not press to hard
- Place your finger on the enrolment module do not slide or roll finger on and off



If the templates have been successfully captured, the message, 'Template Capture Successful' will appear (See Below) you can now save and close.

NOTE: In order to save the templates for your specified user, the user must have effective access levels to the system in use.

Re-Enrolling

If you wish to change the Fingerprint template that you have saved to the user, simply click the 'Enrol' button and go through the enrolment process again.

Verify Button

The 'Verify' button allows you to compare the current fingerprint template to the fingerprint of the user. When you click the 'Verify' button the acquisition window will appear and the user will have to place his/her finger on the USB enrolment module once to compare with the previously configured template.

Clear Button

By clicking the 'Clear' button you will erase any fingerprint templates and information from the specified user.

Using the Sagem Fingerprint reader

Standard systems

After installing and upgrading your system with the appropriate settings, access your system by pressing the '# '(hash) key on the keypad. The LCD will display the following text 'Please place your finger on the reader', place the finger that you used to give the sample onto the face of the reader. If successful the door will open and the user can use the cabinet as normal.

Download Stations

When using the Sagem reader with the iFob Per Person download station, the user identification process is slightly different. Please refer to the Download Station topic for information.

Reader and/or PIN option

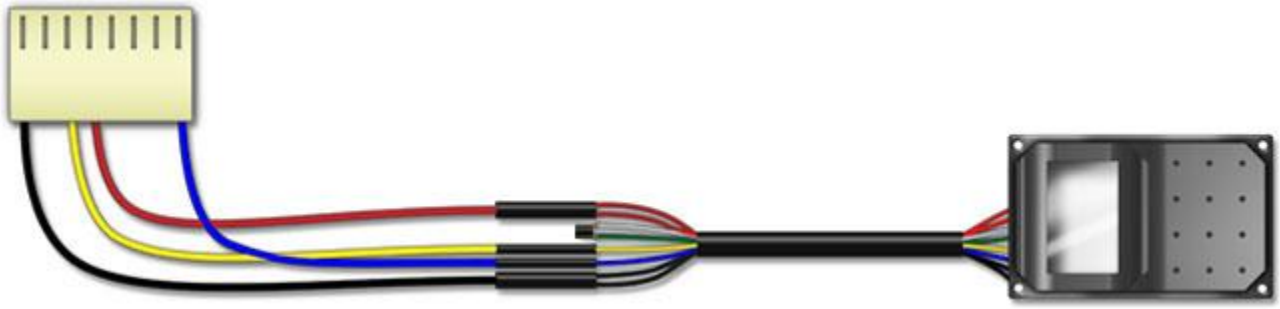
The reader and/or PIN option is now available when using a Sagem fingerprint reader. If enabled, this will allow a user to enter the PIN number instead of using their fingerprint to authenticate at the cabinet. To enter your PIN instead of using the fingerprint reader press and hold the # button. The system will then ask you to enter your PIN.

5.18.4 8BIT SAGEM FINGERPRINT READER CONFIGURATION

The version of control board you have will determine the way the Sagem reader is wired up.

8-bit PCB V2.31.00 and Above

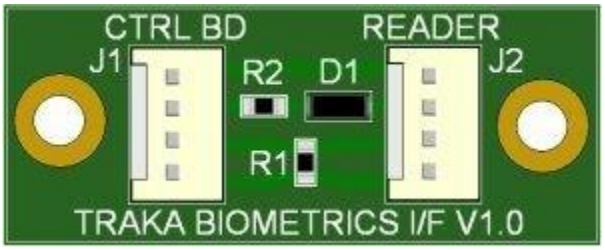
V2.31.00 and above and the Sagem reader will be wired directly into the 8bit PCB and will look as pictured below.

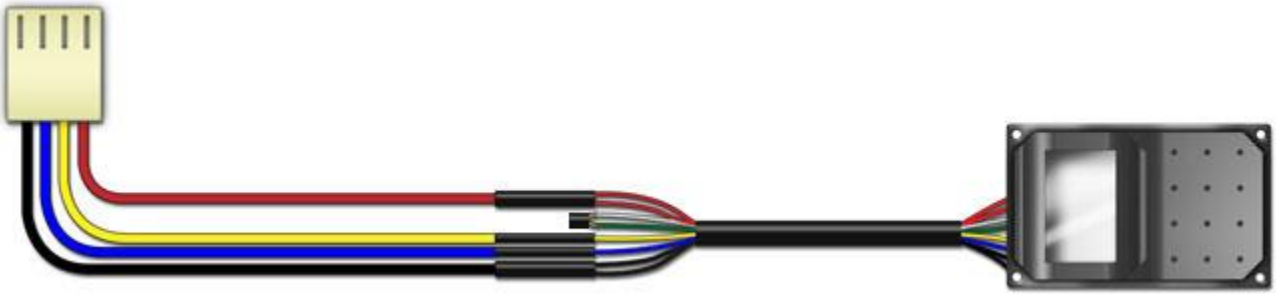


Each system will be provided with the USB enrolment module.

8-bit PCB V2.30.04 and Below

Below V2.31.00 and the Sagem reader will require a separate cable and interface PCB to connect to the 8bit PCB and will look as pictured below.

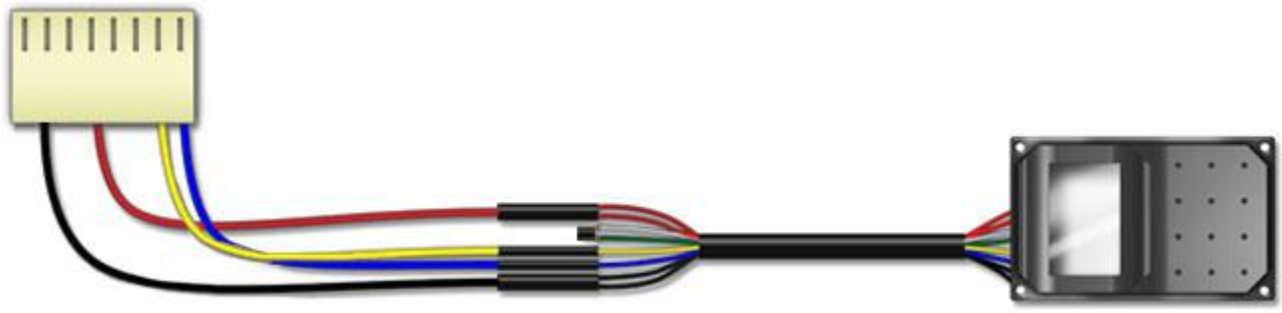




Each system will be provided with the USB enrolment module.

5.18.5 16BIT SAGEM FINGERPRINT READER CONFIGURATION

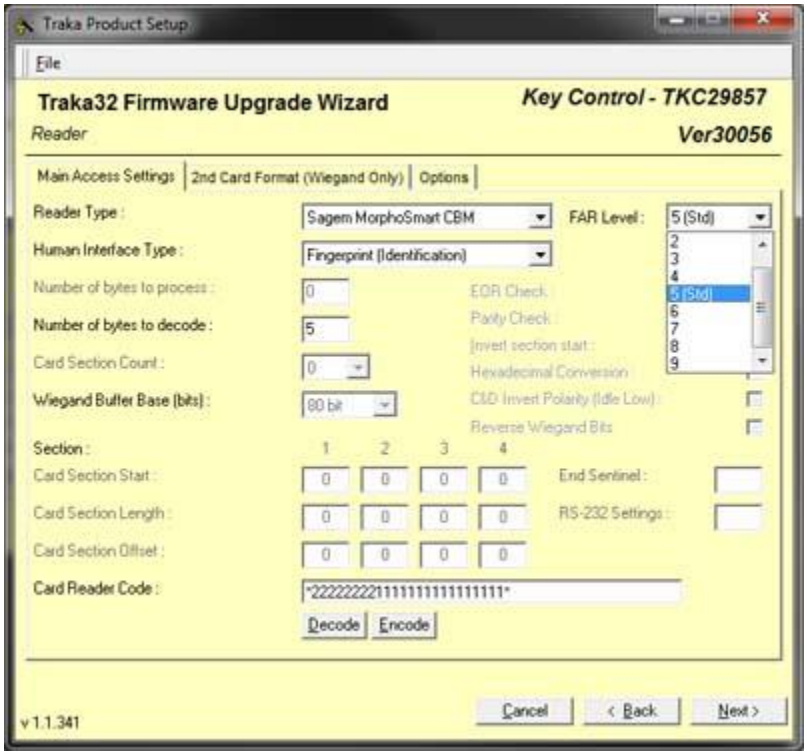
The 16bit PCB does not require any additional hardware modifications, however the wiring on the reader cable is different to the 8bit, please see below.



Each system will be provided with the USB enrolment module.

5.18.6 SAGEM FINGERPRINT READER - FALSE ACCEPTANCE RATE

The Sagem Morphosmart reader is currently hardcoded in the 8 and 16 bit firmware to use a matching threshold level of 5, when identifying a user. This corresponds to a False Acceptance Rate (FAR) of <0.01%. This can now be adjusted on a cabinet-by-cabinet basis in the 'Configure Firmware' dialogue.



The following levels can be set:

1 FAR < 1 % There are less rejections, but more recognitions

2 FAR < 0.3 %

3 FAR < 0.1%

4 FAR < 0.03 %

5 FAR < 0.01 % Recommended value

6 FAR < 0.001 %

7 FAR < 0.0001 %

8 FAR < 0.00001 %

9 FAR < 0.0000001 % There are less recognitions and more rejections.

Adjusting the value below 3 or above 7 is not recommended except in special circumstances.

5.18.7 SAGEM TROUBLESHOOTING

Below is a list of common error codes you might encounter when using the SAGEM Fingerprint Reader.

NOTE: The description will not appear on the LCD only the code will appear.

SAGEM Reader Errors

-6	The finger detection time out has expired.
-9	The specified database doesn't exist.
1	Authentication or Identification succeeded.
2	Authentication or Identification failed.
5	The database is empty.
34	False finger detected.
53	The finger may be too moist or the scanner is wet.

Traka Reader Errors

300	Sagem reader Initialisation Fail
301	Sagem reader Initialisation OK
302	Sagem reader is not Responding to Communications.
303	Sagem reader Acknowledge Received
304	Sagem reader Communication Command Error Received
305	Valid Header Received
306	Invalid Header Received

5.19 LOCKERS

5.19.1 LOCKERS OVERVIEW

Most standard Traka32 features such as Adding Systems, Adding Users and running Reports are carried out in the same way for Lockers as for Key Cabinets. This 'Lockers' section of the guide assumes knowledge of the basic Traka32 features and focuses on specific details for customers using locker systems. It is intended to be used in conjunction with the rest of the Traka32 Help Guide.

Traka Lockers are custom built to suit a particular customer's requirements, often holding assets such as radios, laptops, tablets, cash draws, PDA's, etc. Traka can provide a full audit trail with the lockers in the same way as the key cabinets. Utilising RFID tagging for every compartment (if desired), the asset is automatically audited as it is taken and returned to the locker. So the user is fully accountable for the use of the asset whilst its in their possession. Additionally, the asset can be continuously monitored whilst in the locker, to ensure that it is in its designated location.

Lockers, in most cases, can also be fitted with chargers if required. This allows for battery powered devices such as radios, PDA's, laptops and tablets to be continuously charged up whilst stored in the locker system.

There are 3 main designs of Traka Locker System:

- Modular Lockers
- Laptop Lockers
- Tablet Lockers

Modular Lockers

Modular Lockers are the most customisable range of Traka Lockers. They can have up to 100 customisable compartments fitted with RFID in a single system. Generally the locker compartments are separate to the pod, much like an L-Series system (see below).

Laptop Lockers

Laptop Lockers are available in either 10 or 15 compartment versions. They can be extended with further 10 or 15 compartment banks to make a single system containing up to 100 compartments. The compartments can be fitted with a custom design bracket to suit a particular laptop to enable reliable RFID reading, and can also be designed with or without charging capabilities.

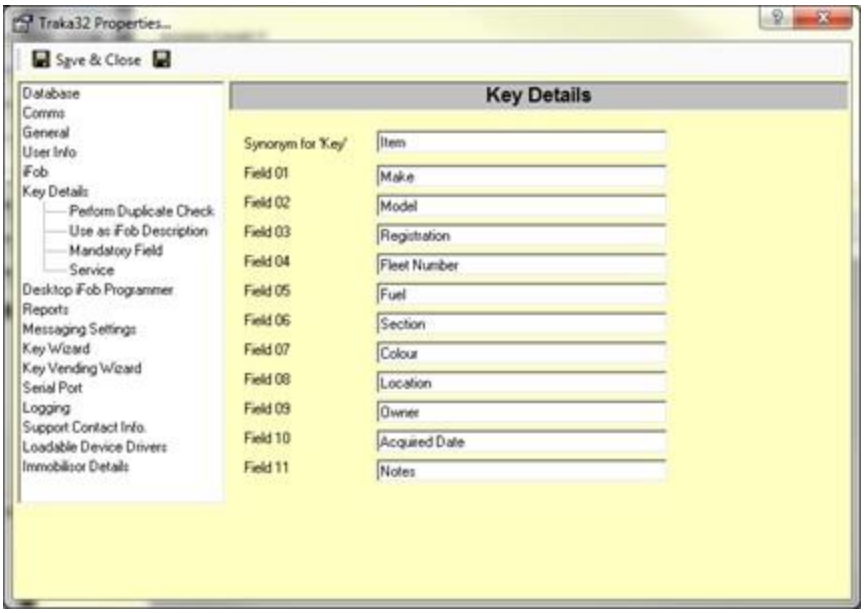
Tablet Lockers

Tablet Lockers are available in either 20 or 30 compartment systems. Much like the laptop lockers, they can be fitted with a custom design bracket to suit a particular tablet to enable reliable RFID reading, and can also be designed with or without charging capabilities.

5.19.2 SYNONYM FOR 'KEY'

Traka's legacy products are key cabinets and key related products, therefore Traka32 by default is configured to work with 'key cabinets' and 'keys'. As a result there are many places within the software that refer to 'keys'. Traka32 allows you to assign a synonym that replaces the term 'key' in most places throughout the software.

1. Go to **File>Properties**.
2. From the browser on the left hand side of the Properties window, select **Key Details**.
3. At the top of the window is a field titled 'Synonym for Key'. Here is where you will enter your new term e.g. radio, laptop, PDA or simply Item. For the purpose of this guide we will use 'Item'.



4. Once you have entered the correct information, click **Save & Close**.
5. Several places within the software will now display your synonym. For example on the system viewer page the 'Key Events' tab will now display 'Item Events' or whatever term you entered.

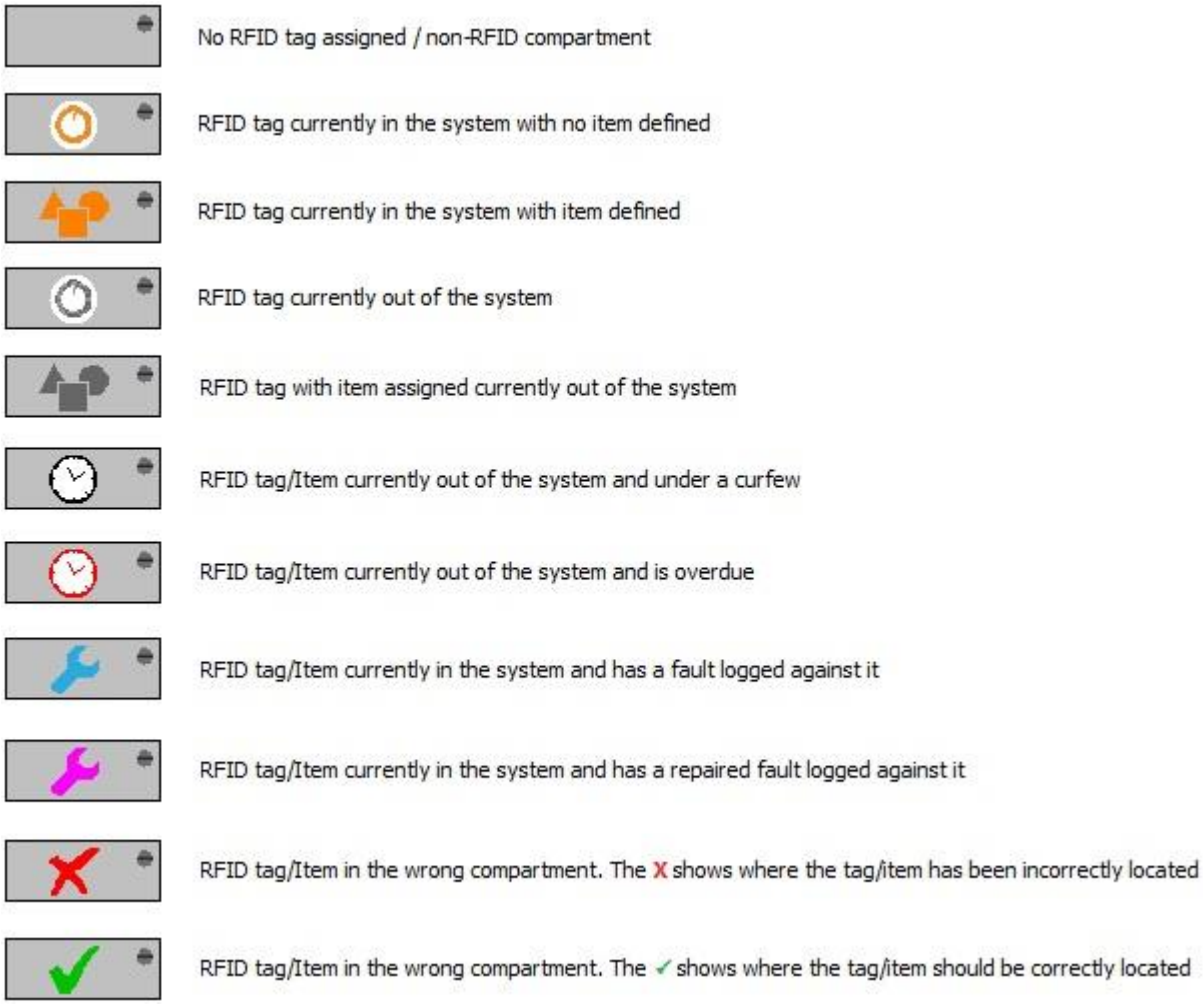
5.19.3 LOCKER SYSTEM VIEWER

This topic describes some of the features shown from the System Viewer page more specifically for lockers. For a complete overview of the System Viewer page refer to the System Viewer Overview section.

System Display

The icons shown on each compartment on the system image change depending on their current status.

NOTE: The icons may vary slightly depending on the system type selected in the System Configuration.



iFob/Locker Events Tab

This tab shows all event history for the past 1 month only for the currently selected compartment. To view events older than one month, go to **Reports>Crystal Reports>iFobs>Standard iFob Event Report** and filter as required. See Crystal Reports - iFobs for more details.

Item Events Tab

By default this tab is called 'Key Events'. When using lockers in Traka32 it makes sense to change this term for a word of your choice (such as 'Item') to better suit your requirements. Refer to the Synonym for 'Key' section for details on how to do this.

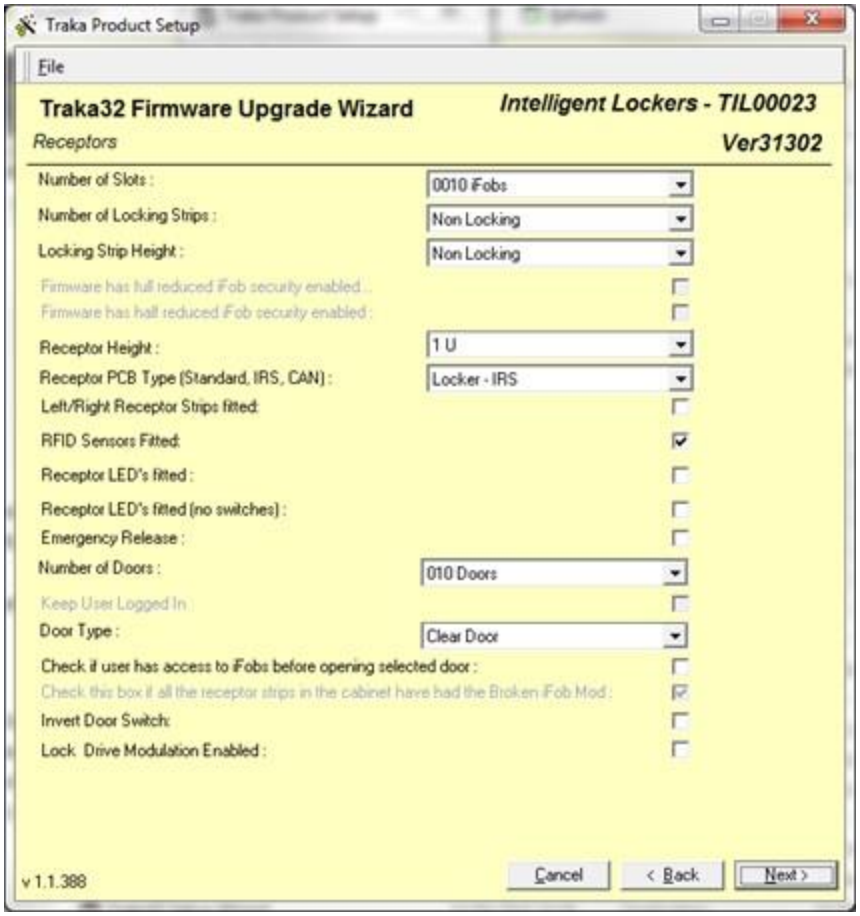
The tab shows all item event history for the past 1 month for the currently selected item. To view events older than 1 month, you can run a report from **Reports>Crystal Reports>Keys>Standard Key Event Report** and filter as required. See Crystal Reports - Keys for more details.

iFob/Locker Access Tab

This tab shows which users have access to the currently selected item.

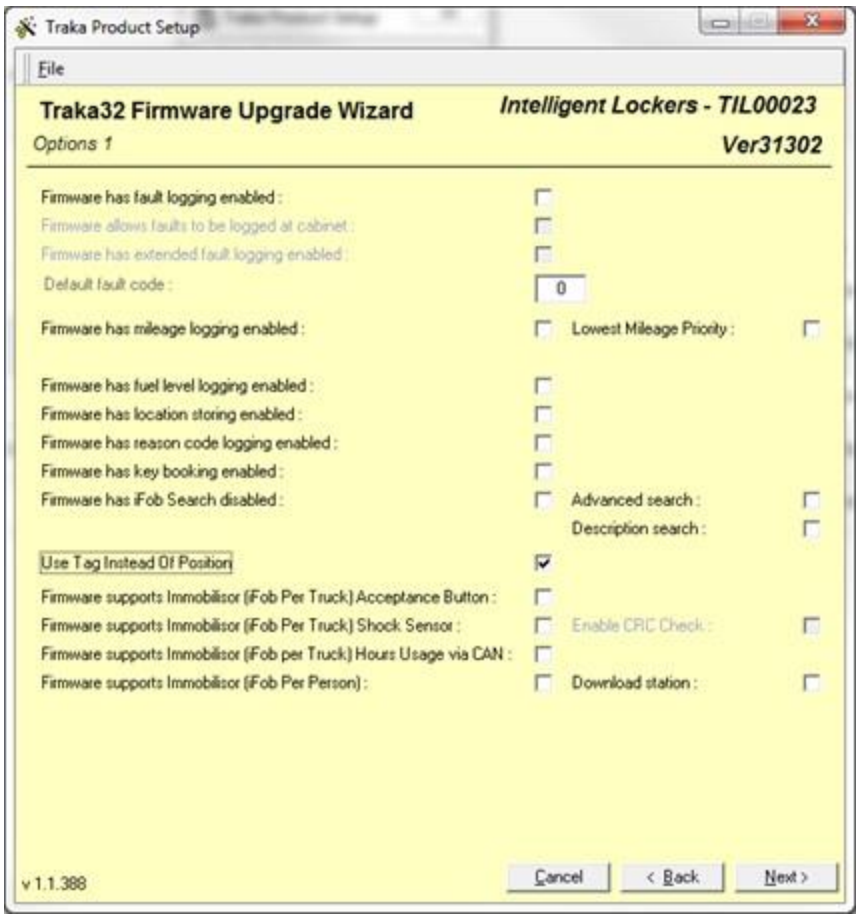
5.19.4 LOCKER FIRMWARE OPTIONS

To allow the functionality of a Traka locker certain options must be enabled within the firmware...

