



Elite System Manual

KEYper® Systems





Version History

Rev	Date	Editor	Description	ECN
A	12/1/2020	John Bishop	USB Port Declaration	
B	12/2/2020	John Bishop	Added Version History Table	
C	12/03/2021	Allan Parsons	UI Redesign Image Update, Default Elite Web Admin UN/Password, Browser Agnostic Fob Reading	
D	12/30/2021	Allan Parsons	Updated User Import Table Sample	
E	2/22/2022	Allan Parsons	Included Process Step Section	
F	06/02/2022	John Bishop	Included Biometric Policy	
G	01/16/2023	John Bishop	Included Product Privacy Notice	



Contents

<i>Biometric Policy</i>	5
<i>Product Privacy Notice</i>	8
Personal Information we collect from you	8
Sharing Personal Information	10
Uses made of the information	10
Retention of your information.....	10
Disclosure of your information	11
Where we store your personal data	12
Your rights.....	12
Complaints	12
Links	13
Changes to our Privacy Notice	13
Contact.....	13
<i>Elite Web Administration Site Guide</i>	14
<i>Connect to the Web Administration Site</i>	15
<i>The Dashboard</i>	16
<i>Manage Users – Edit, User Change Log</i>	17
Add New User	17
Edit a User.....	19
Deleting a User.....	19
Importing a User List.....	20
<i>Manage Assets – Edit Assets, Assets with Attributes, Asset Change Log</i>	21
Loading Fob Reading Drivers (MX/MX+ only).....	21
Importing Assets	22
Adding Assets.....	23
Adding Assets from a Blank Record (MX/MX+ Only).....	23
Adding Imported Assets (MX/MX+ Systems).....	24
Adding Unregistered Assets (MX/MX+ Systems).....	24
Adding Unregistered Assets (HC/MXi Systems).....	25
Deleting Assets.....	26



Assets with Attributes (Manage Assets > Assets with Attributes)	27
Assets Change Log (Manage Assets > Assets Change Log)	27
<i>Access Groups – Edit, Access Group Change Log</i>	<i>27</i>
Creating New Access Group (Access Groups > Edit Access Groups)	27
Configuring / Editing Access Group Settings & Restrictions (Access Groups > Edit Access Groups).....	28
Access Group Change Log (Access Groups > Access Group Change Log)	29
<i>Asset Attributes.....</i>	<i>29</i>
<i>Reports</i>	<i>31</i>
<i>Settings.....</i>	<i>32</i>
<i>Support.....</i>	<i>37</i>
<i>Elite Series Kiosk Administration Guide.....</i>	<i>38</i>
<i>Login.....</i>	<i>39</i>
<i>Check In, Identify Asset, Check Out.....</i>	<i>39</i>
<i>Device Enrollment - Configuring Access for Users.....</i>	<i>40</i>
Pin Code Access	40
Fingerprint Access.....	40
Prox ID or Swipe ID Card Access	41
<i>Unregistered Assets</i>	<i>42</i>
<i>Diagnostics.....</i>	<i>42</i>
<i>Manage Assets.....</i>	<i>43</i>
Add New (Manage Assets > Add New)	43
Edit/Delete (Manage Assets > Edit/Delete).....	44
<i>Exit Application</i>	<i>45</i>
<i>USB Port Declaration.....</i>	<i>46</i>
<i>Elite Series Kiosk User Guide</i>	<i>47</i>
<i>Login.....</i>	<i>48</i>
Pin Code Access	49
Fingerprint Access.....	49
Proximity (Prox) or Magnetic Strip Card Access	49
Reset Kiosk.....	49
Unable to Login?	49
<i>Check In</i>	<i>49</i>
Single Cabinet Check In.....	49
Asset Not Locked In (MX+ Only)	49
Multi-Cabinet Check In	50



Process Step Check In	50
<i>Identify Asset (MX ONLY)</i>	51
<i>Check Out</i>	52
Check Out by Name	53
Check Out by List	54
Check Out – Filter Assets	54
Unable to Locate or Check Out an Asset?	57
Multi-Cabinet Checkout	57
<i>Log Out</i>	58
<i>Optional Features</i>	59
Issue Reason and Comment	59
Print Receipt	60
Lot Location	61
<i>Installation Guide</i>	62
Safety	63
Care and Handling	63
Large Cabinet Wall Mounting	64
Small Cabinet Wall Mounting	65
Mini Cabinet Wall Mounting	66
Installation of Wall Mounted System	67
Installation of Stand Mounted System	69
Connections	71



Biometric Policy

KEYper Systems (“KEYper”) has instituted the following policy related to any finger-sensor or biometric data that KEYper may possess, if any, as a result of KEYper’s customers’ and customers’ employees’ and/or other individuals who are provided access to the KEYper devices (“User” or “Users”) and/or use of KEYper products and services and whose data is transmitted or disclosed to KEYper by its customers. KEYper’s customers are responsible for developing and complying with their own biometric data policies, including retention and destruction policies, as may be required under applicable law as further set forth below.

BIOMETRIC DATA DEFINED

As used in this policy, biometric data means any biological characteristics of a person, or information based upon such a characteristic, including characteristics such as those defined as “biometric identifiers” and “biometric information” under the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, et seq. (“BIPA”). Biometric identifier” means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. “Biometric information” means any information, regardless of how it is captured, converted, stored, received through trade or otherwise obtained or shared, based on an individual’s biometric identifier used to identify an individual. The KEYper devices utilize a finger-sensor which may be considered to collect biometric data.

COLLECTION, STORAGE, USE, AND TRANSMISSION OF BIOMETRIC DATA

KEYper’s customers are responsible for compliance with applicable law, governing any collection, capture, receipt through trade or otherwise obtained, possession, storage, use, and/or transmission of biometric data they conduct or facilitate, including, but not limited to, BIPA; Tex. Bus. & Com. Code § 503.001; Wash. Rev. Code § 19.375.020; Virginia Consumer Data Privacy Act, § 59.1-574(A)(5); “the New York Stop Hacks and Improve Electronic Data Security Act, N.Y. Gen Bus. Law § 899-bb; “Arkansas Code § 4-110-103(7); Colorado Privacy Act. Colo. Rev. Stat. 6-1-1301 et.seq. and any other local, state and



federal statute enacted into law. KEYper's customers shall obtain written authorization from each User of KEYper devices to collect, capture, receive or otherwise obtain, possess, store, use, and/or transmit biometric data prior to the collection of such data. Specifically, KEYper must inform its customers that they must:

1. Establish a retention and destruction schedule that complies with any required statute including, but not limited to, BIPA, must make such policy available to the public and need to follow that schedule with timely data deletion;
2. Notify the subjects of collection or Users, in writing, that finger-sensor data is being collected, captured, received through trade, otherwise obtained, possessed, stored, used, and disclosed by KEYper's customers and/or KEYper;
3. Notify the subjects of collection or Users in writing of the purposes and length of term that finger-sensor data is being collected, captured, received through trade, otherwise obtained, possessed, stored, used and disclosed by KEYper's customers and/or KEYper; and
4. Obtain a written release consenting to the collection, capture, receipt through trade or otherwise obtain, possession, storage, use and disclosure of finger-sensor data by KEYper customers and/or by KEYper.

KEYper and/or its vendors may receive, store, use and/or transmit any biometric data solely for access to KEYper devices and keys stored therein. Neither KEYper nor its vendors will sell, lease or trade any biometric data that it receives from customers or customer employees as a result of their use of KEYper devices and services.

RETENTION SCHEDULE

KEYper will retain any client's employee's or User's biometric data in KEYper's possession, if any, until the customer notifies KEYper Systems that it has terminated the employee or User or discontinued their access to the KEYper devices. When KEYper Systems receives notification that (1) a customer's employee's employment has been terminated or the employee's or User's access has been discontinued; or (2) the customer otherwise has discontinued using the KEYper devices; or (3) the User requests in writing that his/her data be deleted. KEYper's retention of finger-sensor or biometric data shall be no



longer than the earlier of the date when (i) the customer ceases to have a relationship with KEYper or (ii) within three (3) years after the customer informs KEYper that its last interaction with User has occurred.

BIOMETRIC DATA STORAGE

KEYper and/or its vendors shall use the reasonable standard of care in KEYper's industry to store, transmit and protect from disclosure any finger-sensor or biometric data collected or received, and shall store, transmit, and protect from disclosure all finger-sensor or biometric data in a manner that is the same as or more protective than the manner in which KEYper stores, transmits, and protects other personal information of Users.



Product Privacy Notice

Marcon International, Inc. doing business as KEYper Systems (“We”, “Us”, or “Our”) are committed to protecting and respecting your privacy. The practices of our processing of your personal data when using this KEYper service and/or submitting feedback to us are described herein. This Privacy Notice sets out the basis on which we will process the personal data we collect from you, or that you provide to us.

We act as a Service Provider and/or Data Processor which may receive and process information on behalf of our business customer which is the Data Controller for their own business purposes. The business customer should have its own separate Privacy Notice, which you should read to understand their views and practices. Data submitted through, or received from, the service is owned and controlled by the business customer.

In some limited instances we may be the entity responsible for the processing and act as Data Controller. We only collect the minimal information (as set out below) necessary for our legitimate interests:

- Ensure reliability and quality of the service, correct faults if needed; and
- Identify aspects of the service which could be improved
- Protect against, identify, and prevent fraud and other unlawful activity

Where practical, we anonymize or statistically aggregate the information we collect. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it.

The Data Controller for the data described in this Privacy Notice is Marcon International LLC t/a KEYper Systems 5679 Harrisburg Industrial Park Dr, Harrisburg, NC 28075, USA.

Personal Information we collect from you

When using the KEYper service, we will collect and process the following data about you:

- When you are logged in, your unique user identifier, which is linked to your portal login.
- Your browser “user-agent”, which may include information on the web browser you are using and your operating system.
- Features you interact with while using the service
- Errors or exceptions that occur during your session.

With your consent we may also collect:

- Analytics data, relying on cookie technologies regarding usage of our services
- Crash data that contains a short log of events that occurred in the run up to a crash

For clarity, we do not collect data you submit to the service, or receive from it, as part of our monitoring activities. Only the act of submitting or receiving is recorded. For example, we may record that you entered information in a particular



form field, but not the information itself, or, we may record that you ran a particular report, but not the resulting details of the report.

When you submit feedback, we will collect and process the following data about you:

- The information you submit in the feedback form or via email.
- The URL of the page you were on when you submitted the feedback.
- The web browser you used to submit the feedback.
- The user account you submitted the feedback from.

In more detail, we have collected the following categories of personal information from consumers within the last twelve (12) months where a 'YES' is indicated in the relevant category. Note the business customer could be processing additional categories for which we are not the responsible organization.

Category	Examples	Collected
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name	YES
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code §1798.80(e))	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	NO
C. Protected classification characteristics under California or federal law	Age, race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	NO
D. Commercial information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	NO
E. Biometric information	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	NO
F. Internet or other similar network activity	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	YES
G. Geolocation data	Physical location or movements.	NO
H. Sensory data	Audio, electronic, visual, thermal, olfactory, or similar information.	NO
I. Professional or employment-related information	Current or past job history or performance evaluations.	NO
J. Non-public education information (per the Family Educational Rights	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	NO



and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).		
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	NO

Sharing Personal Information

ASSA ABLOY Global Solutions takes your privacy seriously and does not monetize your personal information. Certain states such as California and Nevada define the “sale” of data broadly, including the sharing of data with third parties. Under CCPA using cookie related technologies to collect usage analytics from our end users may be defined as a “sale”. The following section describe the “sharing, disclosing, selling of personal information.

We may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract. In the preceding twelve (12) months, we have disclosed the following categories of personal information for a business purpose:

- Category A: Identifiers
- Category F: Internet or other similar network activity

Uses made of the information

We use information held about you in the following ways:

- Information we collect about you. We will use this information:
 - to administer the service and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes.
 - to improve the service to ensure that content is presented in the most effective manner for you and for your computer.
 - as part of our efforts to keep the service safe and secure.
- Feedback you give to us. We will use this information:
 - to improve the goods or services.
 - to investigate and correct faults.
 - to provide you with information regarding relevant improvements (for example, we may notify you if a change you suggested is made).

We hold this data under “legitimate interests”.

Retention of your information

- Information we collect about you. We keep this information for a maximum of 90 days, with exception of analytics that we keep for 1 year.
- Feedback you give to us. We will keep this information for a maximum of 1 year.



Disclosure of your information

We may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract.

- We may transfer your personal data for the purposes set out above, to other companies within the ASSA ABLOY group.
- To third party business partners who provide services connected to the purposes defined above.
- Analytics providers who supply us with services for collecting and analyzing feedback and usage information.
- Our customers, channel partners or their agents for which you have engaged in a business contract.

We will disclose your personal information to third parties:

- In the event that we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets.
- If we are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets.
- If we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply our terms of use or terms and conditions of supply and other agreements; or to protect the rights, property, or safety of us, our customers, or others.

Some recipients may be in countries outside the EU/European Economic Area (EEA). When transferring personal data to countries outside the EU/EEA we use standard contractual clauses approved by the European Commission to ensure a sufficient level of protection for your personal data. These standard contractual clauses, as well as information on countries approved by the European Commission can be found [here](#).

With regards to the United States, certain states such as California and Nevada define the

“sale” of data broadly, including the sharing of data with third parties. Under CCPA using cookie related technologies to collect usage analytics from end users may be defined as a “sale”. In the preceding twelve (12) months, we have not sold any personal information.

The following section describe the “sharing, disclosing, selling of personal information. In the preceding twelve (12) months, we have disclosed the following categories of personal information for a business purpose:

- Category A: Identifiers
- Category F: Internet or other similar network activity

We take measures to protect all personal data transferred to a third party, or to other countries, in accordance with applicable data protection laws and as stated above which includes a data processing agreement where required.



Where we store your personal data

We take your safety and security very seriously and we are committed to protecting your personal information. All information you provide to us is stored on secure servers. Where we have given you (or where you have chosen) a password that enables you to access certain parts of our service, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to us; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorized access.

Your rights

Data protection legislation gives you the right to access, rectify or erase information held about you. Your right of access can be exercised in accordance with the data protection legislation. You can exercise these rights at any time by emailing us at support@keypersystems.com.

We do not discriminate when exercising your privacy rights by denying use of our services or provide a different level or quality of Services. We will provide you with a copy of any personal data undergoing processing free of charge. Where processing of your personal data is based on consent, you can withdraw consent at any time.

You have the right:

- to ask us not to process your personal data where it is processed based on legitimate interests if there are no compelling reasons for that processing.
- to ask for the information we hold about you to be rectified if it is inaccurate or incomplete.
- to ask for data to be erased provided that the personal data is no longer necessary for the purposes for which it was collected, you withdraw consent (if the legal basis for processing is consent), you exercise your right to object, set out below, and there is no overriding legitimate ground for processing, the data is unlawfully processed or the data needs to be erased to comply with a legal obligation.
- to ask for the processing of that information to be restricted if the accuracy of that data is contested, the processing is unlawful, the personal data is no longer necessary for the purposes for which it was collected, or you exercise your right to object (pending verification of whether there are legitimate grounds for processing); and
- to ask for data portability if the processing is carried out by automated means and the legal basis for processing is consent or contract.

Complaints

If you have a complaint regarding our processing of your personal information you are entitled to report this to the applicable Supervisory Authority or Attorney General in your Member State.



Links

This portal may, from time to time, contain links to and from external websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

Changes to our Privacy Notice

Any changes we make to our Privacy Notice in the future will be posted on this page. Please check back here to see any updates or changes to our Privacy Notice.

Contact

If you have any questions or comments about this Privacy Notice, the ways in which we collect and use your personal information, your choices and rights regarding such use, or wish to exercise your rights, you may contact us via email at support@keypersystems.com.

Last updated March 2022



Elite Web Administration Site Guide

Log in to **USHRR0002**
Enter Password

Version: 7.0.7335
Primary WS: CONNECTED
Primary DB: CONNECTED

 **KEYper Systems**
Key Management Simplified

www.keypersystems.com
www.keyperstore.com



Connect to the Web Administration Site

*NOTE: Your system will arrive with a **Default Admin** administrative profile installed. The PIN is **1234**. Use this to login to the **Web Admin Site** to begin key system administration. If using the 'Enhanced Web Security Feature' (see hardening guide for full details) which requires a username and password to log into the **Web Admin Site**, the **Default Admin** profile username is **default.admin** and the password is **1234**. As soon as you create an Admin profile, the Default Admin profile is automatically deleted, and the PIN of 1234 may no longer be used.*

Warning: 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 we want to ensure that you are aware of the associated risks. If you wish to configure your system to be publicly available on the internet, you can complete the form at the following link [Internet Security Acknowledgement Form](#).

Connect to the **Web Admin Site** from a PC **on the same network** by opening a web browser and entering IP address of the key system in the URL bar. The IP address displays on the system info form which is accessible by clicking the question mark icon on the login form of the kiosk cabinet (e.g. 192.168.25.15).

