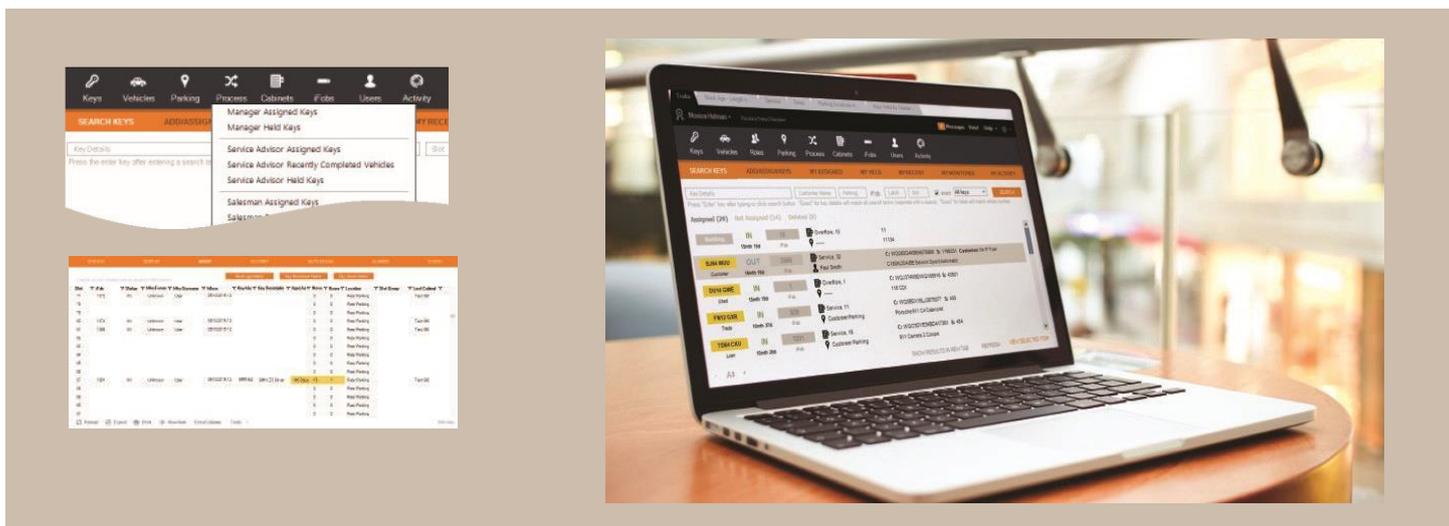


TRAKA AUTOMOTIVE ADMINISTRATOR GUIDE

Assigning Non-vehicle key
Locking Row access Group
Key Curfews
Adding new user

How to Modify a User
User Enrolment Problems
Auto Extend Expiry Date if Inactive
Cabinet Inactivity

V1.4



HOW DOES TRAKA WORK

Vehicle keys are stored in the key cabinet and quickly searchable to find where the keys are, including the parking location of the vehicle or current process step.

Electronic tracking iFobs are used to allow the key cabinet to know where the keys are. As well as physically attaching the keys to the iFob there is a simple process to link the key within the software with key details picked up and synchronised with your DMS.



ABC 123 IN 1450 🏠 Customer System, 9
 Customer 25mins iFob 📍 Service Bay 4

Users authenticate themselves via Fingerprint, PIN, access token or your existing swipe card system to gain access to the key cabinet.

All access and movements are recorded within extensive software providing audit trails of all transactions. When a key is removed, anyone else searching will see who is holding the key.



ABC 123 OUT 1450 🏠 Customer System, 9
 Customer 25mins iFob 👤 Traka User 07

TRAKA AUTOMOTIVE: ASSIGNING A NON-VEHICLE KEY

V1.4

STEP 1

- To assign a key click on "Add/Assign a Key" then select the type e.g., Building, Safe or Other
- Type in a name for the key and click on "Check if there is a key with these details" button

STEP 2

- The software will search for any matches that are in the database (to avoid duplicate entries)
- Always click on the correct match if it is there to avoid any further re-typing and click "Select Highlighted Key"
- If the key is not in the list, click on "The key is not in the list" button

