KEYper electronic key management system KEYper GO Web & Web Admin quick start guide



Key management simplified

Introd	lucti	ion
KEYpe	er GC	Web vs. the Web Admin 2
Conne	ect t	o KEYper GO Web
Conne	ect t	o the Web Admin
Add a	sset	s 🕰
1.	Add	assets using blank fobs stored in the cabinet
	1.1	With the Identify Asset feature
		1.1.1 With KEYper GO Web (for SaaS Subscribers)
		1.1.2 With the Web Admin (for on-premise users) 🖳
	1.2	From the Unregistered tab of the Assets screen (for SaaS subscribers)
	1.3	From the Asset Count list (for on-premise users) 📝
Add u	ser	G
1.	Adm	nin vs. user – know the difference
	1.1	User roles
2.	Add	user with KEYper GO Web (for SaaS subscribers)
3.	Add	new user with the Web Admin (for on-premise users) 📝
۸dd م		
Auu a	VVi+h	$Sgroup \rightarrow $
1.	1 1	
	1.1 1 7	Oser list
	1.2 1 2	Asset list
	1.5 1 <i>1</i>	Access times
7	1. 4 \\/i+ŀ	$\frac{1}{24}$
۷.	7 1	Configure/edit access group restrictions
-	2.1	211 Access times
		21.1 / Access times
		21.3 Asset list
		2.1.4 Physical access list.
	. 1=	
кероі	TTS LE	<u>-</u> 28

Introduction

This quick start guide has been prepared to help you get started managing assets, users, and access groups with your KEYper software. It is not meant to be exhaustive. For further information about any of the processes or features mentioned in this quick start guide, see the **KEYper Electronic System Manual** that is included with your software or contact Support.

KEYper GO Web vs. the Web Admin

KEYper GO Web is the new web-based application for SaaS subscribers that expands upon the administrative functionality of our mobile application, KEYper GO. Its modern, user-friendly design makes managing your users, assets, inventory, reservations, and more easier than ever. While the functionality of KEYper GO Web continues to be built upon, there are certain tasks that can only be managed within the classic web application known as the Web Admin. Customers with an on-premise solution who are not subscribed to SaaS will continue to use the classic Web Admin to administer their systems. To subscribe to SaaS and take your key management administration into the cloud, contact Support.

This guide fully explains the functionality of both KEYper GO Web and the Web Admin. Features available within the classic Web Admin only are notated with the *model* icon.

Connect to KEYper GO Web

KEYper GO Web may be opened in a web browser, such as Internet Explorer, Microsoft Edge, Google Chrome, etc.

To log in to KEYper GO Web, do the following:

- 1. Launch a browser window on your computer, tablet, or mobile device.
- 2. Enter the unique URL provided to you by KEYper, generally **keypergo.com/CustomerName**.
 - **?** You are taken to the login screen, as shown in **Fig. 1**.
- 3. Log in with the default admin credentials.

Note: Your system arrives with a default admin profile installed. The PIN is 1234. Use this to log into KEYper GO Web to begin key system administration.

Once you have created your own admin profile, delete the default admin user as a security measure..

Generation Assa are	per BLOY
Lusername	
Password	O
Login	
👼 Biometric Aut	hentication

Fig. 1 – KEYper GO Web login screen

- 4. The first time you log in, you must **acknowledge** a number of legal documents to proceed, as shown in *Fig. 2*.
 - Use the navigation buttons to zoom in/out and scroll through the pages to read the agreements.
 - **The documents include the following:**
 - SaaS Terms of Service
 - End User License Agreement
 - Product Privacy Notice

	~
Software as a Songice (SaaS) Terms of Songice	<u>46'KEYper</u>
Software-as-a-service (Saas) Terms of Service	ASSA ABLOY
	Key management simplified
THESE TERMS OF SERVICE ("TERMS OF SERVICE") ARE THE TERMS AND CONDITIONS UPC ANINDRIVIDUAL END USER, MAKES USE OF ASSA ABLOY GLOBAL SOLUTIONS', INCLUDING AS A-SERVICE OFFERINGS [ACAL A "SERVICE[S]"), FOR CLARIFY, THESE TERMS OF SERVIC PROFESSIONAL SERVICES.	ON WHICH YOU, AN END CUSTOMER, AND/OR GITS ATFILIATIS, 's ("ASSA ABLOY") SOFTWARE- TE DO NOT GOVERN THE SALE OR USE OF
YOU MUST BE AGED 13 YEARS OLD OR OVER TO ACCESS AND USE THE SERVICE(S).	
PLASE RAD THEST FEMS OF SERVICE CAREFULLY BEFORE YOU ACCESS THE SERVICES). THIST TERMS OF SERVICE ANY YOU UPIPSINT A ADVARANT YOUR PULL AUTHORITY BEHALF OF THE END CUSTOMER ANAJOR END USER. THISE TERMS OF SERVICE ANY THE UP WINDOUT NOTICE TO YOUL YOU ANY ARVIVET THISE TERMS OF SERVICE. ANY THE UP ANY ADVARCESS OF SERVICES ANY ADVARCESS ANY ADVARCESS ANY ADVARCESS ANY ADVARCESS ADVARCESS OF UPIPER ANY ADVARCESS ANY ADVARCESS ANY ADVARCESS ANY ADVARCESS ADVARCESS OF USERVICESS.	LPY ACCESSING THE SERVICE(S), YOU ACGEE TO YO INTERINTO THESE TRANS OF SERVICE ON PROTED BY ASSA ABLOY FROM TIME TO TIME PARTMONG OUR WEBSITE HERE: <u>https://www.</u> REE WITH THESE TERMS OF SERVICE, YOU MUST
IF YOU ARE A CHANNEL PARTNER OR OTHER THIRO-PARTY SERVICE PROVIDER ACTING A OTHERWISE SETTING UP THE END CUSTOMER OR END USER ACCOUNT OR PROVISIONIN CUSTOMER OR END USER, YOU AGREE TO BIND END CUSTOMER TO TERMS SUBSTANTIAL	AS AN ACCOUNT ADMINISTRATOR OR NG THE SERVICE(S) DIRECTLY TO THE END LLY SIMILAR TO THOSE SET FORTH HEREIN.
 DEFINED TERMS *AMBIEND* or *AMBIEND* manage antitian which we controlled by a party which controlled by a party which	teak a nativorshich is under common control
with a party, where "control" means the direct or indirect ownership of at least fifty to vote for the directors thereof or the equivalent, so long as such control exists.	percent (50%) of the shares or interests entitled
"APIs" or "APIs" means application programming interfaces provided by ASSA ABLC	DY as part of the Service(s).
measurements of correlating to, an identified or identifiable individual. This includes of an individual's facial features, into er retina, finger or handprins, write, genetics, o Biemetric information also includes data derived from such depictions, images, dos would be reasonably gossible to identify the individual from whose information the	or desimilation to the second se second second sec
"Customer Application" means an application developed or used by End Customer "Customer Application" does not include the Service(s) and is separately provided I integrator that sells compatible software-as-a-service and/or on premise offerings.	r that utilizes APIs and/or the Service(s), by either End Customer or a third-party
"Customer Materials" means End Customer's information, Customer Application, E Personal Data from end users, software, document and any other materials used or s connection with the Service(s).	End Customer Data, Personal Data, including submitted by End Customer or its end users in
"Data Processing Terms" means the terms located at and made part of ASSA ABLOY com/abbal(eng)macy-center/product-prhacy-poilse. If ASSA ABLOY processes an Service(s), ASSA ABLOY shall do so in accondunce with the applicable Data Processis modified by ASSA ABLOY from time to time in accordance with its terms.	's Privacy Notice: https://www.keypersystems. ny Personal Data as a result of providing the ng Terms. The Data Processing Terms may be
"Documentation" means the guides and manuals for use with the Service(s), which customers.	are customarily supplied by ASSA ABLOY to its
"End Customer" means the Customer, or if the Customer is a Reseller, the end custo through a written sale transaction, as applicable for the internal use of such Custom	omer to which the Reseller sells the Service(s)
"Intellectual Property Rights" means worldwide common law and statutory right applications; (b) works of authership, including mask work rights, copyrights, copyri This document is the subject of the copyright and must not be copie	is associated with (a) patents and patent right applications, copyright registrations of or otherwise reproduced,
either in whole or in part, without the express written penniesion	nerkörper ASSA ARLOY.