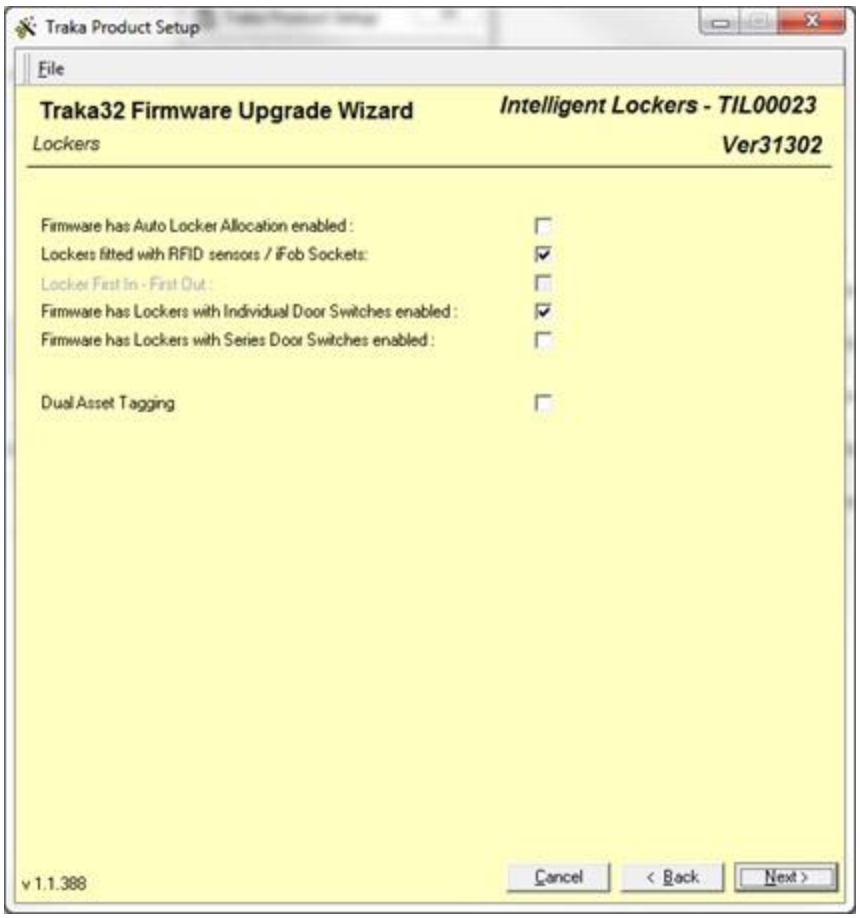


- **Receptor PCB Type**
  Select 'Lockers - IRS' from the drop down menu for all 8bit and 16bit lockers.

- **RFID Sensors Fitted**
  This tick box enables the use of RFID on the Locker interface board. RFID is an optional cost feature and only needs to be enabled if required.



- **Use Tag Instead Of Position**
  This option enables a user to open a locker compartment door by specifying the tag number instead of the position number.



- **Firmware has Auto Locker Allocation Enabled**
  This option when ticked allows a user to 'Auto Allocate' a device within the locker compartments. Also Auto Allocation' functions so that...

  If a user has Access Level 197 (or level 5 for RUS), they can open any locker door effectively overriding the auto allocation (for either FIFO or Rotation).

  If a user has more than one Access Level, they can select which type of device to auto allocate (for either FIFO or Rotation). If the user only has 1 access level, the system will just auto allocate that level automatically.

- **Lockers Fitted with RFID Sensors**
  This tick box tells the locker whether or not it will have as an asset in its compartment that can be read via RFID. RFID is an optional cost feature and only needs to be enabled if required.

- **Locker First In - First Out**
  First In, First Out (FIFO) is an option that automatically issues devices (e.g. radios, laptops etc.) in an order in which they have been in the locker for the longest amount of time. This then gives the maximum amount of charge time possible between uses. This option also takes into account the users access levels and so will only issue a device that the user has access to and has been in the locker for the longest amount of time.

  NOTE: Auto Locker Allocation must also be enabled in order to use the 'First In - First Out' feature.

- **Firmware has Lockers with Individual Door Switches Enabled**
  Tick this box if the locker requires the use of individual Door Switches

- **Firmware has Lockers with Series Door Switches Enabled**
  Tick this box if the locker requires the use of the original Series Door Switches

- **Dual Asset Tagging**
  This option allows 2 RFID tags to be read by the same compartment.

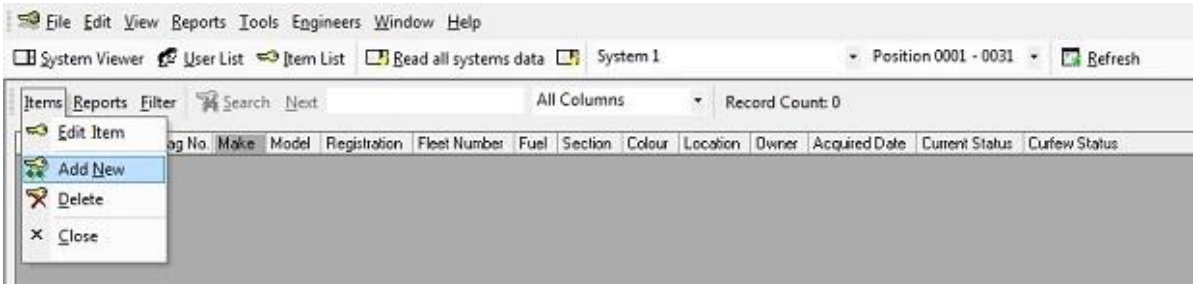
5.19.5 DEFINING AND EDITING ITEMS

Much the same as Keys can be added to iFobs in Traka32, with Lockers you can assign an Item (or whatever term you have specified in the Synonym for 'Key' section) to a locker compartment. A list of all Items and their specific details can be created in the Traka32 database.

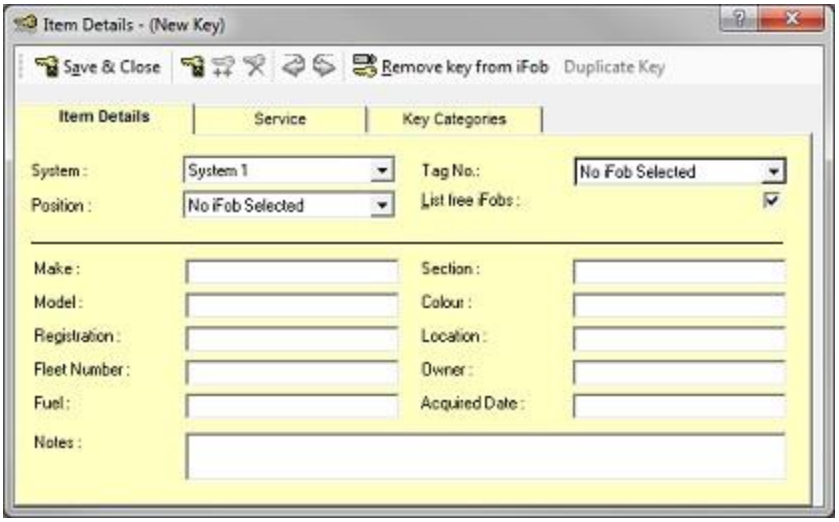
Adding an Item

To add an Item to the Traka32 database:-

1. Click on the **Item List** button to open the Item List.
2. Click on **Items>Add New**.



3. A blank item record is created.



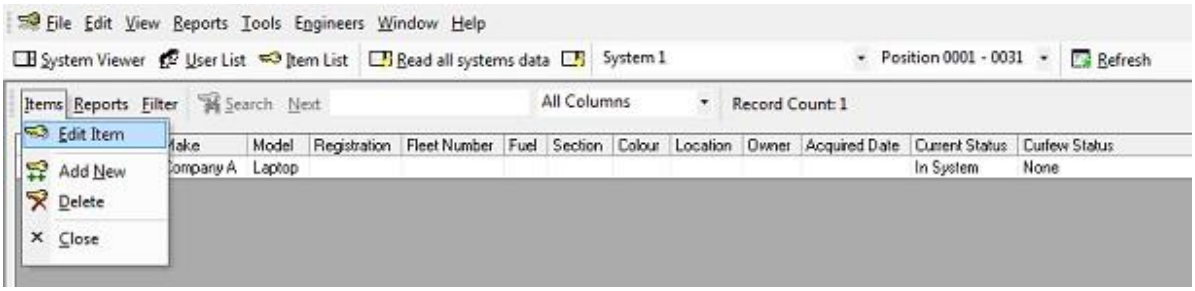
4. Select the System and Position (compartment) the item will be assigned to from the drop down lists. Alternatively you can choose not to assign the item to a compartment at this stage and edit this later on. This can be useful is you wish to enter all the item details onto the system but do not yet know which compartment the item will be assigned to. Items that are not assigned to a system and compartment are referred to as "unallocated items".
5. Complete the item details fields as required. It's possible to edit the field headings and/or make any number of the fields mandatory so that the item can only be saved if the field has been filled in. To edit and make fields mandatory refer to the Properties section.

   NOTE: The Properties section refers to the default name of 'Key' Details. If you changed the Synonym for 'Key' this will have updated to the term you specified.
6. Once you have entered all of the necessary details click **Save & Close** to save the Item to the database. Or if you wish to add further items click the **Save** button and then click the **Add New** button.
7. Once you return back to the System Viewer page, any compartments that have had items assigned will now display an updated icon. For more details on the icon types, refer to the Locker System Viewer section.

Editing an Item

To edit an item:-

1. Click on the **Item List** button.
2. Select the Item you wish to edit from the list.
3. Click on **Items>Edit Item**.

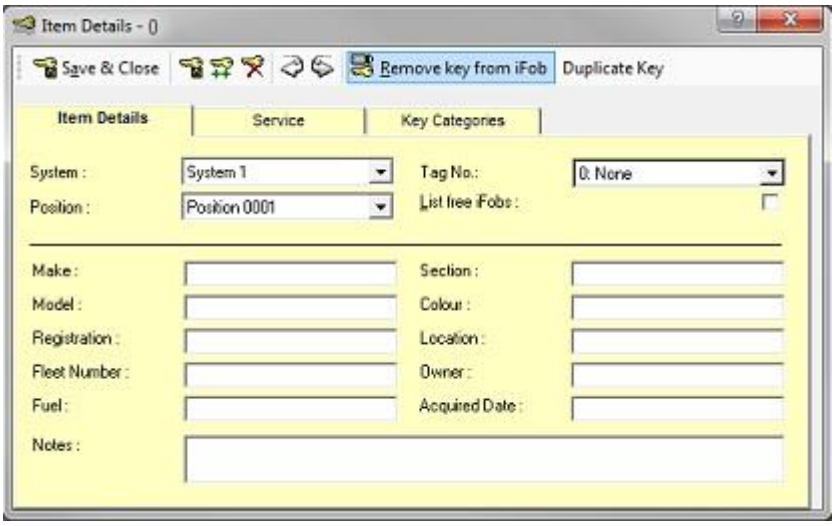


5.19.6 DELETING/REMOVING ITEMS

It is not usually recommended that an item is permanently deleted. Traka has the ability to hold the event history and information that is associated to an item even if it is not attached to an object. It is instead recommended that you remove the item from the compartment only so as not to lose the event history.

To do this:-

1. Click on the **Item List** button.
2. Double click the required item from the list or select it and go to **Items>Edit Item**.
3. Click on the **Remove key from iFob** button, followed by **Save & Close**. The item is now referred to as an "unallocated item". Of course it can be re-allocated to a compartment at a later date if needed.



When you have removed an item in Traka32 it must of course also be physically removed from the system.

Should an item record need to be deleted permanently this can be achieved by doing the following:-

1. Click on the **Item List** button.
2. Click on the item you wish to delete and select **Items>Delete**.
3. A message will appear asking to confirm the deletion. Click **Yes** and the item record will be permanently deleted from the database.

5.19.7 RFID LOCKERS

5.19.7.1 RFID OVERVIEW

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

It is possible as an optional extra to 'tag' each item in the locker. This allows the item to be identified as 'in or out' of the system, and used by whom. Each item is individually tagged with one of Traka's robust and discreet RFID tags.

Depending on the items being tagged, Traka will design the locker compartment around the item and ensure the appropriate sized tag is used.

The largest tag Traka use is the 50mm Adhesive Tag which is typically used on larger items such as laptops and tablets. The smallest tag used is the 12mm glass tag, which is generally used on smaller assets such as radios, PDA's or mobile phones.

5.19.7.2 TAGGING A NEW ITEM

If your locker system uses Traka RFID technology, you will need to secure a new tag to the item before allocating it to the compartment.

Traka supply every customer who uses RFID with a 'Tagging Guide'. This will show how to correctly tag the items in your system. Please consult the tagging guide and ensure you tag the item correctly using the correct Traka RFID tag.

5.19.7.3 ALLOCATING A NEW ITEM

1. Access the locker compartment that you wish to allocate the new item to.
2. Insert the item into the compartment. The LCD will display a message similar to the example below.

3. Ignore this message and close the door.
4. Ensure the no-one accesses the system during this time. If the computer running Traka32 is located far away from the locker, it is a good idea to get a second person to stand by the locker to ask users just to wait a minute until this process has been completed.
5. From Traka32 select the system you wish to allocate the new item to.
6. Right click over the compartment to display the Item menu.
7. Click **Edit iFob/Locker Details** to open the Item Details window.

8. Click **Read Serial Number** to read the serial number from the RFID tag.
9. If the serial number is successfully read it will be displayed. Simply click on **Yes** to allocate the item to the position. The system will now be updated.

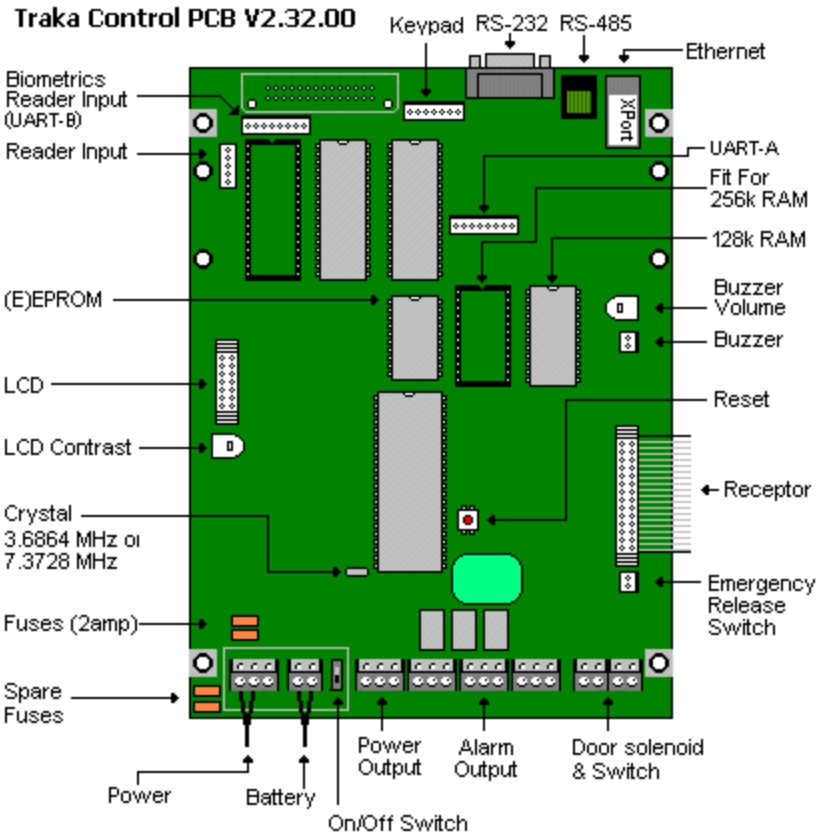
   If the serial number could not be read, ensure that no one is trying to access the locker and retry. Also ensure that when you inserted the item the LCD displayed "item not recognised" as this is the indication that the slot can detect the item ok.
10. Users may now access the system and remove the item as normal.