STEP 3

- Confirm, correct or populate the key details as required

STEP 4

- Type in the iFob label number (Tag number) that the keys will be attached to on the right-hand section of the screen then click the search button
- Once it has been found, click on the text of the iFob then click the "save" or "save and open key" button

UNASSIGNING

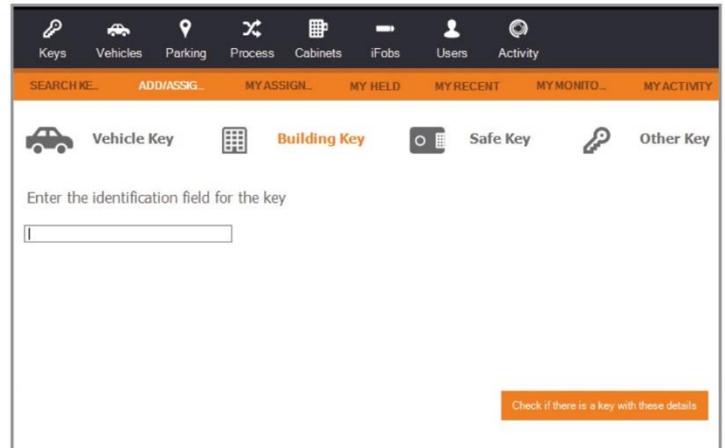
When you have finished tracking a key you should unassign it from the iFob within the software:

Search for the key

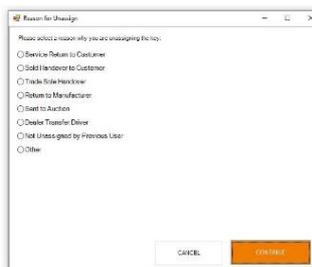
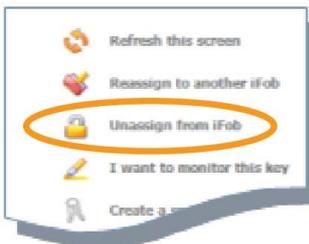
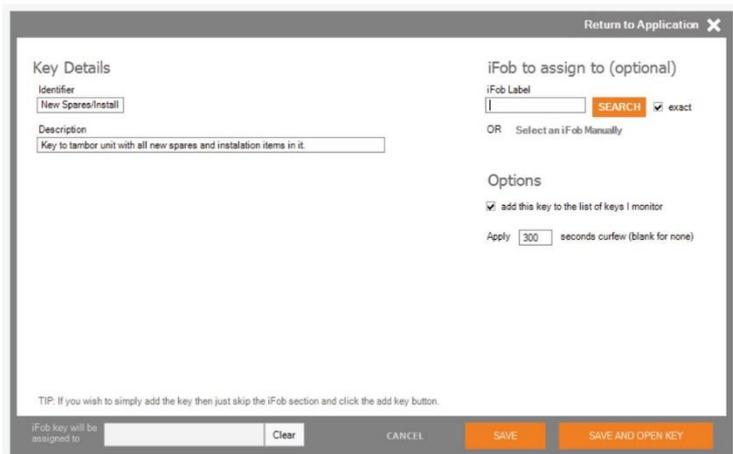
Once the details have been found, double click on the record and it will open up a new tab with the vehicle information, then click on "Un-assign from iFob"

REASON FOR UNASSIGNING

- If your dealership is using **Reason for Unassigning key**, once you clicked **Unassign** from iFob, you will be presented with a list of reasons
- Select a reason and then click **Continue**



Rank	Identifier	Description	
6	New Spares/Install Cupboard		Stu's
6	Tambor Unit behind Stu		Stu's C
6	Unit 14 Key		???