Fig. 2 – Acknowledge the agreements to proceed

Connect to the Web Admin

Note: KEYper systems should not be assigned a public IP address or made publicly accessible on the Internet. We do not recommend a publicly exposed Internet connection for our products due to the associated security concerns. Ultimately, it is your decision and there may be a particular reason you wish to configure the system in this way, but be aware of the associated risks. If you wish to configure your system to be publicly available on the Internet, complete the Internet Security Acknowledgment Form. Otherwise, we highly suggest subscribing to SaaS/ KEYper GO if you wish to access your system remotely or from a mobile device.

The Web Admin may be opened in a web browser, such as Internet Explorer, Microsoft Edge, Google Chrome, etc.

To log in to the Web Admin, do the following:

- 1. Tap on the **System Info** button on the kiosk Login screen, as shown in Fig. 3.
 - You are taken to the System Info screen, which contains your IP address (e.g., 197.168.25.10).



- Fig. 3 Location of the System Info icon
- Connect to the Web Admin from a PC on the same network 2. by opening your browser and entering the **IP address** of the system in the URL bar, as shown in Fig. 4.

Note: Primary Web Service (WS) and Primary Database (DB) should always indicated CONNECTED.

3. Log in with the default admin credentials.

Note: Your system arrives with a default admin profile installed. The PIN is 1234. Use this to log into the Web Admin to begin key system administration.

9 Once you have created your own admin profile, delete the default admin user as a security measure.

Log in to DESKTOP-J3JTITE Enter Password Login Version: 9.0.8770 Primary WS: CONNECTED Primary WS: CONNECTED Kisk: ID# 871567 View Mobile Registration Code	
ASSA ABLOY	
Fig. 4 – Web Admin login screen	

Add assets 🗣

Note: Only admins may add assets.

Your cabinet arrives without assets attached to the fobs, meaning all fobs in the cabinet are available to be attached to a key or dealer plate. You may register individual assets using KEYper GO Web or register larger quantities of assets using the import function in the classic Web Admin.

Registering an asset means inputting the asset attributes and assigning that information to a particular Sturdifob or iFob, depending on which system you have. Once an asset is registered and assigned to a fob, attach the key and optional Smart Tag to the fob. There are multiple ways of adding assets to your system. This quick start guide only covers one such option. See our comprehensive <u>Asset</u> <u>Registration and Fob Labeling Guide</u> for further information.

1. Add assets using blank fobs stored in the cabinet

Individual assets can be registered on an as-needed basis by adding new assets from unregistered assets (**unused fobs without keys attached that are stored in the cabinet**). Unregistered assets associated with blank fobs that begin with "U-" and can be edited using the Identify Asset feature or by locating the unregistered asset in the Asset Count list.

1.1 With the Identify Asset feature

Check out unregistered assets from the kiosk as needed to add new assets to the system using the Identify Asset feature. This method requires the use of a desktop fob reader. See the **Fob Reader Installation Guide** for installation instructions.

Note: The first section of this procedure, performed at the kiosk cabinet, is the same regardless of whether you are a SaaS subscriber with KEYper GO Web or have an on-premise solution with the legacy Web Admin. Specific steps for KEYper GO Web and the Web Admin are notated.

To add an asset using a blank fob with the Identify Asset feature, do the following:

- 1. Log in to the **kiosk application** as an admin.
- 2. Tap Admin, as shown in Fig. 5.



Fig. 5 – Kiosk Admin menu screen

3. Tap **Unregistered Assets** shown in **Fig. 6** to display a list of all the blank fobs currently in the cabinet.

Note: These instructions assume there are blank, unregistered fobs in the cabinet. If that is not the case, stop here and fill the cabinet with fobs. This allows the fobs to be recognized and their status set to Unregistered.



Fig. 6 – Kiosk admin Settings screen

4.	Select a Check C	s many entries as needed and tap Dut , as shown in Fig. 7 .	Unregistered	Please select 1 or more assets from the list	
	The blan light	cabinet door unlocks. Remove the k fob(s) indicated by the ring(s) of 	Q		
	🕈 The	- The fobs light up sequentially after each	U-503597824		\uparrow
	fob i	s removed until all the fobs selected	U-503598806		\uparrow
	are r	are retrieved.	U-503614928		
			U-503621932		\downarrow
			U-503624673		\downarrow
			Select All D	Deselect All	1-5 of 64
			\leftarrow		\mathcal{L}_{Θ} Check Out
			Fig.	7 – Kiosk Unregistered assets list	

The remaining steps depend on whether you are a SaaS subscriber with **KEYper GO Web** or are running an on-premise solution with the legacy **Web Admin**. The steps for each are as follows.

- 5. Log in to **KEYper GO Web** from a desktop computer with a connected fob reader.
- 6. Click the **Search bar**, as shown in **Fig. 8**.
- 7. Hold the Sturdifob flush against the bottom of the desktop Sturdifob reader or insert the iFob into the desktop iFob reader until you hear a click.
- 8. Click Identify a Fob, as shown in Fig. 8.
- 9. When the unregistered asset is found, click the **quick action menu** in the upper right of the Asset Overview screen, as shown in Fig. 9.
- 10. Click Edit to open the Edit Asset screen.