*Note: Primary Web Service (WS) and Primary Data Base (DB) should always indicate **CONNECTED**.*

Log in to USHRR0002
Enter Password

Login

Version: 7.0.7335
Primary WS: CONNECTED
Primary DB: CONNECTED

 **KEYper Systems**
Key Management Simplified

www.keypersystems.com
www.keyperstore.com



The Dashboard

The **Dashboard** is the Home Screen of the **Web Admin Site**. It provides an “at a glance” view of the status of the key system. The menus located at the top of the **Web Admin** window provide navigation to all other windows.

- **Assets In** – Count of assets that are physically in the key system(s). Clicking this button provides a current **Assets by Status** view, filtered by a status of **In**.
- **Assets Out** – Count of assets checked out to users. Clicking this button provides a current **Assets by Status** view, filtered by a status of **Out**.
- **Assets Overdue** – Count of assets checked out to users past the allowed time limit. Clicking this button provides a current ‘**Assets by Status**’ view, filtered by a status of **Overdue**.
- **Unregistered Assets** – Key Fobs that are in the database, but not programmed to an asset. Clicking this button provides a current **Assets List** view, filtered by asset type **Unregistered**.
- The **Add New Asset** & **Add New User** hot buttons will take you straight to the respective window.
- The grid view lists the last 10 transactions.

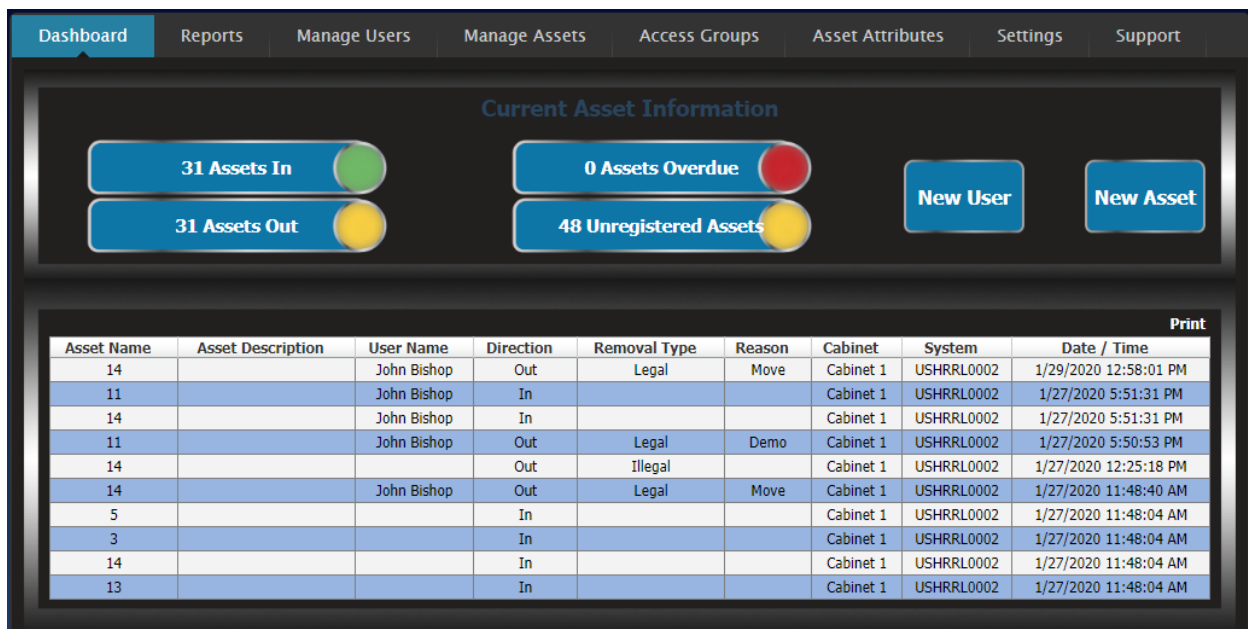


Figure 1: Dashboard Screen with last 10 transactions displayed



Manage Users – Edit, User Change Log

Admin vs. User – Know the Difference

ADMINS:	USERS:
<ul style="list-style-type: none">• Can access the KEYper® Web Admin Site• Override all Access Group restrictions• Have Access to the Admin functions of the kiosk	<ul style="list-style-type: none">• Cannot access the KEYper® Web Admin Site• Adhere to assigned Access Group restrictions• Can only Check In, Check Out, and Identify assets at the kiosk

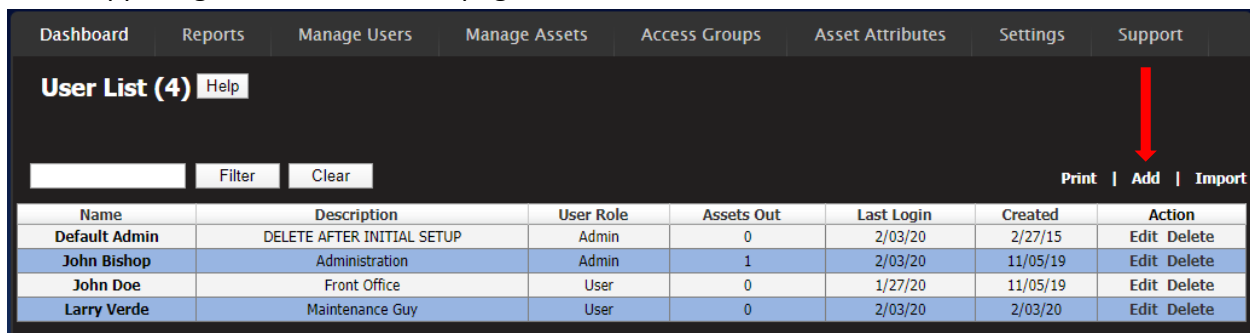
 **Add/Edit/Delete Users** (Manage Users > Edit Users)

It is recommended that after adding **just key system administrators**, the need, if any, for additional **Access Groups** be decided. Creating additional groups (Sales, Vendors, etc.) enables easier **Access Group** assignment when adding **Users**. There is no need to create an **Access Group** for Key System administrators as they are **not restricted in any way**.

From the **Users List** page, you can **Add, Edit, Delete, Print** and **Import** user information. Enter a first or last name in the search bar next to the **Filter** option to find a particular **User**.

Add New User

- In the upper right of the **Users List** page, click the “**Add**” button.



Name	Description	User Role	Assets Out	Last Login	Created	Action
Default Admin	DELETE AFTER INITIAL SETUP	Admin	0	2/03/20	2/27/15	Edit Delete
John Bishop	Administration	Admin	1	2/03/20	11/05/19	Edit Delete
John Doe	Front Office	User	0	1/27/20	11/05/19	Edit Delete
Larry Verde	Maintenance Guy	User	0	2/03/20	2/03/20	Edit Delete

Figure 2: User List

- Fill in the **Users** information
 - First Name
 - Last Name
 - Description (i.e. position title)
 - Password (Numeric only, 4-digit minimum)
 - Role (Admin or User)



- Access Web Reports – If marked '**True**' this feature allows a **User** to login to the **Web Admin Site** and access **Reports only**.
- Access Web Assets – if marked **True** this feature allows a **User** to login to the **Web Admin Site** and access **Assets only** (Add, Delete, Edit).
- Email Address (For Email Alerts)
- Phone Number (For SMS Alerts)
- Carrier (For SMS Alerts)
 - If desired carrier is not listed, contact KEYper® to see about adding it as a selection
- Prox/Swipe ID – for systems incorporating either a proximity card reader or a magnetic strip card reader. If you know the number, enter it when adding the **User** to the system. Primarily, this field will be auto-filled when reading the **User's** card during **Device Enrollment**.
- Issue Limit – the number of keys this user may have checked out of the key system at any given time. Use this feature to assign a unique Issue Limit that differs from the users assigned **Access Group** Issue Limit.

Select the **Default Group** or assign the User to another listed **Access Group**. This is why creating **Access Groups** before entering **Users** is helpful. Otherwise, for **Access Groups** created after user registration, you must edit a **User's Access Group membership** through the user's profile or by editing individual **Access Groups**.

Figure 3 on the following page is a representation of the Add New User Screen.



Dashboard Reports Manage Users Manage Assets Access Groups Asset Attributes Settings Support

User List (4) Help

Add New User

First Name

Last Name

Description

Keyboard Password

Confirm

Role

Access Web Reports ☐ True ☐ False

Access Web Assets ☐ True ☐ False

Email Address

Cell Phone Number

Cell Phone Carrier

Receive Messages ☐ No ☐ Email only ☐ SMS only ☐ Both email and SMS

Prox ID or Swipe ID

Issue Limit (0 indicates no limit)

Access Groups

Select	Name	Description
<input type="checkbox"/>	Default Group	Boom

Save Cancel

Figure 3: Add New User Screen

Edit a User

- From the main **User** List page, find the User you wish to modify in the list of **Users**.
 - You can enter any part of a user's first or last name in the search bar, and then click **Filter** to find entries that contain the typed characters.
- Click the **Edit** button to the right of the desired user.
- Make adjustments and click **Save**.

Deleting a User

- Find the user you wish to delete in the list of users.
- Click **Delete** button to the right of the desired user.
- Confirm that you wish to delete the user.



Importing a User List

- It is possible to import a group or list of users into the system (biometric enrollment requires individual registration for each user at the kiosk cabinet).
- Must save file in .CSV format (Comma Separated Value).
- The **User** info in the .CSV file must be in the format shown in figure 4.

Note: Column headers (row 1) are for reference only, removal is required prior to import. (A)dmin & (U)ser must have a capital first letter. A minimum 4-digit number is required in the Prox column (Prox numbers must be unique for each user).

First	Last	Description (job title)	PIN	Role (Admin or User)	Prox	Email	Phone
Adam	Smart	Sales	4321	User	4321	adam@company.com	555-555-4321
Jane	Smith	Controller	5923	Admin	5923	janer@company.com	555-888-3232
Tom	Jones	Maintenance	7894	User	7894	tjones@company.com	555-543-3312

Figure 4: User Import Format

- In the upper right of the Users screen (figure 5) select Import.
- Browse to the user file you have created, select the file and click the Import button.
- If the file format is correct, you will see all of the users in the user grid view.

The screenshot shows the 'User List (4)' screen with a navigation bar at the top containing 'Dashboard', 'Reports', 'Manage Users', 'Manage Assets', 'Access Groups', 'Asset Attributes', 'Settings', and 'Support'. Below the navigation bar, there is a 'User List (4)' header with a 'Help' button. A search bar with 'Filter' and 'Clear' buttons is present. On the right side, there are 'Print', 'Add', and 'Import' buttons. A red arrow points to the 'Import' button. Below the buttons is a table with columns: Name, Description, User Role, Assets Out, Last Login, Created, and Action. The table contains four rows: 'Default Admin' (DELETE AFTER INITIAL SETUP, Admin, 0, 2/03/20, 2/27/15, Edit Delete), 'John Bishop' (Administration, Admin, 1, 2/03/20, 11/05/19, Edit Delete), 'John Doe' (Front Office, User, 0, 1/27/20, 11/05/19, Edit Delete), and 'Larry Verde' (Maintenance Guy, User, 0, 2/03/20, 2/03/20, Edit Delete).

Figure 5: Import User Button

The screenshot shows the 'Import Users' screen. At the top, there is a navigation bar with 'Dashboard', 'Reports', 'Manage Users', 'Manage Assets', 'Access Groups', 'Asset Attributes', 'Settings', and 'Support'. Below the navigation bar, there is a 'User List (4)' header with a 'Help' button. In the center, there is a section titled 'Import Users' with a 'Choose File' button, a 'No file chosen' status, and an 'Import' button.

Figure 6: Import User Screen



User Change Log (Manage Users > User Change Log)

This date searchable database displays information regarding changes to the **User Database**. The information displayed includes the type of change, the date of change, and the name of the user making the change.

Manage Assets – Edit Assets, Assets with Attributes, Asset Change Log

Import / Add / Delete Assets (Manage Assets > Edit Assets)

Loading Fob Reading Drivers (MX/MX+ only)

Note: You must have administrative privileges on the PC to load the Active X and drivers.

Note: You must access the Web Admin Site using Internet Explorer 9, 10, or 11.

When selecting the **Asset** menu after logging into the **Web Admin Site** for the first time, look for a pop-up on the screen requesting **Active X** control installation. Depending on the operating system, browser, network restrictions, etc., the **Active X** prompt may not appear. If it does, install the control.

In addition, you may see a pop-up referring to the improper configuration of **intranet** settings. Select the option to turn **intranet** settings on.

Now click on the **Identify Asset** button. You should see the text depicted in figure 7.



Figure 7: FOB Reader Drivers

Determine if your PC has a 32-bit or 64-bit operating system and load both of the appropriate drivers. Accept the default options throughout each driver installation.

After loading the drivers, connect the fob-reading device to a USB port on your PC. To determine proper operation, place a fob on the reader and click **Identify Asset**. A nine-digit number should appear. If you have trouble, contact KEYper® Support.



Importing Assets

A manual import of assets is possible. There is a version for automotive applications, and a version for other applications. This feature is especially useful during initial key system installation, as it facilitates rapid asset registration by populating the **Asset Attribute** databases.

For automotive imports, the data must be in the format shown in figure 8. There may not be information in every column. In fact, the “**Code**” column is always empty, and that is fine. What is important is that there are (8) columns.

Stock #	Make	Model	Year	Ext Color	Code	Int Color	VIN
1234	Chevrolet	Impala	1996	Blue		Blue	1234
C12548	Ford	F150	2005				23154687
KM7894	Mercedes-Benz	C300	2011	Silver			

Figure 8: Web Admin Vehicle Import Format

Stock #	Make	Model	Year	Ext Color	Int Color	VIN
1234	Chevrolet	Impala	1996	Blue	Blue	1234
C12548	Ford	F150	2005			23154687
KM7894	Mercedes-Benz	C300	2011	Silver		

Kiosk Figure: Kiosk Vehicle Import Format

Note: Column headers (row 1) are for reference only, removal is required prior to import.

Save the file as a .CSV document.

From **Manage Assets > Edit Assets** select Import (DMS Style). Browse to the saved .CSV document and Import.

For other applications, the **Import (6 Attributes)** style of import is used. If this option is not available on the main **Asset List** page, contact KEYper® Support. It is very important that any changes to the **Attribute** names be made *before* adding assets to the system. Contact KEYper® Support for assistance editing any of the (6) **Attribute Names** (Attribute 1, Attribute 2, etc.).

Figure 9 illustrates the required format for **Import (6 Attributes)** style of importing. Again, there may be little or even no data in the attribute columns, which is not a problem. Just be sure there are (8) columns and the asset name column is populated.

Asset Name	Attribute 1	Attribute 2	Attribute 3	Attribute 4	Attribute 5	Attribute 6
1071						
2071						
3071						

Figure 9: Web Admin 6 Attributes Import Format



Asset Name	Description	Attribute 1	Attribute 2	Attribute 3	Attribute 4	Attribute 5	Attribute 6
1071							
2071							
3071							

Kiosk Figure: Kiosk 6 Attributes Import Format

Adding Assets

There are three methods for adding assets:

1. **Add** – blank record
2. **Filter** – imported data
3. **Unregistered Asset** – using “empty” fobs stored in cabinet(s)

Name	Description	Status	Registered Type	System	Last Checked Out	Created	Action
U-142384932		Out	Unregistered	USHRRRL0002	1/16/20	1/10/20	Edit
U-142385492		Out	Unregistered	USHRRRL0002	1/16/20	1/10/20	Edit
U-142387205		Out	Unregistered	USHRRRL0002	1/16/20	1/10/20	Edit

Figure 10: Assets Count Main Page

Adding Assets from a Blank Record (MX/MX+ Only)

- Click the **Add** option in the upper right area of the **Asset Count** page.
- Fill in the **Asset Information** (** Indicates Required Field).
 - **Name**** – (eg. Stock Number, Unit Number, etc.)
 - **Description** – (for automotive applications, the model is suggested here)
 - **Fob Number**** – (hold fob on the **Fob Reader** and select **Read Fob**)
 - **Status** – not editable
 - **Registered Type** – always select Registered
- Fill in **Asset Attributes**, if desired.
 - Select a value from the dropdown menus.
 - If your desired value is not in the dropdown menu, select the **Enter** option to allow manual entry of a value.
- Select the **Access Group(s)** for the asset.
- Click **Save**.

Note: If using label printing, select Print Asset Label. Click Save.



Dashboard Reports Manage Users Manage Assets Access Groups Asset Attributes Settings Support

Asset Count(81) Help

Add New Asset

Name

Description

Fob Number

Status

Registered Type

Access Groups

Select	Name	Description
<input checked="" type="checkbox"/>	Default Group	Boom

☐ Print Asset Label

New Asset Attributes

Year Enter

Make Enter

Model Enter

Ext. Color Enter

Int. Color Enter

Type Enter

VIN

Single Values

Figure 11: Add/Import Asset

Adding Imported Assets (MX/MX+ Systems)

- Utilizing the **Filter** feature on the main **Asset List** page (figure 10), find the unregistered **Asset**. Click the **Edit** option.
- Verify imported information is correct (figure 12). Make any desired changes to **Asset Information** and/or **Asset Attributes**. If your desired value is not in the drop-down menu, select the **Enter** option to allow manual entry of a value.
- Assign a fob to the asset (place the fob on the reader and select **Read Fob** to assign the fob to the asset).
- Ensure to set **Registered Type** to **Registered**.
- Select the **Access Group(s)** for the asset.
- Click **Save**

*Note: If label printing is enabled, select **Print Asset Label**. Click **Save**.*

Adding Unregistered Assets (MX/MX+ Systems)

This method is for systems where unused fobs (no keys connected and **Registered Type** is **Unregistered**) are stored in the key cabinet(s) and are checked out as needed to add new assets to the system.