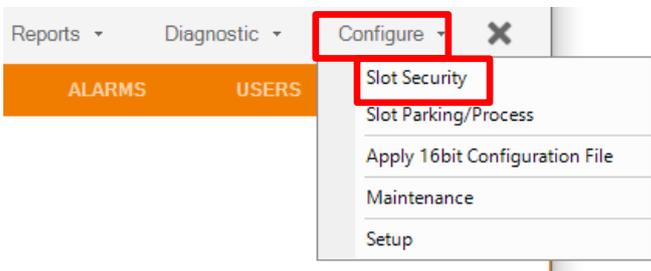


TRAKA LOCKING ROW

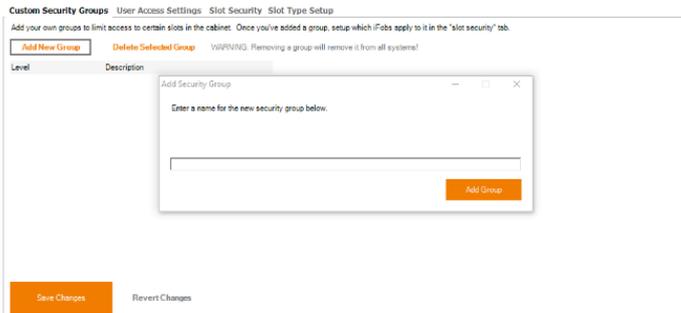
Traka key management systems can be configured to work with locking and non- locking rows. It is a common practice for many dealerships to have at least 1 locking row in each of the cabinets to store fuel cards or business keys.

CREATING ACCESS GROUP

- On the left-hand side of the main Traka screen, select the cabinet you wish to apply access group to.
- On the new screen, select “**Configure**” in the top right corner followed by “**Slot Security**” from the drop-down menu.



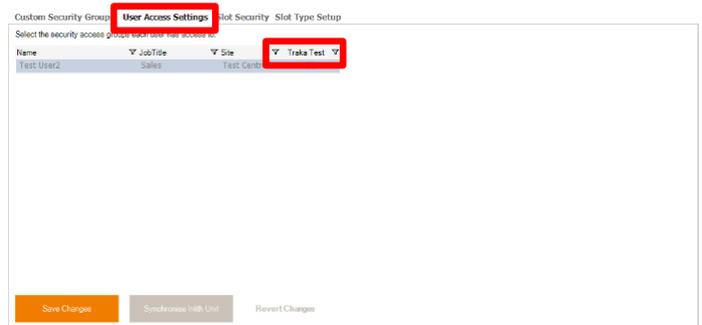
- Within the new window, select Custom Security Groups and “**Add New Group**”
- Add new group name on the pop-up screen and click “**Add Group**” Followed by **Save Changes**



Follow the same steps for all access groups that you wish to create.

USER ACCESS SETTING

- Once above step has been complete, select **User Access Setting** on the top ribbon
- Within the new window, select all users you wish to grant access to.
- Click **Save Changes**



SLOT SECURITY

- To apply access group to locking row, select **Slot Security**
- Click on the drop-down arrow on all positions you wish to apply the access group to.
- Once complete, click **Save Changes**



SETTING A CURFEW DURING KEY ASSIGNMENT

In the final step of assigning a key, there is an "Options" area where you can enter a maximum time period that the key should be out of the key cabinet. This can be set both to vehicle and non-vehicle keys. Simply apply the curfew time in "Options" section. Please note the curfew is set in seconds.

SEARCH RESULT CURFEW VISIBILITY

Within the search results the "OUT" status will be red if the duration that the key has been out, is past the curfew duration that has been entered.

VIEWING CURFEW HISTORY FOR A KEY

When viewing a key you can click on the "curfew" tab and show the history of the durations the key was out. You can also edit the curfew duration if you wish to.

REPORTING OVERDUE & SOON TO EXPIRE KEY

Within the "Keys" menu there is a "Overdue Keys" report that lists the keys that have a curfew set and how much time is remaining, or the key is overdue by.

- Click on **Keys** on the black ribbon
- Followed by Overdue Keys

You will now be presented with a list of keys which have a curfew applied to and are either overdue or how much time is remaining.