Fig. 8 – Search screen with Identify a Fob indicated

Overview Acce	ess Groups Transaction	ns Change Log		
Fob N/A Process Ste N/A	Fob Number 503598806	Change	Recent Activity 1123AU MM ¹⁹ 2025 1 Removed asset	Comparing the second seco

- 11. Fill in the Asset Details, as shown in Fig. 10:
 - **Asset Type**: This field is read-only.
 - **Asset Name**: Replace the name of the unregistered asset with an identifier, such as the stock number.
 - **Description**: Enter a description for the asset (e.g., 2011 Jeep Compass).
 - **Registered Type**: Always toggle the switch to **Registered**. This step is critical to allow the asset to be checked out of the cabinet.

← Edit Asset	Save
Asset Details	
Asset Type	
💬 Asset	Ŧ
Asset Name	
U-1043710	
Description	
Registered	

Fig. 10 – Edit Asset screen – Asset Details

- Fill in the Asset Attributes, if desired, as shown in
 Fig. 11, by selecting a value from the dropdown menus.
 - If your desired value does not appear in the dropdown menu, you may manually enter a value.

Note: The default asset attributes (Make, Model, etc.) are set for the Automotive industry. Asset attributes are configurable for your industry within the Web Admin.

7 Type in the vehicle's **VIN**.

usset Attributes			
Year			
Make			
Model			
Ext. Color			
Int. Color			
Туре			
VIN			

Fig. 11 – Edit Asset screen – Asset Attributes

13. Fill in the Asset Settings, as shown in Fig. 12.

- Lot Location Group: If using Lot Location, choose the lot location group. Selecting a lot location group determines the options available in the Lot Location dropdown menu. If unknown, leave blank.
- **Control Content** If using Lot Location, choose the lot where the asset is parked. If unknown, leave blank.
- **Parking Space:** If using Lot Blocking, select the parking space where the vehicle is parked. If unknown, leave blank.
- **Checkout Requires 2nd Authenticator**: If toggled **On**, this user must be verified by another user (authenticator) to log in.
- 14. Click **Save** to commit your changes and return to the Overview tab.
- 15. Click the Access Groups tab, as shown in Fig. 13.
- 16. Select the Access Group(s) for the asset.
 - The members of the selected access groups are the only users able to check out this asset. Admins are automatically made members of all access groups and thus have no restrictions on the assets they may check out.
 - The asset is automatically assigned to the default access group. Uncheck the box if that does not apply.

Note: If an asset is assigned to multiple access groups, the broadest permissions will override the more restrictive permissions in place for a bespoke access group. For example, if you have an access group for Maintenance employees with permissions restricted to specific

hours or the assets within the Maintenance process step, those restrictions are overridden by the broader, non-restricted access afforded by the default access group. To utilize the parameters of the more restricted access group, you **must** remove the asset from the default access group.

- 17. Click the **back** arrow to save your changes and return to the Home screen.
- 18. Attach the key to the fob as described in the Asset Registration and Fob Labeling Guide.
- 19. Check in the **asset** using the kiosk application.

Asset Settings	
- Lot Location Group default	•
Lot Location (None)	-
Checkout Requires 2nd Authenticator	



Overview Access Groups Transactions Change Log	
3 items C F	≷efresh
□ Name ↑ Enabled Description	
Default Group	
Mobile Access Group Group for Mobile Users	
Sales of the sales te	am

Fig. 13 – Asset screen – Access Groups tab

- 1.1.2 With the Web Admin (for on-premise users)
- Log in to the Web Admin. 5.
- 6. Navigate to the Asset Count screen by clicking the Assets tab and choosing Edit Assets.
- 7. Hold the Sturdifob flush against the bottom of the desktop Sturdifob reader or insert the iFob into the desktop iFob reader until you hear a click.
- 8. Click Identify Asset, as shown in Fig. 14.

C	ashbo	ard Repo	rts Users	Fobs	Assets	Access Group	ps Asset Attri	butes Settings	Support		
Asset Co	ount((68)			Ide	ntify Asset					
		Filter	Clear			А	sset registered typ	e Anv 🗸 Svs	tem All		~
				Print	Add Im	port(DMS Style)	Import(Gas D	ata) Delete All Unre	gistered D	elete Sele	ected
Name	Tag	Туре	Description	Status	Registe	ered Type	System	Last Checked Out	Created	Action	
100114		Dealer Plate		Out	Re	gistered I	DESKTOP-J3JT1TE	10/26/2022	10/3/2022	Edit	
1007		Asset	NEW	Out	Re	gistered I	DESKTOP-J3JT1TE	10/26/2022	9/29/2022	Edit	
1008		Asset	NEW	Out	Re	gistered I	DESKTOP-J3JT1TE	10/26/2022	9/29/2022	Edit	
1009		Asset	NEW	Out	Re	gistered I	DESKTOP-J3JT1TE	10/26/2022	9/29/2022	Edit	
1010		Asset	COURTESY	Out	Re	gistered I	DESKTOP-J3JT1TE	10/26/2022	9/29/2022	Edit	

Fig. 14 – Asset Count screen with Identify Asset indicated

9. When the unregistered asset is found, as shown in Fig. 15, click Edit to open the asset record.



Fig. 15 – Unregistered asset found

Update Asset Information

- 10. Fill in the asset information, as shown in Fig. 16.
 - **Name**: Replace the name of the unregistered asset with an identifier, such as the stock number.
 - **Description**: Enter a description for the asset (e.g., 2011 Jeep Compass).
 - Serial Number: This field is read-only and auto-populated by the fob Ŷ reader.
 - **Tag:** If using fob labeling, enter the number of the Smart Tag. For further instructions, see the section on fob labeling in the Asset **Registration and Fob Labeling Guide.**
 - **Status**: This field is read-only.
 - Registered Type: Always change to Registered. This step is critical to allow the asset to be checked out of the cabinet.
 - **Lot Location Group**: If using Lot Location, choose the lot location group. Selecting a lot location group determines the options available in the Lot Location dropdown menu. If unknown, leave blank.
 - **Lot Location**: If using Lot Location, choose the lot where the asset is parked. If unknown, leave blank.



- 9 **Mileage Total**: If you have mileage tracking enabled, enter the vehicle's total mileage.
- P Mileage This Month: If you have mileage tracking enabled, enter the mileage the vehicle has driven so far in the current month.







- 11. Fill in the **asset attributes**, if desired, as shown in **Fig. 17**.
 - **?** Select a **value** from the dropdown menus.
 - If your desired value does not appear in the dropdown menu, click **Enter** to manually enter a value.
 - **7** Type in the vehicle's **VIN**.

Note: The attributes are set for the Automotive industry by default (make, model, etc.). These values are configurable to your industry. Contact Support for further information.