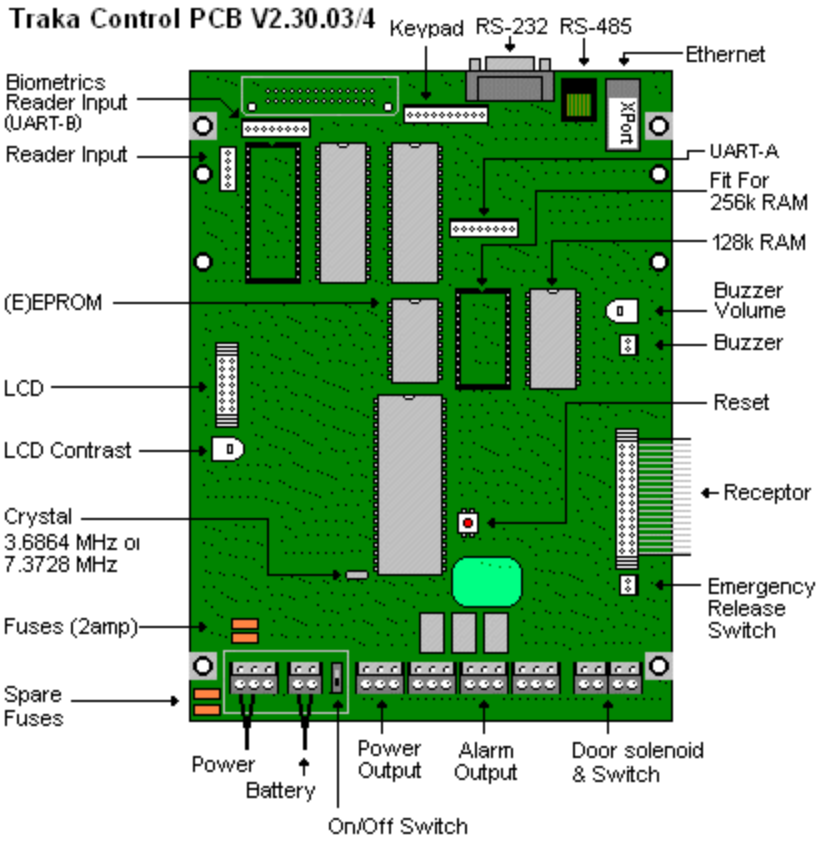
6 TRAKA HARDWARE

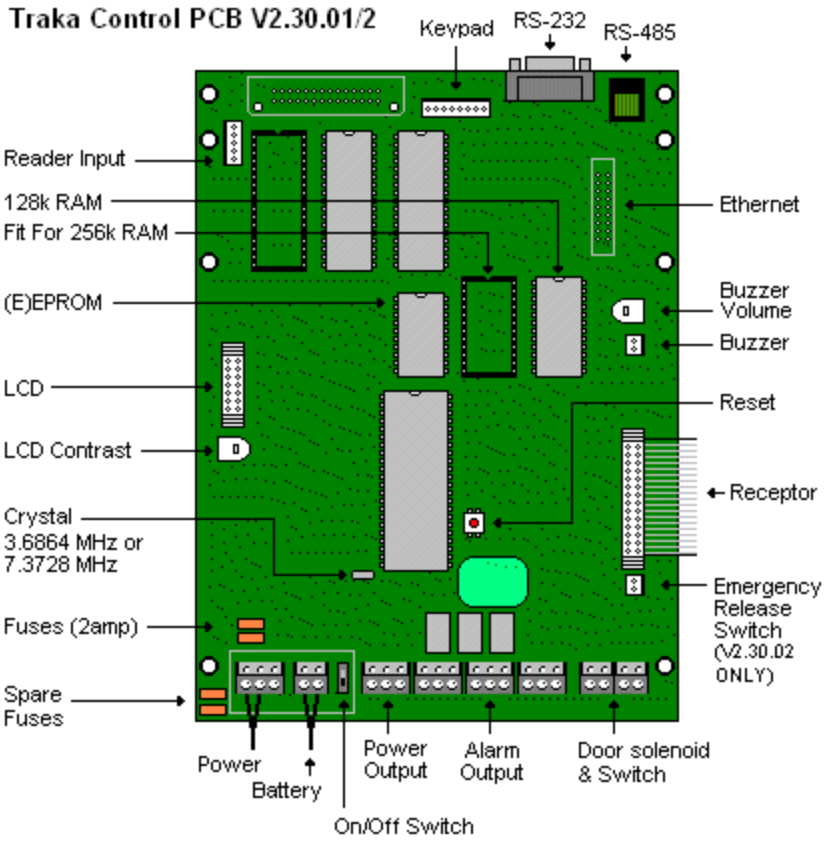
6.1 TRAKA CONTROL PCB

6.1.1 8BIT CONTROL PCB

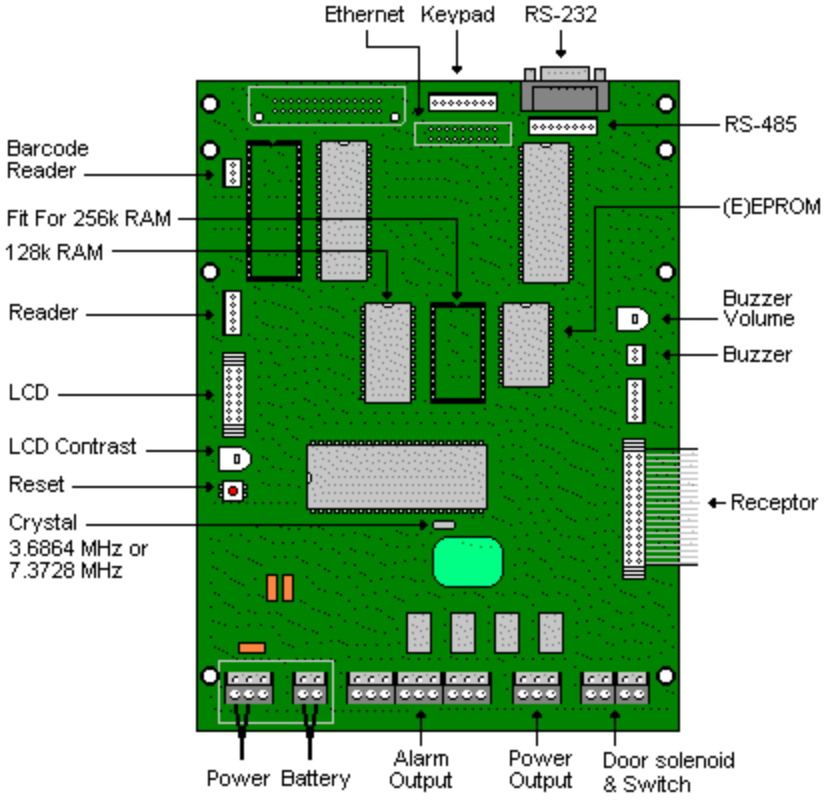
6.1.1.1 8BIT CONTROL PCB LAYOUT



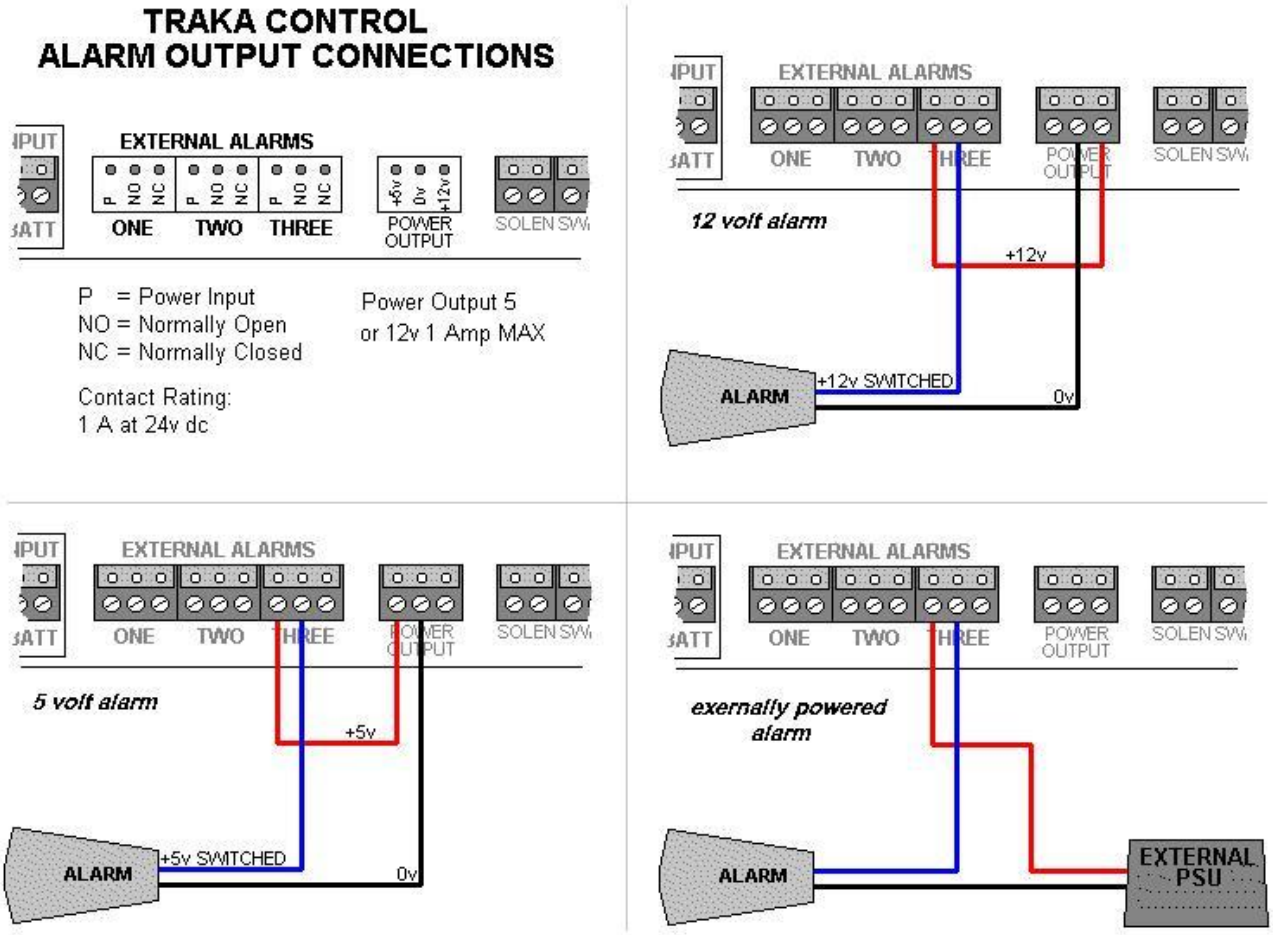




Traka Control PCB V2.20



6.1.1.2 8BIT CONTROL PCB ALARM OUTPUTS



NOTE: At no point should mains be wired into the Alarm Output

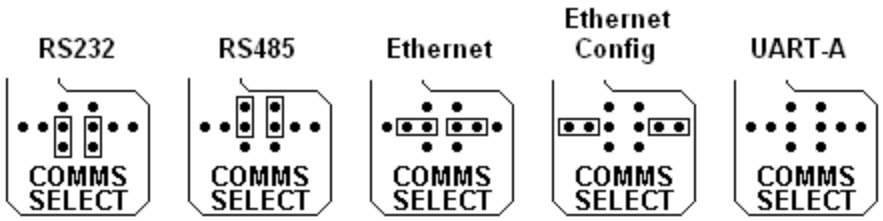
Alarm Output Functions in firmware version 6.06.18 and below...

1. Power Fail.
2. iFob forced from cabinet or unauthorised iFob taken.
3. Door left open or forced open.

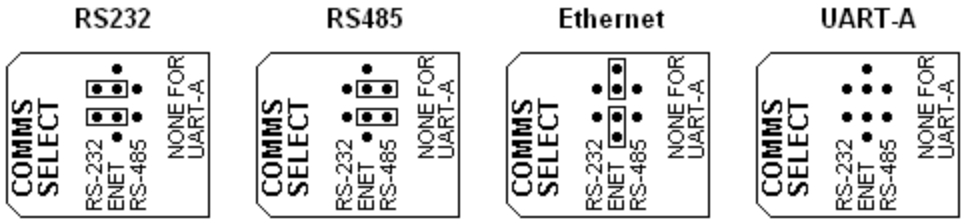
The Alarm Output Functions in firmware version 6.07.00 and above are configurable by the user. Please refer to the Configure Firmware section for more details.

6.1.1.3 8BIT CONTROL PCB COMMUNICATION JUMPER SETTINGS

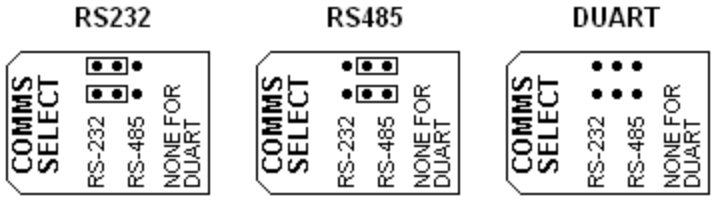
Traka Control PCB V2.30.04



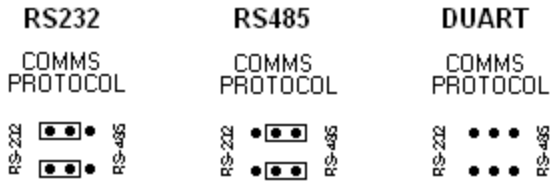
Traka Control PCB V2.30.03



Traka Control PCB V2.30.01-2



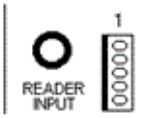
Traka Control PCB V2.20



6.1.1.4 8BIT CONTROL PCB READER JUMPER SETTINGS

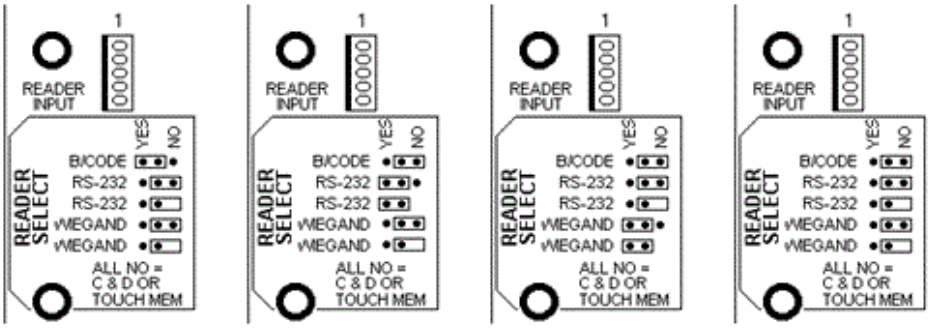
Traka Control PCB V2.30.01-4

PINOUTS



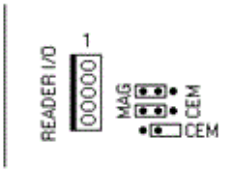
Pin 1 +12v
Pin 2 +5v
Pin 3 Data 1 / Data / Rx
Pin 4 0v
Pin 5 Data 0 / Clock

BARCODE **RS232** **WIEGAND** **CLOCK & DATA or TOUCH MEM**



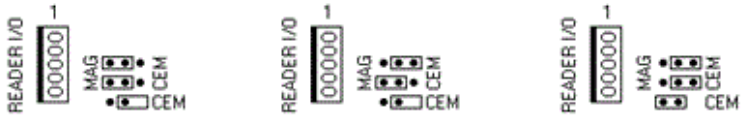
Traka Control PCB V2.20

PINOUTS

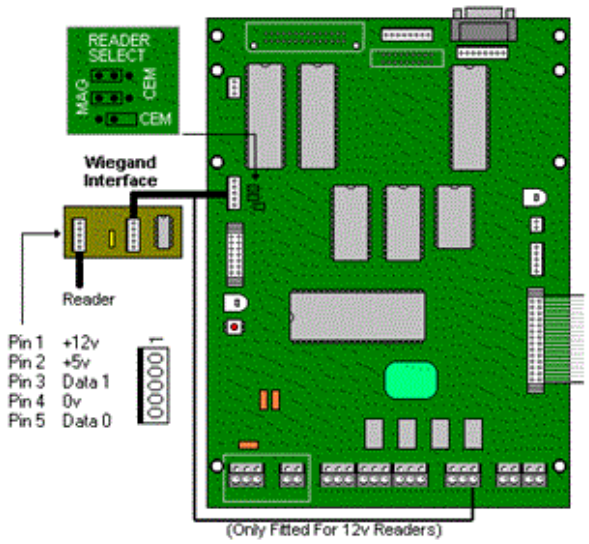


Pin 1
Pin 2 +5v / +12v
Pin 3 Data 1 / Data / Rx
Pin 4 0v
Pin 5 Data 0 / Clock

+5v CLOCK & DATA **+12v CLOCK & DATA** **+12v RS232**

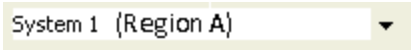


WIEGAND



6.1.1.5 REPLACING THE 8BIT CONTROL PCB

NOTE: Replacing the Control PCB may take up to half an hour to complete. Please ensure that any important keys are removed from the systems prior to the replacement, as it may be difficult to obtain the keys.

1. Load the Traka32 software by double clicking on the  icon.
2. Select the appropriate system from the 

drop down menu that you wish to work on.
3. Click on the  button.
4. Please refer to the Anti Static Precautions before working on the Traka system.
5. Using the **Master Key**, unlock the **Pod Lock**. The **Control Panel** is hooked in at the bottom and locked at the top. Carefully begin to remove the **Control Panel**.
6. You will see that there are several wires connected to the Printed Circuit Board (PCB) that are attached to the control panel. Determine which version of the Control PCB you have using the Control PCB Diagrams.
7. If you have **V2.20** of the **Control PCB** then...
    a. Disconnect the Battery.
    b. Disconnect the Power Supply.
8. If you have **V2.30.01 or above** of the **Control PCB** then...
    a. Set the On/Off switch to Off.
9. Carefully **disconnect any remaining wires** noting where and how they connect and completely remove the control panel.
10. Place the Control Panel on a suitable flat surface.
11. **Remove the four fixing screws** the hold the Control PCB in place and remove the Control PCB

    NOTE: There will be four fibre washers between the Control PCB and the Control Panel. Please put these in a safe place until needed.
12. Place the Control PCB on a flat surface and carefully **remove the EEPROM** from its socket and place it in the socket on the new Control PCB.

    NOTE: Please ensure that all the legs of the EEPROM are correctly located before firmly pushing the EEPROM in place.
13. Check that all the **Jumper Settings** are set correctly on the new Control PCB by copying the settings of the old Control PCB. Please ensure you check the Reader Select, Comms Select and ROM Select settings.
14. Place the new Control PCB back on the Control Panel ensuring the fibre washers are in place and secure with the four fixing screws.
15. Hook the **Control Panel** into the bottom of the **Pod**. Whilst holding the control panel, re-connect all the wires to the Control PCB.
16. If you have **V2.20** of the **Control PCB** then...
    a. Reconnect the Power Supply.
    b. Reconnect the Battery.
17. If you have **V2.30.01 or above** of the **Control PCB** then...

a. Set the On/Off switch to On.

18. Hold down the **#** key on the keypad. At the same time press and release the **Reset** button on the Control PCB.

19. **Press 2** to reset the systems memory.

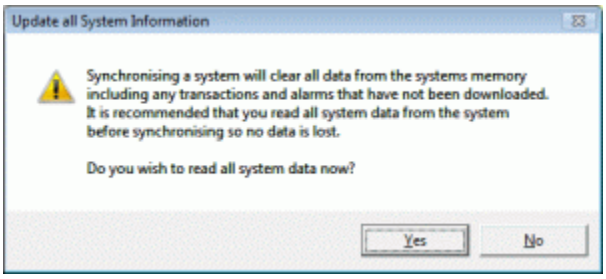
20. To reset, press the **#** key.

21. **Press *** to escape from the configuration menu.

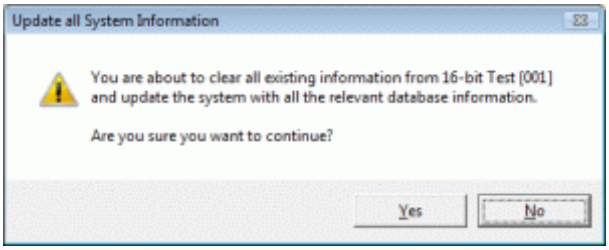
22. Close the **Control Panel** carefully into the **Pod** and lock with the **Master Key**.
The Control Panel should fit easily, if not check that no wires have become caught or trapped between the Control Panel and the Pod.

23. Please ensure nobody uses the system until the work is complete.

24. From the system viewer of Traka32, right click over the picture of the pod again and click on **Synchronise System**.



25. Click on **No** first.



26. Then click on **Yes**.

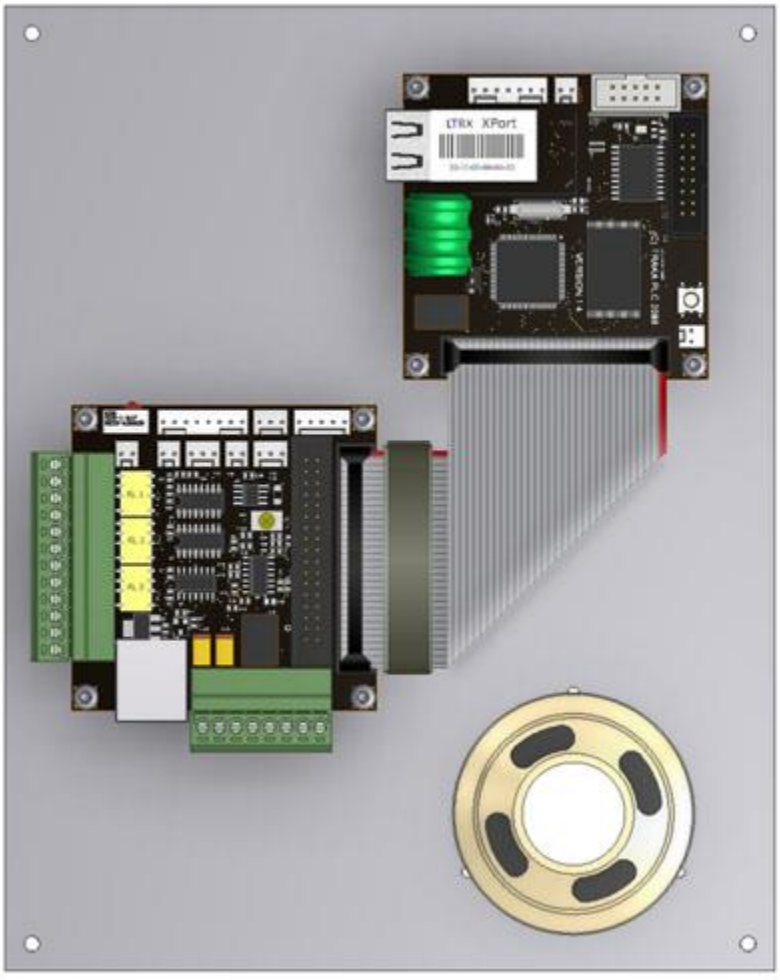
27. Please refer to the Testing section for further details on fully testing the system.

6.1.2 16BIT CONTROL PCB

6.1.2.1 16BIT CONTROL PCB OVERVIEW

The 16bit Control Board now comes as 2 separate PCB's. There is the main Control PCB that contains the 16bit processor, LCD & Keypad interfaces, Flash (program memory), SD-RAM (data memory) and Ethernet communications. There is also an I/O Interface PCB that contains the RS-232 & RS-485 Communications, Reader interfaces, Speaker interface, Emergency Release interface, 3 x Relay interfaces, PSU interface, Battery interface, Door interfaces and Receptor interface. The 2 PCB's link together with a short 34 way ribbon cable.

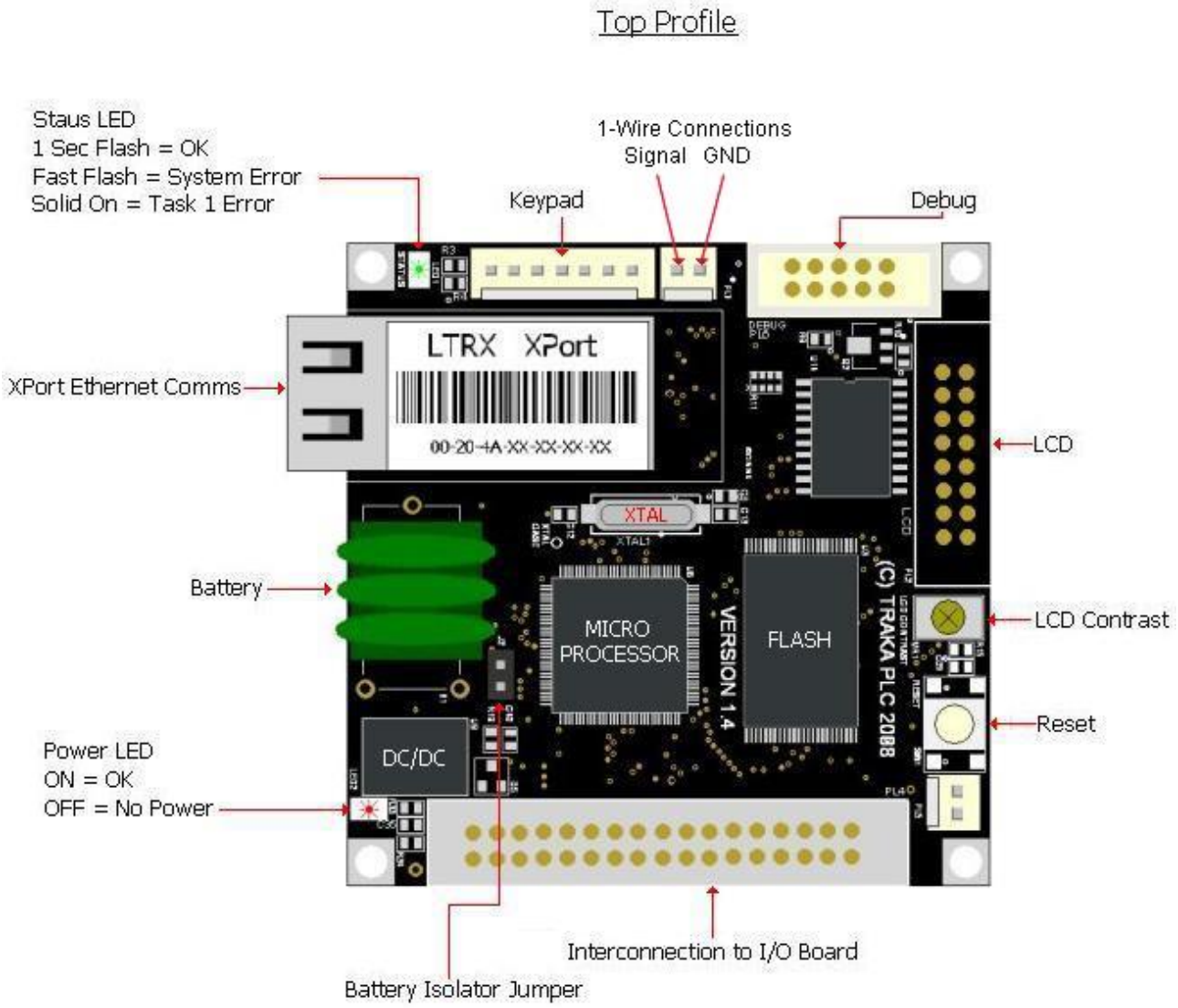
Initially the 2 PCB's will be mounted on a metal bracket which is the same size as the existing 8bit Control PCB. This will allow the new Control PCB and I/O Interface PCB to be fitted into any existing Traka Pod. In the future we will re-design the Traka Cabinets and Pods to be smaller.



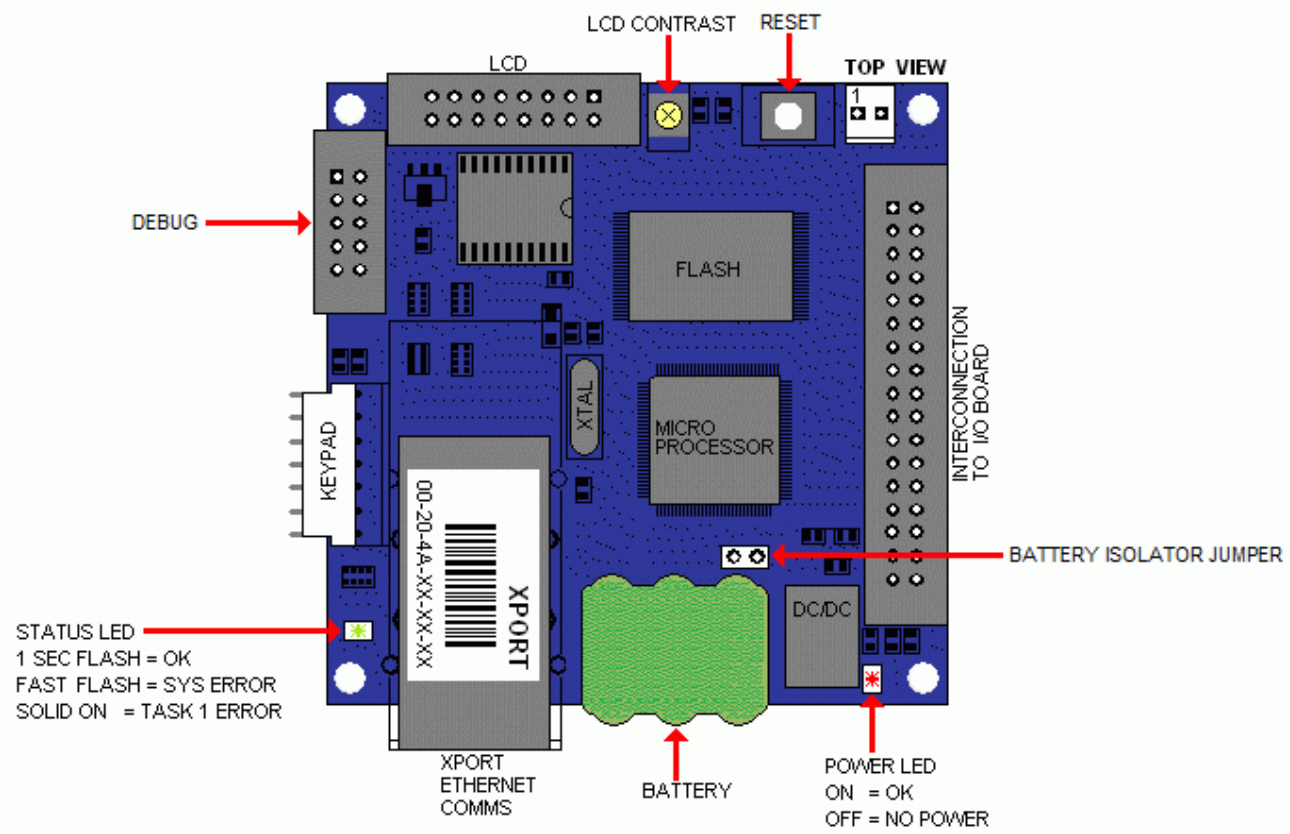
6.1.2.2 16BIT CONTROL PCB LAYOUT

Also view 16bit_I/O_PCB_Layout.htm.