Options

add this key to the list of keys I monitor

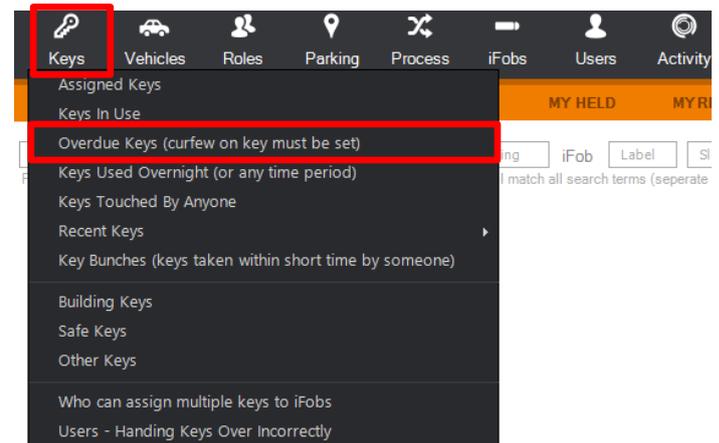
Apply seconds curfew (blank for none)

ABC 123	OUT	1436	Service, 5	C: ----- S: ----- Customer: Traka Customer 02
Customer	15mth 2d	iFob	Traka Customer 01	VW Golf 1600 Diesel Manual Grey
New	OUT	1416	Sales, 16	C: AAAA000BBBB1111 S: 487
	15mth 10d	iFob	Traka Customer 01	911 Carrera Targa

SUMMARY	EDIT DETAILS	ACTIVITY	HELD BY	CURFEW	SPARE KEYS (0)	REVISIONS	SIMILAR KEYS
Show: All Entries	Apply Filter	Drag a column header here to group by that column					
D	V	Month	Time	Duration	Took	Returned	
3	June	16:18:5	10:4D	16:22	T. Admin 01	T. Admin 01	
1	June	17:03:3	10	14:05	T. Admin 01	T. Admin 01	
29	May	17:10:1	20	13:46	T. Admin 01	T. Admin 01	
27	May	16:10:5	10	14:48	T. Admin 01	T. Admin 01	
27	May	07:06:1	9	miss	T. Admin 01	T. Admin 01	
26	May	16:14:0	14:39		T. Admin 01	T. Admin 01	

This key should only be allowed to be out for a maximum of seconds.

Save Changes



USER GROUPS

Traka advises to group users into 3 levels.

Level 1 – typically are back of house staff who do not have customer interaction i.e technicians or valeters. They require cabinet access but not necessary software access.

Level 2 – front of house staff who are required to add, assign keys and perform basic searches on the software i.e. Service Advisor or Sales Executive.

Level 3 - system administrator who is able to add/modify users, add new iFobs and most importantly go through system reports. Level 3 access is normally given to the management team.

ADDING NEW USER

- To add a new user click on the **User** icon and Select **"Add New User"**
- For all users, please complete the following section: **Forename, Surname, Position, Primary Site** (drop down option), **Roles** located at the top part of the Add a New User screen.
- If sites are configured, then selecting the "Primary Site" will assign the user to that site and automatically select access to the cabinets for that site. Selecting primary site will also make reporting easier in the future. Alternatively, manually click on the tick boxes to give the user access to the specific cabinets they require
- All users should have their own Key cabinet access, Enrol user to the cabinet by following one of the enrolment procedures in **Key Cabinet Login** Section. For different authentication options, please see page 7.
- If adding Level 1 user, Click **Add User & Close**.

Add a New User Return to Application X

Forename	Surname	Position	Telephone / Mobile	Primary Site	Key System Access	Roles
Traka	Test	Saes Manager		Test Centre	<input checked="" type="checkbox"/> Traka Demo	<input type="checkbox"/> Valet

Software Login

Username:

Password: Verify:

Mobile App Login

Mobile App PIN:

(Leave blank to use Key Cabinet PIN)

Only prompt for PIN once per day

Key Cabinet Login

KeyPad PIN or Access Card: [Generate PIN](#) OR [Read Last Card from](#)

Secondary PIN:

Fingerprint Template (Sagem): [Capture Fingerprint Template](#)

Fingerprint Alternate PIN (Sagem):

NOTE: to use alternative PIN (i.e. where a user does not wish to register their fingerprint) then you will need the "card and/or pin" firmware option enabled

Permissions

Create, assign and unassign keys

Mobile App Access

User is an administrator for iFobs (take any iFob) Keep user on the cabinet even if no activity

Access from: until: Auto extend expiry date if user is still performing activity

[Add User & Start Adding Another User](#) [Add User & Close](#) [Add User & View User](#)

ADDING LEVEL 2 USER

- In addition to the above steps, for Level 2 users, please complete **Software Login** section by giving a user a software username and password.
- Your IT team will be responsible for installing Traka Client Software on all users' PCs.
- For mobile app access please ask the user to create their own 4-digit pin, the username remains the same as for Software Login
- To complete Level 2 user, under **Permissions** section, please tick the option **Create, Assign and Unassign Keys** for all users who will be performing those functions
- If you have many users to add, you can click "Add User & Start Adding Another User". This allows you to quickly add users and then use the separate batch user editing features to batch enrol fingerprints/swipe cards, set permissions, etc.