View/Edit Asset Attributes

		Collections	
Year	Select	~	Enter
Make	Select	~	Enter
Model	Select	~	Enter
Ext. Color	Select	~	Enter
Int. Color	Select	~	Enter
Туре	Select	~	Enter
		Single Values	
VIN			



- 12. Select the Access Group(s) for the asset, as shown in Fig. 18.
 - Other than admins, who can check out any asset, the members of the selected access groups are the only users able to check out this asset.

Note: The asset is automatically assigned to the default access group. Uncheck the box if that does not apply.

13. Click **Save** to register the new asset.

Note: If using label printing, select Print Asset Label before saving.

- 14. Attach the key to the fob as described in the Asset Registration and Fob Labeling Guide.
- 15. Check in the **asset** using the kiosk application.

	Access	Group	S	
Select	Name		Description	
~	Default Group			
	-			
	Print Asset Label	Save	Cancel	

Fig. 18 – Access Groups

1.2 From the Unregistered tab of the Assets screen (for SaaS subscribers)

You may also add assets directly to blank fobs listed within KEYper GO Web. To add an asset using a blank fob found on the Unregistered tab of the Assets screen, do the following:

- 1. Log in to **KEYper GO Web**.
- 2. Hover over **Assets** and select **Unregistered**, as shown in **Fig. 19**.
 - Alternately, you can click Assets, then click the Unregistered tab.

ASSA ABLOY	Q Search for something	(CLASSIC [2]) ⊕ Add Z Transfer
🛧 Home 🕠		My Hald
Ov Assets	c∞ Keys se Card⊚	No items to show.
🖽 Equipment)	Plates	
🙇 Admin 🕠		
Reports		
	Reservations	
	Outgoing Transfers No items to show.	
	Collect Now	

Fig. 19 – Hover over Assets and select Unregistered

- 3. Choose an **unregistered asset** from the list to navigate to the Asset Overview screen, as shown in Fig. 20.
 - All unregistered assets in your system are displayed in a list view by default.
 Click Grid or Table to change the view, if desired.



Fig. 20 – Select an unregistered asset

- 4. Click the **quick action menu** in the upper right of the Asset Overview screen, as shown in Fig. 21.
 - **?** Click **Edit** to open the Edit Asset screen.



Fig. 21 – Unregistered asset found

- 5. Fill in the Asset Details, as shown in Fig. 22:
 - **Asset Type**: This field is read-only.
 - **Asset Name**: Replace the name of the unregistered asset with an identifier, such as the stock number.
 - Description: Enter a description for the asset (e.g., 2011 Jeep Compass).
 - **P** Registered Type: Always toggle the switch to Registered.

← Edit Asset	Sav
Asset Details	
Asset Type	
O= Asset	v
Asset Name	
U-1043710	
Description	
Registered	

Fig. 22 – Edit Asset screen – Asset Details

- Fill in the Asset Attributes, if desired, as shown in Fig. 23, by selecting a value from the dropdown menus.
 - If your desired value does not appear in the dropdown menu, you may manually enter a value.

Note: The default asset attributes (Make, Model, etc.) are set for the Automotive industry. Asset attributes are configurable for your industry within the Web Admin.

7 Type in the vehicle's **VIN**.

Asset Attributes		
Year		
Make		
Model		
Ext. Color		
Int. Color		
Туре		
VIN		

Fig. 23 – Edit Asset screen – Asset Attributes

- 7. Fill in the Asset Settings, as shown in Fig. 24.
 - Lot Location Group: If using Lot Location, choose the lot location group. Selecting a lot location group determines the options available in the Lot Location dropdown menu. If unknown, leave blank.
 - **Control Content** If using Lot Location, choose the lot where the asset is parked. If unknown, leave blank.
 - **Parking Space:** If using Lot Blocking, select the parking space where the vehicle is parked. If unknown, leave blank.

Asset Settings	
Lot Location Group	
default	-
- Lot Location	
(None)	•
Checkout Requires 2nd Authenticator	
Checkout Requires 2nd Authenticator	

Fig. 24 – Edit Asset screen – Asset Settings

- Checkout Requires 2nd Authenticator: If toggled On, this user must be verified by another user (authenticator) to log in.
- 8. Click **Save** to commit your changes and return to the Overview tab.
- 9. Click the Access Groups tab, as shown in Fig. 25.
- 10. Select the Access Group(s) for the asset.
 - The members of the selected access groups are the only users able to check out this asset. Admins are automatically made members of all access groups and thus have no restrictions on the assets they may check out.
 - The asset is automatically assigned to the default access group. Uncheck the box if that does not apply.

Note: If an asset is assigned to multiple access groups, the broadest permissions will override the more restrictive permissions in place for a bespoke access group. For example, if you have an access group for Maintenance employees with

← A	sset			:
Overview	Access Groups	Transactions	Change Log	
3 items				C Refresh
	ame 🛧	Enabled	Description	
	Default Group	Ø		
	Nobile Access Group	\bigcirc	Group for Mobile	e Users
	Sales		members of the	sales team

permissions restricted to specific hours or the assets within the Maintenance process step, those restrictions are overridden by the broader, non-restricted access afforded by the default access group. To utilize the parameters of the more restricted access group, you **must** remove the asset from the default access group.

- 11. Click the **back** arrow to save your changes and return to the Home screen.
- 12. Check out the **asset** at the kiosk cabinet.

Note: If you do not see the new asset, try restarting the kiosk application.

- 13. Attach the key to the fob as described in the Asset Registration and Fob Labeling Guide.
- 14. Check in the **asset** using the kiosk application.

Fig. 25 – Asset screen – Access Groups tab

1.3 From the Asset Count list (for on-premise users)



- 1. Log in to the **Web Admin**.
- 2. Navigate to the Asset Count screen by clicking the **Assets** tab and choosing **Edit Assets**.
- 3. Select **Unregistered** from the Asset registered type dropdown menu, as shown in **Fig. 26**.
 - A list of assets with the Registered Type of Unregistered appear.

	Dashbo	ard Repo	ts Users	Fobs	Assets	Access Group	s Asset Attri	butes Settings	Support		
Asset	Count	(68) Eilter	Clear		Ide	ntify Asset					
		T III.en	Jiean			As	sset registered typ	e Any 🗸 ys	tem All		×
				Print	Add Im	port(DMS Style)	Import(Gas Da	ata) Delete All Unre	gistered L	elete Sele	cted
Name	Tag	Туре	Description	Status	Registe	ered Type	System	Last Checked Out	Created	Action	U.,
100114		Dealer Plate		Out	Reg	jistered D	DESKTOP-J3JT1TE	10/26/2022	10/3/2022	Edit	
1007		Asset	NEW	Out	Reg	jistered D	ESKTOP-J3JT1TE	10/26/2022	9/29/2022	Edit	
1007											
1007		Asset	NEW	Out	Reg	gistered D	DESKTOP-J3JT1TE	10/26/2022	9/29/2022	Edit	