- Login to the key system kiosk (must be an administrator). Tap **Unregistered Assets** button. A list of all unregistered assets (unused or empty fobs) displays. Select as many displayed entries as needed and check out.
- From the **Web Admin Site**, go to **Manage Assets**, place unregistered fob on reader and click **Identify Asset**. The page depicted in figure 12 will display. Select **Edit**.



Figure 12: Identify Unregistered Asset

- Fill in the **Asset Information** (** Indicates Required Field)
 - **Name**** – (e.g. Stock Number, Unit Number, etc.)
 - **Description** – (for automotive applications, the model is suggested here)
 - **Fob Number**** – (hold fob on the **Fob Reader** and select **Read Fob**)
 - **Status** – not editable
 - **Registered Type** – **always** select Registered
- Fill in **Asset Attributes**, if desired.
 - Select a value from the dropdown menus.
 - If your desired value is not in the dropdown menu, select the **Enter** option to allow manual entry of a value.
- Select the **Access Group(s)** for the asset.
- Click **Save**.

Adding Unregistered Assets (HC/MXi Systems)

This method is for systems where unused fobs (no keys connected and **Registered Type** is **Unregistered**) are stored in the key cabinet(s) and used to add as new assets to the system.

- From the **Web Admin Site**, go to **Manage Assets > Edit Assets**, select an unregistered fob and click **Edit**. A page similar to figure 13 will display.
- Edit the **Asset Information** (** Indicates Required Field)
 - **Name**** – (e.g. Stock Number, Unit Number, etc.)
 - **Description** – (customizable and used to describe/reference the asset)
 - **Fob Number**** – DO NOT EDIT (must remain the same as it was read by the system hardware)
 - **Status** – not editable
 - **Registered Type** – **always** select Registered
- Fill in **Asset Attributes**, if desired.
 - Select a value from the dropdown menus.



- If your desired value is not in the dropdown menu, select the **Enter** option to allow manual entry of a value.
- Select the **Access Group(s)** for the asset.
- Click **Save**.

Asset Count(95) [Help](#)

Update Asset Information

Name:

Description:

Fob Number:

Status:

Registered Type:

Access Groups

Select	Name	Description
<input checked="" type="checkbox"/>	Default Group	Boom

☐ Print Asset Label

View/Edit Asset Attributes

Attribute	Value	Action
Attribute 1	Select....	Enter
Attribute 2	Select....	Enter
Attribute 3	Select....	Enter
Attribute 4	Select....	Enter
Email	Select....	Enter
Precaution	Select....	Enter

Figure 13: Add Unregistered Asset

*Note: If using label printing, select **Print Asset Label**. Click **Save**.*

Deleting Assets

The procedure for deleting of assets is the same for all industries. The following is an example of the procedure for automotive applications.

When an asset (vehicle) leaves inventory, whether sold, traded or otherwise, cut the tamper seal securing the key(s) to the fob and discard. The key(s) will obviously go with the vehicle. Place the fob in a container designated for the purpose. At whatever intervals are required, a key system administrator, or a user with proper permissions, will “disassociate” the fob from the asset, thereby making the fob ready to be associated with another asset *and* releasing the asset from **User’s Issue Limit** total.

- **MX/MX+ Only** - Place the fob on the fob reader, click **Identify Asset**, and then **Delete**.
- **MX/MX+/HC/MXi** - filter or scroll through the **Asset List** page, locate the asset, check the adjacent box and select **Delete**.



Assets with Attributes (Manage Assets > Assets with Attributes)

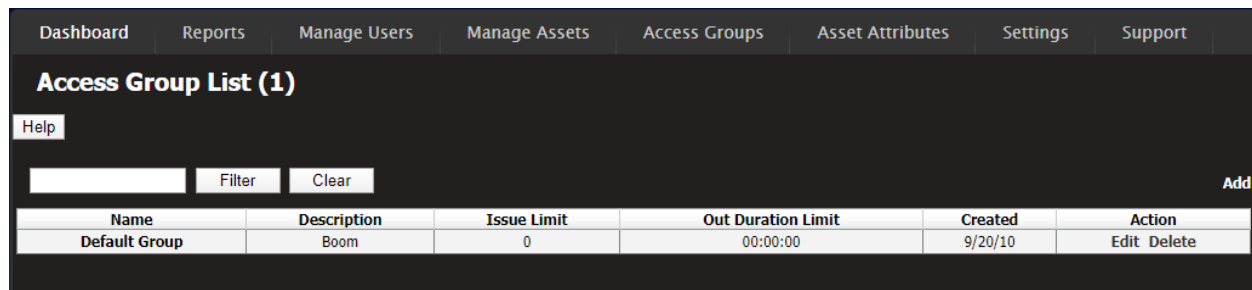
Displays a list of all **Assets**, and any assigned **Attributes**. You may **Edit** or **Delete** an **Asset**.

Assets Change Log (Manage Assets > Assets Change Log)

This date searchable database displays information regarding changes to the **Asset database**. The information displayed includes the type of change, the date of the change, and the name of the user making the change.

Access Groups – Edit, Access Group Change Log

There is a factory-loaded default **Access Group** named **Default Group**.



Name	Description	Issue Limit	Out Duration Limit	Created	Action
Default Group	Boom	0	00:00:00	9/20/10	Edit Delete

Figure 14: Edit Access Group Screen



Create / Configure / Edit Access Groups (Access Groups > Edit Access Groups)

This facilitates rapid system configuration, quickly making the system operational. You may edit the default group, but DO NOT delete it. Standard settings for the Default Group are:

- 0 (Zero) Asset Issue Limit per user (0 = No Limit)
- 0 (Zero) Out Duration Limit per Asset (0 = No Limit)
- 24/7 access to remove and return Assets
- Access to all Locations, Systems, and Cabinets

Creating New Access Group (Access Groups > Edit Access Groups)

- From the **Access Group** home screen (figure 14) > click the **Add** button in the upper right.
- Fill In the desired **Name** for the access group (e.g. Managers).
- Fill in the **Description** for the access group (e.g. 3rd Shift Manager Access). ****Not a required entry****
- Set the desired **Issue Limit** for the group. ****0 indicates unlimited****
 - **Issue limit** – the number of keys each user in the group may have checked out of the system at any given time (e.g. If the limit is 10, each user in the group may have up to 10 keys checked out at any given time).
- Set the desired out duration time limit. ****0 indicates unlimited****



- **Out Duration** – Once a key is out of the system past the set time limit, the assets status will change from **Out** to **Overdue**, and an alert will be sent to all recipients on the **Out Duration Exceeded Alert** list. 23 Hours, 59 Minutes is the maximum time that can be set for out duration.
- Click the **Save** button. This will add the group into the system and allow for configuration of the final settings.

Configuring / Editing Access Group Settings & Restrictions (Access Groups > Edit Access Groups)

Note: Always click the 'Save' button after configuring or editing Access Group settings!

From the **Access Groups** home screen, select **Edit** for the desired group.

Access Times

- Click the **Access Times** header to expand.
- Select **Add Time** from the upper right.
- Select the desired **Day**, **Start Time** and **End Time** (utilize 24 hr. format) and click **OK**.
- Repeat the process for each day of the week that you wish to allow users in the **Access Group** access to the system.

User List

- Click the **User List** header to expand.
- Select **Edit** to see the list of all users in the system.
- Choose **Select All** or use the check box to assign individual users to the group.
- Click **Save**.

Asset List

- Click the **Asset List** header to expand.
- Select **Edit** to see the list of all assets in the system.
- Choose **Select All** or use the check box to assign individual assets to the group.
- Click **Save**.

Physical Access List

- Click the **Physical Access List** header to expand.
- The **System Map** displays.
- Select the check box next to all **Locations**, **Systems** and **Cabinets** that you wish to assign to this group.
- Click the **Update** button.

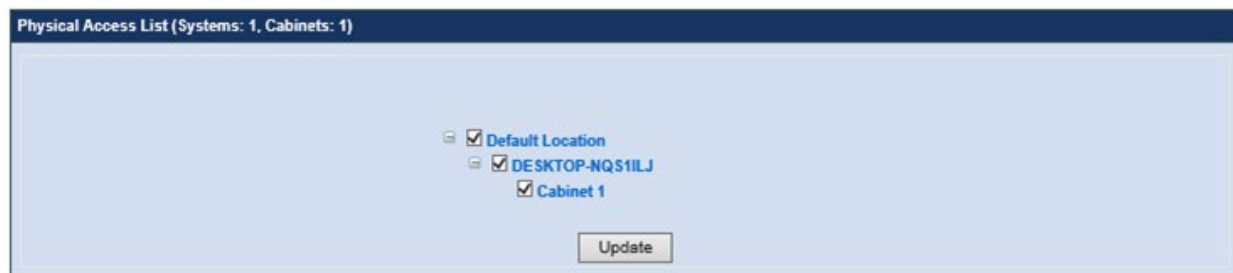


Figure 15: Access Group Physical Access List

Once you have completed all of the above steps, click **Save** under '**Update Access Group Information**' to lock in all of your changes

Access Group Change Log (Access Groups > Access Group Change Log)

This date searchable database displays information regarding changes to the **Access Group database**. The information displayed includes the type of change, the date of the change, and the name of the user making the change.

Asset Attributes

Asset Attributes are descriptive values that are associated with assets. Attributes can provide additional information about assets stored in the system (e.g. Stock #, Make, Model, Unit #, Building #).

All **Asset Attribute** databases are empty by default configuration. They may be populated manually (see below) or by Asset Import.

*Note: Assigning attributes to assets is necessary if using the **Filter Assets** method of check out at the Kiosk.*

There are two types of attributes:

- Collections (limit 6)
 - These attributes will be stored in a group. These values may apply to many different assets. (e.g. Make, Model, Floor, Building)
- Single Value Attribute (limit 1)
 - This attribute is associated only with one asset (e.g. VIN numbers, Key Codes).

*Note: **Attribute Names** are customizable to meet your preferences but requires the assistance of KEYper® Support.*

Warning: Changing attribute names after they have been associated with assets will “break” any asset reports containing previous attribute names.

You can manage your **Attribute Collections** by clicking the **Edit Collection** option. From here, you can edit values, correct misspellings, and add/delete values (you cannot delete a value once it is assigned to a record).



Asset Attributes [Help](#)

Attribute Collections (6)

Name	Parent Attribute	Action
Year		Edit Collection
Make		Edit Collection
Model	Make	Edit Collection
Ext. Color		Edit Collection
Int. Color		Edit Collection
Type		Edit Collection

Single Value Attributes

Name
VIN

Figure 16: Attributes for Automotive Applications

Notice in Attributes Collection, for automotive applications, the 'Make' is the Parent Attribute to the 'Model' collection. If you are adding 'models' to the collection, ensure you have selected the appropriate 'parent make' (figure 18).

Value collection for 'MODEL' (1)

Parent name: **Make** Parent value: **Chevy** ▼

Add new value [Add Value](#)

Value	Action
Silverado	Edit Delete

Figure 18: Edit Attributes

Asset Attributes [Help](#)

Attribute Collections (6)

Name	Parent Attribute	Action
Attribute 1		Edit Collection
Attribute 2		Edit Collection
Attribute 3		Edit Collection
Attribute 4		Edit Collection
Email		Edit Collection
Precaution		Edit Collection

Figure 17: Attributes for Other Applications



Reports

The Reports section consists of the following reports and a report builder.

Asset Transaction Report

- Provides real time reporting on **User/Asset** transactions.
- Filter **Asset Transactions** to search for desired data.
- Filters available for searching:
 - User
 - Asset
 - System (Networked Systems)
 - Cabinet (Multi-Cabinet Systems)
 - Date Range

Note: filters are combinable to find specific events.

Assets by Status

- Provides the status of all assets in the system (In, Out, or Overdue).
- Select **Assets by Status** from the **Reports** menu.
- Set any filters to view desired data.
- Filters available for searching:
 - Status – In, Out, and Overdue
 - System
 - Cabinet
 - Individual Asset Name

Cabinet Socket Map Report

- View a physical map of the assets in your cabinet.
- Hover over a particular asset to view details.
- Key Map - Optional cloud based backup
 - For users that have the optional cloud based backup, a map of key locations is saved in the cloud.
 - Access your cloud map by clicking the **Key Map** button on the right hand side (figure 18).

*****Personal Data Disclaimer: report entries may contain the first/last names of users*****

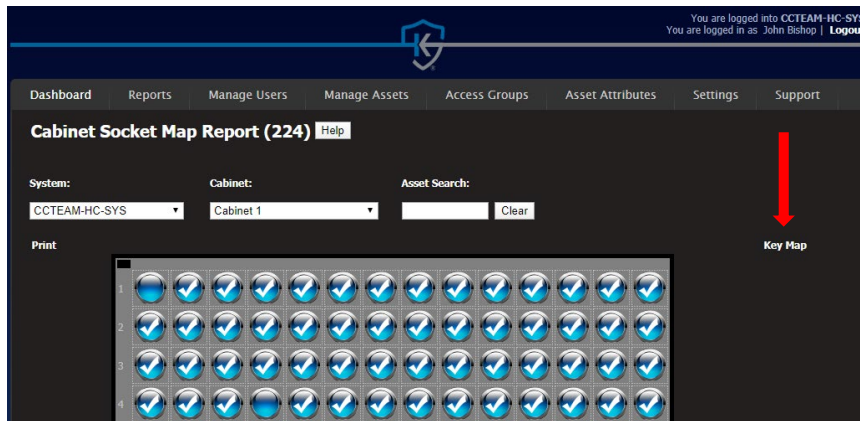


Figure 18: Cabinet Socket Map Report

Report Builder

- Create Customized reports with email and spreadsheet import capability.

View Kiosk Photos

- If system is camera equipped and enabled, a photo is stored with every successful and unsuccessful login. The view provides information about each login and the ability to view and/or print photos.

Web Login Audit Report

- Provides a list of key system **Administrative** login/login attempts for a specific date or specific period.

Alerts Report

- Provides a list of system alerts searchable by alert type and date.

Change Log Report

- Provides a comprehensive list of all change log activity (user, asset, and access group) searchable by date.

Assets by Process Step Report

- Provides a list of all assets in a process step and what process step they are in. Along with a duration of how long the asset has been in that process step.

Settings

Some settings are password protected and only KEYper® Systems personnel can access these menus. The following items fall under the user accessible **Settings** menu.

Alert Settings (Settings > Alert Settings)



- There are eight different alerts that will trigger an email and/or SMS alert from the KEYper® System. Any **User** properly configured in the system can receive these alerts. Configure phone number, phone service carrier, and email addresses during **User** setup.

To add a **User** to receive a specific alert, select the **Edit** button in the upper right of the desired alert, select the check box next to the desired user name(s), click **Save**, and then **Close**.

- **Illegal Asset Removal** – an asset removal occurred without following the proper checkout procedure.
- **Out Duration Exceeded** – an asset has not been returned to the system in the allotted time allowed as specified by the user's **Access Group**
- **Door Open** – a user has opened a door to the system and failed to close it within the allotted time allowed.
- **Nightly Reports** – a report of assets in 'Out' status as of the time the alert is sent
- **System Power Loss** - the system has recovered from an unexpected loss of power.
- **Cabinet-to-Kiosk Communication Loss** - serial communication between the PC and the hardware inside the cabinet has failed or become intermittent.
- **Asset Not Locked In (MX+/MXi Only)** - a fob inside the cabinet is not in not fully secured and locked into the socket.
- **Check In Mismatch** - the user that removed the asset is not the user that returned the asset.

Some of these alerts have accompanying **Alarms** that require configuration by KEYper® Support. These alarms include the **Door Open** Alarm, **Illegal Asset Removal** Alarm, **Asset Not Locked In (MX+/MXi Only)**, and an alarm that triggers when the Kiosk experiences an unexpected **Power Loss**. MX/MX+/MXi systems include a speaker that plays a siren sound when alarming.

Personal Data Disclaimer: alerts may contain the first/last names of users

Email Settings (Settings > Email Settings)

- Configure email settings to allow your KEYper® System to send out email alerts.
- The KEYper® System does not receive emails, it only sends.
- The KEYper® System allows the user to configure their SMTP server, user name and password. Certain network security protocols will not allow the default settings to forward emails, and in this case, the end user must work with their IT team to provide SMTP Server and Authentication credentials that will work with the KEYper® System.
- To test the email functionality, enter an email address into the box under **Test Settings**, click **Send Test Message**, check to see if the test message delivered.
- If the test message does not deliver, you will need to contact your IT to have the default SMTP settings changed. Contact KEYper® Support if assistance is required.