The screenshot shows a multi-section form for creating a user. The 'Software Login' section includes fields for Username (Traka.Test), Password, and Verify. The 'Mobile App Login' section includes a Mobile App PIN (2023) and a checkbox for 'Only prompt for PIN once per day'. The 'Key Cabinet Login' section includes fields for KeyPad PIN or Access Card (8023), Secondary PIN, and Fingerprint Template options. The 'Permissions' section is highlighted with a red box and contains several checked options: 'Create, assign and unassign keys', 'Mobile App Access', and 'Auto extend expiry date if user is still performing activity'. There are also date pickers for 'Access from' (21/09/2022) and 'until' (21/09/2023).

ADDING ADMIN USER LEVEL-3

- To add System administrator, Level 3, please complete the previous steps, however, when completed, please click **Add User & View User**
- Within the new window, please click **Security** on the orange ribbon, followed **Permissions** on the grey ribbon
- Ensure that all options under 3 groups Basic iFob Management and User admin are ticked
- Click **Save** in the bottom right corner

The screenshot shows the 'User - Traka Test' management interface. The 'SECURITY' ribbon is selected, and the 'Permissions' tab is active. A list of permissions is shown with checkboxes in the 'Access' column, all of which are checked. The permissions are grouped into three categories: 'Area' (Assign Keys, Unassign Keys, Create New Keys), 'iFob Management' (Transfer Fobs To Anyone, Transfer Fobs To Self (Receive), Unrecognise iFobs, Mark iFobs as Lost, Remote Release iFob, Batch label iFobs, Rename iFobs), and 'User Admin' (Administer Users). A red box highlights the 'Access' column. 'REVERT' and 'SAVE' buttons are visible at the bottom right.

PIN ONLY

- Enter a unique 4-digit PIN number for the user to use in the Primary PIN box
- Alternatively click the "Generate" button to have a unique PIN automatically generated



FINGER IDENTIFICATION - SAGEM

- You do not need to enter any PIN as the Sagem reader will automatically identify the user from the fingerprint
- Ensure that you have the Sagem desktop enrolment module installed on your PC and then click the "Capture Sagem Fingerprint Template". You will need to present the same finger three times - you can optionally enrol an optional second finger. You must make sure the orientation is the same i.e. white space to the left with finger pointing upwards
- Save the user and the fingerprint template will be automatically synchronised across all key cabinets the user has been given access to. You can now go to the key cabinet and press the "#" key then place your finger on the reader to gain access



FINGERPRINT ALTERNATIVE

- In the event where cabinets are using Sagem access control and a user has very bad fingerprints, it is possible to offer PIN access too.
- Under Key Cabinet Login section, Enter a unique 4-digit PIN number in Fingerprint Alternative PIN (Sagem) box
- To access the cabinet, press and hold the # on the keypad until prompted to enter the PIN.
- Enter the pin and press the # key again

Key Cabinet Login

KeyPad PIN or Access Card

Generate PIN OR

Read Last Card from

Secondary PIN

Traka Demo

Fingerprint Template (Sagem)

Capture Fingerprint Template

Fingerprint Alternate PIN (Sagem)

NOTE: to use alternative PIN (i.e. where a user does not wish to register their fingerprint) then you will need the "card and/or pin" firmware option enabled

TOKEN/CARD

- Swipe Users' Access Card or Proximity Token against the reader at the cabinet. You will hear a "Beep" after which, the LCD will say "ID not recognised"
- Using the software, select the key cabinet used in step 1 from the dropdown menu and click "Read Last Card from". The card ID number should appear in the KeyPad Pin or Access Card box.