Fig. 26 - Asset Count screen with Asset registered type indicated

- 4. Find an unregistered asset that has a name that begins with the U- prefix.
- 5. Click **Edit**, as shown in **Fig. 27**.

ount	(44)							
				Identify Asset				
- 14	Filter	Clear			Asset registered ty	pe Unregistered v Syst	tem All	
			Print /	Add Import(DMS St	yle) Import(6 Attrib	utes) Delete All Unre	gistered I	Delete Sel
Tag	Туре	Description	Status	Registered Type	System	Last Checked Out	Created	Action
	Asset		In	Unregistered	DESKTOP-3V35H7R	2/4/2025	2/4/2025	Edit
				10 State 10	DECICTOR 202EU20	2/4/2025	2/4/2025	C dia
	Asset		In	Unregistered	DESKTOP-3V35H/K	2/7/2023	2/4/2025	Eart
	ount(Filter Tag Type Asset	Filler Clear Tag Type Description Asset	Hilter Clear Filter Clear Tag Type Description Status Asset In	Hilter Clear Filter Clear Print Add Tag Type Description Status Registered Type Asset In	Identify Asset Hilter Clear Asset registered ty Print Add Import(OMS Style) Import(6 Attrib Tag Type Description Status Registered Type System Asset In Unrevisitered DESCRIPTION 3735767 Status Registered Type System	Hiller Clear Asset registered type Unregistered vg Syst Print Add Import(DMS Style) Import(6 Attributes) Delete All Unregistered vg Tag Type Description Status Registered Type System Last Checked Out Asset In Unregistered Type Description Status Registered Type System Last Checked Out	Hiller Clear Asset registered type Unregistered vsystem Ail Print Add Import(OMS Style) Import(6 Attributes) Delete All Unregistered vsystem Ail Tag Type Description Status Registered Type System Last Checked Out Created Asset Description Status Registered Type System Last Checked Out Created

- 6. Fill in the asset information, as shown in Fig. 28.
 - **Name**: Replace the name of the unregistered asset with an identifier, such as the stock number.
 - **Description**: Enter a description for the asset (e.g., 2011 Jeep Compass).
 - **Serial Number**: This field is read-only and auto-populated by the fob reader.
 - Tag: If using fob labeling, enter the number of the Smart Tag. For further instructions, see the section on fob labeling in the <u>Asset</u> <u>Registration and Fob Labeling Guide</u>.
 - **Status**: This field is read-only.
 - **Registered Type**: Always change to **Registered**. This step is critical to allow the asset to be checked out of the cabinet.
 - Lot Location Group: If using Lot Location, choose the lot location group for where the asset is parked. Selecting a lot location group determines the options available in the Lot Location dropdown menu. If unknown, leave blank.
 - **Control Content** If using Lot Location, choose the lot where the asset is parked. If unknown, leave blank.
 - **Parking Space**: If using Lot Blocking, choose the space where the vehicle is parked. If unknown, leave blank.

Asset Type Asset Name U-1229515712 Description Description Search 1229515712 Tag 1229515712 Tag Status Out Charles Status Out Charles Select.... Select.... Mileage Total Mileage This Month

Update Asset Information



- **Mileage Total**: If you have mileage tracking enabled, enter the vehicle's total mileage.
- **Mileage This Month**: If you have mileage tracking enabled, enter the mileage the vehicle has driven so far in the current month.

- 7. Fill in the **asset attributes**, if desired, as shown in **Fig. 29**.
 - **?** Select a **value** from the dropdown menus.
 - If your desired value does not appear in the dropdown menu, click **Enter** to manually enter a value.
 - **?** Type in the vehicle's **VIN**.

Note: The attributes are set for the Automotive industry by default (make, model, etc.). These values are configurable to your industry. Contact Support for further information.

View/Edit Asset Attributes

		Collections	
Year	Select	~	Enter
Make	Select	~	Enter
Model	Select	~	Enter
Ext. Color	Select	~	Enter
Int. Color	Select	~	Enter
Туре	Select	~	Enter
		Single Values	
VIN			



- 8. Select the Access Group(s) for the asset, as shown in Fig. 30.
 - Other than admins, who can check out any asset, the members of the selected access groups are the only users able to check out this asset.

Note: The asset is automatically assigned to the default access group. Uncheck the box if that does not apply.

9. Click **Save** to register the new asset.

Note: If using label printing, select Print Asset Label before saving.

10. Check out the **asset** at the kiosk cabinet.

Note: If you do not see the new asset, try restarting the **kiosk application**.

- 11. Attach the key to the fob as described in the Asset Registration and Fob Labeling Guide.
- 12. Check in the **asset** using the kiosk application.

	Access	Group	<u>s </u>
Select	Name		Description
	Default Group		
	Print Asset Label	Save	Cancel

Fig. 30 – Access Groups

Add user 🗣

GDPR Statement (for European markets only): All organisations using KEYper products supported by Traka should be mindful of their obligations under GDPR (General Data Protection Regulations) in the UK and the EU, and any similar legislation in other jurisdictions that relate to personal data. The organisation should have determined its lawful basis for holding and using personal data, including a separate determination for any "special" categories of data. Where data is used on the basis of "consent," this consent must be given freely (i.e., there is a genuine alternative), must be recorded, and must be capable of being withdrawn. Data backups should be stored securely for as long as necessary (but no longer), and then destroyed securely. Any hardware containing personal data (E.g., KEYper cabinets and lockers or servers holding user databases) should have the data securely destroyed once the data is no longer needed in that hardware.

Note: When setting up a new system, it is recommended that you add just essential system administrators, then decide on the need for additional access groups. Creating additional groups (Sales, Vendors, etc.) enables easier access group assignment when adding users. There is no need to create an access group for essential system administrators as they are not restricted in any way.

Only admins may create new users.

1. Admin vs. user – know the difference

Admins

- 🕈 By default, can access KEYper GO Web and the Web Admin
- Ŷ Override all access group restrictions
- Have access to the admin functions of the kiosk, KEYper GO Web, and the Web Admin

Users

- By default, cannot access the KEYper Web Admin, but an admin can grant any user such access according to the permissions explained in User roles
- Ŷ Adhere to assigned access group restrictions
- **?** Can only check in, check out, and identify keys at the kiosk

1.1 User roles

User access permissions are further split into None, Limited, and Full:

- **None**: These users may only check assets in or out at the kiosk. They have no permissions within KEYper GO Web or the Web Admin.
- Limited: These users may view and transfer assets, view and create quick reservations, and view scan sessions within KEYper GO Web and/or the Web Admin.
- **Full**: These users may additionally edit assets, reservations, and scan sessions.

2. Add user with KEYper GO Web (for SaaS subscribers)

To add a new user using KEYper GO Web, do the following:

- 1. Log in to **KEYper GO Web**.
- 2. Click Add, then click Add User, as shown in Fig. 31.
 - ♀ The Create User screen opens.