Issue Reasons (Settings > Issue Reasons)



- To enable Issue Reasons for any system, click the desired System (i.e. USHRR0002), check the Enable Issue Reasons box and select IRL from the dropdown menu (figure 19).

Issue Reasons [Help](#)

Issue Reason Lists (1)

Name	Description	Action
irl	desc.	Edit Collection

[Add](#)

Update System

System Name USHRR0002

Description

Facility/Alias

Assigned Location [Default Location](#) ▼

Enable Issue Reasons ☒ [irl](#) ▼

[SAVE](#) [CANCEL](#)

System Structure

- Default Company
 - Default Location
 - USHRR0002

Figure 19: Enabling Issue Reasons

*Note: **System Structure** and **System Settings** are only accessible by KEYper® Support*

Process Steps (Settings > Process Steps)

- To enable your Process Step workflow click on 'Process Steps' under the Settings navigation menu.
- Select the system(s) you would like to include in the Process Step workflow
 - Check the 'Enable Process Steps' checkbox and select the default process step list
 - Click 'Save'.

Language: [English \(United States\)](#) ▼
You are logged into USHRR0035
You are logged in as: Keyper Default | [Logout](#)

[Dashboard](#) [Reports](#) [Users](#) [Assets](#) [Access Groups](#) [Asset Attributes](#) [Settings](#) [Support](#)

Process Steps

Process Step Lists (1)

Name	Description	Action
default		Edit Collection

[Add](#)

Update

System Name USHRR0035

Description USHRR0035

Facility/Alias

Assigned Location [Default Location](#) ▼

Enable Process Steps ☒ [default](#) ▼

[SAVE](#) [CANCEL](#)

System Structure

- Default Company
 - Default Location
 - USHRR0035 (USHRR0035)



- Now click on 'Edit Collection' Action in the 'Process Step Lists' table
- Begin adding process steps to the default process step list by using the input box labelled 'Add new value' and click the 'Add Value' button to add each process step.

Language: English (United States) You are logged into USHRRL0035 You are logged in as Keyper Default | Logout

Dashboard Reports Users Assets Access Groups Asset Attributes Settings Support

Process Steps

Name	Description	Action
default		Edit Collection

Add

Value collection for 'DEFAULT' (2)
Value has been added

Add new value: Add Value

Value	Access Group	Duration	Action
step 1		no limit	Edit Delete
step 2		no limit	Edit Delete

System Structure

- Default Company
 - Default Location
 - USHRRL0035 (USHRRL0035)

- Go to Edit Access Groups under the Access Groups navigation menu and click 'Add'
- Create an Access Group with Access Group Type 'Process Step'

Language: English (United States) You are logged into USHRRL0035 You are logged in as Keyper Default | Logout

Dashboard Reports Users Assets Access Groups Asset Attributes Settings Support

Access Group List (1)

Add New Access Group

Name:

Description:

Access Group Type:

Issue Limit (0 indicates no limit):

Out Duration Limit (0 indicates no limit): hour(s) minute(s)

External Access Group ID:



- Once the process step Access Group has been created, make sure to update 'Access Times', 'User List', and 'Physical Access List'

Language: English (United States) You are logged into USHRRL0035 You are logged in as Keyper Default | Logout

Dashboard Reports Users Assets Access Groups Asset Attributes Settings Support

Access Group List (3)

Update Access Group Information

Name: Maintenance

Description: process step access group for ma

Access Group Type: Process Step

Issue Limit (0 indicates no limit): 0

Out Duration Limit (0 indicates no limit): 0 hour(s) 0 minute(s)

External Access Group ID:

Save Cancel

Access Times (0)

User List (1)

Filter Clear Edit

Name	Description
test test	

Asset List (0)

Physical Access List (Systems: 1, Cabinets: 1)

- Now navigate back to the Process Steps web page to
 - Assign different access groups to different process steps
 - Assign durations to different process steps
 - If assets are left in a process step longer than the duration set, the asset becomes "Overdue" in that process step

Language: English (United States) You are logged into USHRRL0035 You are logged in as Keyper Default | Logout

Dashboard Reports Users Assets Access Groups Asset Attributes Settings Support

Process Steps

Process Step Lists (1)

Name	Description	Action
default		Edit Collection

Add

Value collection for 'DEFAULT' (3)

Value has been updated

Add new value: Add Value

Value	Access Group	Duration	Action
step 1	Sales	1.00:00:00	Edit Delete
step 2	Management	2.00:00:00	Edit Delete
step 3	(None)	dd hh mm	Update Cancel

System Structure

- Default Company (default)
- Default Location
- USHRRL0035

Dropdown menu options: (None), (None), Maintenance, Management, Sales



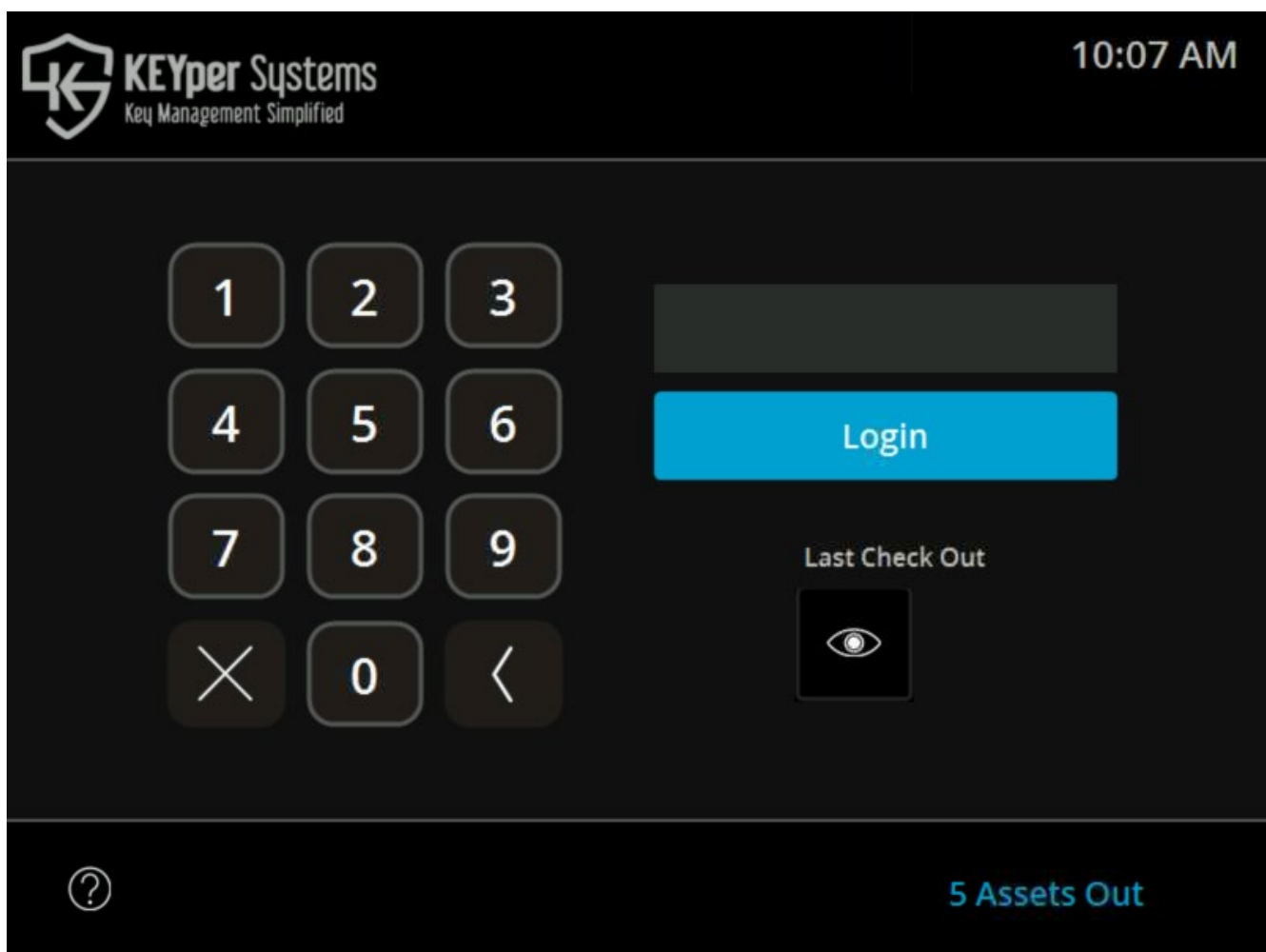
Support

Under the Support menu, you will find the following links

- Support Website – send support questions directly to KEYper® Support
- FAQs – link to support documents addressing frequently asked questions
- How To Videos – link to tutorials on the KEYper® website
- Remote Support – opens a webpage that will allow KEYper® Support to connect to your PC
- System Manual – link to the system user guide
- Shop at KEYper® Systems – a direct link to the online KEYper® store where supplies and accessories may be purchased
- Zebra Printer Drivers – provides label printer drivers for installation



Elite Series Kiosk Administration Guide





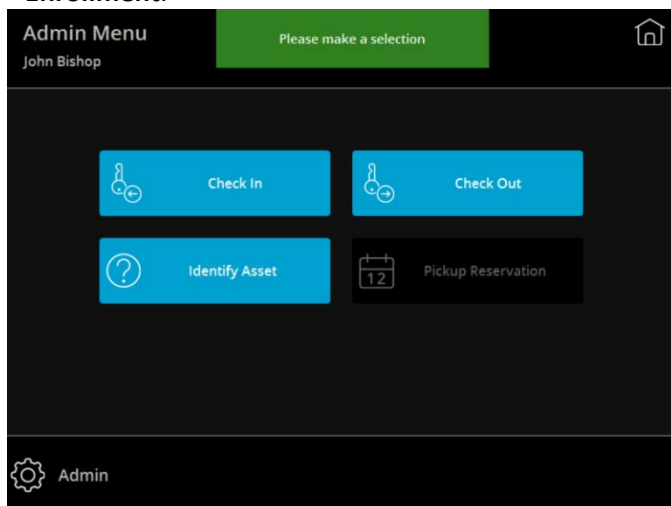
If the screen is displaying the desktop, start the KEYper® kiosk program by double tapping the Elite Kiosk icon.



Figure 1: Desktop Icon

Login

The methods for logging into the kiosk are via **Pin Code**, **Fingerprint**, **Proximity (Prox) Card**, or **Magnetic Strip Card** (Prox and Magnetic Strip Card are optional add-ons). As the **Admin**, you will setup the appropriate access type(s). See **Device Enrollment**.



After you login, the screen will display two-three rows of buttons depending on your settings (figure 2).

NOTE: Admins have the additional “Admin” options button in the bottom left

Figure 2: Main Screen

Check In, Identify Asset, Check Out

On the main screen, the top row of buttons (**Check In**, **Identify Asset** (MX Only), and **Check Out**) behave the same for both **Admins** and **Users**. See the **Kiosk User Guide**.

Device Enrollment, Unregistered Assets, Diagnostics, Manage Assets and Exit Application



These buttons are available to **Admins** only.

Device Enrollment - Configuring Access for Users

Pin Code Access

Pin Codes are configured when adding or editing user profiles. See the **Web Admin Guide**.

Fingerprint Access

To register user fingerprints, select a user on the **Device Enrollment** screen and press the **Fingerprint** button.

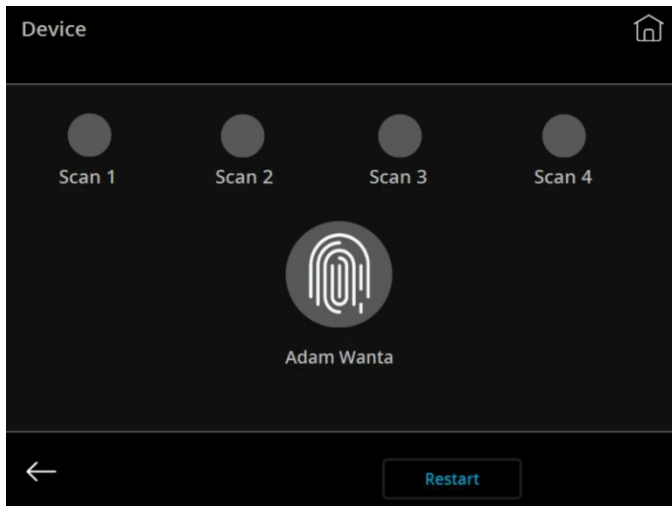
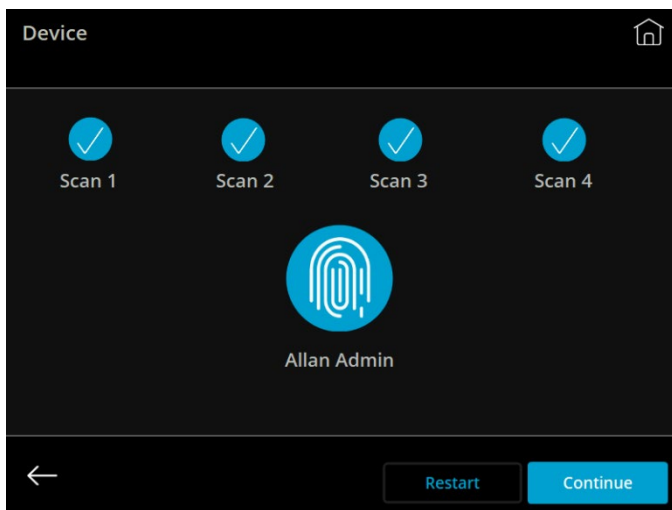


Figure 3: Fingerprint Scan Screen

On the **Scan Screen**, ask the user to touch a finger to the fingerprint reader lens. Cover as much of the lens as possible with fingertip and press flatly and firmly. A red light will appear briefly in the lens when touched; when the light goes out remove fingertip and wait for a green check mark indicating a successful scan (figure 3). Repeat the process until you achieve four successful scans and a successful **Scan Result**. Press the **Continue** button to save the scan (figure 4).



Select the next **User** and repeat the process.

Figure 4: Four successful finger print scans



Prox ID or Swipe ID Card Access

There are two ways to setup a user with a proximity or magnetic strip access card.

1. If known, enter the Prox or magnetic strip card number in the “**Prox ID or Swipe ID**” field of the **Add New** or **Update User Information** page. See **Web Admin Guide**.
2. Use the **Device Enrollment** feature of the **Kiosk**.

Login to the kiosk as an **Admin**. Press **Device Enrollment**. Select a user from the list or use the **Search** button to locate the user (figure 5). Press the **Prox** button to bring up the screen shown in figure 6 below.

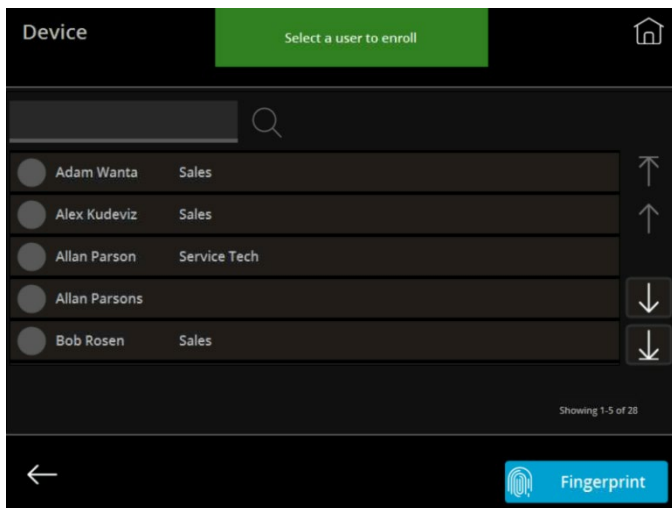


Figure 5: Device Enrollment Screen

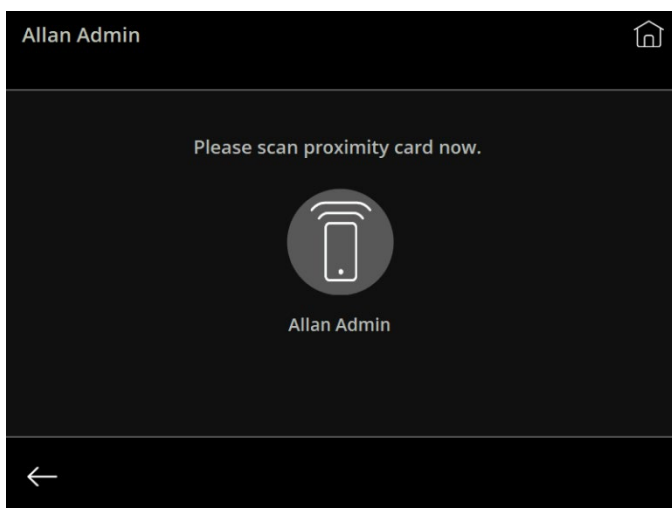


Figure 6: Prox Screen

When the **Prox Scan** screen appears (figure 6), place the selected user’s Prox card over the card scan device or pass the magnetic strip card through its reader. The device will beep and the number will be displayed indicating successful enrollment. Thereafter the card is valid for login.



Unregistered Assets

An **Unregistered Asset** is a fob in a cabinet that may or may not have keys attached and may or may not have data associated with it in the database, but has a **Registered Type of Unregistered**.