Version 1.4.0 (Black)



Version 1.3.0 (blue)



Battery Isolator

The battery isolator jumper **must** be connected so as the database (users, iFobs, events etc) can be retained in RAM (random access memory) upon removal of operating system power.

Memory

The 16 bit Control PCB hardware includes:

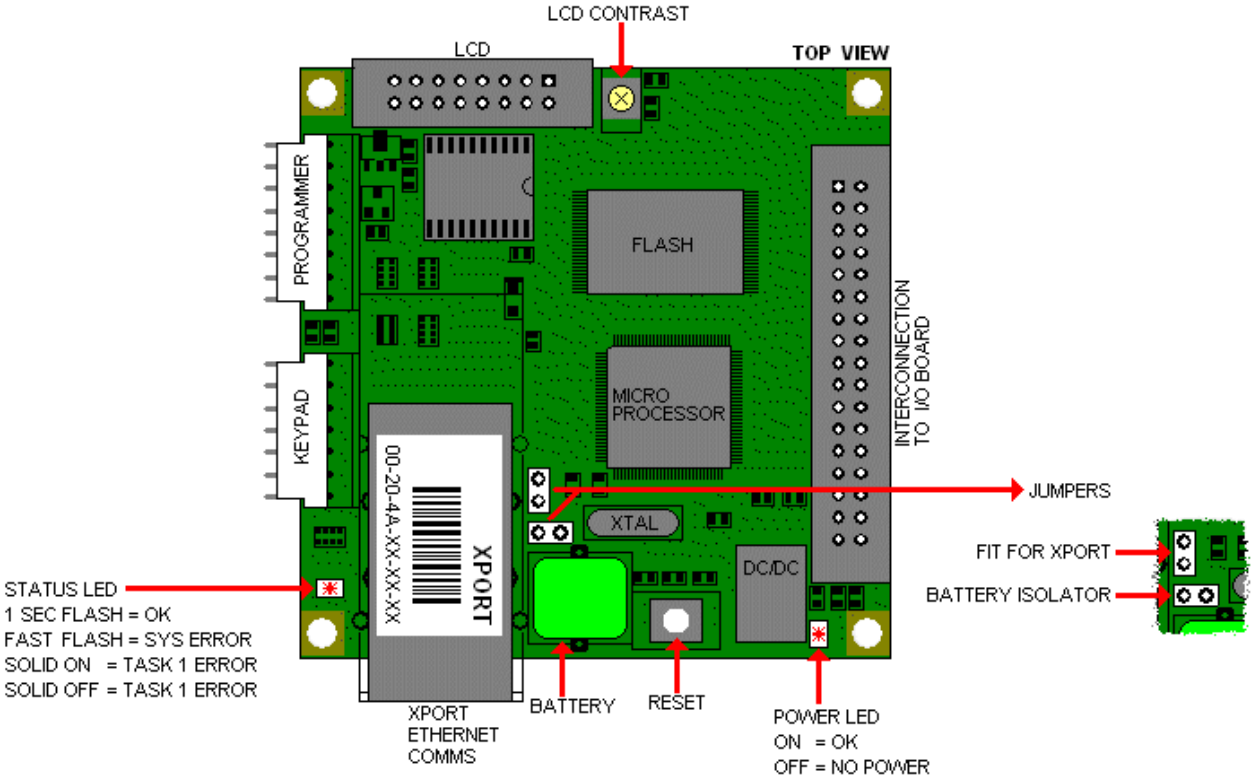
- 512K Words of Flash Program Memory (that's 1M bytes or 8M bits)
- 8M Words of SD-RAM Data Memory (that's 16M bytes or 128M bits)

We can increase the size of the Flash and SD-RAM in the future simply by fitting bigger memory chips. This does mean replacing the Control PCB but the reason for fitting smaller memory values at the moment is to keep the cost down.

Status LED's: The new hardware includes 2 status LED's to show Power Status and Processor status.

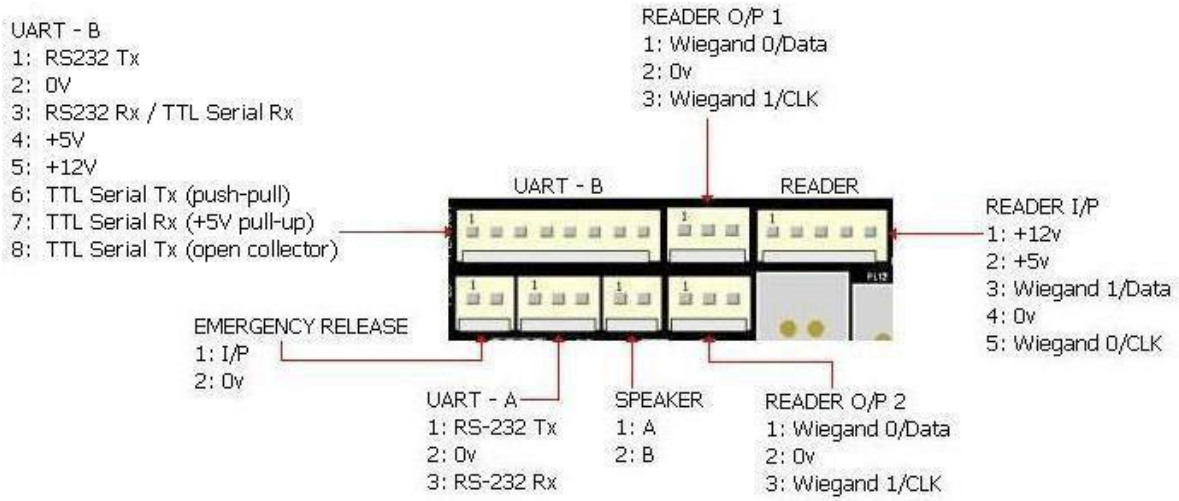
Control PCB Serial Number (CPSN): The new Control PCB will have an electronic serial number. This will allow us to track what Control PCB's are fitted to what system. This will also be used as security for enabling the cost options that are available such as Mileage Logging, Key Booking etc.

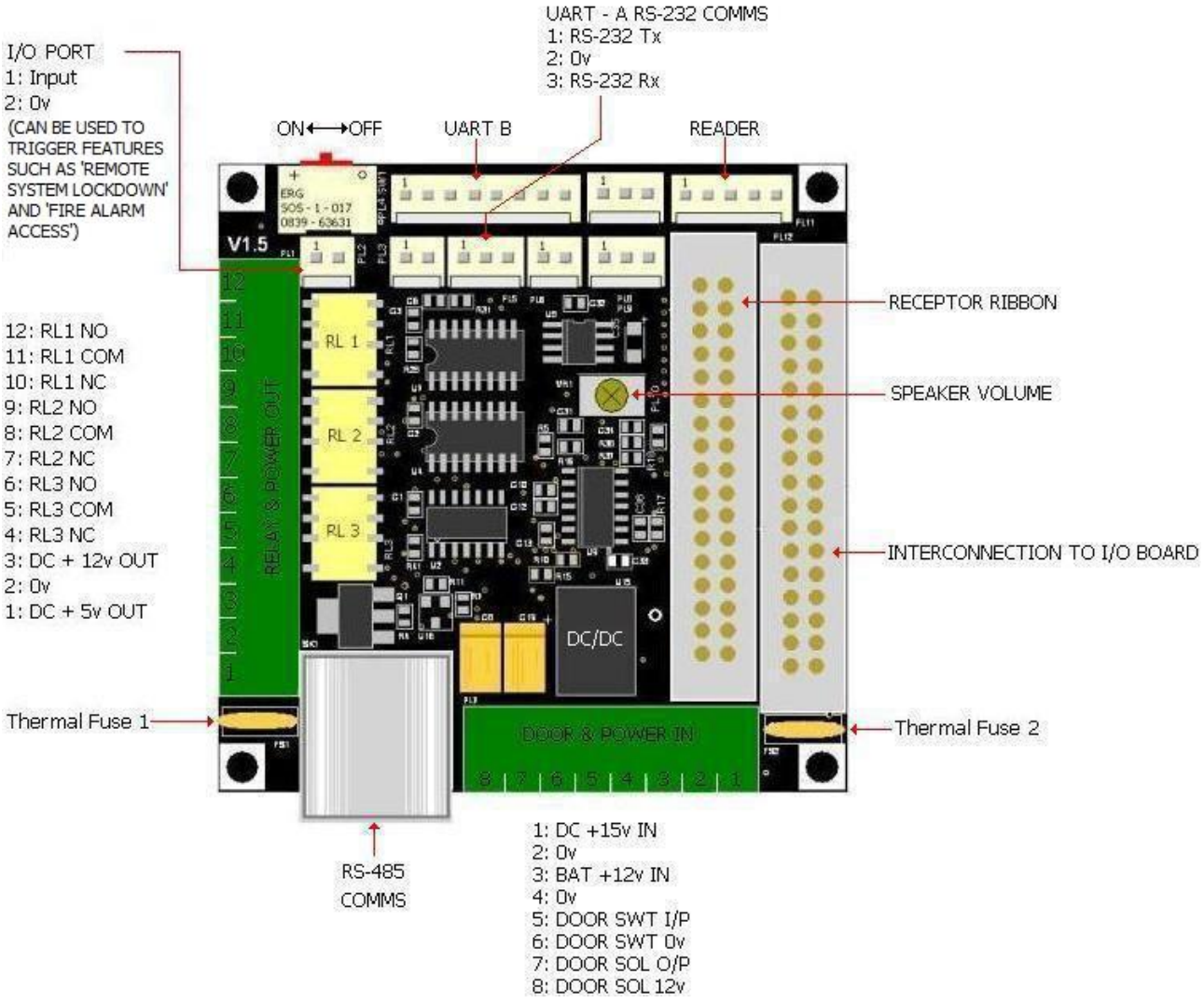
Version 1.2.0 (green)



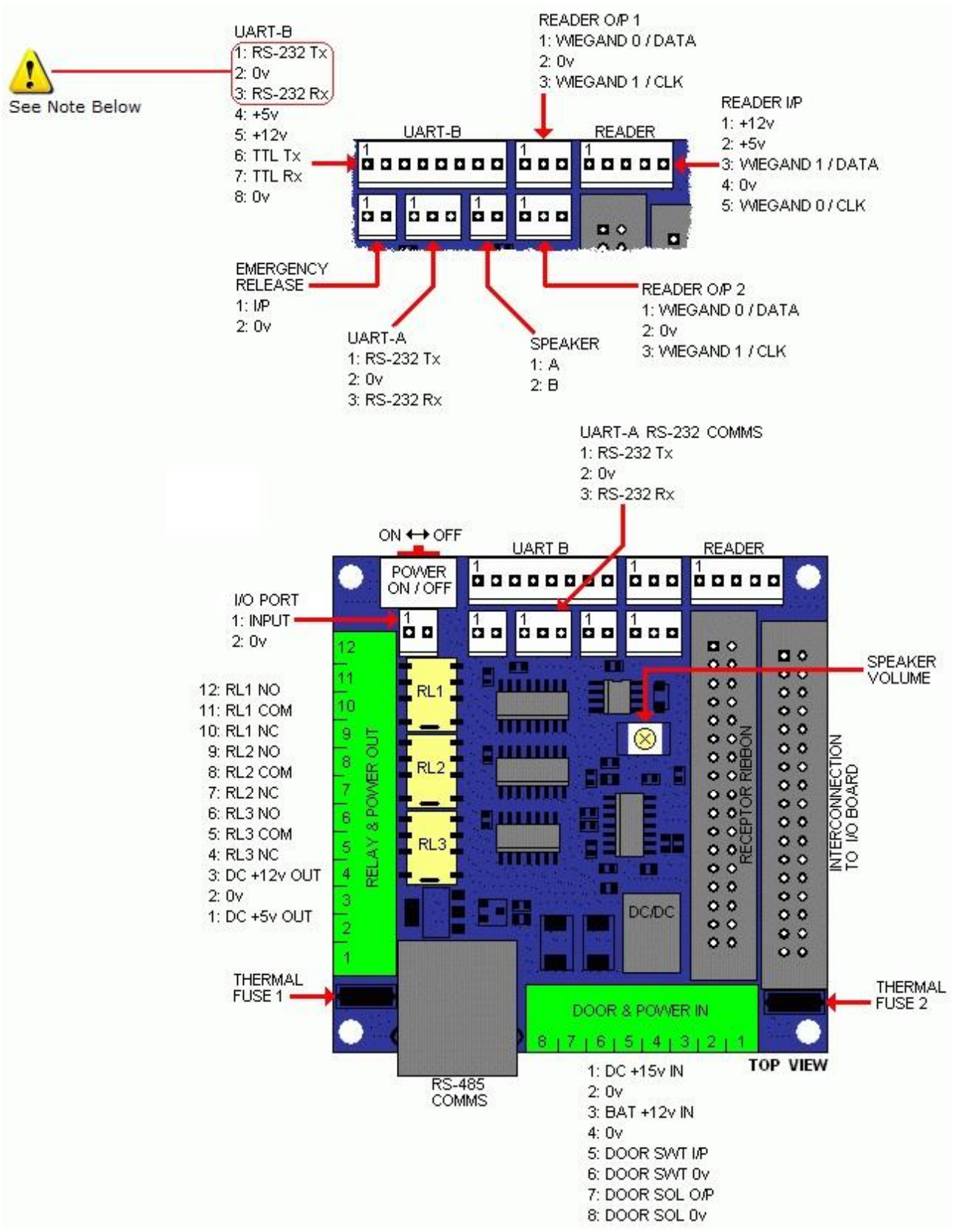
6.1.2.3 16BIT I/O PCB LAYOUT

Version 1.5.0 (Black)





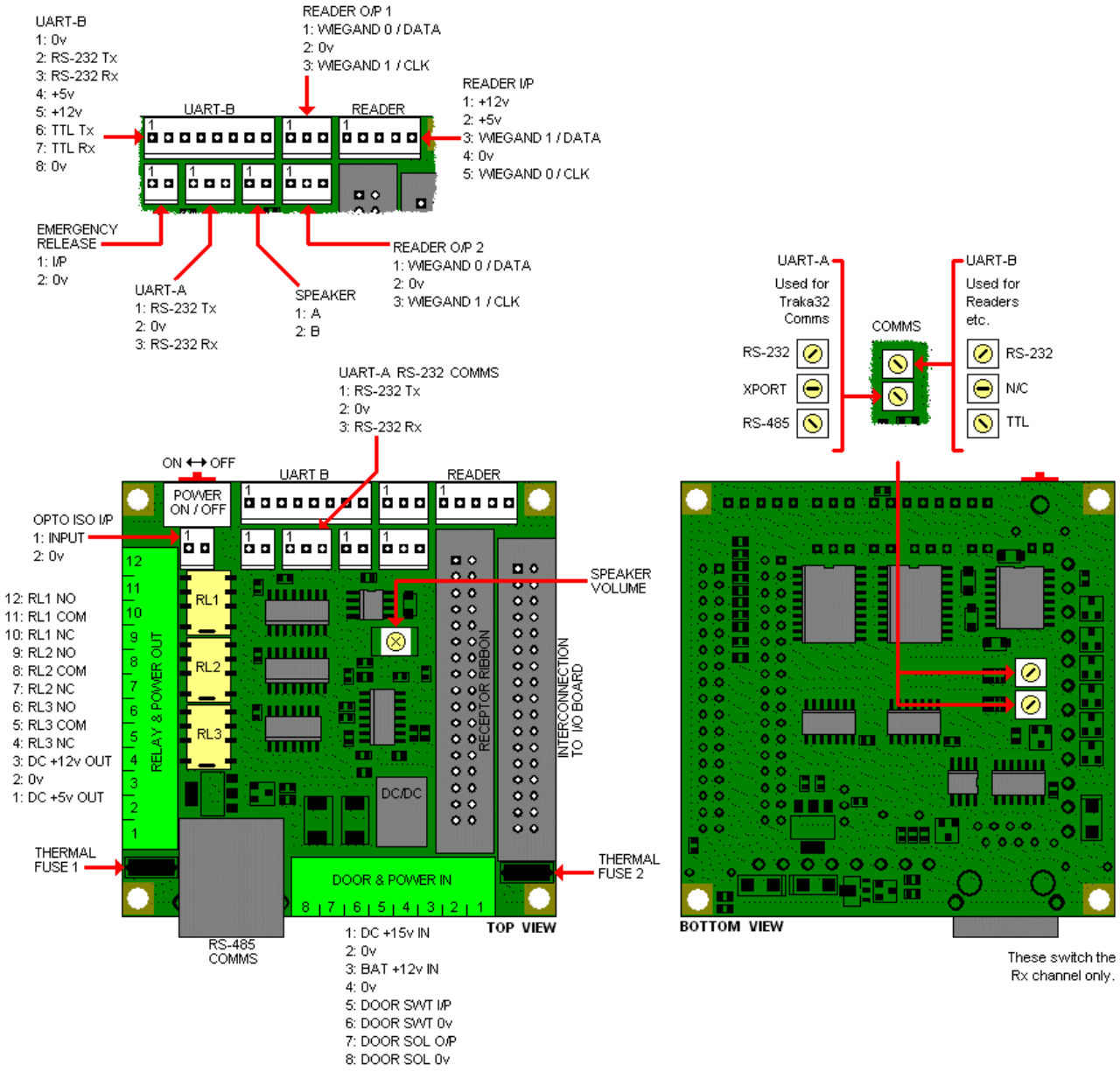
Version 1.3.0 (blue)



NOTE: Version 1.3.0 UART-B pins 1 and 2 (RS-232 TX and 0v) have been switched (compared with Version 1.2.0) so as the same RS232 cable can now be used for UARTA *and* UARTB.

NOTE: Notice that no bottom view of Version 1.3.0 is provided here, this is because the communication selector pots that previously occupied the PCB underside have now been completely removed. The 16-bit system now auto-detects the communications protocol used so there are no controls to worry about setting!

Version 1.2.0 (green)



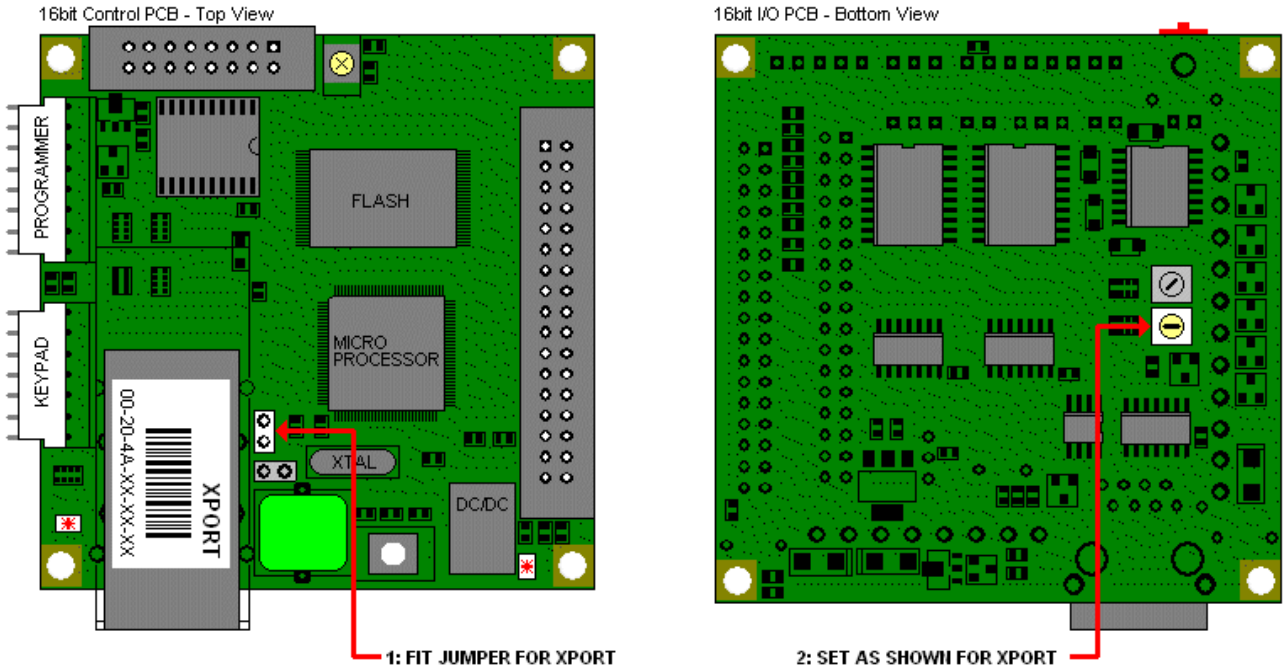
6.1.2.4 16BIT CONTROL PCB COMMUNICATION SETTINGS

Version 1.3.0 (blue) & Version 1.4.0 (Black)

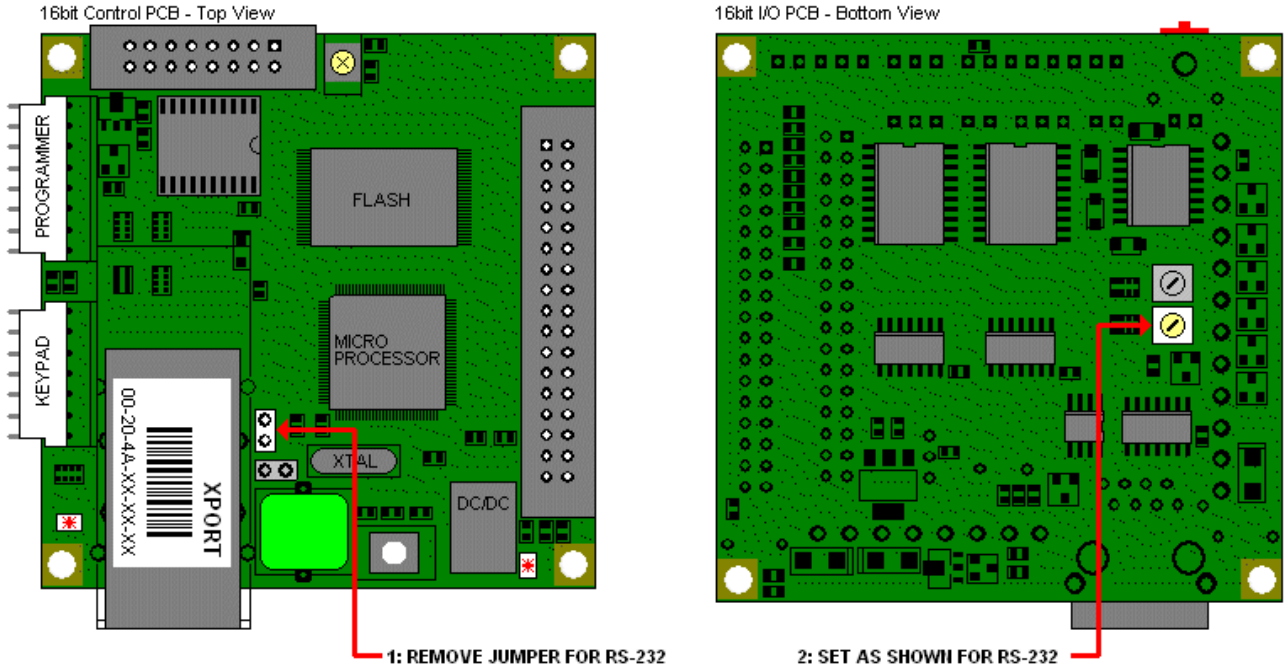
A major improvement over Version 1.2.0 is the communication settings. **The communication selector pots that previously occupied the PCB underside have now been completely removed**. The 16bit system now auto-detects the communications protocol used so there are no controls to worry about setting!