3.	Fill in the User Information , as shown in Fig. 32 :	Lios Information
(🕈 First Name	USEI IIIOITTAUOIT
(🕈 Last Name	First Name
(P Description	
	• A description of the user (e.g., position title).	Last Name
(🕈 Email Address	
	 This field is required if you wish to have the user receive email notifications. 	Description
(Password/Confirm Password Must contain a minimum of seven alphanumeric characters with 	Email
	 at least one special character. Used for logging into the mobile app and the Web Admin. 	New Password
	• Can be the same as other users' passwords.	Confirm Password
(PIN/Confirm PIN Must contain a minimum of four numeric digits. 	e PIN
	 Only required if the user requires cabinet access, as the PIN is used to log in at the kiosk cabinet. 	Confirm PIN
	Must be unique from other users' PINs.	Preferred Locale
(Preferred Locale	English (US)
	 Select the user's preferred language. This ensures the klosk software is automatically set to the user's preferred language when they log in at the cabinet. 	Rephone Number
(🕈 Phone Number	Time Zone
	For SMS notifications	📋 🕓 (UTC-05:00) Eastern Time (US & Canada)

- For SMS notifications.
- **†** Time Zone
 - Ensure you enter the time zone where the user is located, not that of the admin inputting the user's information, if they differ.

Fig. 32 – Create User screen – User Information

(ED024 Rev G 06/20/25

4. Set the User Permissions, as shown in Fig. 33:

🕈 Role

 Set to Admin or User. See Admin vs. user – know the difference.

Access Permissions

- None: These users may only check assets in/out at the kiosk. They have no permissions within KEYper GO Web, the Web Admin, or the mobile app.
- Limited: These users may additionally view/transfer assets, view/ create quick reservations, and view scan sessions within the mobile app.
- **Full**: These users may additionally edit assets, reservations, and scan sessions within KEYper GO Web, the Web Admin, or the mobile app.

📍 Issue Limit

• The number of keys this user may have checked out of the key system at any given time. Zero indicates no limit.

🕈 Requires Transfer Approval

• By default, users must have admin approval before transferring a key. Toggle **off** to disable this requirement.

🕈 Dual Authentication Authorizer

• If toggled **on**, this user is able to verify another user to enable them to log in. An authenticator need not be an admin.

P Requires Dual Authentication

• If toggled **on**, this user must be verified by another user (authenticator) to log in.

📍 Locked Out

• If toggled **on**, the user has been locked out after too many failed login attempts. An admin must restore access by toggling the switch **off**.

🕈 Allow On Behalf Of

• Toggle **on** to allow a user to check out an asset and then hand it over to another party without formally transferring it into their possession. One such use case may be a one-time, temporary handover of a key to a third party contractor who is not set up as a user in the system. The user who checked out the asset is ultimately responsible for it.

5. Configure the User Settings, as shown in Fig. 34:

9 Notification Settings

- Check to allow notifications regarding reservations and alerts (admins only) via SMS text message, email, or both.
- To enable two-factor authentication, you must provide a phone number or email address and select at least one notification option. You will receive a text and/or email with a six-digit code to confirm your enrollment in two-factor authentication.

🕈 Assigned Dealer Plate

• If a user is assigned a specific dealer plate, select it from the dropdown menu.

📍 Prox or Swipe ID

• For systems incorporating a proximity card reader. If the number is known, it may be entered at the time the user is added to the system. This field is auto-filled when the user's card is read during device enrollment.

📍 Fob Login ID

• Use this field to scan a fob that the user can use to log in to the kiosk application.

User Access Permissions None \cap Limited Full \cap # 0 Requires Transfer Approval Dual Authentication Authorize 1 Requires Dual Authentication Locked Out Allow On Behalf Of assets to temporarily give them to someone else



User Settings		
Notification Settings		
Allow SMS	Allow Email	
Assigned Dealer Plate		
I None		•
O Prox or Swipe ID		
# Fob Login ID		

Fia	31-	Croato	1 lcor	scroon	_ llcor	Sotting
i ig.	JT -	CICUIC	USCI	SCICCII	- 0301	Julings

- 6. Click Save.
 - You are redirected to the Access Groups tab as shown in *Fig.* 35.
- 7. Select the Access Group(s) to which the user belongs.
 - The user is automatically assigned to the default access group. Uncheck the box if that does not apply.

← Use	er				:
Overview	Access Groups	Held Assets	Transactions	Change Log	
4 items					C Refresh
Enabled	Name ↑			Description	
0	Default Group				
	Demo			vehicles currently in the demo process step	
	Maintenance			Members of the Maintenance team	
	Only Thursday			Only Thursday	



Admins are automatically made members of all access groups and thus have no restrictions on the assets they may check out.

Note: Creating access groups before entering users is helpful. Otherwise, for access groups created after users have been entered into the system, a user's access group membership must be edited through the user's profile or by editing the user list for individual access groups. See Add access groupu.

8. Click the **back arrow** to return to the Users tab of the Admin screen.

3. Add new user with the Web Admin (for on-premise users) 📝

To add a new user using the legacy Web Admin, do the following:

- 1. Log in to the **Web Admin**.
- 2. Click the **Users** tab.
- 3. Select Edit Users, as shown in Fig. 36.



Fig. 36 – Dashboard with Edit Users selected

4. On the User List screen, click **Add**, as shown in *Fig.* **37**.

User List (6)	Filter Clear				Print Add	Import Delete S	Selected			
Name	Description	User Role	Assets Out	Last Kiosk Login	Created	Action				
KEYper Admin	Owner	Admin	0	6/3/2024	9/6/2022	Edit Delete				
User 02	User 02 Sales		0	10/19/2022	9/6/2022	Edit Delete				
User 03	Marketing	User	0	9/6/2022	9/6/2022	Edit Delete				
	Fig. 37 – User List screen with Add indicated									

- 5. Fill in the user's information, as shown in Fig. 38:
 - 🕈 First Name
 - 📍 Last Name
 - **P** Description
 - A description of the user (e.g., position title).
 - Preferred Locale
 - This ensures the kiosk software is automatically set to the user's preferred language when they log in at the cabinet.

Note: Alerts regarding a user whose locale is different than the default locale for the system is generated in the user's preferred language. For example, if a user's preferred language is Spanish and they check out a key without permission, an alert is generated in Spanish and sent out to the names on the notification list, regardless of the recipients' preferred language(s). The log entry also appears in the user's preferred language rather than the system's specified language.



Fig. 38 – Add New User screen

- 📍 Time Zone
 - Ensure you enter the time zone where the user is located, not that of the admin inputting the user's information, if they differ.

9 Email Address

• This field is required if you wish to have the user receive email notifications.

Password

- Must contain a minimum of seven alphanumeric characters with at least one special character.
- Used for logging into the mobile app and the Web Admin.
- Can be the same as other users' passwords.