If the **Dashboard** of your **Web Admin** indicates there are **Unregistered Assets** in your system and you wish to remove them (see the **Web Admin Guide**), login to the kiosk, select the **Unregistered Assets** button, highlight the entries, and **Check Out**.

*NOTE: The optional **Check-Out Receipt** feature is not available for Unregistered Assets.*

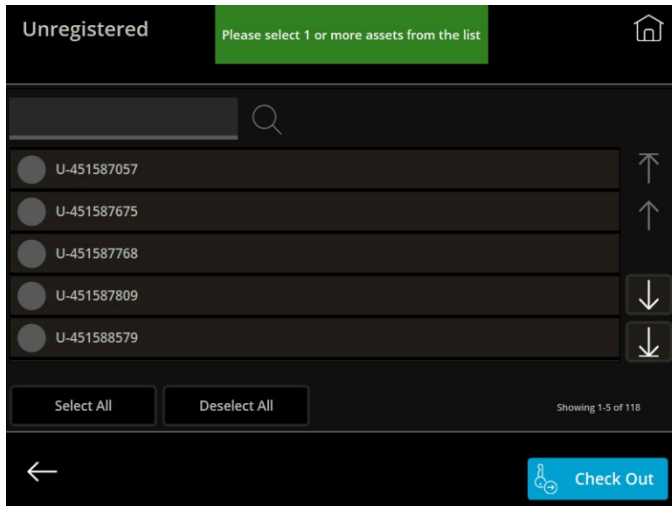


Figure 7: Unregistered Assets Screen

Diagnostics

The diagnostics screen is only for use by **Keyper® Support**, or by an **Admin** under the guidance of **Keyper® Support**.

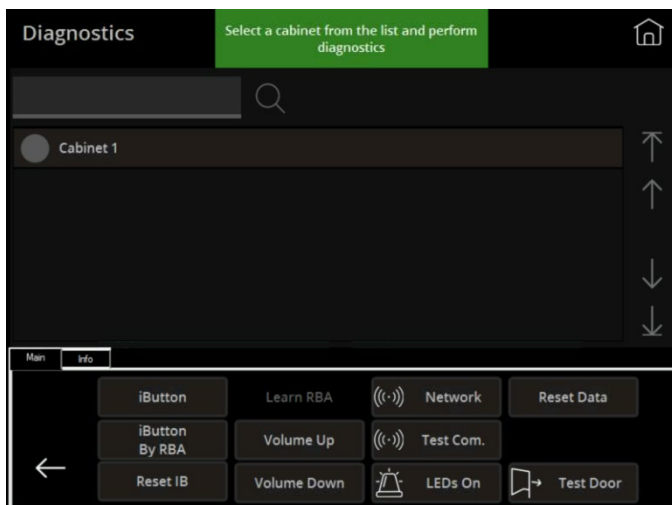


Figure 8: Diagnostics Screen



Manage Assets

The manage assets screen gives the admin user two options, **Add New** or **Edit/Delete**.

Add New (Manage Assets > Add New)

Add New enables an admin user to register an asset via the Kiosk.

Figure 9: Add New Asset Screen

Add an asset by filling in the **Asset Name** or by **importing** an asset by using the **Load File** button. Refer to the Web Admin Guide for importing guidelines.

Description and **Attribute** fields (automotive attributes are year, make, model, ext. color, int. color, and VIN) are optional. See Web Admin Guide for more details.

****Property Management Only****

- The **Email** field is also optional but if used should reflect the email address of the resident that occupies the property for which the key is registered (in property management cases). Removing or returning an asset generates an automatic email alert to the resident. The email contains the date/time of issue as well as the issue reason if applicable.
- The **Precaution** field is also optional and pertains to the use of the optional **HC Fob Reader**. When reading a fob, the **Precaution** will show on the screen of the fob reader. Such **Precautions** may address entrance conditions (e.g. dog on premises) or any other information applicable to the user or property. The **Precaution** field must not be more than 16 characters. This information is stored on the smart fob.

*NOTE: When registering the optional HC Fob Reader, **BE SURE** to check the box next to Fob Reader **immediately before clicking continue**.*

Figure 10: Registering optional HC Fob Reader

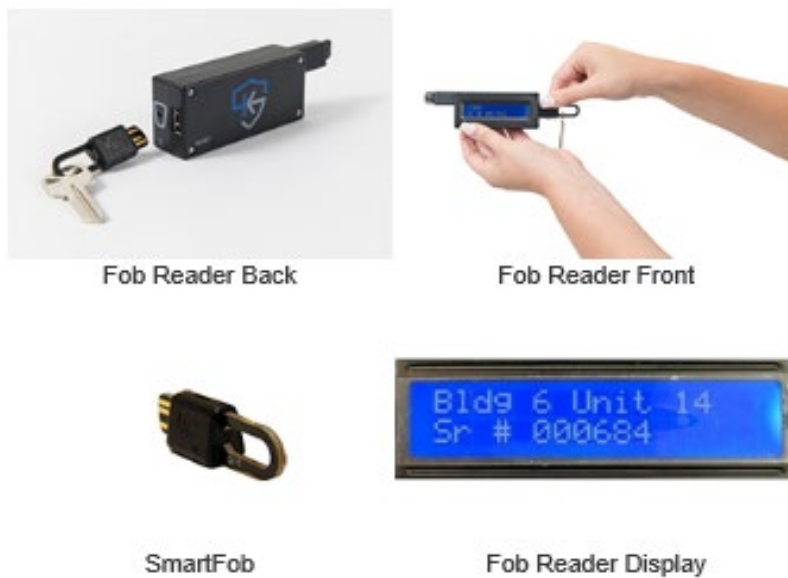


Figure 11: Optional HC Fob Reader and Smart Fob

Edit/Delete (Manage Assets > Edit/Delete)

Edit allows an admin user to edit a **registered** asset from the **Kiosk**. To **edit** an asset, select an asset from the list shown or use the **Search** or **Show All** buttons. Select the asset by clicking on it and it will be highlighted blue, click **Edit** at the bottom.

****Property Management Only****

On the right hand side of the edit screen, you will see the **Write Description** button. Use this button when there are assets present from registration via the Web Admin site. When registering an asset via the Web Admin site, the **Name** and **Precaution** (if applicable) do not store to the fob itself. By logging into the Kiosk as an admin, going to this **Edit**

screen and clicking **Write Desc.**, the **Description** and **Precaution** (if applicable) are pulled from the main database and written to the fob's internal storage.

NOTE: Write Description is mandatory if asset registration occurred in the Web Admin and the optional HC Fob Reader is used.

NOTE: When writing multiple descriptions to fobs you may encounter an error stating that not all descriptions wrote successfully. In this case, click the Write Description button again. If descriptions do not write successfully after multiple tries, contact KEYper® Support.

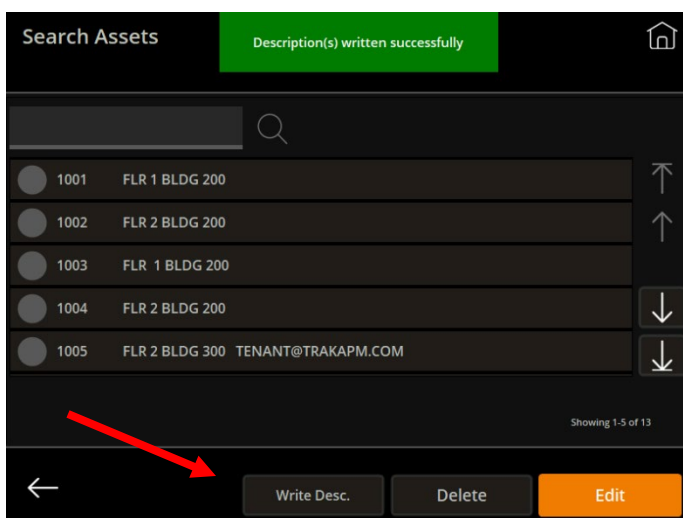


Figure 12: Write Description Button



Delete allows an admin user to **delete** a registered asset from the **Kiosk**.

To **delete** an asset, select an asset from the list shown or use the **Search** or **Show All** buttons. Select the asset by clicking it to highlight it blue, and then click **Delete** at the bottom. A prompt will ask you to click **Delete** again and upon doing so the asset will permanently delete from the system.

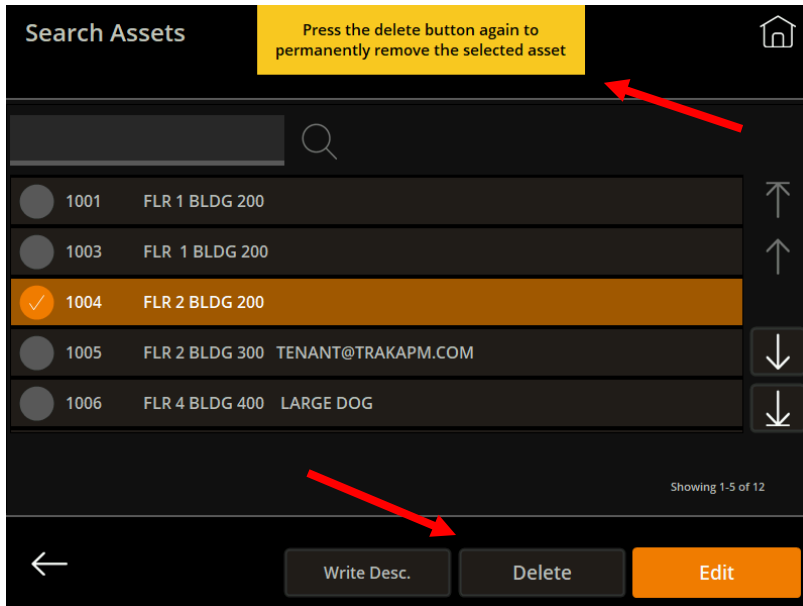


Figure 13: Deleting an Asset

Exit Application

To end the program, touch the Exit Application button on the admin settings screen. Then either restart the computer or restart the program by clicking the icon on the desktop.

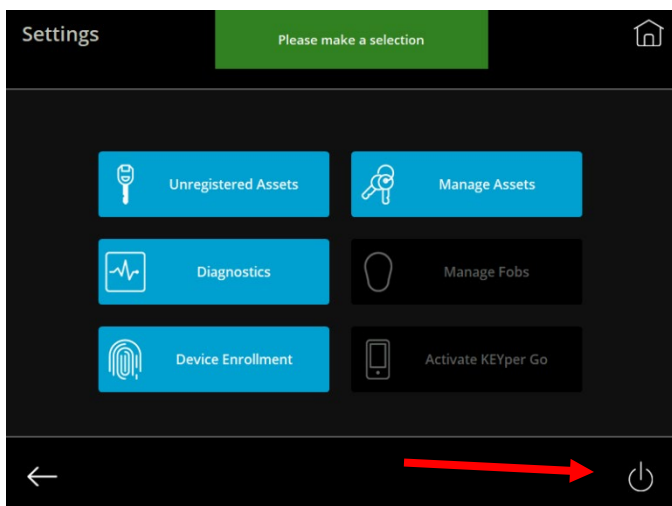


Figure 14: Exit Application Button (Power Symbol)

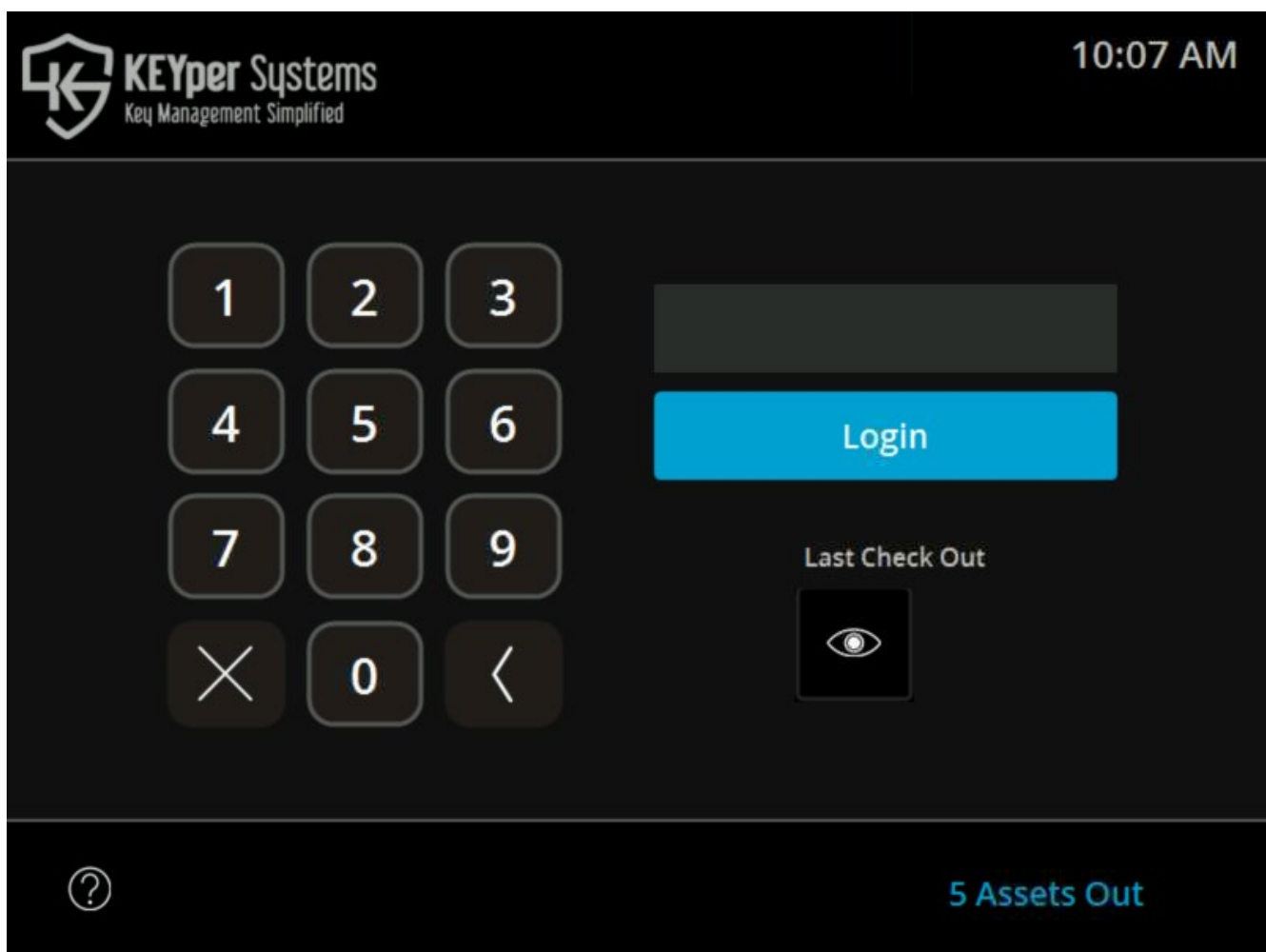


USB Port Declaration

USB ports are located on the exterior or interior of the cabinet depending on manufacture date. For some this may pose an inherent security concern. The USB ports can be disconnected/disabled to prevent them from being accessible/active.



Elite Series Kiosk User Guide





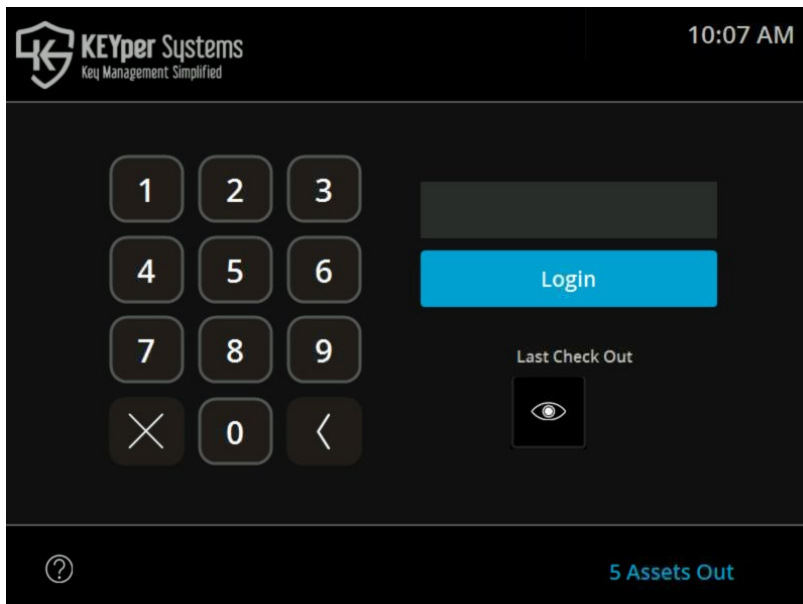
If the screen is displaying the desktop, start the KEYper® kiosk program by double tapping the Elite Kiosk icon.



Figure 1: Desktop Icon

Login

When the system is ready, you will see the login screen (figure 2). The login screen shows the current system status. On this screen, you will see if the system can connect to the Primary Web Service (WS) or the Primary Database (DB) under the logo in the upper left. Both of these must have the status of CONNECTED displayed on the main screen for the system to function properly.