Version 1.2.0 (green)

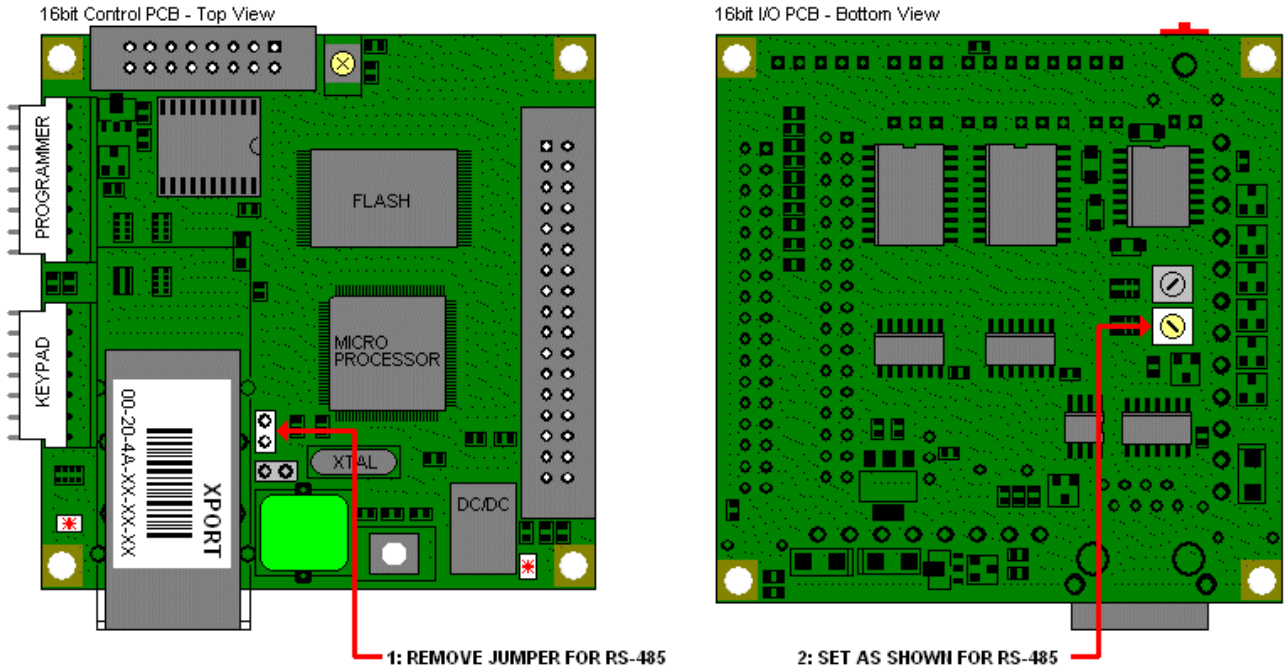
XPort Ethernet



RS-232



RS-485

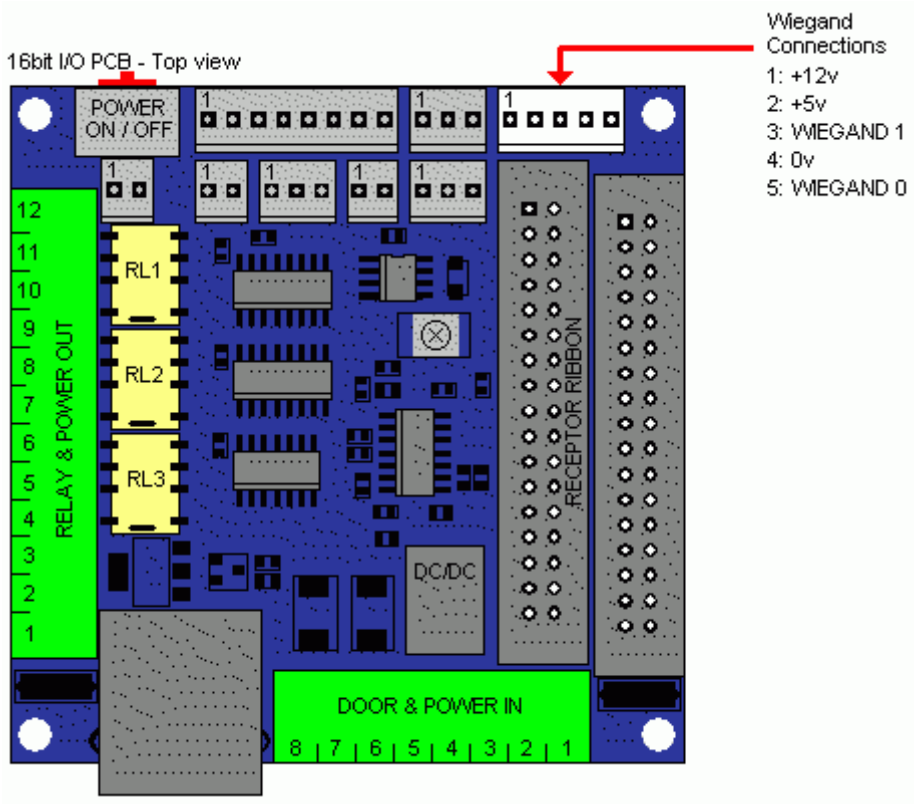


6.1.2.5 16BIT CONTROL PCB READER CONNECTIONS

The 16bit Control PCB does not have any Jumper settings unlike the 8bit Control PCB for the various reader settings. Different connectors are used for the various readers as follows...

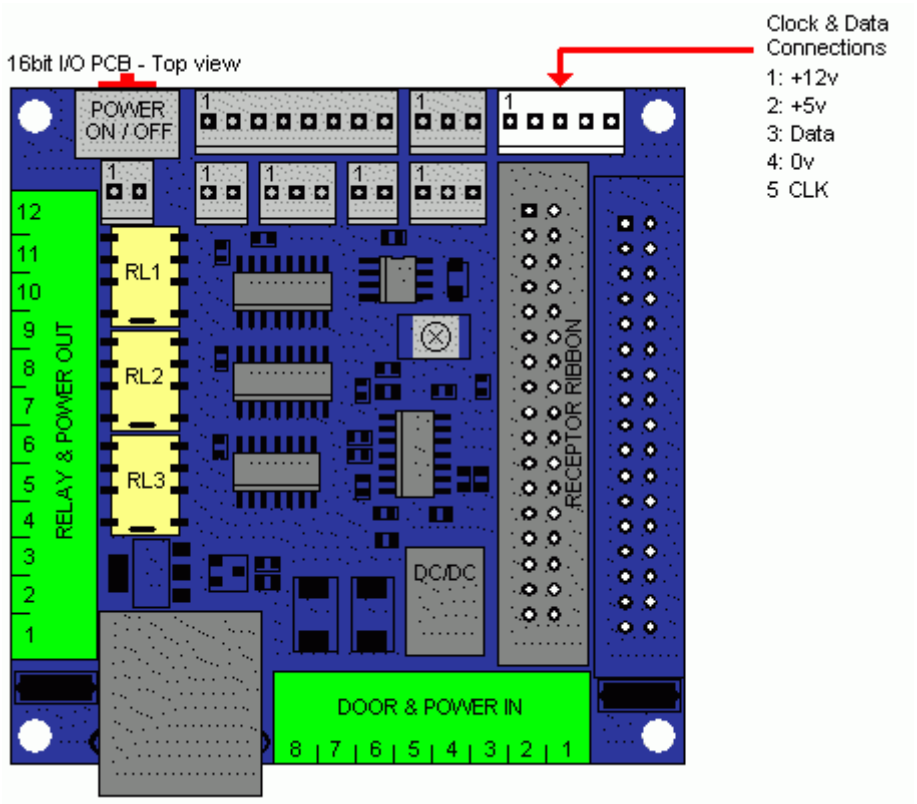
Wiegand

The Wiegand card reader connections are the same for Versions 1.2.0,1.3.0 and 1.4.0



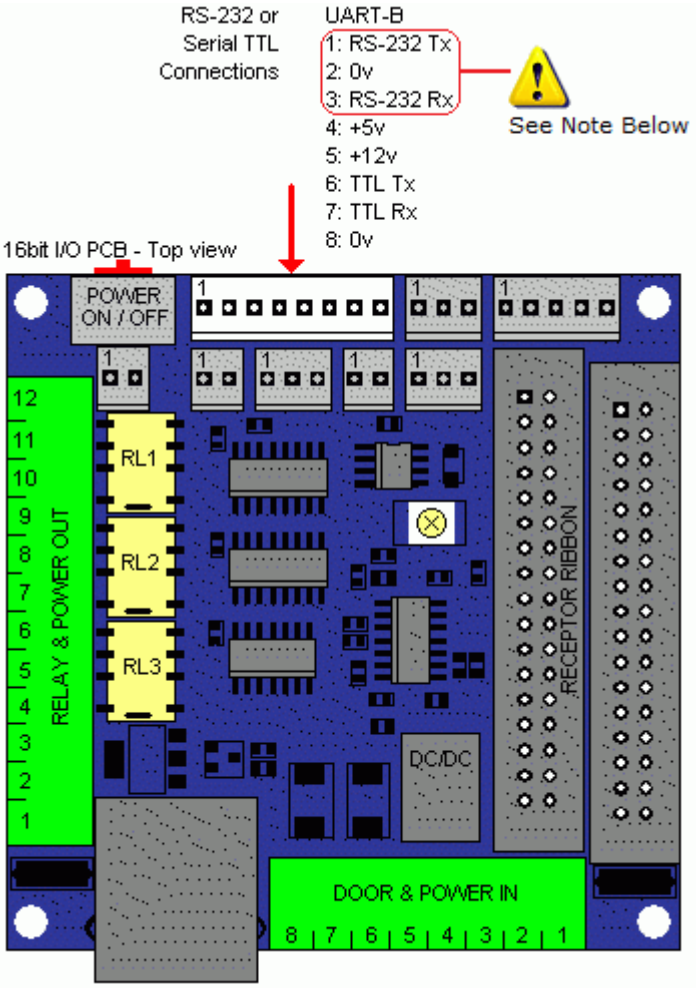
Clock & Data

The Clock & Data card reader connections are the same for Versions 1.2.0,1.3.0 and 1.4.0



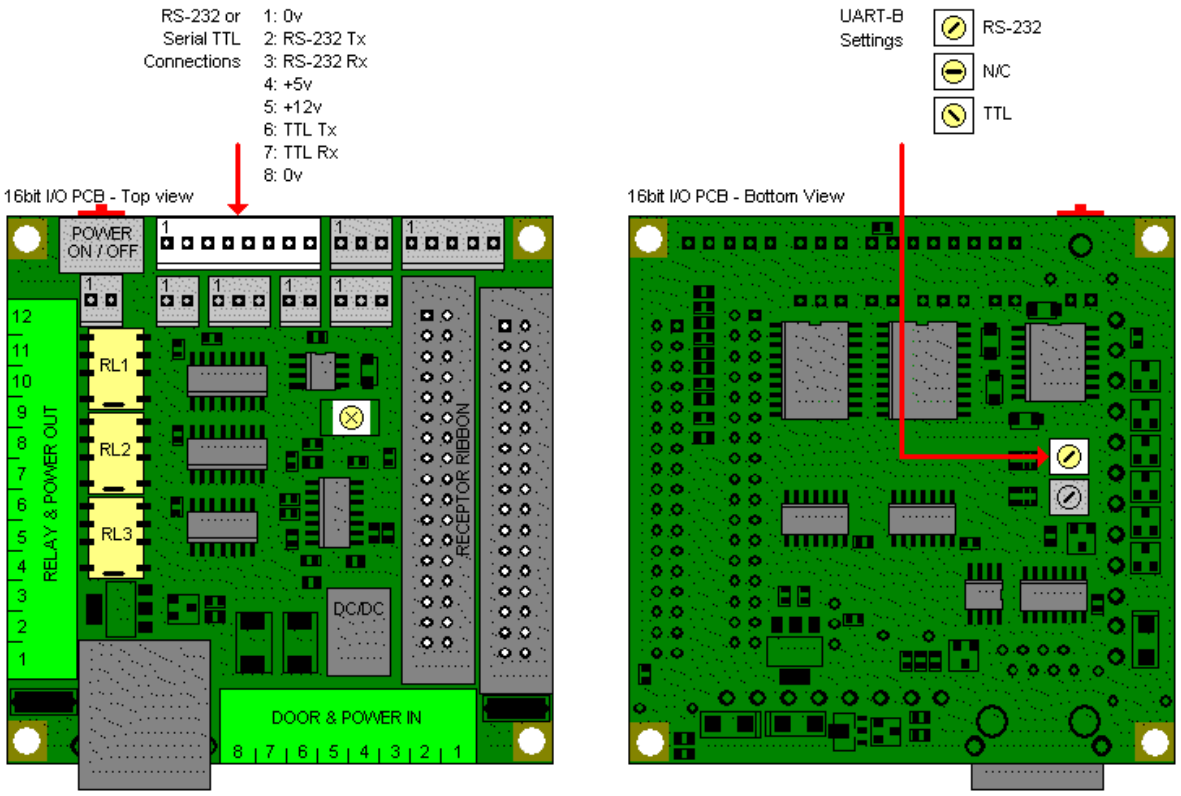
RS-232 / TTL

Version 1.3.0 (blue)



NOTE: Version 1.3.0 UART-B pins 1 and 2 (RS-232 TX and 0v) have been switched (compared with Version 1.2.0) so as the same RS232 cable can now be used for UARTA *and* UARTB.

Version 1.2.0 (green)

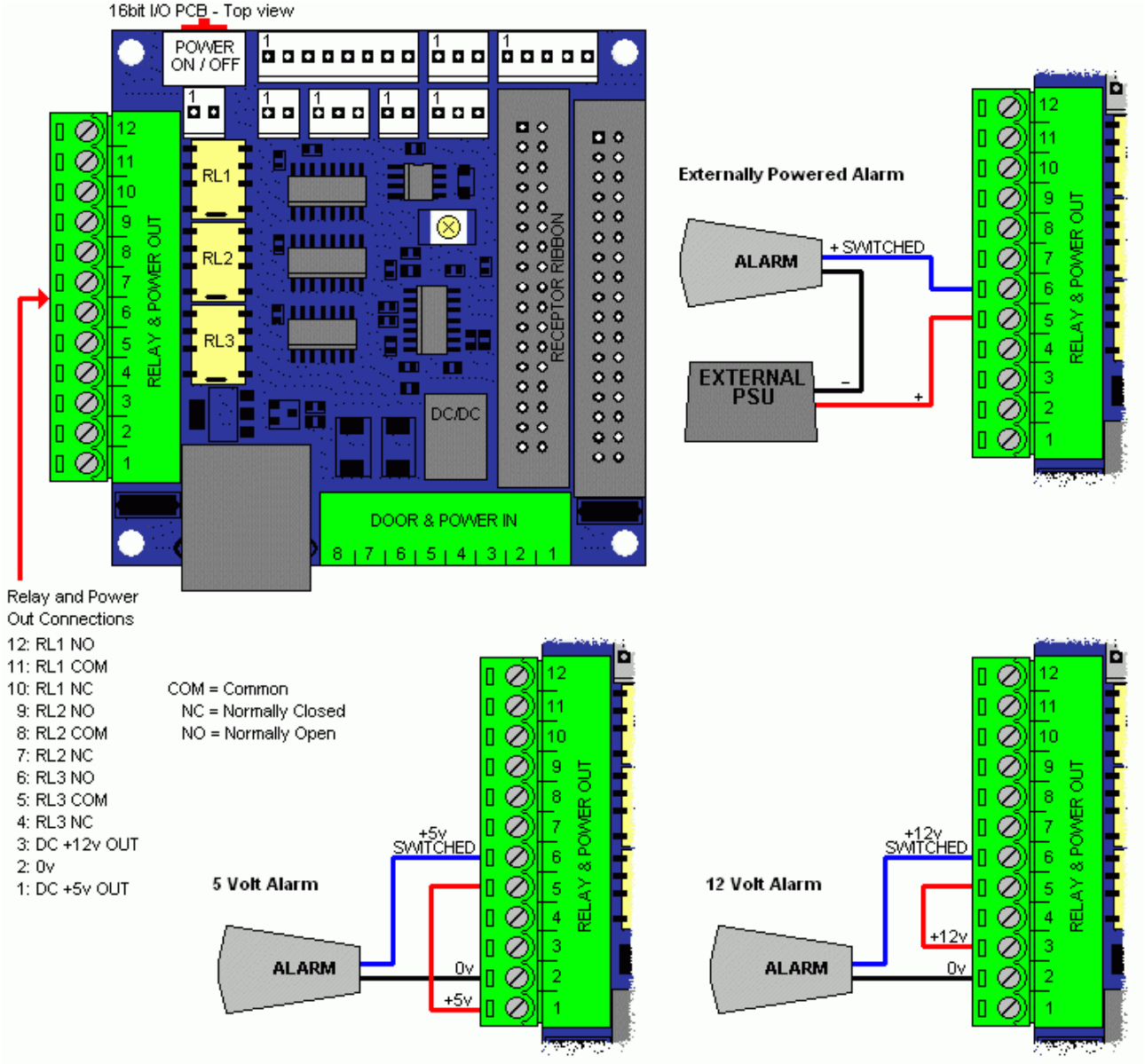


Barcode

The barcode decoder chip that was fitted to the 8bit Control PCB is no longer used. Traka will use Barcode reader with either an RS-232 or Wiegand output temporarily to overcome this problem and will look into the firmware required to accept TTL signals directly from barcode readers and decode them directly.

6.1.2.6 16BIT I/O PCB ALARM OUTPUTS

Alarm Relay Connections



NOTE: At no point should mains be wired into the Alarm Relay Output.

Relay Contact Rating

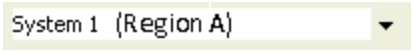
- 1A at 30V DC

Power Output

- +5V 1A (Regulated) or
- When running on mains: +15V 1.7A
  When running on battery: +12V 1A

6.1.2.7 REPLACING THE 16BIT CONTROL PCB

NOTE: Replacing the 16bit Control PCB may take up to half an hour to complete. Please ensure that any important keys are removed from the systems prior to the replacement, as it may be difficult to obtain the keys.

1. Load the Traka32 software by double clicking on the  icon.
2. Select the appropriate system from the 

drop down menu that you wish to work on.
3. Click on the  button.
4. Please refer to the Anti Static Precautions before working on the Traka system.
5. Using the **Master Key**, unlock the **Pod Lock**. The **Control Panel** is hooked in at the bottom and locked at the top. Carefully begin to remove the **Control Panel**.
6. You will see that there are several wires connected to the 16bit Control PCB and 16bit I/O PCB that are attached to the control panel.
7. Set the On/Off switch to OFF on the 16bit I/O PCB.
8. Carefully **disconnect any wires** from both PCB's noting where and how they connect and completely remove the control panel.
9. Place the Control Panel on a suitable flat surface.
10. **Remove the four M3 x 12mm hex fixing screws** that hold the 16bit Control PCB in place.
11. Check that the Communication Settings are set correctly on the new 16bit Control PCB by copying the settings from the old 16bit Control PCB. A **jumper** is required on the top side of the PCB if the XPORT device is required for Ethernet communications.
12. If not already connected, connect the Secondary Battery Backup Isolator jumper**.**

    NOTE: It is highly recommended that when spare 16bit Control PCB's are transported or stored that the Battery Backup Isolator Jumper is removed. This will prolong the life of the battery.
13. Place the new 16bit Control PCB back on the Control Panel and secure with the **four fixing screws**.
14. Re-connect the short **34 way ribbon cable** from the 16bit bit I/O PCB to the 16bit Control PCB.
15. Hook the **Control Panel** into the bottom of the **Pod**. Whilst holding the control panel, carefully **re-connect the wires** to the **16bit Control PCB** and **16bit I/O PCB**. Refer to the 16bit Control PCB Layout and 16bit I/O PCB Layouts for their respective connection diagrams.
16. Set the **On/Off switch** on the 16bit I/O PCB to **On**.
17. Check the Power LED comes on and after a few seconds and the Status LED starts to flash. If there is no Power LED, set the On/Off switch on the 16bit I/O PCB to Off and re-check all of the connections.

    NOTE: The status LED should flash when the application firmware is loaded and running. If there is no application firmware loaded, then the status LED will be solid on and the LCD will show:

    In this case a 16 bit firmware upgrade will be required. Contact your distributor for more information.

    Because the **16bit firmware is generic**, the 16bit Control PCB will usually be supplied with the application **firmware already loaded**.

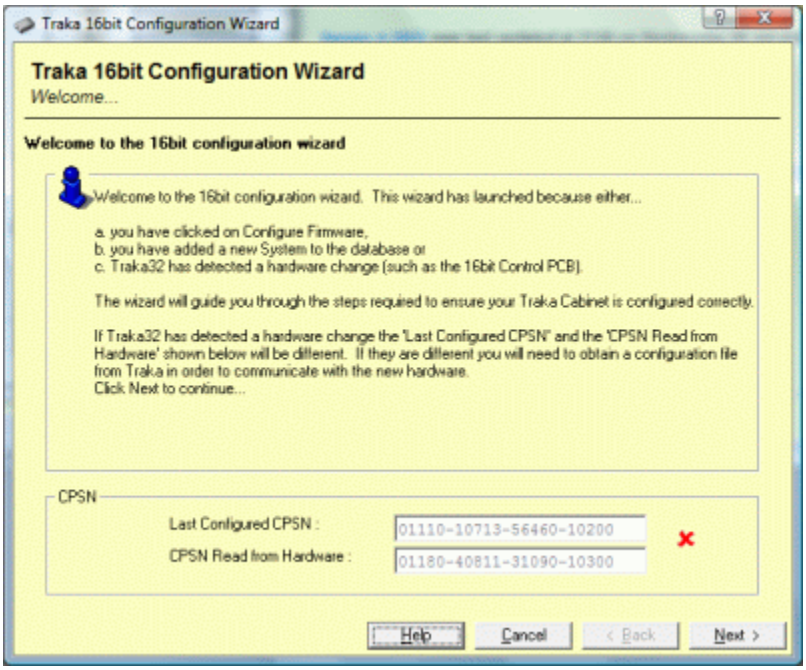
18. Close the **Control Panel** carefully into the **Pod** and lock with the **Master Key**.
    The Control Panel should fit easily, if not check that no wires have become caught or trapped between the Control Panel and the Pod.

19. Check the **LCD** is **On** and scrolling with the date and time displayed.

    NOTE: It is more than likely that the date and time displayed will be incorrect. This should be of no concern at this stage.

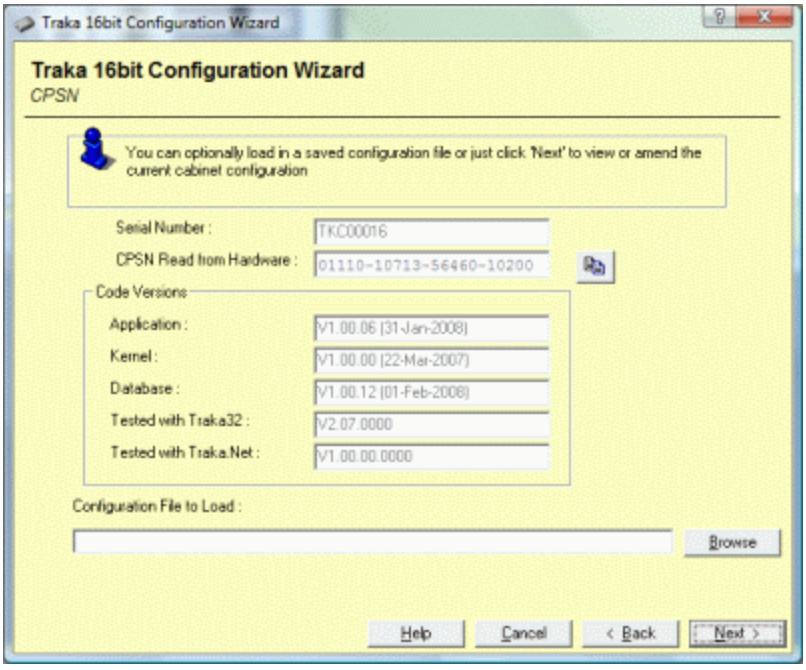
20. The new 16bit Control PCB is required to be registered to the existing Traka database with a **configuration file**. Load the 16bit Configure Firmware Wizard from the Traka 32 software.