Key Cabinet Login

KeyPad PIN or Access Card

Generate PIN OR

Read Last Card from

Secondary PIN

Traka Demo

Fingerprint Template (Sagem)

Capture Fingerprint Template

Fingerprint Alternate PIN (Sagem)

NOTE: to use alternative PIN (i.e. where a user does not wish to register their fingerprint) then you will need the "card and/or pin" firmware option enabled

HOW TO MODIFY A USER

- To modify a user click on User icon followed by Search Name/Pin
- Type in User's name in the search box and click **Find**. Once the user has been found, double click on their name
- Within the new window, click **Security** on the orange ribbon
- To change mobile app pin or software password, click reset under the window and generate new pin/password.

ACCESS CARD RESET

- For Card access changes, click **Reset** next to KeyPad PIN or Access card.
- Swipe Users' access card or Proximity Token against the reader at the cabinet. You will hear a "Beep" after which, the LCD will say "ID not recognised"
- Using the software, select the key cabinet used in step 2 from the dropdown menu and click "Read Last Access Card Swipe from". The card ID number should appear in the KeyPad Pin or Access Card box.

The screenshot shows the 'Security' tab of the user management interface. Under the 'Key Cabinet Login' section, there are fields for 'KeyPad PIN or Access Card' and 'Fingerprint Template (Sagem)'. Both fields have a 'Reset' button next to them, which is highlighted with a red box. There are also options for 'Generate New KeyPad PIN' and 'Read Last Access Card Swipe from'. A 'Clear Template' button is also visible next to the fingerprint template field.

RE_ENROLL FINGER - SAGEM

- Ensure that you have the Sagem Desktop Enrolment Module installed on your PC.
- Click **Clear Template** next to Fingerprint Template (Sagem)
- Next click "Capture Sagem Fingerprint Template". You will need to present the same finger three times - you can optionally enrol an optional second finger. You must make sure the orientation is the same i.e., white space to the left with finger pointing upwards

- Save the user and the fingerprint template will be automatically synchronised across all key cabinets the user has been given access to. You can now go to the key cabinet and press the "#" key then place your finger on the reader to gain access.

USER MOVING SITES

- If any of your new starters have moved sites within the group, the chances are they might already have a Traka Account and there is no need to create another one for them. This is only possible if all sites are linked together.
- First find the user using the user search or user lists e.g., clicking the Users icon then selecting the "Search User" or "List users" reports etc.
- You should double-click the user's entry to open up the users details which will take you to their summary page
- Click on **Edit Details** to change User's Primary site to current location and click **Save**.
- Click on Security followed by **Key Cabinet Access**
- Select which cabinets the user should have access to and click **Save**.

The top screenshot shows the 'Edit Details' tab of the user management interface. The 'Primary Site' dropdown menu is set to 'Test Centre' and is highlighted with a red box. Below this, there are checkboxes for various roles: Valet, Technician, Salesman, Service Advisor, Manager, Driver, Third Party, and Parts.

The bottom screenshot shows the 'Security' tab of the user management interface. The 'Key Cabinet Access' sub-tab is selected and highlighted with a red box. It shows a list of systems the user is allowed access to, with 'Traka Demo' checked.

CHECKS

View the user and check the Security tab:

- Check the "Key Cabinet Access" to ensure they have been given permission to access the cabinet
- Check the "Key Cabinet Access Times" to ensure they have not been given incorrect access times
- Check the "Login"
- Check their active start and end date
- Check the account is not set to disabled
- Check there is a PIN or fingerprint template captured
- View the user and then select "Synchronise this User" to re-attempt downloading the user permissions to the cabinet

View the cabinet and check the Users tab:

- Ensure the user is present in the list – if they are not then they have not been given permission to access the cabinet. You can edit this in their user record
- Confirm the "Is On" column for the user has a tick and the "Put On" date time is valid
- Scroll across to the "Checked Code" column – if there is a code here then there was a problem downloading the user permissions to the cabinet