If the **Lot Location** or **Lot Blocking** feature is activated, the **View Last Check Out** button will display the stock number and vehicle location of the most recent check out(s). The **Print Last Check Out** will print that information. On the top right of the screen you will see the status of your assets in the cabinet. Use this for a quick look to be sure all assets are in at the end of the day or just to check and see how many assets are out as you walk by the system.

Figure 2: Login Screen

The methods for logging into the kiosk are via **Pin Code**, **Fingerprint**, **Proximity (Prox) Card**, or **Magnetic Strip Card**. An **Admin** from your company will help you register for the system in one of these ways. Your **Admin** will setup the appropriate access type.



Pin Code Access

To login with your pin code, simply type it on the touch-screen monitor and press the **LOGIN** button. If you press a wrong number, use the backspace button (left arrow), or clear all of your numbers by pressing “C” for Clear.

Fingerprint Access

Simply touch your finger to the fingerprint reader to login. Always use the same finger with which you registered.

*NOTE: You and your **Admin** must register your fingerprint into the system before you will be able to login. If your company has more than one kiosk system, you may have to register at each one.*

Proximity (Prox) or Magnetic Strip Card Access

Swipe your card over the card reader to login.

*NOTE: You and your **Admin** will need to register your **Prox** or **Magnetic Strip** card with the system before you will be able to login. If your company has more than one kiosk system, you may have to register at each one.*

Reset Kiosk

After three failed login attempts while the system is initializing, you may see the option to restart the system. If you have waited and the kiosk is not responding, press “Yes” to restart the system. In some software versions, the popup does not appear and a restart will occur automatically.

Unable to Login?

Common reasons are:

- Incorrect PIN entered
- Login at the current time of day or day of week is not allowed (access groups not properly configured)
- Account disabled by admin

Check In

Single Cabinet Check In

To return a key to the cabinet, login and press **Check In** and the door will unlock. Open the door and insert the key fob into any illuminated socket. Close the door. Logout occurs when you close the door.

Asset Not Locked In (MX+ Only)

If an asset is not correctly inserted (locked in position), the system will alert the user through a series of visual and audible alarms. First, the location on the panel that the asset is located will light up amber for 5 seconds. If you do not lock-in the asset after 5 seconds, it will begin to flash red and there will be an audible beeping noise.

Depending on the configuration of the Kiosk alarm/alert settings, the asset not locked in may also trigger a Kiosk alarm (see **Web Admin Guide**).

Aside from the alarms, an Asset Not Locked In Alert will be generated and distributed to assigned users (see **Web Admin Guide**).



Multi-Cabinet Check In

Login and press **check in**. Choose one or more cabinets from the **Cabinet Selection Screen** (figure 3). The wait screen appears and the door on the first cabinet will unlock. Open the door and insert the asset into any illuminated socket. Close the door. Additionally selected cabinets will unlock. Logout occurs when you close the last door.

Figure 3: Multi-cabinet Check In

Process Step Check In

Login and press **check in**. Return your key to the cabinet and close the door. A Process Step screen will be displayed asking to select the process step. Select the process step and click ‘Continue’ (Or ‘Use for All’ if you are checking in multiple assets to a process step)

Figure 3: Process Step Check In



Identify Asset (MX ONLY)

To get information on a fob in your possession, login to the kiosk and press the **Identify Asset** button the main screen. Once on the **Identify Asset** screen, hold the asset against the asset reader on the kiosk, and press the **Read** button. The screen will display information about that asset (figure 4).

Identify Asset		Home	
Fob Number	472802058	Last Accessed By	travis ray
Asset Name	02058	Last Checkout Date	11/10/21 8:20 AM
Description	AMG M1165		

Figure 4: Identify Asset



Check Out

To check out an asset, login to the kiosk, or if already logged in, press the **Main** button. Press the **Check Out** button. You have three options for checking out an asset: **By Name**, **By List** or by **Filter Assets**.

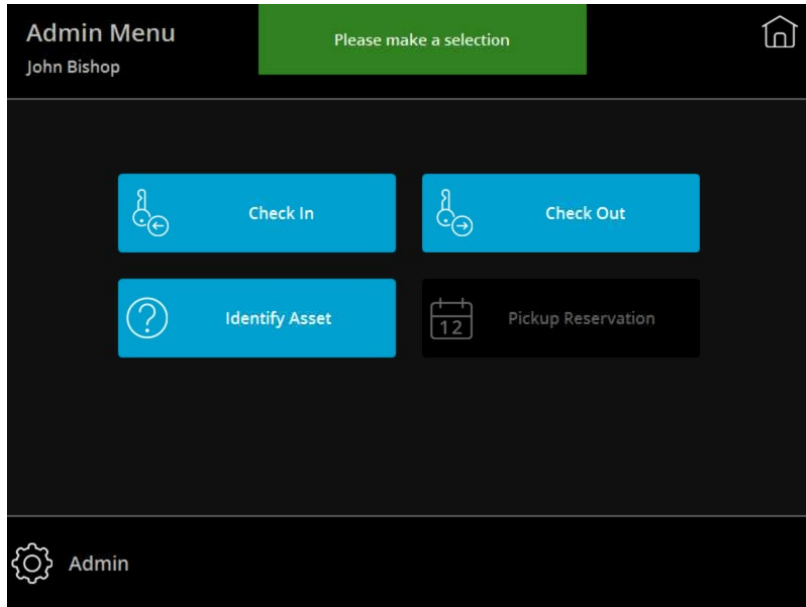


Figure 5: Check Out Screen

NOTES:

- *Regardless of the checkout method used, if Issue Reasons are activated on the system you will be required to choose an issue reason for each asset being checked out of the system prior to the checkout process beginning.*
- *For automotive applications, NAME equals Stock Number*



Check Out by Name

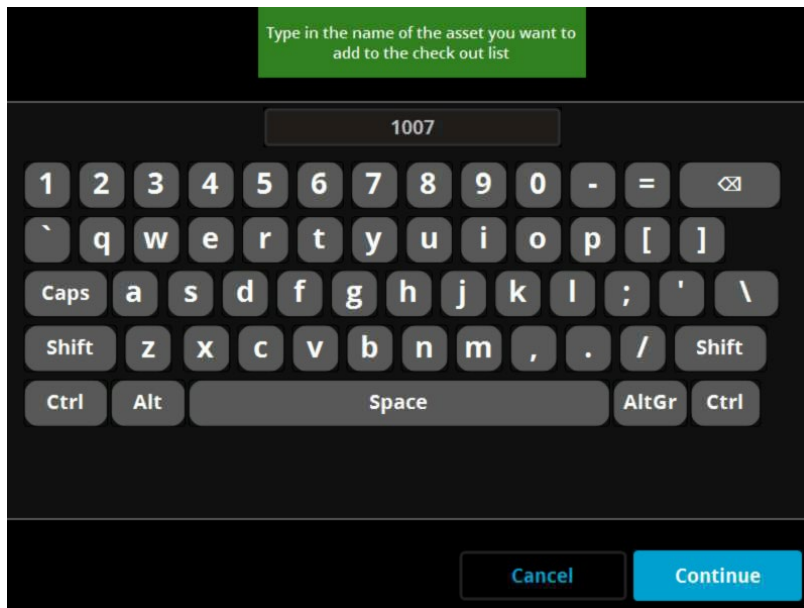


Figure 6: Check out By Name

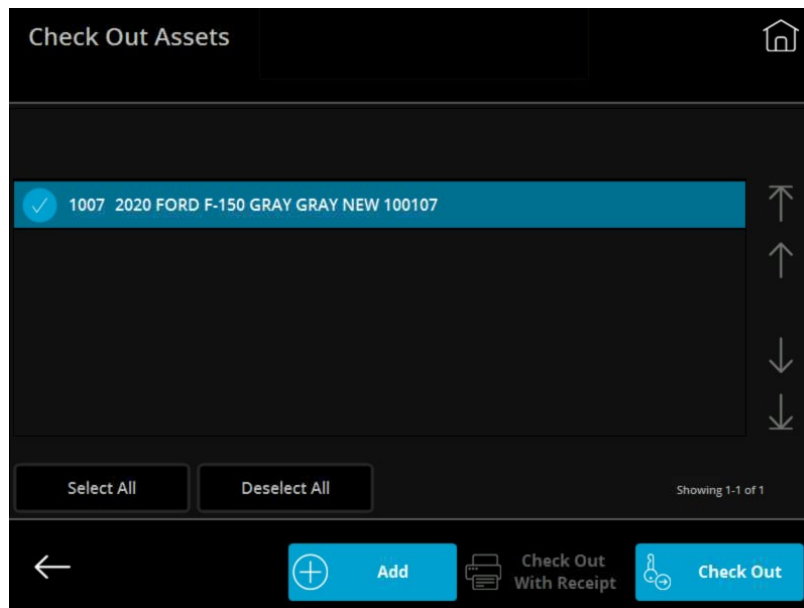


Figure 7: Check out By Name - asset found

Along the bottom of the screen are four (4) buttons: **Main**, **Check Out**, **Add** and **Log Out**.

- Pressing **Main** will ignore any selected assets and switch back to the main screen.
- Press **Check Out** to remove the chosen asset(s).
- **Add** will allow you to add more assets to your list.
- **Log Out** will ignore any selected assets and immediately log you out.

When you press “**Check Out by Name**”, you will see the **Keyboard** screen. Enter the complete asset name with the keyboard. Press the **Continue** button.

If the name exists, it displays in the list (figure 7). You can press the **Check Out** button now or press **Add** to return to the keyboard screen and find additional assets.

If the asset is missing, a message will appear at the top of the screen indicating this fact (if another user has checked out the asset, the message will identify the user).

If you have more assets than can be displayed on one page, the buttons on the right side of the screen will allow you to navigate the list. All lists in the system function in the same manner.

Top and **Bottom** will take you to the first and last pages, while **Up** and **Down** will move one page at a time. **Clear List** will remove items from the list.

Be sure to select the assets you want to check out. Selected assets have a blue background. Unselected assets have a white background. You can press the **Select All** and **Deselect All** buttons to change every asset in the list. To select or deselect one asset, press on that row to toggle the selection on and off.



- *NOTE: The number of keys you may have out at one time (**Issue Limit**), the systems and the cabinets you may access, and the days and times you may access the system(s), depend on the restrictions of the **Access Group** of which you are a member.*

Check Out by List

Pressing **Check Out by List** will display a list of all assets currently in the cabinet(s) that you have access to; based on your **Access Group** restrictions. Press each record (row) you wish to checkout. Displayed from left to right is the asset name, description, then attributes.

Press **Select All** to select all records, even if there are many pages. Likewise, **Deselect All** will deselect every selected record.

The buttons on the right side of the screen assist in scrolling through a list that is longer than one (1) page. The total number of registered assets in the cabinet displays above those buttons.

Along the bottom of the screen are three (3) buttons: **Main**, **Check Out**, and **Logout**. Pressing **Main** will ignore any selected assets and switch back to the main screen. Press **Check Out** to remove chosen asset(s). Log out will ignore any selected assets and immediately log you out.

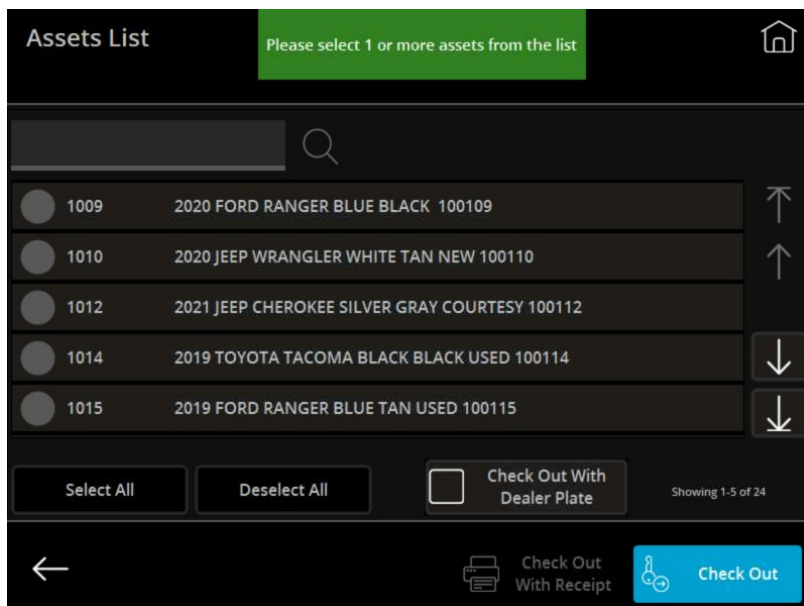


Figure 8: Check out By List

Check Out – Filter Assets

Use **Filter Assets** to search for assets by attributes, such as make, model, year, color, etc.

NOTE: This example is from a system setup for the automotive industry. Your filter attributes may differ. Entering Partial attribute values is acceptable. (i.e. Toy for Toyota, Civ for Civic, Bui for Building, etc.)

To search for assets by filtering attributes, enter an attribute value, then press the applicable filter button. For example, enter a year (4 digits), then press the **Year** filter button.



NOTE: To add an asset for check out by name on this screen, enter the full name and press the **Add** button.

Figure 9: Filter Screen

Now the **Year** filter button says “2020” and the green message box indicates the filter narrowed the total to six (6) assets (figure 10).

Figure 10: Filter Screen

Continuing the example, the Year is filtered on “2020” and *before* the **Review** button is pressed, the **Ext. Color** is filtered on “Silver” (figure 11).



Asset Filter

silver Add

Year (2020) Make (Not Set) Model (Not Set) Ext. Color (Not Set) Int. Color (Not Set) Type (Not Set) VIN (Not Set)

1 2 3 4 5 6 7 8 9 0 - =

` q w e r t y u i o p []

Caps a s d f g h j k l ; ' \

Shift z x c v b n m , . / Shift

Ctrl Alt Space AltGr Ctrl

← Review

Figure 11: Filter Screen

the narrowing of the list to two (2) assets.

Now in figure 12, the green message box indicates

Asset Filter

Filter 'silver' on 'Ext. Color' narrowed total to 2 assets

silver Add

Year (2020) Make (Not Set) Model (Not Set) Ext. Color (silver) Int. Color (Not Set) Type (Not Set) VIN (Not Set)

1 2 3 4 5 6 7 8 9 0 - =

` q w e r t y u i o p []

Caps a s d f g h j k l ; ' \

Shift z x c v b n m , . / Shift

Ctrl Alt Space AltGr Ctrl

← Review

Figure 12: Filter Screen

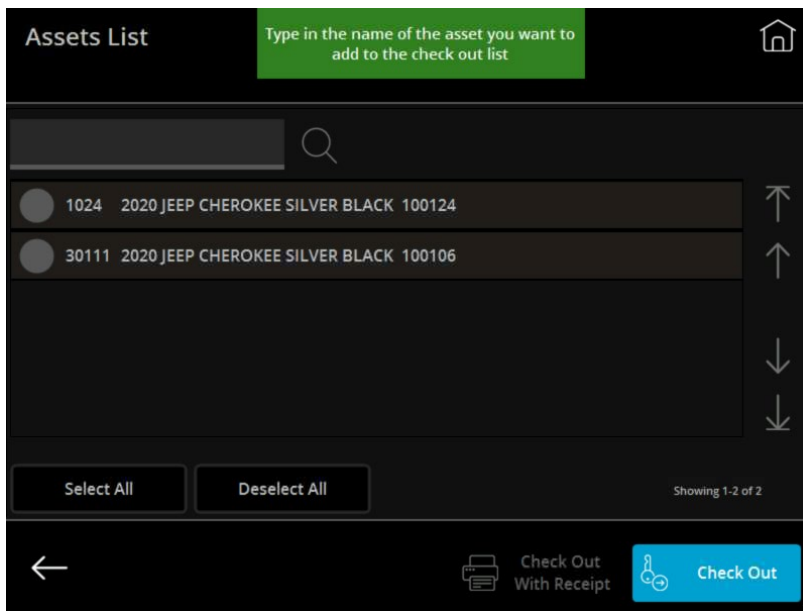


Figure 13: Filter Screen

Pressing **Review** shows the filtered assets (figure 13). Selecting the asset and pressing the **Check Out** button opens the cabinet.

*NOTE: Once in the **Review Assets** screen, you must **Check Out**, **Logout**, or go back to the **Main** screen. You **cannot** go directly back to the filtering screen.*

Unable to Locate or Check Out an Asset?

If you are unable to Checkout a particular asset, consider these common reasons:

- Asset already checked out by someone else
- Asset moved to another Kiosk
- Checkout at the current time of day or day of week is not allowed
- Asset limitation rules
- Asset permission disabled by Administrator
- Asset not registered by Administrator

Multi-Cabinet Checkout

When one or more cabinets are attached to the Kiosk cabinet (2+ cabinets total), it is a multi-cabinet system. When you check out several assets at one time, they may be stored in several cabinets. The cabinets will unlock one at a time. The second cabinet unlocks after the first cabinet closes. The third cabinet unlocks after the second cabinet closes, and so on.



Log Out

To log out from the Main screen, simply press the **Home** button in the upper right corner.