21. The following **16bit Configuration Wizard** will be displayed.



22. Click on **Next**.

23. The CPSN window is displayed confirming the Serial Number, CPSN Read from Hardware, the Hardware and Code versions and in addition the Traka32 version the firmware was tested with.



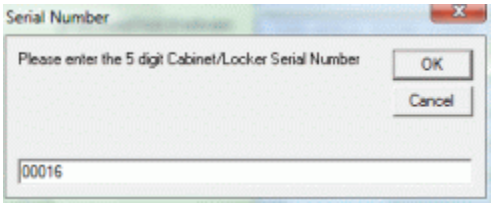
If you do not already have the correct configuration file you will need to contact your distributor quoting the **CPSN Read from Hardware**. The distributor will then be able to e-mail you with a configuration file for your hardware.

TIP: Click the  button to **copy** the CPSN to the clipboard for pasting into a file or email.

24. Once you have obtained the configuration file from Traka or your distributor, **save** it to the machine from which you wish to load it.

25. Click **browse** to search for the configuration file.

26. Enter the **5 digit serial number** of the Traka system (excluding TKC,TIL etc).



27. Click OK and browse to the location the configuration file was saved to. Only configuration files matching that of the entered serial number will be available for selection.

    The configuration file name is structured as follows…

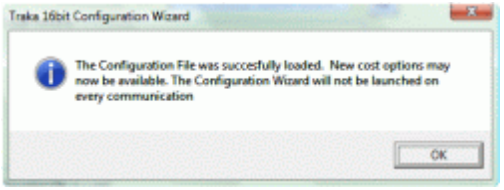
    <Serial Number> - <CPSN Number> - <Firmware Version>.TKCcfg

    For example, for a system with a serial number TKC12345, a CPSN of 01041006164704010200 and a firmware version of 1.00.00, the following file is required:

    12345 - 01041006164704010200 - 010000.TKCcfg

28. When you have selected the path to the configuration file, click on **Next**.

    If the configuration file was correct a message will be displayed indicating the hardware will be licensed to the database and any cost options will become available. A message is displayed indicating the file has been successfully loaded.



    NOTE: This indicates it has been loaded into the Traka32 database only at this stage and not yet applied to the cabinet.

    If the configuration file was incorrect, check that you have the correct file via the file name and try again. An incorrect file may be may be because…

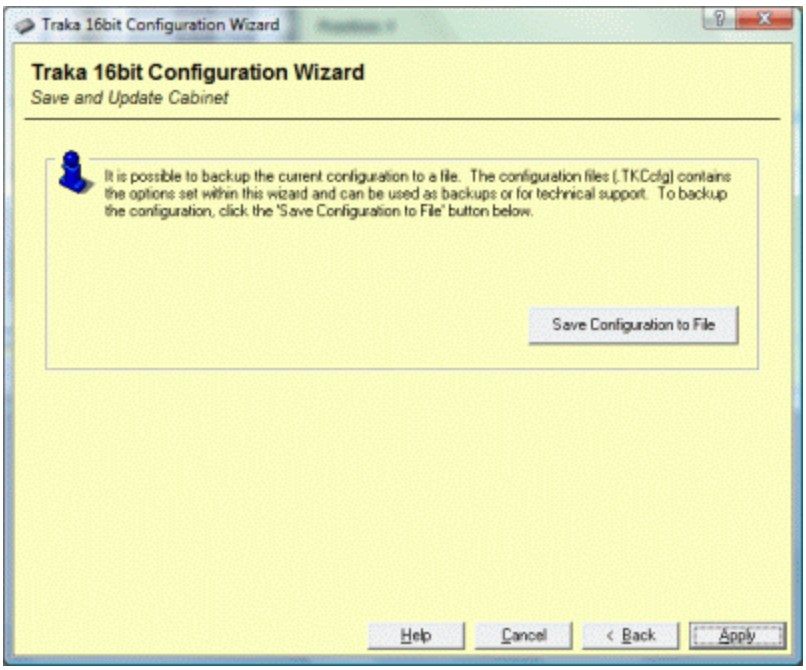
    a. The CPSN did not match,

    b. The Hardware Key did not match or,

    c. The Firmware Version did not match.

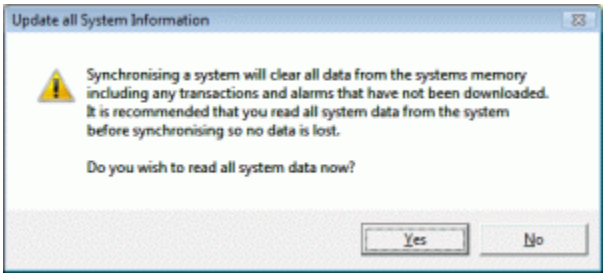
29. Follow the wizard through, checking ALL the settings and amend as required. For details on the various settings, please refer to the Firmware Options & Settings section.

30. Finally click on **Apply** to load the configuration into the cabinet.

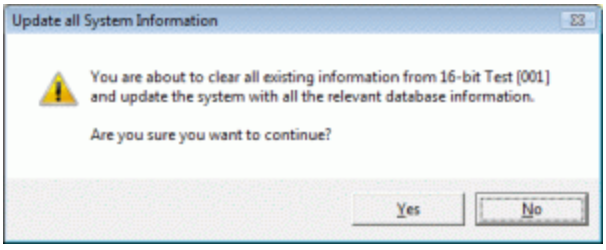


If you wish you may also save the current configuration (with any changes) to a File. Click on Save Configuration to File to do so and provide a suitable name for the file perhaps indicating any specific options that it contains.

31. Now that the new 16bit Control PCB's CPSN has been registered, you will be able to communicate as normal.
32. From the system viewer of Traka32, right click over the picture of the pod and click on **Synchronise System** to restore the database.



33. Click on **No** first.



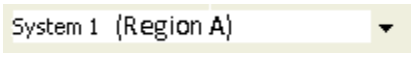
34. Then click on **Yes**.

Please refer to the Testing section for further details on fully testing the system.

6.1.2.8 REPLACING THE 16BIT I/O PCB

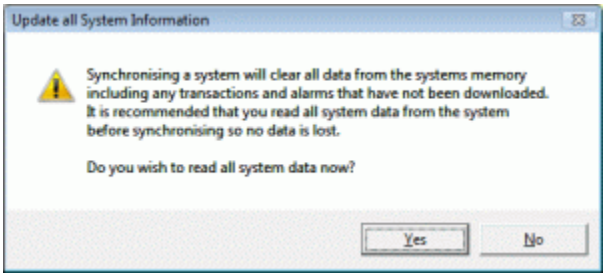
NOTE: Replacing the 16bit I/O PCB may take up to half an hour to complete. Please ensure that any important keys are removed from the systems prior to the replacement, as it may be difficult to obtain the keys.

NOTE: The small secondary backup battery (located on the 16bit Control PCB) can retain the data held in memory for only 30 minutes. After this time the data will be lost for good. Therefore it is more important than ever to complete a 'Read All System Data' prior to servicing a 16bit Traka system.

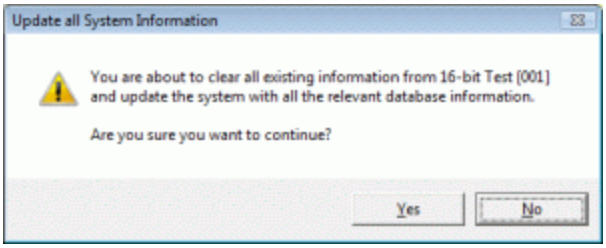
1. Load the Traka32 software by double clicking on the  icon.
2. Select the appropriate system from the 

drop down menu that you wish to work on.
3. Click on the  button.
4. Please refer to the Anti Static Precautions before working on the Traka system.
5. Using the **Master Key**, unlock the **Pod Lock**. The **Control Panel** is hooked in at the bottom and locked at the top. Carefully begin to remove the **Control Panel**.
6. You will see that there are several wires connected to the 16bit Control PCB and 16bit I/O PCB that are attached to the control panel.
7. Set the **On/Off switch** to **Off** on the 16bit I/O PCB.
8. Carefully **disconnect any wires** from both PCB's noting where and how they connect and completely remove the control panel.
9. Place the Control Panel on a suitable flat surface.
10. **Remove the four M3 x 12 hex fixing screws** that hold the 16bit Control PCB in place.
11. Check that the Communication Settings are set correctly on the new 16bit I/O PCB by copying the settings from the old 16bit I/O PCB. The Traka 32 communications **switch setting** is on the **bottom side** of the PCB.
12. If an RS232 reader or other serial peripheral device is using UART B, then ensure the UARTB **switch setting** is also set correctly. This is located on the bottom side of the PCB.
13. Place the new **16bit I/O PCB** back on the Control Panel and secure with the **four fixing screws**.
14. Re-connect the short **34 way ribbon cable** from the 16bit I/O PCB to the 16bit Control PCB.
15. Hook the **Control Panel** into the bottom of the **Pod**. Whilst holding the control panel, carefully re-connect the wires to the 16bit Control PCB and 16bit I/O PCB. Refer to the 16bit Control PCB Layout and 16bit I/O PCB Layouts for their respective connection diagrams.
16. Set the **On/Off switch** on the 16bit I/O PCB to **On**.
17. Check that Power LED comes on and after a few seconds that the Status LED starts to flash. If there is no Power LED, set the **On/Off switch** to **Off** and **re-check all of the connections** before trying again.
18. Ensure the **LCD is scrolling** with the date and time displayed.
19. Close the **Control Panel** carefully into the **Pod** and lock with the **Master Key**.
    The Control Panel should fit easily, if not check that no wires have become caught or trapped between the Control Panel and the Pod.
20. Double check the LCD is still On and scrolling with the date and time displayed.
21. If the database has **not** been retained in the 16bit Control PCB memory due to it being disconnected for more than 30 minutes, it will need to be synchronised with the Traka 32 database. From the system viewer of

Traka32, right click over the picture of the pod and click on S**ynchronise System**.



22. Click on **No** first.



23. Then click on **Yes**.

Please refer to the Testing section for further details on fully testing the system.

6.1.2.9 UPGRADING FROM AN 8BIT TO A 16BIT CONTROL PCB

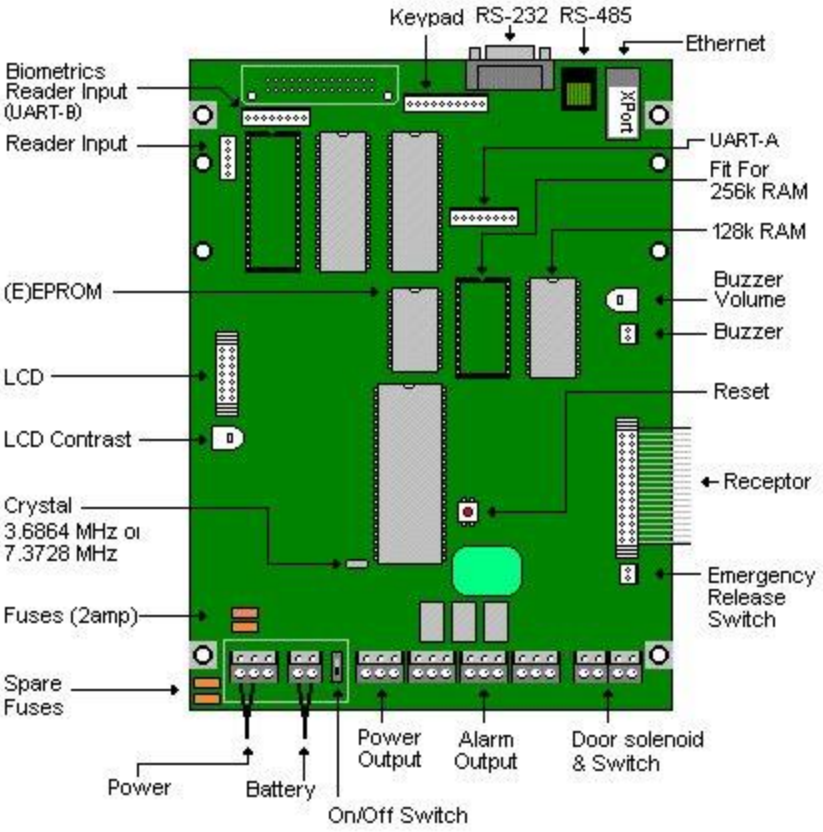
This section gives an overview for upgrading an existing Traka System fitted with an 8bit Control PCB with the new 16bit Control PCB. This covers all systems in general but does not go into detail for types of systems.

Backup Data

Before upgrading it is important backup any data from the 8bit Control PCB.

1. Open the Traka32 software.
2. Select the appropriate system from the drop down menu.
3. Click the Read All System Data from the selected system button.

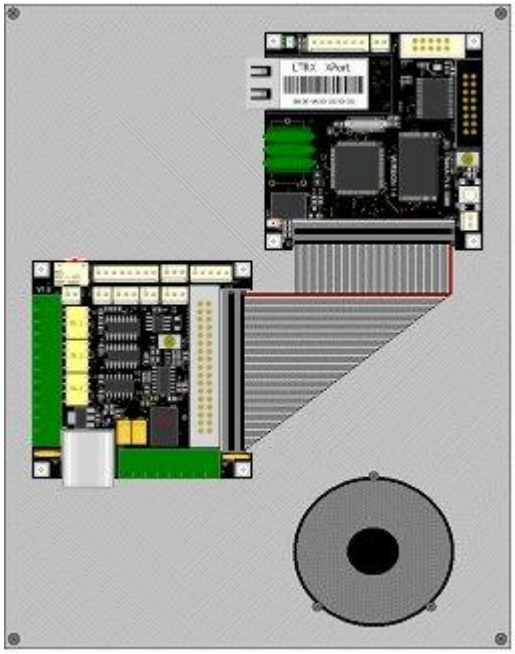
Removing the 8bit Control PCB



1. Using the Master Key, unlock the CAM Lock of the Control Panel.
2. Switch off the Control PCB via the on/off switch.
3. Disconnect the External Battery and Power Supply.
4. Disconnect all other cables noting where and how they connect.
5. Remove the Control Panel.
6. Unscrew the four mounting screws and carefully remove the 8bit Control PCB.

Installing the 16bit Control PCB Panel

The 16bit Control Panel is the same size as the 8bit Control PCB and uses the same mounting points.



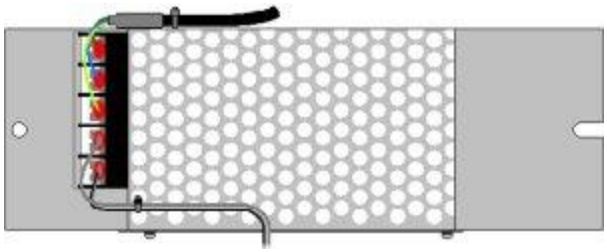
1. Place the 16bit Control Panel on the 4 mounting points with the Keypad Connector at the top and the Speaker at the bottom.
2. Using the 4 mounting screws, affix the panel.

All new systems fitted with the 16bit Control PCB will also have the new Power Supply. The Old Power Supply can be used with the new 16bit Control PCB. You do not need to upgrade the power supply but if it is required, follow these steps.

Removing the old Power Supply (if required)

1. Switch off the mains supply and disconnect the power supply from the mains.
2. Disconnect the DC cable from the Control PCB if not already done.
3. Carefully remove the 2 mounting nuts and washers retaining these for installing the new Power Supply.
4. Carefully remove any Earth Leads that were attached to the Power Supply mounting points and retain these for use with the new Power Supply.

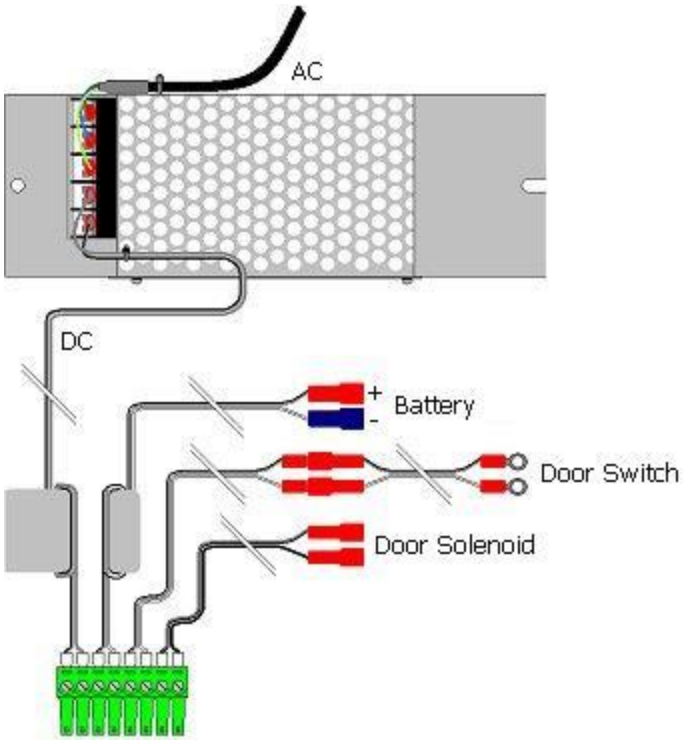
Installing the new Power Supply (if required)



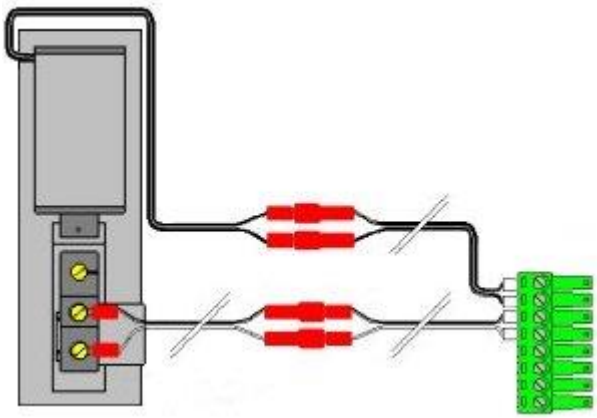
1. Place the new Power Supply on the 2 mounting points.
2. Re-attach any Earth Leads that were previously attached.
3. Any additional Earth Lead is also provided from the Power Supply that can be used to bond the Earth to the various cabinets.

NOTE: Wiring Alterations. The majority of the wiring on the new 16bit Control PCB is the same or where it differs simple modifications are required. Please read each section carefully and make the necessary changes accordingly.

The most noticeable difference with the wiring is in the Power Supply and Door Solenoid / Switch Connections. A new 8 way green connector block is now used instead of the various black / grey connectors. For the upgrade kit Traka supplies a complete set of cables as follows…



1. Connect the green connector to the 'Door & Power In' Connector on the 16bit I/O PCB.
2. Remove the existing ring terminal connections from the Door Switch and replace with the ring terminal connections on the new wiring loom.
3. Disconnect the in-line connector from the existing Door Solenoid cable and replace with the in-line connectors on the new wiring loom.

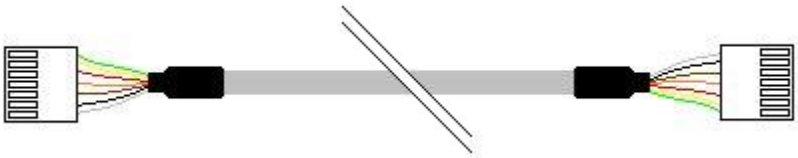


When upgrading a system, you will be able to re-use some of the existing cables.

- The old Power Supply can be re-wired into the new green connector block
- The old Battery Cable can be re-wired into the new green connector block but will require a Ferrite Core as supplied in the upgrade kit for EMC purposes.
- The Door Solenoid / Switch cables can be re-wired into the new green connector block but please note that an additional in-line connector has been added to the Door Switch to match that of the Door Solenoid as you cannot disconnect the Door independently of the Power Supply. When we ship a Pod separately from the Cabinet as with the L-Series you will connect the Door Solenoid and Switch via these in-line connectors.

Keypad Cable

A new keypad cable must be fitted with the 16bit Control PCB as it is wired differently from that used with the 8bit Control PCB. The new keypad cable is wired straight through making it easier to manufacture whereas the old keypad cable had wires crossed over. No damage will result if you accidentally use the wrong cable, however the keypad will not operate correctly.

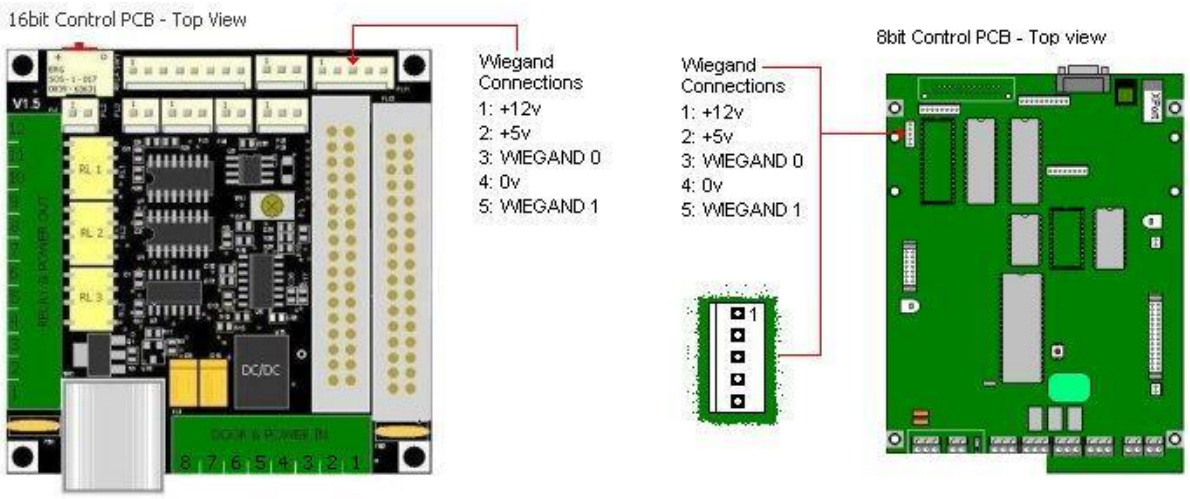


Readers

The 16bit PCB is not fitted with reader jumper settings. All the 16bit PCB requires is the reader connections wired correctly, see below for details.

1. Wiegand Readers

The wiring for Wiegand Readers does not change as the reader connector still has the same pin connections. With the 16bit Control PCB there are no jumper settings for Wiegand Readers.



2. Clock & Data Readers

The wiring for Clock & Data Readers does not change as the reader connector still has the same pin connections.

3. Serial RS-232 / TTL Readers

The reader connector will require re-wring as follows. In addition to supporting Serial RS-232 Readers, the 16bit Control PCB also has the ability to communicate at a TTL level. Also there is an additional Tx channel for both RS-232 and TTL allowing two way communications to readers if required.

When upgrading you will need to change from a 5 way connector to an 8 way connector and re-wire using the diagram below:

a. Barcode Readers

The barcode decoder chip that was fitted to the 8bit Control PCB is no longer used. Traka will use a Barcode reader with either an RS-232 or Wiegand output temporarily to overcome this problem and will look into the firmware required to accept TTL signals directly from barcode readers and decode them directly.