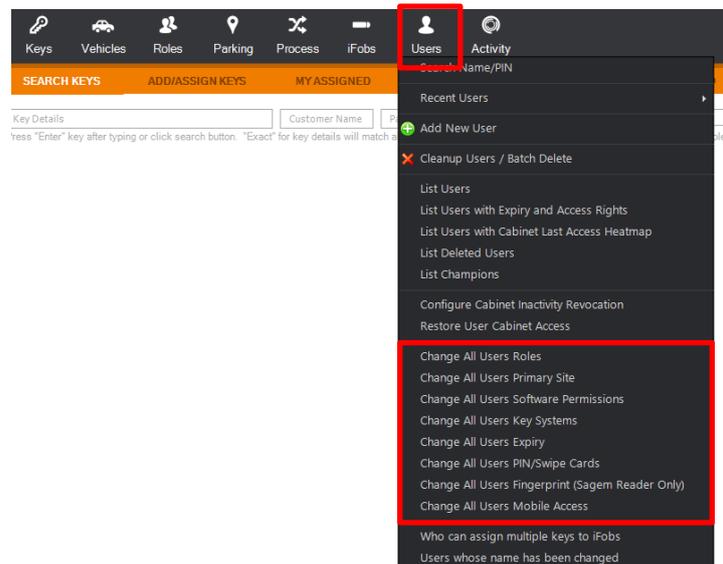
REQUIREMENTS

- If you use a PIN code, then each user must have their own unique code
- If you capture a fingerprint template, then this needs to be unique across users – if you have added the user twice by mistake then you must delete the other records and then resync the one remaining user
- If you capture an optional second fingerprint template this must be from a different finger

BATCH USER CHANGES

There are number of batch user changes that an administrator can perform across multiple users without the need to individual search for them. The functionality is especially useful when trying to review all user roles or adding them to new key system should one be installed.

To access, batch user changes, click on **Users** on the black ribbon and select the task you wish to perform.



TRAKA AUTOMOTIVE: AUTO EXTEND EXPIRY DATE IF INACTIVE

V1.4

traka
ASSA ABLOY

PURPOSE

Users are given an expiry date when they are first added onto the system. By default, this is ten years from the date the user is added.

An expiry date can also be set that is different to the default, for example three months.

As users approach the date of their expiry, you may wish to allow their expiry date to be extended if they are still causing activity on the system within a specific time window.

The user's expiry date will continue to be extended indefinitely if they continue to cause activity.

CONFIGURING EXTENSION PERIOD

Go to the configure menu (cog) and select Configure Global Settings.

From there you can set the amount to extend a user's expiration date by if the user causes activity within the system in a time window of their expiration date.

The default is to extend the expiry date of a user by 90 days if they cause activity within 30 days of their expiration date.

ENABLING AUTO EXTENSION FOR USERS

When adding new users, the default is to automatically extend if there is activity—you can untick the box if you want to exclude the user from this.

By default, existing users will not have their expiry date extended. You can either edit individual users or use the batch edit function.

Go to the user's menu and select Change All Users Expiry. You can then change user's expiry date or enable/disable users from auto-extending their expiry date if they cause inactivity.

Name	Position	Site	ActiveDate	ExpiryDate	Auto Extend	Ignore Inactivity
Traka Admin		None	15/08/2015	15/08/2026	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Test Extend1		None	15/08/2015	15/08/2026	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Test Inactivity		None	16/08/2015	16/08/2026	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Test SixDigitPIN		None	15/08/2015	15/08/2026	<input type="checkbox"/>	<input type="checkbox"/>

Configure Settings

System Defaults | User Defaults | Mandatory Fields | Sites

Guest account enabled

Allow login with PIN on Desktop App

Field Lockdown for Keys: Warnings (Strongly Recommended)

Auto-generate PIN numbers of 6 digits in length

Extend users expiry date by 90 days

when they cause activity within 30 days of their expiry date

Access from 16/08/2015 until 16/08/2026 automatically extend if still causing activity

User is an administrator for iFobs (take any iFob)

Keep user on the cabinet even if no activity

Messages | Vote! | Help

iFobs | Users | Activity

Search Name/PIN

Recent Users

Add User

List Users

- List Users with Expiry and Access Rights
- List Users with Login and PIN codes
- List Users with Cabinet Last Access Heatmap
- List Deleted Users
- List Champions

Configure Cabinet Inactivity Revocation

Restore User Cabinet Access

Change All Users Roles

Change All Users Primary Site

Change All Users Software Permissions

Change All Users Key Systems

Change All Users Expiry

Change All Users PIN/Swipe Cards

Change All Users Fingerprint (Sagem Reader Only)

Change All Users Mobile Access

PURPOSE

Users may be given access permission to one or more cabinets to remove and return keys. Sometimes a user may be given permission to access cabinets they no longer have a need to access or given access to a cabinet inadvertently.