Logout

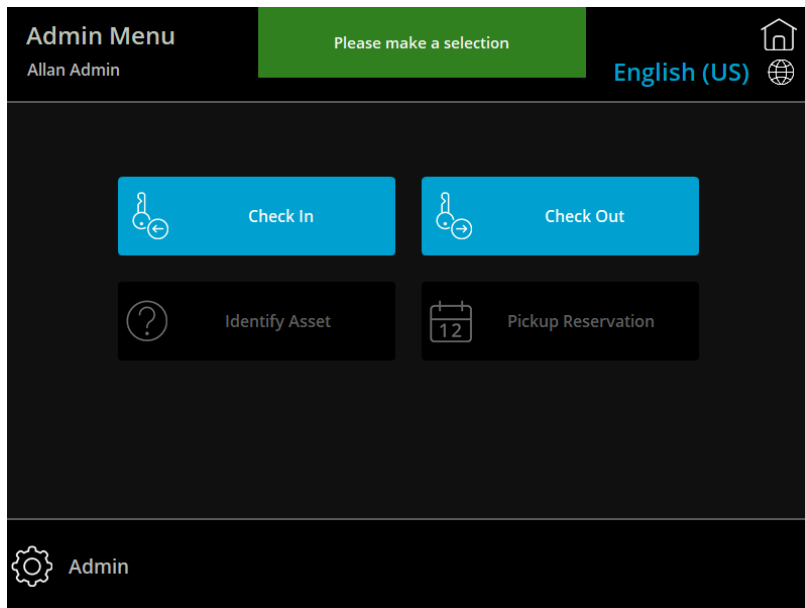


Figure 14: Main Screen



Optional Features

This section describes the use of optional features available for the system. Some or all of these features may not be applicable to your system.

Issue Reason and Comment

If the system configuration requires an **Issue Reason** during check out, the screen depicted in figure 15 will appear (your **Issue Reasons** may differ). Select a reason from the list. Choose **Continue** to return to the Checkout menu and finish the Checkout process.

Issue Reason

Select issue reason for '1007'

☐ Detail

☐ Move

☐ Sales Demo

☐ Service

Showing 1-4 of 4

Cancel Use For All Continue

Figure 15: Issue Reason Screen

*NOTE: Your admin can choose to make the selection of an **Issue Reason** mandatory or not.*

If you are checking out multiple assets and the **Issue Reason** will be the same for all, press the “**Use for All**” button instead of **Continue**. Thereafter, you can select more assets without returning to this screen.

After selecting a reason, you may type a comment about this **Issue Reason** by pressing in the gray **Comment** box. The on-screen keyboard will appear, allowing you to type a comment. The system saves the comment and displays it on the **Asset Transaction Report**.



Print Receipt

If **Print Receipt** is active, during **Checkout** the system will show the Check out with Receipt button being highlighted. If receipt printing is mandatory, only the **Check Out/Print Receipt** button will appear. Using the **Check Out/Print Receipt** button will create and print a list of assets checked out (figure 17).

The screenshot shows the 'Assets List' interface. At the top, there is a green banner with the text 'Please select 1 or more assets from the list'. Below this is a search bar with a magnifying glass icon. A table lists five assets, each with a selection radio button, an ID number, and a description. To the right of each row are up and down arrow icons for sorting. At the bottom of the table are 'Select All' and 'Deselect All' buttons. Below the table, there is a navigation bar with a back arrow, a 'Check Out With Receipt' button (highlighted in blue), and a 'Check Out' button. The text 'Showing 1-5 of 23' is visible at the bottom right of the table area.

ID	Description
02058	2022 AMG M1165 TAN TAN FLEET
1007	2020 FORD F-150 GRAY GRAY NEW 100107
1013	2019 FORD F-150 GRAY TAN USED 100113
1015	2019 FORD RANGER BLUE TAN USED 100115
1016	2018 JEEP WRANGLER WHITE BLACK USED 100116

Figure 16: Print Receipt Checkout Button

The screenshot shows a 'Checkout List for C Pierce (8/22/2011 12:53 PM)'. It lists three assets with their IDs and descriptions: 222783114 1995, BMW, 750 HYBRID, 2011, FORD, RED, and 222453536 1995, AUDI, TT, RED, LONER. Below the list is a signature line with the name 'John Hancock'. There are also fields for 'Name', 'Returned by', 'Date', and 'Time'.

Checkout List for C Pierce (8/22/2011 12:53 PM)

222783114
1995, BMW, 750 HYBRID,

2011, FORD, RED,

222453536
1995, AUDI, TT, RED, LONER,

John Hancock

Name

Returned by Date Time

Figure 17: Sample Receipt



Lot Location

If your system is setup with the lot location feature, a prompt asks a user to select the location of an asset following check in. The asset name displays in the message bar so that the user will know which asset they are assigning to a location. Figure 19 below is what the user will see following check in.

Check In - Lot

Select the current location of asset 02058

- ☐ (None)
- ☐ Back Lot
- ☐ Front Lot
- ☐ Off Site Lot

Showing 1-4 of 4

Cancel Use For All Continue

Figure 19: Lot Location Prompt



Installation Guide





Safety

1. Read these instructions thoroughly before attempting to install or operate the equipment.
2. Keep these instructions.
3. Heed ALL Warnings, Notes, and Cautions.
4. Do not use equipment near water.
5. Do not block any ventilation openings.
6. To avoid risk of electric shock, do not disassemble any part of the cabinet unit.
7. Do not install near any heat sources, radiators, heat registers, stoves or other apparatus generating heat.
8. Do not defeat the safety purpose of the grounding-type plug. A grounding plug has two blades, and a third grounding prong provided for your safety. If the provided plug does not fit into your outlet, consult an electrician.
9. Protect the power cord from damage, particularly at plugs, convenience receptacles and the point where the cord exits the cabinet.
10. Only use attachments or accessories specified by the manufacturer.
11. Remove power before performing any maintenance.
12. Always use appropriate assistance to lift or move cabinets.

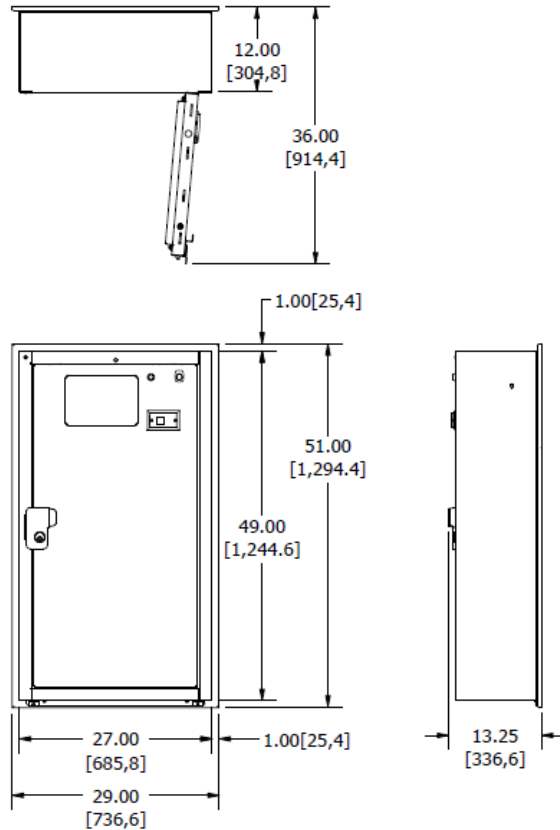
Care and Handling

1. If you believe your system requires service, contact the Technical Support at KEYper® Systems.
2. To clean the biometric lens, place a strip of transparent tape (i.e. Scotch) on the lens and peel off. Repeat as required. **NEVER USE ANY TYPE OF CLEANER OR FLUID & NEVER WIPES WITH ANY TYPE OF CLOTH OR PAPER.**
3. To clean the cabinet(s):
 - a. Perform a normal shutdown of the kiosk computer.
 - b. Unplug the unit from the power outlet.
 - c. Use a cloth, lightly dampened with a mild detergent. Do not use alcohol (methyl, ethyl, or isopropyl) or any strong solvent.
4. Avoid getting liquids inside your key management system. If liquid does get inside, contact KEYper® Technical Support before reapplying power.
5. Clean monitor with commercially available computer screen cleaner. Never apply cleaner directly to the touch monitor. Do not use alcohol (methyl, ethyl, or isopropyl), thinner, benzene, or other abrasive cleaners.



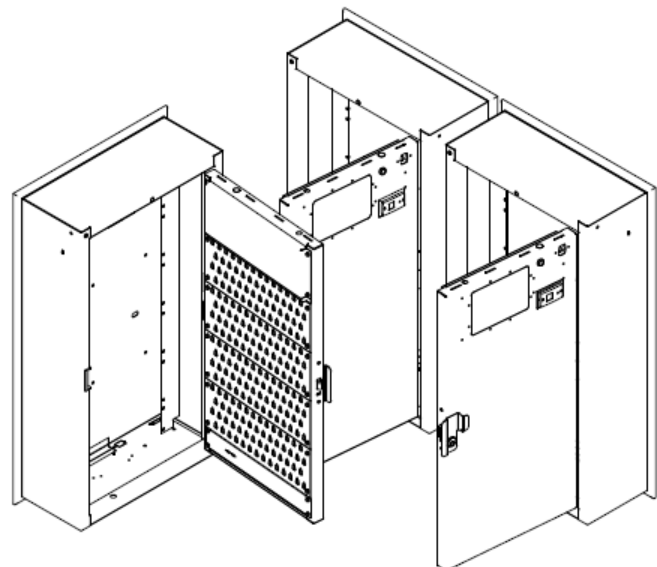
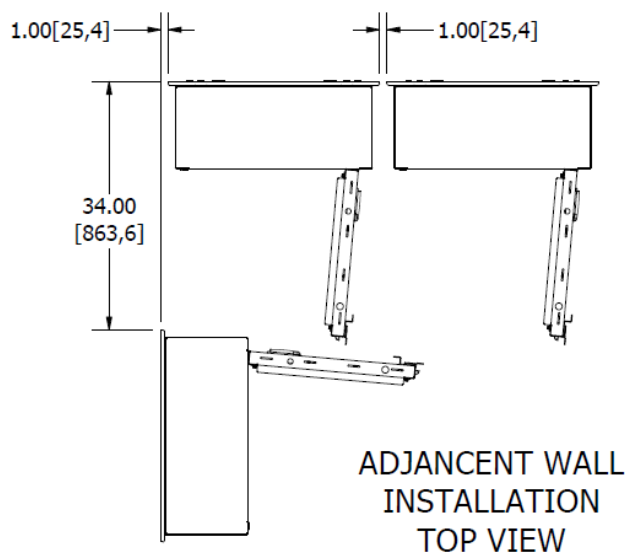
Large Cabinet Wall Mounting

Drawing 1 – Large Cabinet



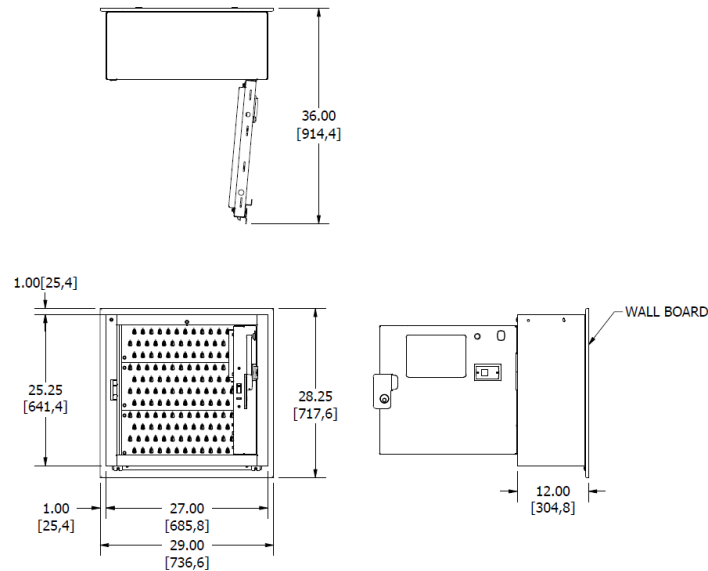
NOTE:

1. For multiple cabinets leave 1"[25,4mm] between wall boards. A 7"[2,3m] cabinet to cabinet cable for add-on cabinets is provided. The maximum distance between cabinets is not to exceed 5'[1,524m]
2. AC mains must be within 48"[1,22m] of the cabinet and preferably on the same wall.
3. Ethernet connections must be within 48"[1,22m] of the main cabinet with controller; if a multiple cabinet system; and preferably on the same wall mounted at the height required by local code.
4. Mounting the wall board is the responsibility of the customer and it is recommended that a professional installer do the installation. The final installation must support the weight of the cabinet, wall board and its contents. The estimated weight is 300lbs[136,1kg]. Local ethernet cable is supplied by customer.
5. The mounting height of the cabinet is 67"[1,70m] from the floor to the top of the cabinet.
6. If this cabinet is mounted above a desk or table, allow at least 3"[76,2mm] between the desk or table and the bottom of the cabinet.
7. Dimensions in [] are metric.



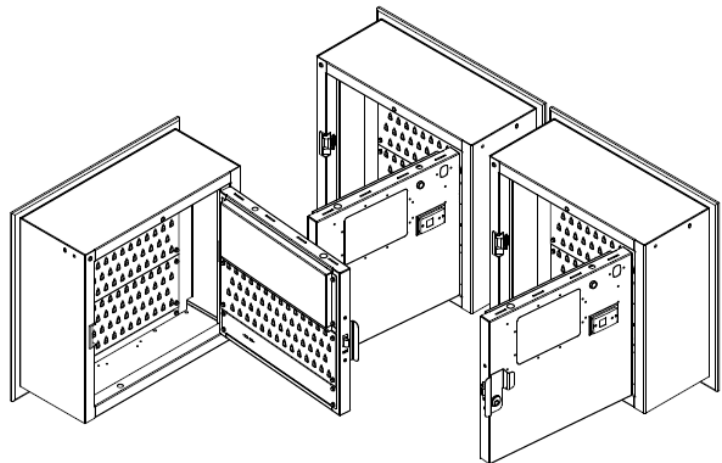
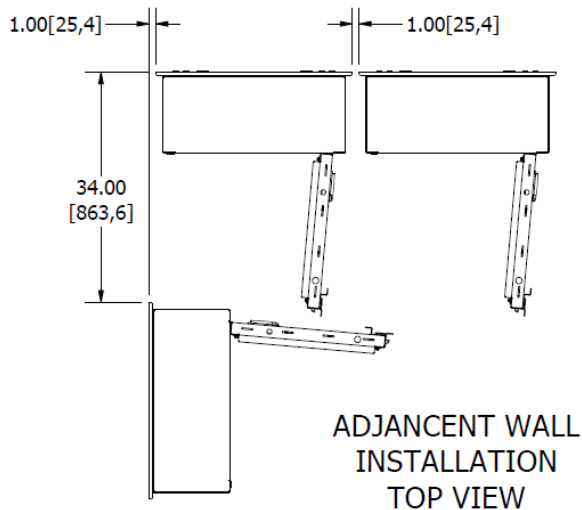
Small Cabinet Wall Mounting

Drawing 2 – Small Cabinet



NOTE:

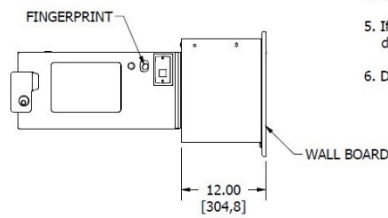
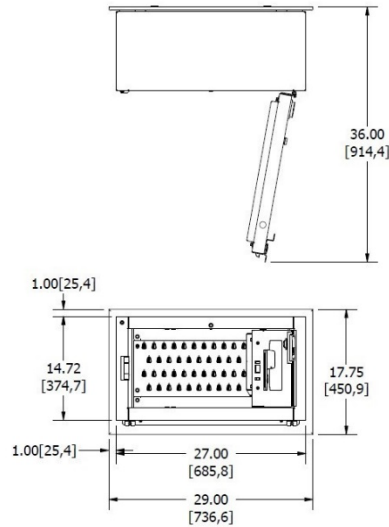
1. For multiple cabinets leave 1" [25,4mm] between wall boards. A 7" [2,3m] cabinet to cabinet cable for add-on cabinets is provided. The maximum distance between cabinets is not to exceed 5' [1,524m].
2. AC mains must be within 48" [1,22m] of the cabinet and preferably on the same wall.
3. Ethernet connections must be within 48" [1,22m] of the main cabinet with controller; if a multiple cabinet system; and preferably on the same wall mounted at the height required by local code.
4. Mounting the wall board is the responsibility of the customer and it is recommended that a professional installer do the installation. The final installation must support the weight of the cabinet, wall board and its contents. The estimated weight is 300lbs [136,1kg]. Local ethernet cable is supplied by customer.
5. The mounting height of the cabinet is 67" [1,70m] from the floor to the top of the cabinet.
6. If this cabinet is mounted above a desk or table, allow at least 3" [76,2mm] between the desk or table and the bottom of the cabinet.
7. Dimensions in [] are metric.