If you are upgrading an existing 8bit system to 16bit that uses a Barcode Reader in conjunction with the Barcode Decoder Chip, please contact the R&D Department prior to your order the to discuss your options.

b. TSSI Biometrics Reader

When upgrading a TSSI Biometrics reader, you will need to re-wire as follows:

- Pin 1 moves to Pin 2
- Pin 2 moves to Pin 6
- Pin 3 stays the same
- Pin 4 stays the same

c. Sagem Fingerprint Reader

When upgrading a Sagem Reader, the small interface board and traka reader cable used with 8bit

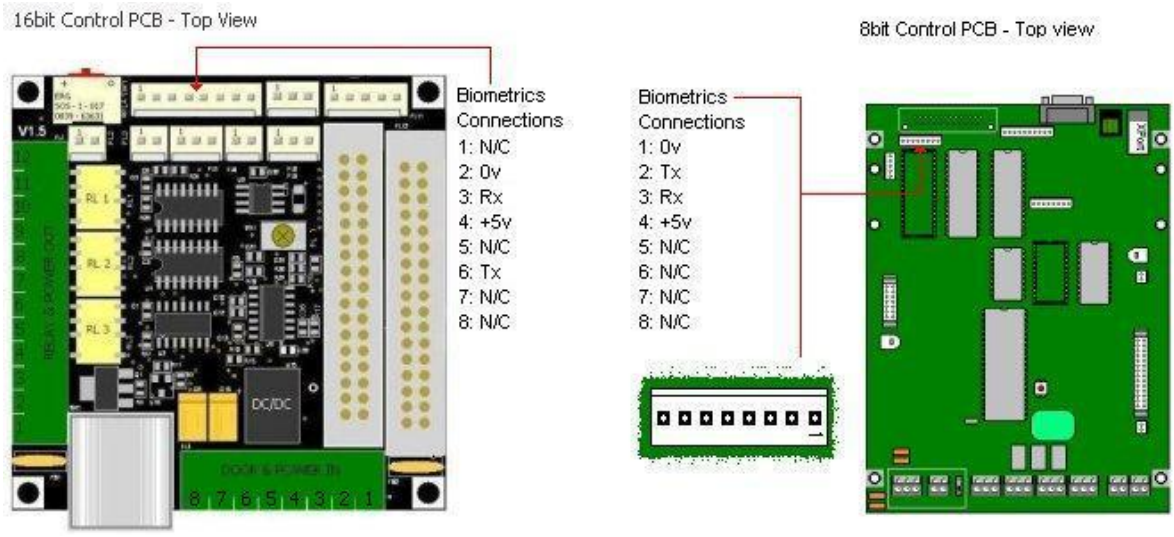
are not needed. The Sagem module itself will need to be rewired. Depending on what type of 8bit wiring you have on your Sagem Reader (prototype or official), the wiring will be as follows:

i. Prototype Wiring 8 way connector

- Pin 1 moves to Pin 2
- Pin 2 moves to Pin 7
- Pin 3 moves to Pin 8
- Pin 4 stays the same

ii. Official Wiring 4 way connector (will need to rewire into an 8 way connector)

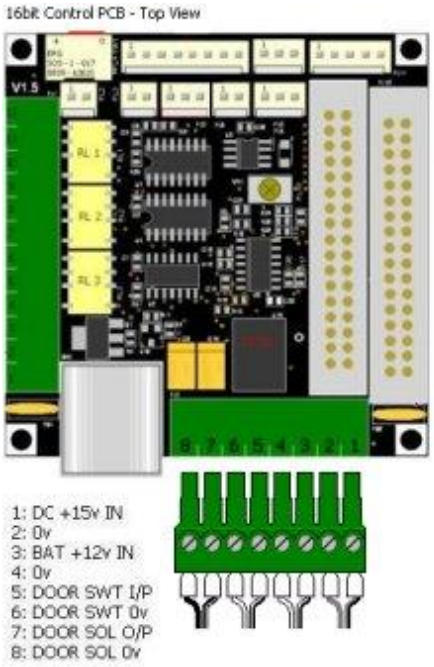
- Pin 1 moves to Pin 2
- Pin 2 moves to Pin 8
- Pin 3 moves to Pin 7
- Pin 4 stays the same



Power Wiring

When upgrading you will be able to re-use the existing power cables which can be re-wired into the new green connector block:

NOTE: When connecting the cables, please double check your connections before powering up the system. Pay particular attention to the polarity and always double check you have wired the Door Solenoid / Switch connections the correct way round otherwise this could result in damage to the 16bit I/O PCB and 16bit Control PCB.



Traka32 Communications

There may be some wiring differences with the various types of readers.

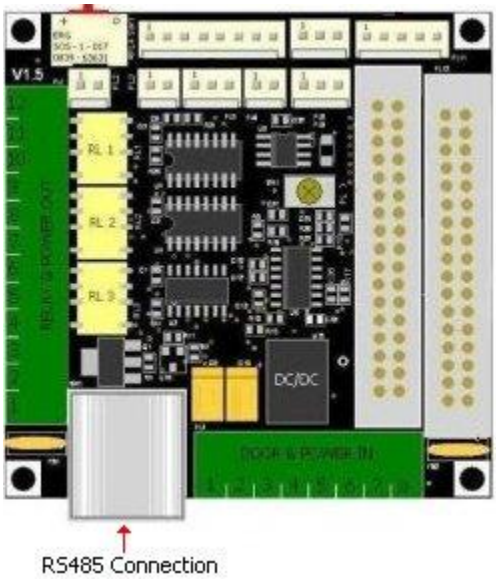
1. **RS-232**

   This connector is also used when connecting to an External Modem or Moxa. To save on space the 16bit Control PCB does not have a 9 Way D-Sub RS-232 Connector. There is a 3 Way header fitted to the 16bit I/O PCB that has the standard connections available. An RS-232 Link Cable is supplied to allow connection to D-Sub RS-232 Connector.

   NOTE: When communicating to a 16bit system via RS-232 the Baud Rate in the System Settings in Traka32 must be set to 38400. Refer to the RS232 Installation section for more details.

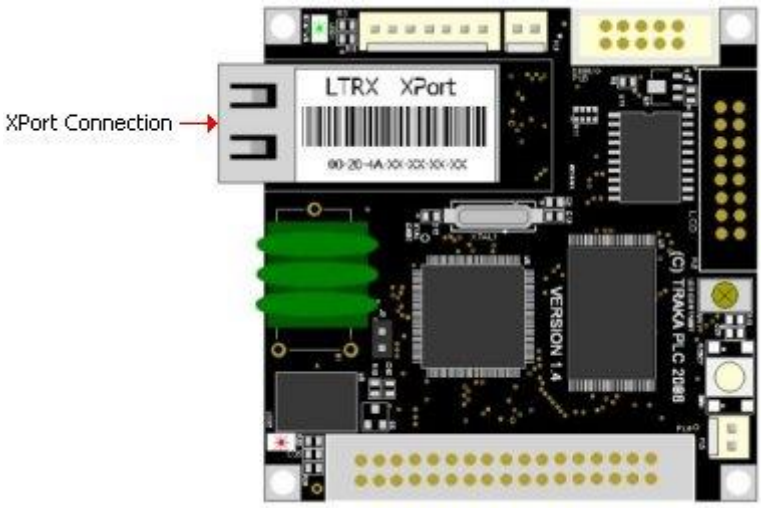
2. **RS-485**

   For RS-485, simply connect the provided cables into the RS485 Connection port on the 16bit PCB.



3. XPort Ethernet

For Ethernet, simply connect the appropriate cable into the X-Port Connection port on the 16bit PCB.



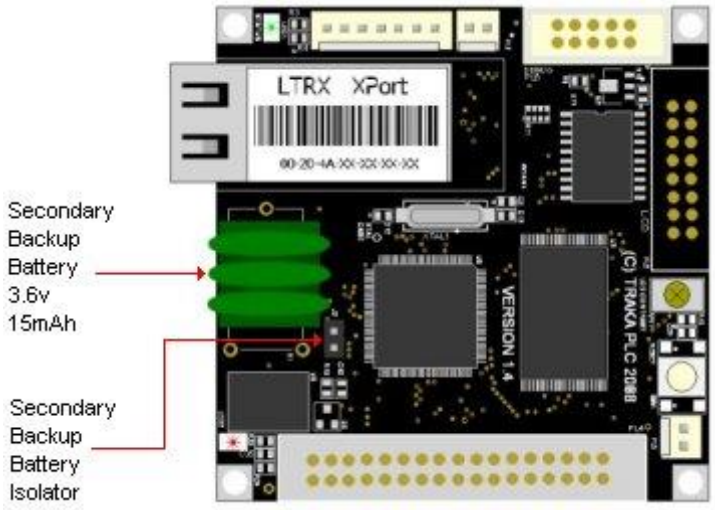
NOTE: Refer to the XPort Configuration section for details on how to configure communications via the XPort device.

Powering up the 16bit Control PCB

Once the 16bit Control Panel has been installed and all the wiring is in place there are a couple of checks that should be made.

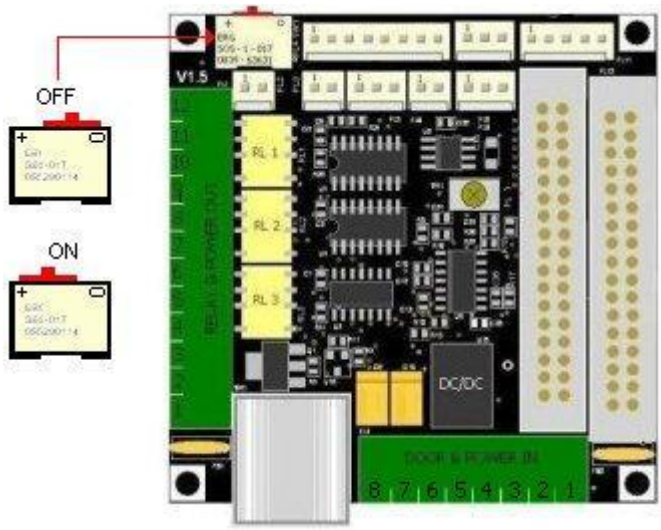
NOTE: It is highly recommended that when spare 16bit Control PCB's are transported or stored that the Battery Backup Isolator Jumper is removed. This will prolong the life of the battery.

1. Fit the Secondary Battery Backup Isolator jumper.

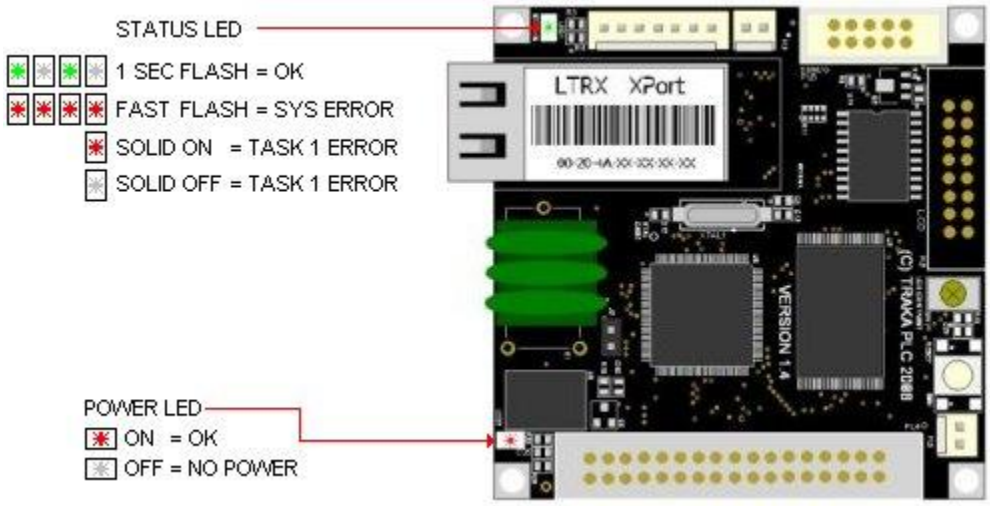


2. Switch on the power to the mains power supply.

3. Switch on the power to the 16bit I/O PCB.



4. Check that Power LED comes on and after a short while that the Status LED starts to flash.



5. NOTE: The status LED should flash when there is an application loaded and is running. If there is no application loaded, then the status LED will be on solid and the LCD will show:

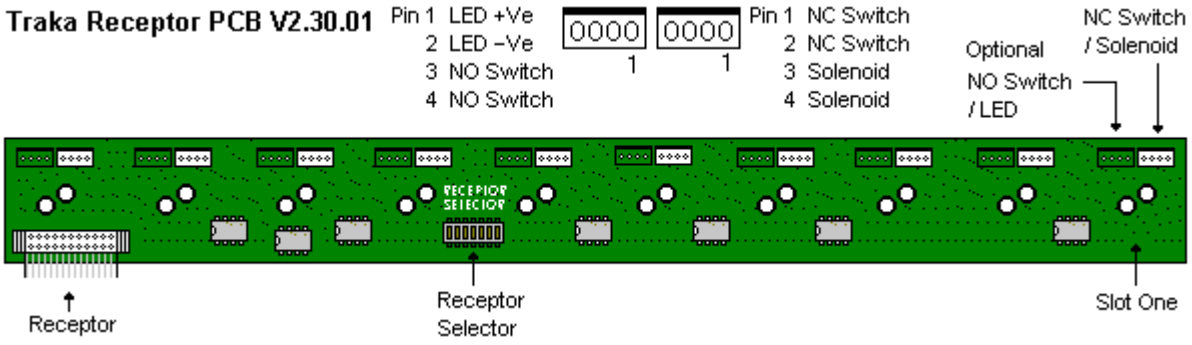
In this case a firmware upgrade will be required. Refer to the 16bit Firmware Upgrade section for more details.

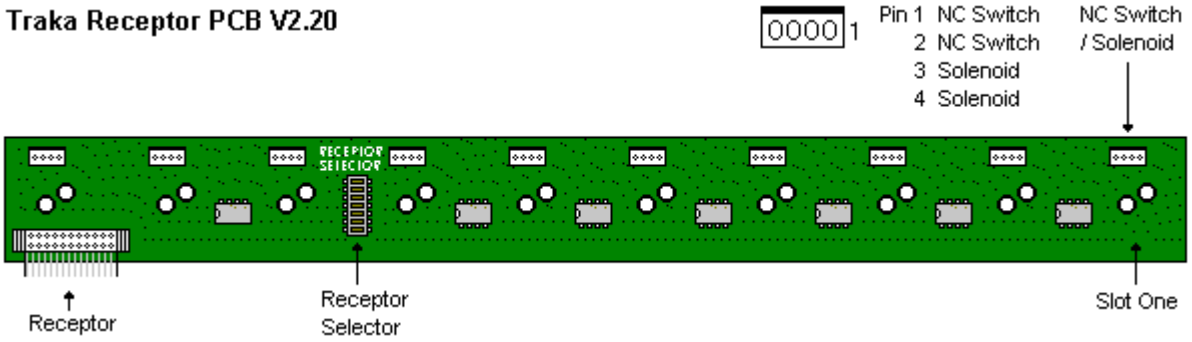
Once the system is powered up refer to the following sections to configure communications and upload a configuration file.

RS232 Installation - To configure communications via RS232
RS485 Installation - To configure communications via RS485
Modem Installation - To configure communications via Modem
XPort Configuration - To configure Ethernet communications via an XPort device
Loading a 16bit Configuration File

6.2 TRAKA RECEPTOR STRIPS

6.2.1 RECEPTOR LAYOUT



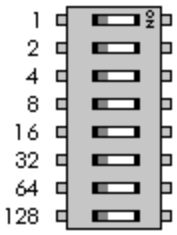


6.2.2 RECEPTOR SELECTOR SETTINGS

On the back of each Traka Receptor Strip is selector switch. Each strip in the system will need an individual number assigned to it via the selector. The first strip in the cabinet is always set to 0, from then on the sequence should increase in increments of one number per strip. E.g. Strip one will be set to 0, Strip two will be set to 1, Strip three will be set to 2 and so on.

The receptor selector settings are usually done at Traka before the system is sent to you however, you may need to change or add strips in the future so it may be useful to refer to the selector settings.

NOTE: When altering the selector settings please ensure that care is taken not to damage the selector or receptor strip. A calibration tool or small flat head screwdriver should be used to adjust the selector settings.

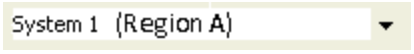


The selector settings are as follows...

SLOTS	1	2	4	8	16	32	64	128
1 – 10	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF
11 – 20	**ON**	OFF	OFF	OFF	OFF	OFF	OFF	OFF
21 – 30	OFF	**ON**	OFF	OFF	OFF	OFF	OFF	OFF
31 – 40	**ON**	**ON**	OFF	OFF	OFF	OFF	OFF	OFF
41 – 50	OFF	OFF	**ON**	OFF	OFF	OFF	OFF	OFF
51 – 60	**ON**	OFF	**ON**	OFF	OFF	OFF	OFF	OFF
61 – 70	OFF	**ON**	**ON**	OFF	OFF	OFF	OFF	OFF
71 – 80	**ON**	**ON**	**ON**	OFF	OFF	OFF	OFF	OFF
81 – 90	OFF	OFF	OFF	**ON**	OFF	OFF	OFF	OFF
91 – 100	**ON**	OFF	OFF	**ON**	OFF	OFF	OFF	OFF
101 – 110	OFF	**ON**	OFF	**ON**	OFF	OFF	OFF	OFF
111 – 120	**ON**	**ON**	OFF	**ON**	OFF	OFF	OFF	OFF
121 – 130	OFF	OFF	**ON**	**ON**	OFF	OFF	OFF	OFF
131 – 140	**ON**	OFF	**ON**	**ON**	OFF	OFF	OFF	OFF
141 – 150	OFF	**ON**	**ON**	**ON**	OFF	OFF	OFF	OFF
151 – 160	**ON**	**ON**	**ON**	**ON**	OFF	OFF	OFF	OFF
161 – 170	OFF	OFF	OFF	OFF	**ON**	OFF	OFF	OFF
171 – 180	**ON**	OFF	OFF	OFF	**ON**	OFF	OFF	OFF
181 – 190	OFF	**ON**	OFF	OFF	**ON**	OFF	OFF	OFF
191 – 200	**ON**	**ON**	OFF	OFF	**ON**	OFF	OFF	OFF
201 – 210	OFF	OFF	**ON**	OFF	**ON**	OFF	OFF	OFF
211 – 220	**ON**	OFF	**ON**	OFF	**ON**	OFF	OFF	OFF
221 – 230	OFF	**ON**	**ON**	OFF	**ON**	OFF	OFF	OFF
231 – 240	**ON**	**ON**	**ON**	OFF	**ON**	OFF	OFF	OFF
241 – 250	OFF	OFF	OFF	**ON**	**ON**	OFF	OFF	OFF
251 – 260	**ON**	OFF	OFF	**ON**	**ON**	OFF	OFF	OFF
261 – 270	OFF	**ON**	OFF	**ON**	**ON**	OFF	OFF	OFF
271 – 280	**ON**	**ON**	OFF	**ON**	**ON**	OFF	OFF	OFF
281 – 290	OFF	OFF	**ON**	**ON**	**ON**	OFF	OFF	OFF
291 – 300	**ON**	OFF	**ON**	**ON**	**ON**	OFF	OFF	OFF
301 – 310	OFF	**ON**	**ON**	**ON**	**ON**	OFF	OFF	OFF
311 – 320	**ON**	**ON**	**ON**	**ON**	**ON**	OFF	OFF	OFF
321 – 330	OFF	OFF	OFF	OFF	OFF	**ON**	OFF	OFF
331 – 340	**ON**	OFF	OFF	OFF	OFF	**ON**	OFF	OFF
341 – 350	OFF	**ON**	OFF	OFF	OFF	**ON**	OFF	OFF
351 – 360	**ON**	**ON**	OFF	OFF	OFF	**ON**	OFF	OFF

6.2.3 ADDING EXTRA RECEPTOR STRIPS

NOTE: Upgrading the system may take up to an hour per Traka system to complete. Please ensure that any important keys are removed from the systems prior to the upgrade, as it may be difficult to obtain the keys.

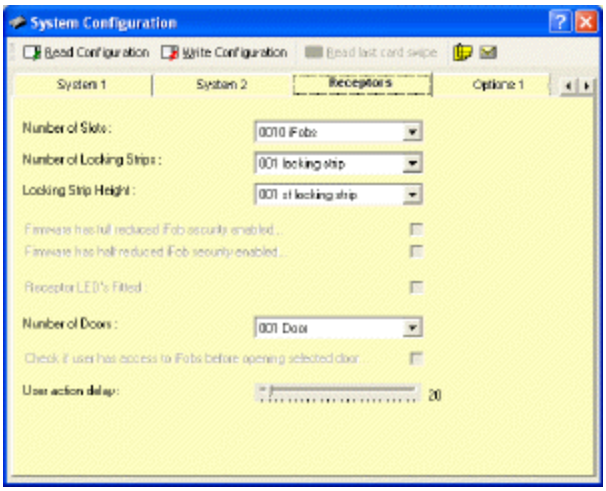
1. Load the Traka32 software by double clicking on the  icon.
2. Select the appropriate system from the 

drop down menu that you wish to upgrade.
3. Click on the  button.
4. Please refer to the Anti Static Precautions before working on the Traka system.
5. Using the **Master Key**, unlock the **Pod Lock**. The **Control Panel** is hooked in at the bottom and locked at the top. Carefully begin to remove the **Control Panel**.
6. You will see that there are several wires connected to the Printed Circuit Board (PCB) that are attached to the control panel. Determine which version of the Control PCB you have using the 8Bit PCB or 16bit PCB.
    a. **8bit**
        i. If you have **V2.20** of the **Control PCB** then...
            - Disconnect the Battery.
            - Disconnect the Power Supply.
        ii. If you have **V2.30.01 or above** of the **Control PCB** then...
            - Set the On/Off switch to Off.
    b. **16bit**
7. Using the I/O diagrams to locate the power switch...
    a. Set the On/Off switch to Off.
8. Add the extra strips replacing the ribbon cable as required.
9. Adjust the Receptor Selector settings. Please refer to the Selector Setting section for details on the correct settings.
10. Power the system back on.
11. **8bit**
    a. If you have **V2.20** of the **Control PCB** then...
        i. Reconnect the Battery.
        ii. Reconnect the Power Supply.
    b. If you have **V2.30.01 or above** of the **Control PCB** then...
        i. Set the On/Off switch to ON.
12. **16bit**
    a. Using the I/O diagrams to locate the power switch...
    b. Set the On/Off switch to ON.

13. Close the **Control Panel** carefully into the **Pod** and lock with the **Master Key**. The Control Panel should fit easily, if not check that no wires have become caught or trapped between the Control Panel and the Pod.

    NOTE: Please ensure nobody uses the system until the upgrade is complete.

14. From the system viewer of Traka32, right click over the picture of the pod and click on **Configure Firmware**. Navigate to the **Receptors** tab.



15. Select the **Number of Slots** to match the new total number of receptor slots within the upgraded system.

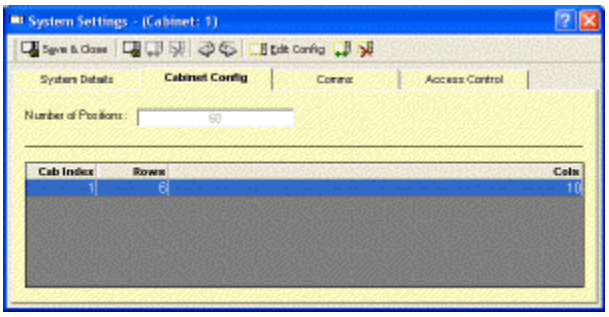
16. Select the **Number of Locking Strips** to match the new total number of locking receptor strips the upgraded system has. For example, if you had a 60 way locking system, this would have 6 locking strips.

17. Select the **Locking Strip Height** to match the new height of the first locking receptor strip within the selected system starting at 1 for the top strip.

18. Once you are happy that the new settings match the system, click on the **Write Configuration** toolbar button which will write the new settings to the system.

19. Right click over the picture of the pod again and click on **Configure System**.

20. Select the **Cabinet Config** tab.

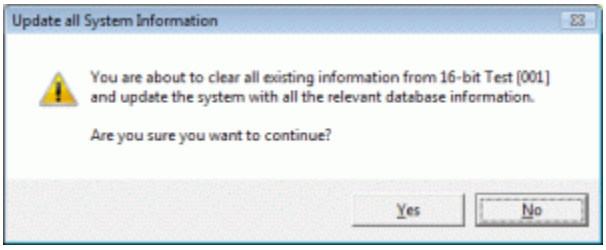


21. Edit the configuration of the cabinets to match that of the upgraded system. Please refer to the System Settings section for further information.