By setting up cabinet inactivity duration, you can enable users to have their permission to access specific cabinets revoked if they do not use that cabinet for a period of time.

Not all users will have their permission revoked due to inactivity. If the user has the "administer systems" permission, then they will not have their inactivity monitored. You can also exclude specific users.

SETTING UP CABINET INACTIVITY DURATION

Go to the user's menu and select **Configure Cabinet Inactivity Revocation**.

Within the **Cabinet Setup** tab, enter the duration of inactivity. You can click the "Set to 30 days" button to quickly set the inactivity duration to 30 days.

Leave this at 0 (or click the reset button) if you want to disable the inactivity revocation.

The **Unaffected Users** tab will show you which users are not affected by inactivity on that cabinet, either as a result of the user being an administrator or the user being specifically excluded.

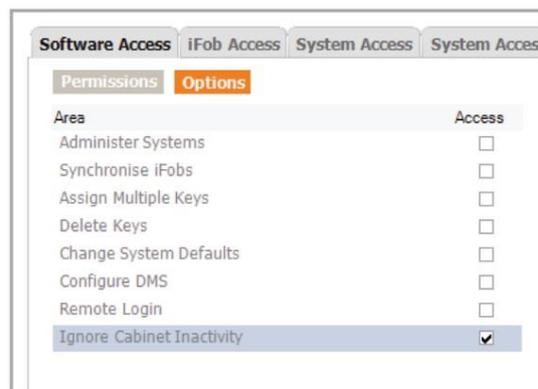
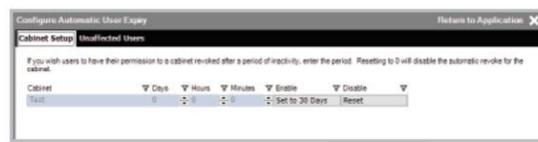
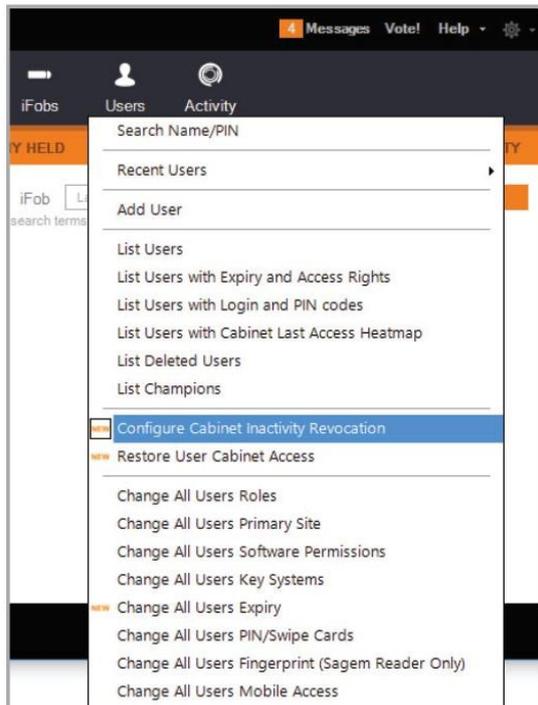
RESTORING CABINET ACCESS TO A USER

Go to the user's menu and select **Restore User Cabinet Access**. You can see which users have recently had their access to a cabinet revoked either due to inactivity or due to an administrator removing their permission.

To restore access, tick the restore box for the user(s) and cabinet(s) and click save.

EXCLUDING USERS

Go to the user's menu and select **Change All Users Expiry**. You can then tick the "Ignore Inactivity" option for the user(s) you wish to exclude and then click save.



You can also exclude a user by editing them and choosing the **Ignore Cabinet Activity** option.