Mini Cabinet Wall Mounting

Drawing 3 – Mini Cabinet



NOTE:

1. AC mains must be within 48" [1,22m] of the cabinet and preferably on the same wall.
2. Ethernet connection must be within 48" [1,22m] of the cabinet.
3. Mounting the wall board is the responsibility of the customer and it is recommended that a professional installer do the installation. The final installation must support the weight of the cabinet, wall board and its contents. The estimated weight is 150lbs [68,0kg]. Local ethernet cable is supplied by customer.
4. The mounting height of the cabinet is 67" [1,70m] from the floor to the top of the cabinet.
5. If this cabinet is mounted above a desk or table, allow at least 3" [76,2mm] between the desk or table and the bottom of the cabinet.
6. Dimensions in [] are metric.



Installation of Wall Mounted System

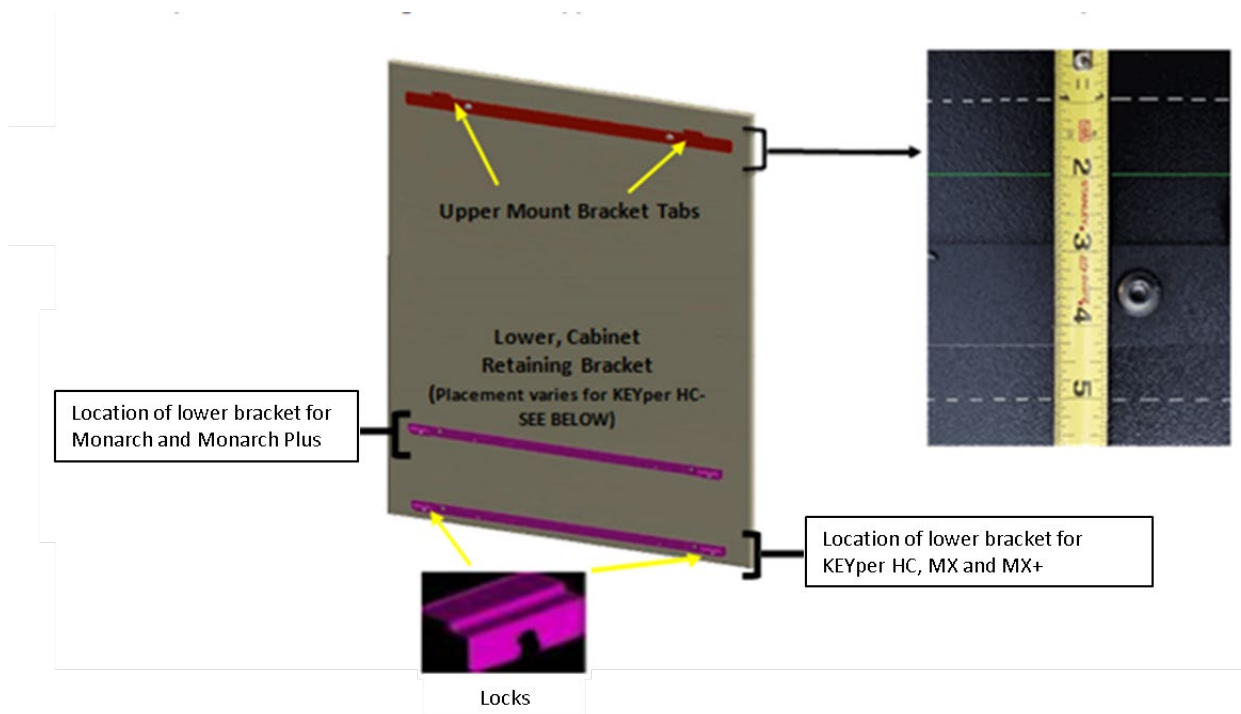
CAUTION: Wall mounts should be installed by a Certified Professional. Cabinets are heavy.

NEVER attempt to install or remove a cabinet without proper assistance.

No mounting hardware is included. Your professional will choose the appropriate type of hardware and the number of pieces required to meet the following requirements:

1. Area of wall selected for key cabinet installation must support up to 300lbs (136kg), or 200lbs (91kg) for small cabinets.
2. Install so top of mount is 67" (1.7m) from the floor for MX and MX+, or 61" (1.55m) from the floor for Monarch and Monarch Plus.
3. Minimum of 24" (61cm) clearance required above wall mount for Monarch and Monarch Plus.
4. Minimum of 1" (2.5cm) space required between adjacent wall mounts and/or walls.

NOTE: Hardware securing the upper area of the mount to wall requires placement between 1" (2.5cm) and 5" (12.7cm) from top of mount, avoiding the metal, upper, cabinet mount bracket. The 2" (5cm) mark is preferred as (figure 1).



Wall mounts arrive with the upper and lower cabinet mounting brackets installed. Two (2) cabinet locks attach to the lower bracket. The tool for the screws strap to one of the locks. Remove the locks just prior to hanging the cabinet. The upper mount brackets have (2) tabs that correspond to slots in the back of the cabinet. The lower bracket may require relocation to hang the cabinet (see above).

NOTE: The two locks secure with 1/4"-20 x 5/8" hex socket button head cap screws.

Lift the cabinet, line up the upper mount bracket tabs with the slots in the cabinet back and let the cabinet gently settle on the tabs (see Fig. 1). Secure the bottom of the cabinet with the lower cabinet locks by sliding the upper part of the lock into its corresponding slot on the bottom of the cabinet and secure with a button-head Allen screw (Fig. 2).

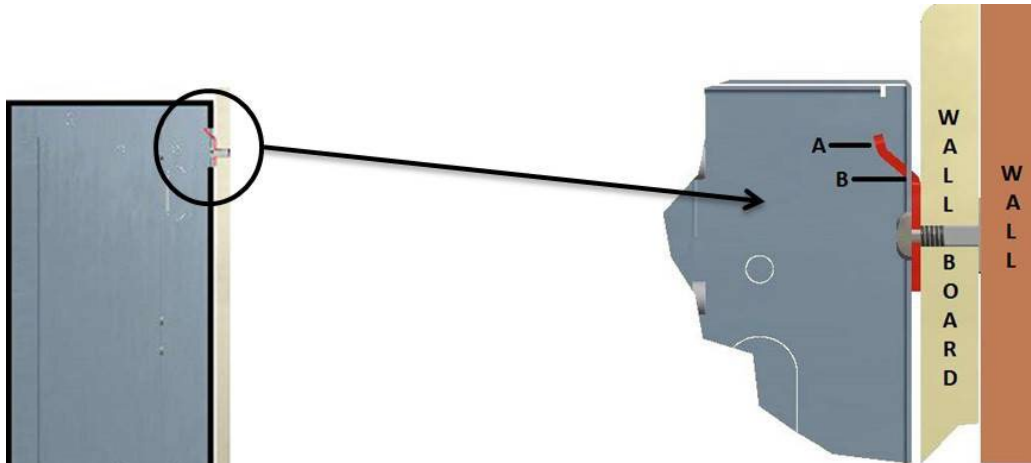


Fig.1

A – Upper Mount Bracket
B – Slot in cabinet back

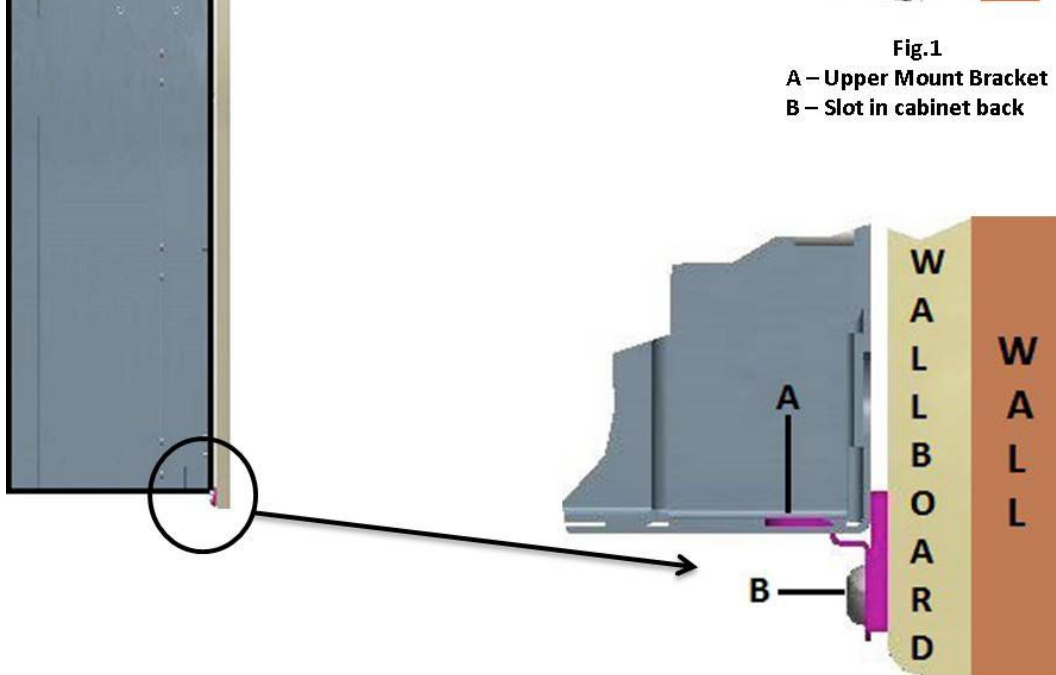


Fig.2

A – Cabinet Lock
B – Button head Allen screw



Installation of Stand Mounted System

If you choose to set the system up as delivered, in a complete stand configuration, install the four nylon-leveling feet, found in the accessories box. **With appropriate assistance**, the cabinet and stand can tilt far enough from side to side to access the predrilled holes in each “corner” of the stand. Insert each leveling foot to maximum depth but do not tighten. Position and level the system.

NOTE: For systems where two cabinets mount to one stand in a “back-to-back” configuration, six leveling feet are included. All six leveling feet require installation to provide proper support.

To reduce the footprint of a single stand mounted cabinet you may detach the back foot of the stand and place the system against a wall.

WARNING! DO NOT REMOVE THE BACK FOOT UNLESS THE CABINET IS MOUNTED ****OVER**** THE FRONT FOOT OF THE STAND! Key system cabinets and stands are heavy! With the back foot removed, the system will easily tip backwards! Never attempt to install or relocate a cabinet without proper assistance.



Figure 3: Detachment of rear stand foot

To do so, remove 4 bolts located near the bottom of the stand with a 5/16” Allen head wrench, or similar, and gently detach the back foot **while ensuring the cabinet is properly supported at all times**. Install four leveling feet, found in the accessories box, on the front foot.



With appropriate assistance, the cabinet and stand will tilt far enough back and forth to access the predrilled holes in the stand, two at the front “corners” and two beneath the upright bars. Insert each leveling foot to maximum depth but do not tighten. Position and level the system.

Also included in the accessories box are brackets for securing the system stand to a wall. A qualified person should accomplish this.



Figure 4: Wall brackets included in accessories box



Connections

Power-Up & Connect to your network

(Refer to Diagram 1)

NOTE: All required cables are included and are included in the Accessories Box. It is the customers' responsibility to provide any additional or longer cables as required for system installation.

- 1) To connect your key system to your network, connect the provided Ethernet cable to a live data port on your network, then to the stand alone, recessed RJ45 connection on the **left** side of the **node bracket** at the **rear, bottom** of each controlling cabinet (figure 5).
- 2) For multi-cabinet systems, connect cabinets together by inserting one end of an Ethernet cable into the recessed RJ45 port on the **right** side of the node bracket at the **rear, bottom** of each controlling cabinet. The other end into **either** of the recessed RJ45 ports on the **right** side of the node bracket at the **rear, bottom** of the second cabinet. If required, run another cable from the open RJ45 port on the second cabinet to either of the open ports on the third cabinet and so on. It is possible to connect up to eight cabinets, including the controlling cabinet.
- 3) To connect power to the system, connect the provided power cable's barrel connector to the receptacle located near the **center**, underneath the cabinet.

NOTE: Route the power cable along the node bracket and secure in order to protect the barrel connector from being disconnected (figure 5).

The other end of the power cable connects to an AC-DC adapter. Plug the adapter into an appropriate power supply. The power required per cabinet is 100-240VAC, 1.3A, 50/60 Hz. We recommend that you connect the system to battery backup and/or surge protection devices.

- 4) The controlling cabinet computer will auto-boot and within a few minutes should display the PIN login screen. The system will attempt to acquire an IP address from your network via DHCP. The IP address displays on the **Kiosk** touch screen as a set of four numbers, such as 192.168.10.12.

*NOTE: If the IP address displayed is 127.0.0.1, you **DO NOT** have network connectivity. Contact your IT support for assistance.*

If your IT department requires the system to have **Static IP** information, you will need to close the KEYper® software. Use PIN 1234 to login to the **Kiosk**. From the available options, select **Exit Application**. You are now at the Desktop and your IT will have access to configure static IP information.

Double tap the **KS** icon on the desktop to restart the KEYper® software.

Contact KEYper Tech Support with questions and for assistance if required.

To connect to the key system from a PC on the same network, please refer to page 2 of the **Web Administration Guide**.

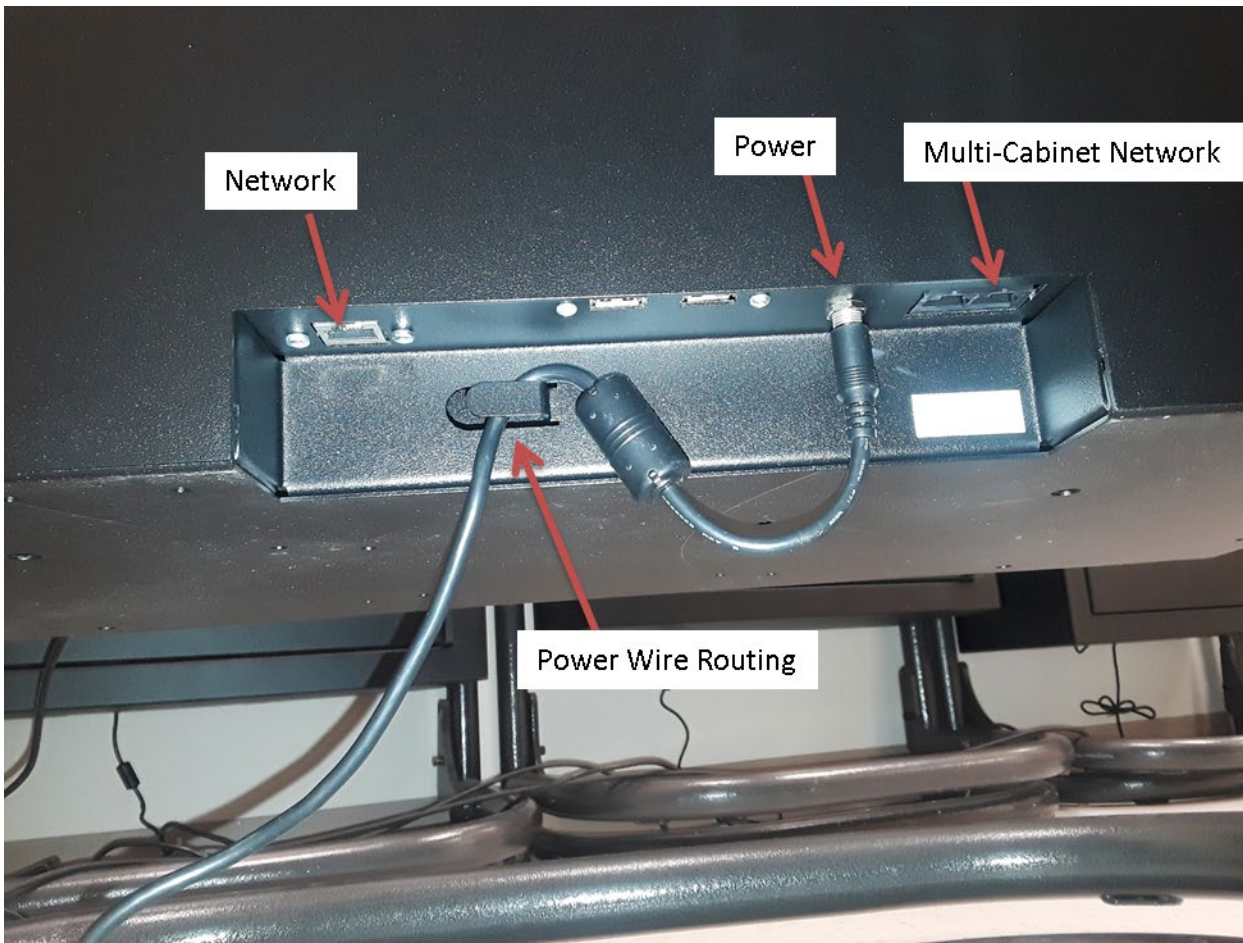


Figure 5: Node Panel, Bottom Center of the Rear Panel of the Cabinet



Diagram 1 – Cabinet Connections

NOTE: Wiring/cabling configuration is the same for wall mounted and stand mounted systems.

CAUTION: For multiple cabinet, wall mounted systems, ensure there is at least 2" between wallboards