22. When you are happy with the new settings click on **Save & Close**.

23. Right click over the picture of the pod again and click on **Synchronise System**.

24. Click on **No** first. This will ensure that no information is cleared before you synchronise the system.



25. Then click on **Yes**.

26. Finally, right click over the picture of the pod again and click on **Synchronise iFobs**.

27. When completed you should see all the iFob appear within the system viewer. If any iFobs are missing, check each iFob in turn. Please refer to the Testing section for further details on fully testing the system.

6.2.4 LOCKING RECEPTOR STRIP

The Locking strip is the most common receptor strip used in Traka Cabinets. Recommended for customers who require a secure method of removing keys, the Locking strip locks the iFob & keys in position and will only release them once the adjacent button has been pushed.

NOTE: Once a user pushes a receptor button the system will check if the user has the correct access level to remove the iFob. If they do not possess the correct access levels, the system will deny the removal of the iFob.

6.2.5 NON-LOCKING RECEPTOR STRIP

The Non Locking strip is Traka's simple receptor strip solution. Recommended for customers who require a less secure method of releasing keys. The iFob can still remain secure behind the door of the cabinet (if required) however, once a user gains access to the system any iFob can be removed at any time regardless of the users Access Levels.

NOTE: Traka32 will still record who took the iFob along with the date & time. If the user did not have access to the iFob but removed it once they accessed the system then an event will be generated informing you of the users actions.

6.2.6 LED RECEPTOR STRIPS

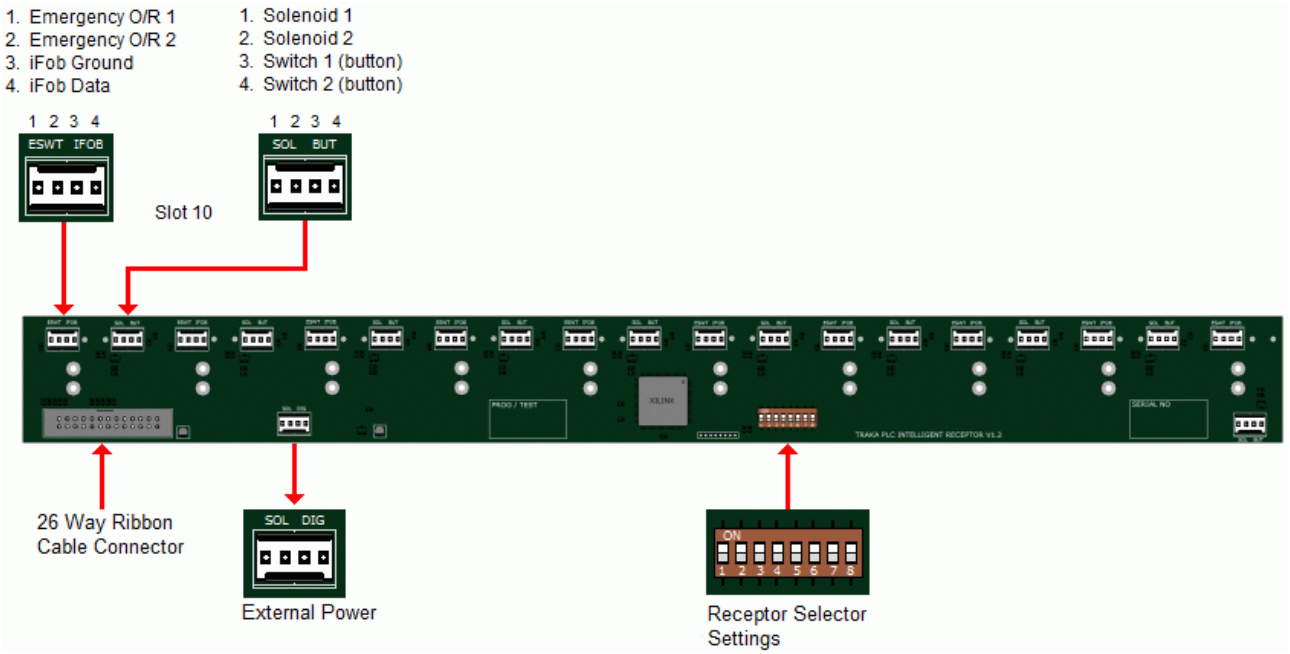
The LED Receptor strip provides clarity as to which iFob(s) a user can remove. The LED strip locks the iFob & keys in position and will only release them once the adjacent button has been pushed, once pushed the LED will illuminate red indicating that iFob can be removed. If a user access' the system the iFobs they are permitted to remove are displayed with a red LED.

LED receptor strips come in the standard 'locking' format but have the option to be with or without buttons. When using LED Locking strips with no buttons, they can be used in conjunction with keypad release. When a user enters the desired iFob via the system keypad, the door will open (if applicable) and the LED will indicate which iFob to remove.

6.2.7 INTELLIGENT RECEPTOR STRIP

6.2.7.1 RECEPTOR LAYOUT

Intelligent Receptor Strip (IRS) PCB Version 1.2



6.2.7.2 INTELLIGENT RECEPTOR STRIP (IRS)

The Intelligent Receptor Strip (commonly referred to as the IRS) is the next generation of the existing receptor strip. The main cosmetic difference with the IRS compared to the standard receptor strip range is the Tri-Coloured LED's, which allow Traka32 to assign a status to the iFob.

Intelligent Receptor Strip (IRS) Features

- **8-bit and 16-bit Control hardware support**

  The IRS will work with both 8-bit and 16-bit PCBs, however the 8-bit is currently limited to driving a single 180 Way L-series cabinet maximum due to power supply limitations. Please consult Traka if you have any queries of specific requirements on this.

- **Ability to drive Tri-colour LED's (Light emitting Diodes)**

A significant improvement over *Receptor Strip v2.03.01* is the ability to have tri-colour LED's instead of a single colour LED. In addition to this all LED's can be illuminated at the same time.

LED Status:

- **Green**

  The user has access to the iFob.

- **Red**

  The user does **not** have access to the iFob.

- Amber

  The User currently accessing the system has the specified iFob out of the system.

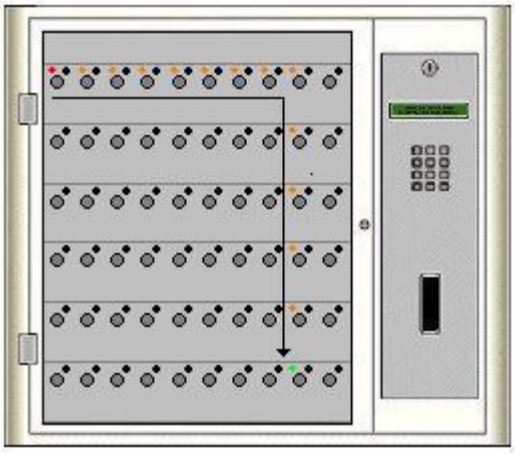
- **LED not lit**

  If the LED is not lit this means that another User has the iFob out of the system.

The LED rules apply to system features, such as iFob Allowance, so that once the user has taken their maximum iFob allowance all LEDs turn red.

- iFob in Wrong Slot

  If you return an iFob to an incorrect position within the cabinet, the IRS will guide you to the correct position using the LED's (see below).



- **Independent Button Control**

  Another significant improvement is independent button control. *Receptor Strip v2.03.01* and prior versions used buttons wired through the iFob, meaning that when the button was pressed, it disconnected the iFob so as it could not be detected. The problem with this is if a large bunch of keys pushes on a button whilst no user is logged into the system (cabinet door is open), the iFob goes undetectable.

  The IRS solves the iFob undetectable problem by wiring the iFob and Button independently of each other. Therefore if a large bunch of keys does happen to press against a button, it has no effect on the status of the iFob.

- **RFID Reader**

  Each IRS also has the ability to be fitted with an RFID (radio frequency identification) reader. It is possible to use the IRS PCB in conjunction with the Traka RFID Reader PCB (as used in our RFID lockers) to read RFID tags instead of iFobs.

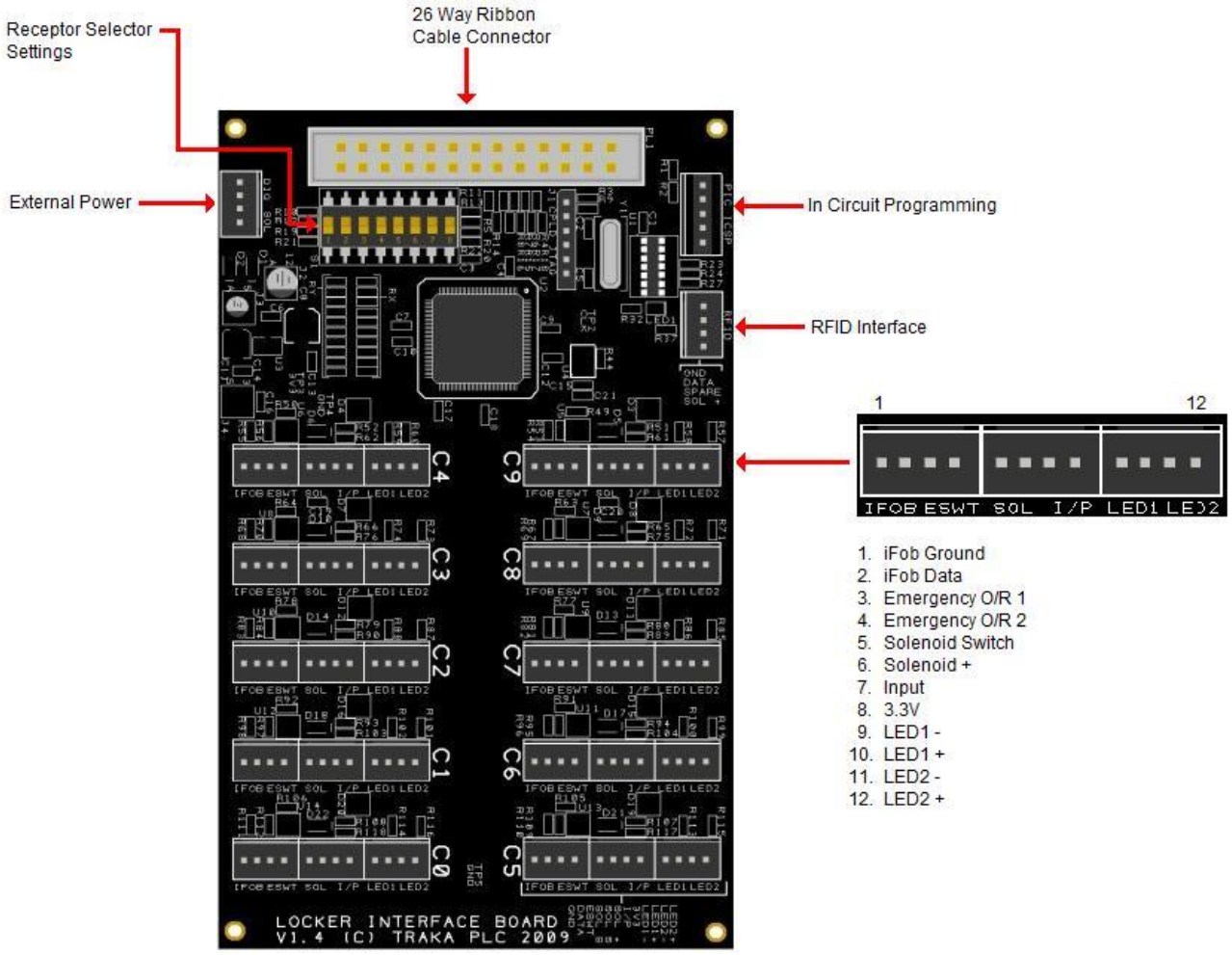
- **iFob Connector**

  The iFob contacts on the IRS have also been brought out to a connector. This can be used for special projects that require the use of the IRS but need receptor sockets that are not directly screwed to the PCB.

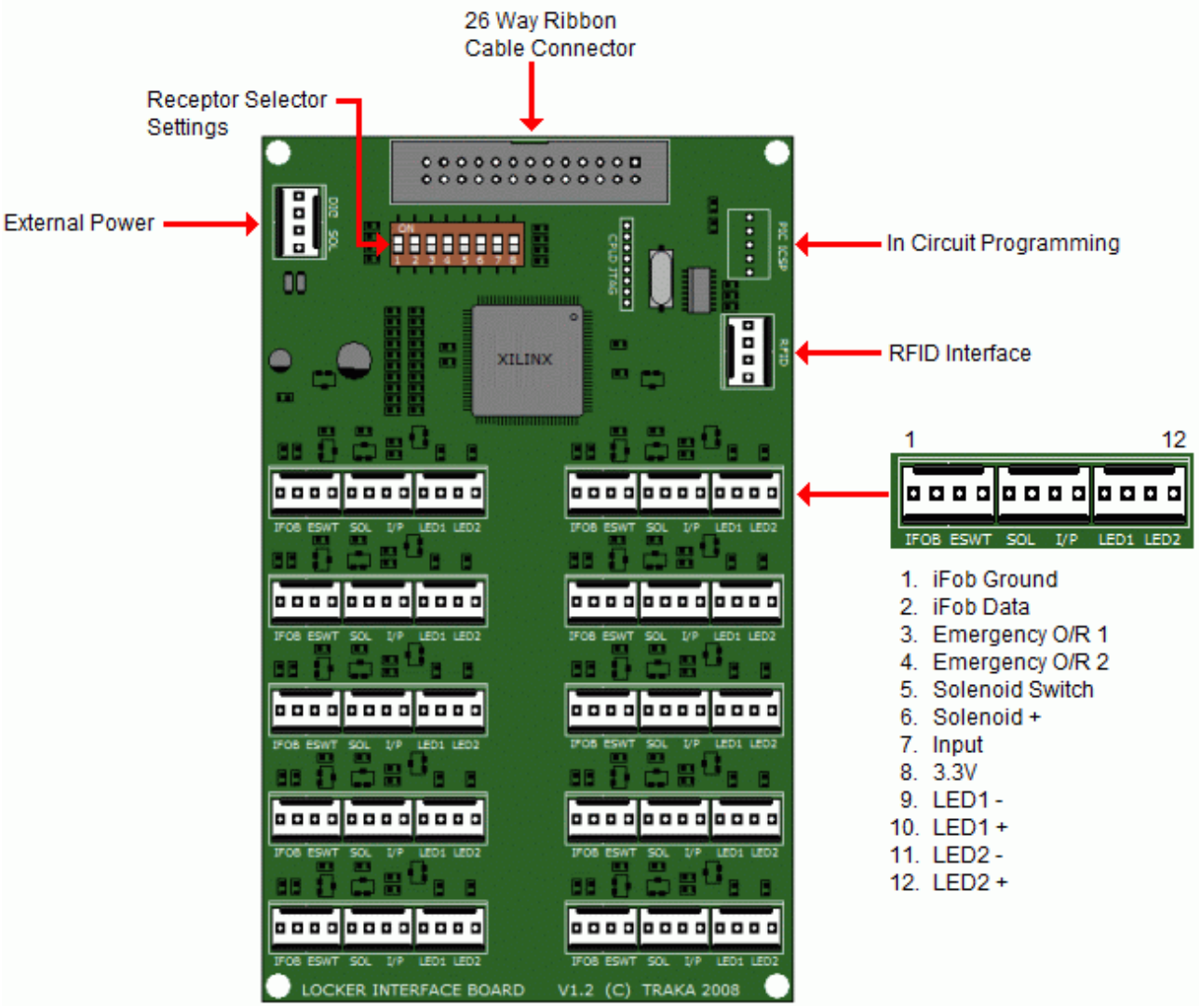
6.3 TRAKA LOCKER INTERFACE PCB

6.3.1 LOCKER INTERFACE PCB LAYOUT

Locker Interface PCB Version 1.4



Locker Interface PCB Version 1.2



6.3.2 LOCKER INTERFACE PCB FEATURES

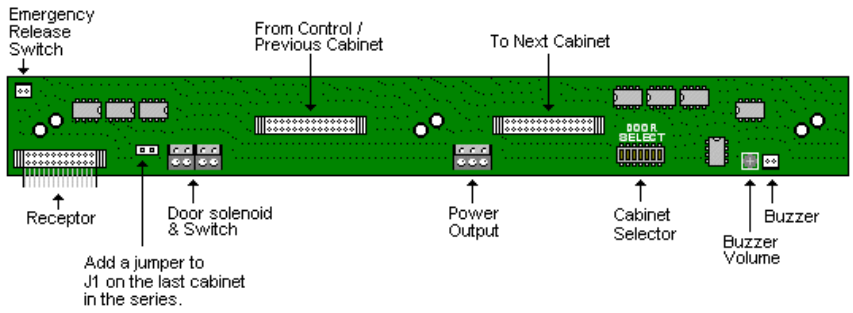
The Locker Interface PCB has all the same functionality as the Intelligent Receptor PCB. Please view Intelligent Receptor Strip for more information.

However the shape of the PCB lends itself to being used for Lockers as well as other bespoke applications.

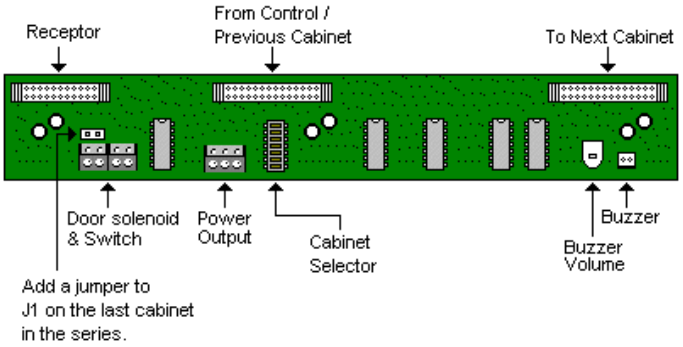
6.4 TRAKA INTERFACE

6.4.1 INTERFACE LAYOUT

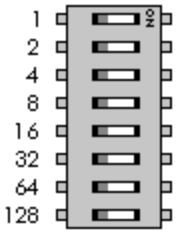
Traka Interface PCB V2.30.02



Traka Interface PCB V1.10



6.4.2 INTERFACE SELECTOR SETTINGS

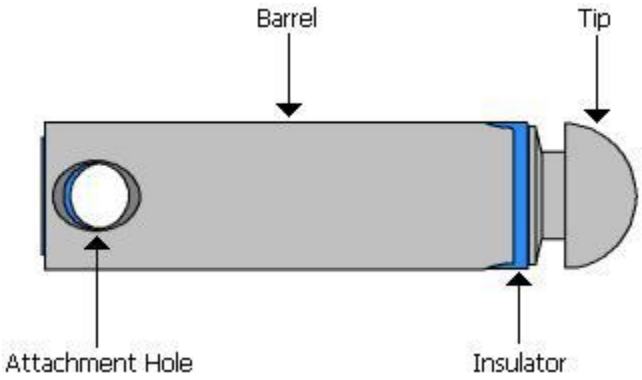


The settings are as follows...

CABINET	1	2	4	8	16	32	64	128
1	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF
2	**ON**	OFF	OFF	OFF	OFF	OFF	OFF	OFF
3	OFF	**ON**	OFF	OFF	OFF	OFF	OFF	OFF
4	**ON**	**ON**	OFF	OFF	OFF	OFF	OFF	OFF
5	OFF	OFF	**ON**	OFF	OFF	OFF	OFF	OFF
6	**ON**	OFF	**ON**	OFF	OFF	OFF	OFF	OFF
7	OFF	**ON**	**ON**	OFF	OFF	OFF	OFF	OFF
8	**ON**	**ON**	**ON**	OFF	OFF	OFF	OFF	OFF
9	OFF	OFF	OFF	**ON**	OFF	OFF	OFF	OFF
10	**ON**	OFF	OFF	**ON**	OFF	OFF	OFF	OFF

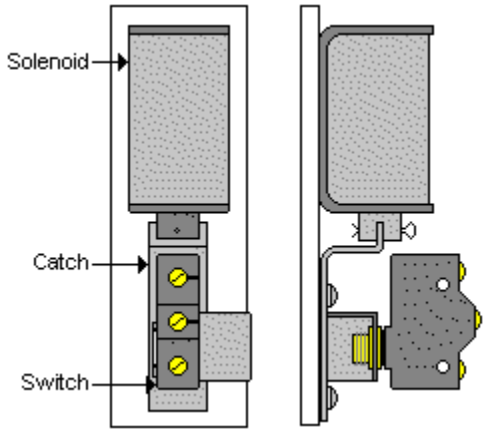
6.5 TRAKA IFOB

6.5.1 IFOB LAYOUT



6.6 TRAKA DOOR LOCK

6.6.1 DOOR LOCK LAYOUT



6.7 TRAKA BATTERY BACKUP

6.7.1 BATTERY CONNECTION DETAILS

WARNING: All Traka Systems have two power sources, mains and battery. Before installing or servicing a Traka System, please ensure both mains and battery power sources are disconnected from the system.

This section will explain how to disconnect the battery from 8bit and 16bit systems.

Battery Disconnection

1. Open the control pod/panel of the system using the master key.
2. Locate the battery. Usually placed at the bottom of the control pod.
3. Disconnect the battery cable from the terminals as shown below.

6.7.2 TRAKA BATTERY SPECIFICATIONS

All the Traka Systems can be fitted with a 12 volt battery backup to keep the system fully operational in the event of a power failure. The choice of battery is dependent on the type of Traka System and how long the battery backup must last in the event of power failure.

12v, 1.2Ah Sealed Rechargeable Lead Acid

Recommended for use with the **B-Series** and **Mini 16** Traka Systems only.

Height: 53mm (including terminals)
Width: 43mm
Length: 97mm
Terminal Size: 5mm

12v, 3.2Ah Sealed Rechargeable Lead Acid

Recommended for use with the **M-Series**, **S-Series** and **L-Series** Traka Systems.

Height: 68mm (including terminals)
Width: 67mm
Length: 134mm
Terminal Size: 5mm

12v, 7.2Ah Sealed Rechargeable Lead Acid

For **optional** use with the **S-Series** and **L-Series** Traka Systems where extended power fail coverage if required.

Height: 97mm (including terminals)
Width: 65mm
Length: 151mm
Terminal Size: 5mm

7 END USER LICENCE AGREEMENT – SOFTWARE

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

1. Definitions

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

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

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

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

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

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

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

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

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

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

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

2. Licence

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

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

3. Patents, Designs and Copyright

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

4. Restrictions

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

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

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

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

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

5. Warranty

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

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

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

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

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

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

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

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

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

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

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

5.6.2 the Customer is in breach of this EULA;

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

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

6. Training

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

7. Limit of Liability

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

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

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

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

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

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

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

8. Disposal

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

9. Force Majeure

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

10. Termination

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

11. Consequences of Termination

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

12. Communications and Notices

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

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

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

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

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

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

13. Assignment

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

14. Waiver

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

15. Severance

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

16. Rights of Third Parties

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

17. Law

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

Data Protection Laws

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

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

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

17.5 The Customer shall:

17.5.1 comply with the Data Protection Laws;

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

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

17.6 The Company:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

17.8.7.1 taking measures to address any Data Security Breach; and

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

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

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

18. Entire Agreement

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

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

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

8 END USER LICENCE AGREEMENT – EMBEDDED SOFTWARE

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

1. Definitions

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

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

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

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

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

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

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

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

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

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

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

2. Licence

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

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

3. Patents, Designs and Copyright

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

4. Restrictions

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

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

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

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

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

5. Warranty

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

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

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

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

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

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

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

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

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

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

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

5.6.2 the Customer is in breach of this EULA;

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

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

6. Training

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

7. Limit of Liability

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

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

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

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

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

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

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

8. Disposal

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

9. Force Majeure

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

10. Termination

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

11. Consequences of Termination

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

12. Communications and Notices

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

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

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

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

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

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

13. Assignment

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

14. Waiver

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

15. Severance

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

16. Rights of Third Parties

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

17. Law

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

Data Protection Laws

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

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

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

17.5 The Customer shall:

17.5.1 comply with the Data Protection Laws;

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

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

17.6 The Company:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

17.8.7.1 taking measures to address any Data Security Breach; and

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

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

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

18. Entire Agreement

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

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

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