📍 Is Locked Out of Website

• If checked, the user has been locked out after too many failed login attempts. An admin must restore access by un-checking this box.

PIN/Confirm PIN

- Must contain a minimum of four numeric digits.
- Only required if the user requires cabinet access, as the PIN is used to log in at the kiosk cabinet.
- Must be unique from other users' PINs.

📍 Fob Login ID

• Use this field to scan a fob that the user can log in to the kiosk application with.

🕈 Role

• Set to Admin or User. See Admin vs. user – know the difference.

9 Administrative Permissions

- None: These users may only check assets in/out at the kiosk. They have no permissions within the Web Admin or the mobile app.
- Limited: These users may additionally view/transfer assets, view/create quick reservations, view scan sessions within the mobile app, and clear alarms (if Support has enabled that capability).
- Full: These users may additionally edit assets, reservations, and scan sessions within the Web Admin or the mobile app and clear alarms (if Support has enabled that capability).

🕈 Multiple Authentication Required

• If marked True, this user must be verified by another user (authenticator) to log in.

9 Multiple Auth Authenticator

• If marked **True**, this user is able to verify another user to enable them to log in. An authenticator need not be an admin.

🕈 Favorite Asset

• Typically used for Fleet management, the Favorite Asset field is tied to the Mileage Tracking feature. If you have the system configured to restrict check-out to the vehicle with the least amount of miles on it, this field overrides that functionality and allows a user to check out the asset specified in this field.

Assigned Asset

 Assigned Asset restricts check-out to the vehicle specified in this field only.

P Dealer Plate

• If a user is assigned a specific dealer plate, select it from the dropdown menu.

? Cell Phone Number

- For SMS notifications.
- **?** Cell Phone Carrier
 - For SMS notifications on on-premise systems only (not applicable to cloud/SaaS systems).

P Receive Messages

• Set to No, Email only, SMS only, or Both email and SMS.

Prox ID or Swipe ID

• For systems incorporating a proximity card reader. If the number is known, it may be entered at the time the user is added to the system. This field is auto-filled when the user's card is read during device enrollment.

📍 Issue Limit

- The number of keys this user may have checked out of the key system at any given time. Zero indicates no limit.
- 6. Select the **Default Group** or assign the user to another listed access group, as shown in Fig. 40.
 - ♀ If users are assigned to multiple access groups, the access permissions of the broadest access group will override the more restricted permissions of the other assigned access groups.

	Access Groups								
Select	Name	Description							
	Default Dealer Plate Group								
	Default Group								
	Service	process step access group for service							
	Save Cancel								
	Fig. 10 - Add New User access group options								

-ig. 40 – Add New Oser access group options

Note: Creating access groups before entering users is helpful. Otherwise, for access groups created after users have been entered into the system, a user's access group membership must be edited through the user's profile or by editing individual access groups.

7. Click Save.



Fig. 39 – Add New User screen continued

Add access group 🗣

Access groups allow admins in your organization to set parameters surrounding groups of users' permissions and access. Admins may enable or disable members of the group and customize access times, set which assets group members may check in and out, and set which cabinets they have permission to use. Common access groups align with the departments within a business, such as Service, Maintenance, and Sales, but it is not necessary to set them up in this way.

Note: It is recommended that you create access groups that suit your business before you begin to import assets and users into your database.

1. With KEYper GO Web (for SaaS subscribers)

To create a new access group using KEYper GO Web, do the following:

- 1. Log in to **KEYper GO Web**.
- 2. Click Add, then click Add Access Group, as shown in Fig. 41.
 - **9** The Create Access Group screen opens.



Fig. 41 – Select Add Access Group from the Add menu

- 3. Enter the desired **name** for the access group (e.g., Managers), as shown in Fig. 42.
- 4. Enter an optional **Description** for the access group (e.g., 3rd Shift Manager Access).
- 5. Select the Access Group Type.
 - The default access group type is Standard, which is used for all access groups not associated with a particular process step.
 - A process step access group is used to give access to keys only when they are in a particular process step.

← Create Access Group			Save
Name			
Description			
Access Group Type			
Standard			*
Issue Limit (0 indicates no limit)			
# 0			
Dava	Out Duration Li	mit	
() ()	0	0	

Fig. 42 – Create Access Group screen

- 6. Set the desired **Issue Limit** for the group.
 - **?** Issue limit is the number of keys each user in the group may have checked out of the system at any given time.
 - 📍 If the limit is 10, each user in the group may have up to 10 keys checked out at any given time.
 - **?** Zero indicates there is no specified limit.
- 7. Set the desired **Out Duration** time limit.
 - Once a key has been checked out past the set time limit, the asset's status changes from Out to Overdue, and an alert is sent to all recipients on the Out Duration Exceeded alert list.
 - ♀ Zero indicates there is no specified limit.
- 8. Click Save.
 - You are returned to the Overview screen on which a success message indicates that the group is added into the system and the final settings can be configured, as described in the following sections.

1.1 User list

To edit the user list for a selected access group, do the following:

- 1. Click the **Users** tab, as shown in **Fig. 43**.
- 2. Click the **enable** bubble beside each user you want to assign to the access group.
- 3. Navigate away from the screen to automatically save your changes.



Fig. 43 – Access Group screen – Users tab

Physical Access

Description

2022 Audi S8

2023 BMW 325

2023 BMW M5

2023 BMW 525

2023 BMW M3

2023 BMW M3

Fig. 44 – Access Group screen – Assets tab

Access Time

C Refres

←

Overview

1386 item

Name 1

1008

1011

1012

1013

1014

1015

Access Group

Enable

1.2 Asset list

To edit the asset list for a selected access group, do the following:

- 1. Click the Assets tab, as shown in Fig. 44.
- 2. Click the **enable** bubble beside each asset you want to assign to the access group.
- 3. To commit mass changes, click the box in the column to **Select All** or **check the box** beside all assets that you want to add to or remove from this group.
 - **?** Click **Add** to add new assets to the group.
 - A message appears asking you to confirm that you want to add the selected assets to the access group.
 - **?** Click **Remove** to remove unwanted assets from the group.
 - A message appears asking you to confirm that you want to remove the selected assets from the access group.
- 4. Navigate away from the screen to automatically save your changes.

1.3 Physical access list

To edit the physical access list for a selected access group, do the following:

- 1. Click the **Physical Access** tab, as shown in **Fig. 45**.
 - 📍 The system map displays.
- 2. Click the **check box** next to all locations, systems, and cabinets that are to be included in this group.
- 3. Click Save to commit your changes.
 - **?** A success message appears when your changes have been saved.





1.4 Access times

To edit access times for a selected access group, do the following:

- 1. Click the Access Times tab, as shown in Fig. 46.
- 2. Click **Add** to open the Create Access Time screen.

<i>←</i> /	Access G	oup		_					
Overview	Users	Assets	Physical Access	Acces	ss Times				
All access	times are in t	he time zon	e of the key system.						
One item									
						Day↑	Start Time	End Time	
						Monday	07:30 AM	07:00 PM	1

Fig. 46 – Access Group screen – Access Times tab

- 3. Select the desired **Day**, then enter the **Start Time** and **End Time** for the access window, as shown in *Fig.* 47.
 - You may have multiple access times per day, if desired. For example, if you want to restrict access during lunch hours, you may restrict access to a block of time in the morning and a second block of time in the afternoon.
- 4. Click Save.
- 5. Follow the same steps for each day of the week during which users in the access group are allowed to access the system.
- If there are existing access times for a given day, you may click the Edit (pencil) icon to make changes, as shown in Fig. 48.
- 7. If there are existing access times for a day on which you do not wish to allow access, check the box next to the time you wish to remove, then click **Delete** to remove the entry.
- 8. Navigate away from the screen to automatically save your changes.



lverview	Users	Assets	Physical Access	Access Times					
II access tir	nes are in t	he time zon	e of the key system.						🕀 Add
One item									C Refresh
					Day↑	Start Time	End Time	_	
					Monday	07:30 AM	07:00 PM		

2. With the Web Admin (for on-premise users)

It is recommended that you create access groups that suit your business before you begin to import assets and users into your database.

To create a new access group using the legacy Web Admin, do the following:

- 1. Log in to the **Web Admin**.
- 2. Navigate to the Access Group List screen by clicking the Access Groups tab and selecting Edit Access Groups.
- 3. Click Add, as shown in Fig. 49.
 - You are redirected to the Add New Access Group screen.



- 4. Enter the desired **name** for the access group (e.g., Managers), as shown in **Fig. 50**.
- 5. Enter a **Description** for the access group (e.g., 3rd Shift Manager Access).
 - **?** This field is not mandatory.
- 6. Select the Access Group Type.
 - The default access group type is Standard, which is used for all access groups not associated with a particular process step.
 - A process step access group is used to give access to keys only when they are in a particular process step.
- 7. Set the desired **Issue Limit** for the group.
 - Issue limit is the number of keys each user in the group may have checked out of the system at any given time.



Fig. 50 – Add New Access Group screen

- \P If the limit is 10, each user in the group may have up to 10 keys checked out at any given time.
- **?** Zero indicates there is no specified limit.
- 8. Set the desired **Out Duration** time limit.
 - Once a key has been checked out past the set time limit, the asset's status changes from Out to Overdue, and an alert is sent to all recipients on the Out Duration Exceeded alert list.
 - ♀ Zero indicates there is no specified limit.
- 9. Click Save.
 - The group is added into the system and the final settings can be configured, as described in the following sections.

Note: Always click Save after configuring or editing access group settings.

2.1 Configure/edit access group restrictions

To configure and/or edit the restrictions for a selected access group, do the following:

- 1. Navigate to the Access Group List screen by clicking the Access Groups tab and selecting Edit Access Groups.
- 2. Click **Edit** for the desired group, as shown in **Fig. 51**.

	Dashboard	Reports		Fobs		Access Groups	Asset Attributes	Settings Supp	port
Access (Group List	(3)							
			_						
	Filte	r Clea	r						A
	Name			Descript	tion	Issue Li	mit Out Duration	Limit Create	d Action
Default I	ealer Plate Grou	p				0	20:00:0	6/14/202	22 Edit
D Gradie e						0	00.00.0	0/20/202	0 Edit Dalata

Fig. 51 – Access Group List screen with Edit indicated

- 3. You are redirected to the Update Access Group Information screen, as shown in *Fig.* **52**. Within this screen, you can edit the following settings:
 - **P** Access times
 - 📍 User list
 - **?** Asset list
 - **Physical access list**



Fig. 52 – Update Access Group Information screen

2.1.1 Access times

To edit access times for a selected access group, do the following:

- 1. Click **Access Times** to expand the window, as shown in *Fig.* **53**.
- 2. Click Add Time.
 - If there are existing access times for a given day, you may click Edit in the Action column of that day to make changes.
 - If there are existing access times for a day on which you do not wish to allow access, click **Delete** to remove the entry.



Fig. 53 – Access Times menu

- 3. Select the desired **Day**, then enter the **Start Time** and **End Time** for the access window, as shown in *Fig.* **54**.
 - Ŷ Use the 24-hour format.
- 4. Click **OK**.
- 5. Follow the same steps for each day of the week during which users in the access group are allowed to access the system.





2.1.2 User list

To edit the user list for a selected access group, do the following:

- 1. Click User List to expand the window, as shown in Fig. 55.
- 2. Click Edit to see the list of all users in the system.





- Click Select All or check the box for each user to be assigned to 3. this group, as shown in Fig. 56.
- 4. Click Save.



Fig. 56 – Select Users pop-up

2.1.3 Asset list

To edit the asset list for a selected access group, do the following:

- 1. Click Asset List to expand the window, as shown in Fig. 57.
- 2. Click Edit to see the list of all assets in the system.



Fig. 57 – Asset List menu

- 3. Click Select All or check the box next to all assets that are to be assigned to this group, as shown in Fig. 58.
- 4. Click Save.



2.1.4 Physical access list

To edit the physical access list for a selected access group, do the following:

- 1. Click **Physical Access List** to expand the window, as shown in *Fig.* **59**.
 - **?** The system map displays.
- 2. Click the **checkbox** next to all locations, systems, and cabinets that are to be included in this group.
- 3. Click Update.
- 4. Click **Save** to commit your changes.







GDPR Statement (for European markets only): All organisations using KEYper products supported by Traka should be mindful of their obligations under GDPR (General Data Protection Regulations) in the UK and the EU, and any similar legislation in other jurisdictions that relate to personal data. The organisation should have determined its lawful basis for holding and using personal data, including a separate determination for any "special" categories of data. Where data is used on the basis of "consent", this consent must be given freely (i.e. there is a genuine alternative), must be recorded, and must be capable of being withdrawn. Data reports should be stored securely for as long as necessary (but no longer), and then destroyed securely. Any hardware containing personal data (e.g., KEYper cabinets and lockers, or servers holding user databases) should have the data securely destroyed once the data is no longer needed in that hardware.

There are a number of reports about your key management system available to you right out of the box. KEYper's software allows you to track a variety of metrics regarding the use of your system, as well as the ability to create custom reports tailored to your business.

Currently, reports are only available using the classic Web Admin. KEYper GO Web users should click **OPEN CLASSIC REPORTING** to launch the Web Admin in a new tab and manage their reports.

To view existing reports and create your own, do the following:

- 1. Log in to the **Web Admin**.
- 2. Click the **Reports** tab, as shown in *Fig.* 60.
- 3. Choose the desired kind of report.



Fig. 60 – Dashboard with Reports selected