Installation & Use of KEYper Elite Series Asset Management Systems
Table of Contents

Safety ........................................................................................................................................ 2
Care and Handling .................................................................................................................. 3
Drawing 1 - Monarch, Large Cabinet .................................................................................... 4
Drawing 2 - Monarch, Small Cabinet ..................................................................................... 5
Drawing 3 - Multiple Cabinets ............................................................................................... 6
Installation of a Wall Mounted System ................................................................................ 7
Installation of a Stand Mounted System ............................................................................ 10
System Connections ............................................................................................................ 11
Diagram 1 – Monarch Cabling ............................................................................................. 12

See the Table of Contents for each of the following sections of this manual for KEYper® software operating instructions.

Management Console
Kiosk

System Specifications and Warranty information can be found in the back of this manual.
**Important Safety Instructions**

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 being walked on or pinched, 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 of the Key Management System

The following tips will help keep your Key System functioning at the optimal level:

- If you believe your system requires service, contact Technical Support at KEYper® Systems.
- 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 WIPE WITH ANY TYPE OF CLOTH OR PAPER.
- To clean the cabinet(s):
  - Perform a normal shutdown of the kiosk computer.
  - Unplug the unit from the power outlet.
  - Use a cloth, lightly dampened with a mild detergent. Do not use alcohol (methyl, ethyl or isopropyl) or any strong solvent.
- Avoid getting liquids inside your key management system. If liquid does get inside, contact KEYper® Technical Support before reapplying power.
- 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.
Notes & Cautions: (Plastic composite wall mounts are included with wall mounted key system orders. Hardware to properly install the mounts must be supplied by the customer)

1. **Proper installation of wall mounts is critical** & must be accomplished by a professional.
   a. always choose a weight bearing wall.
   b. the weight of a fully loaded 280 position Cabinet with a Controller Hood could be as much as 300lbs.

2. Recommended installation height of wall mounts is 61" from the floor to the top edge of the mounts.

3. For multiple cabinets, leave 1" between mounts to allow enough space to plug in AC power cord. The maximum distance between cabinets cannot exceed five (5) feet.

4. Power: 100VAC@3A - 220VAC@1.5A, Input Frequency 50-60Hz. Must be within two (2) feet of the main cabinet, at the height required by local code.

5. Internet/network connection should be within a few feet of the main cabinet, at the height required by local code.
Drawing 2 – Wall Mount, Small Cabinet

Notes & Cautions: (Plastic composite wall mounts are included with wall mounted key system orders. Hardware to properly install the mounts must be supplied by the customer)

1. **Proper installation of wall mounts is critical** & must be accomplished by a professional.
   a. always choose a weight bearing wall.
   b. the weight of a fully loaded 280 position Cabinet with a Controller Hood could be as much as 200lbs.

2. Recommended installation height of wall mounts is 61” from the floor to the top edge of the mounts.

3. For multiple cabinets, leave 1” between mounts to allow enough space to plug in AC power cord. The maximum distance between cabinets can not exceed five (5) feet.

4. Power: 100VAC@3A - 220VAC@1.5A, Input Frequency 50-60Hz. Must be within two (2) feet of the main cabinet, at the height required by local code.

5. Internet/network connection should be within 48” of the main cabinet, at the height required by local code.

Need 23” in front of cabinet for door swing
Drawing 3 – Multi-Cabinet, Adjacent Wall

Recommended Layout using adjacent wall
Installation of a Wall-Mounted KEYper System

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

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

1. Area of wall selected for key cabinet installation must support up to 300lbs (200lbs for small cabinets).
2. Install so Top of Mount is 61” from the floor
3. Minimum of 24” clearance required above Wall Mount
4. Minimum of 1” space required between adjacent Wall Mounts &/or walls

NOTE: Hardware securing the upper area of the Mount to wall must be placed between 1” & 5” from top of Mount, avoiding the metal, upper, cabinet Mount bracket. The 2” mark is preferred.
Wall Mounts arrive with the upper and lower cabinet Mounting brackets installed. Two (2) cabinet locks will be attached to the lower bracket. The tool for the screws will be strapped 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.

**CAUTION:**
Cabinets are HEAVY & AWKWARD.
NEVER attempt to install or remove a cabinet without PROPER assistance.
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 securing with a button-head Allen screw (see Fig. 2).
Installation of a Stand-Mounted KEYper System

If you choose to set the system up as it is delivered, in a complete stand configuration, install the 4 nylon leveling feet, found in the accessories box. With appropriate assistance, the cabinet and stand may be tilted 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.

NOTES:

1. For systems where two cabinets are mounted to one stand in a “back-to-back” configuration, 6 leveling feet are provided – All 6 leveling feet must be installed to provide proper support.
2. To reduce the foot print of a single, stand-mounted cabinet, you may detach the back foot of the stand and place the system against a wall.

CAUTION: DO NOT remove the back foot if the front foot is not mounted over the stand. Key system cabinets and stands are HEAVY. Once the back foot is removed, the system will easily tip backwards. Never attempt to install or relocate a cabinet without proper assistance.

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 may be tilted 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. Included in the accessories box are brackets for securing the system stand to a wall. This should be accomplished by a qualified person. Once installation is complete refer to Key System Connections (pg. 11) and Diagram 1 (pg. 12).
Key System Connections
(Refer to Diagram 1 on the following page)

NOTE: Standard installation cables are included, and will be found in the Accessories box. It is the customer’s 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 flush-mounted RJ45 connection found under each controlling cabinet. For multi-cabinet systems, connect cabinets together by inserting one end of an Ethernet cable into the recessed RJ45 port at the bottom of the controlling cabinet, and the other end into either of the recessed RJ45 ports at the 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 - up to a total of 8 cabinets, including the controlling cabinet.

2) The control cabinet of each Monarch & Monarch Plus system requires two power cables.

Monarch - One cable connects to the IEC receptacle located on the lower right side of the cabinet, and supplies power to the touch screen and all cabinet components. The second cable connects to the IEC receptacle found at the bottom of the control cabinet, and supplies power to the internal computer. Each additional cabinet includes a power cable that connects to the cabinet’s IEC receptacle, found on the lower right-hand side. The power required per cabinet is 100VAC@3A or 220VAC@1.5A, 50-60Hz. It is recommended the system be connected to battery back-up and/or surge protection devices.

Monarch Plus – Both IEC power receptacles are located at the bottom of the control cabinet. Each additional cabinet includes a power cable that connects to the cabinet’s IEC receptacle, found at the bottom of the cabinet.

3) When powered, each cabinet should emit four quick beeps. 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 is displayed 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 log into 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 Management Console section of this manual.
Diagram 1 – Elite Series Cabinet Connections

If your system has a top mounted control box, it is a **MONARCH (A)**
If the control box is side mounted, it is an **ULTRA (B)**

**CAUTION:** For multiple cabinet, wall mounted systems, ensure there is at least 1" between wallboards.

**CAUTION:** Maintain a minimum of 3" from adjacent wall

**NOTE:** For Monarch Plus systems all power receptacles are located at the bottom of the cabinet

- **Ethernet** CAT 5/6
- **Power** 100VAC@3A – 220VAC@1.5A, 50-60Hz

**Up to 8 cabinets**
# Elite Series Management Console User Guide

## Table of Contents

- Connect to the Management Console ....................................................................................................................... 2
- The Dashboard .......................................................................................................................................................... 3
- Manage Users ........................................................................................................................................................... 4
  - Add Users .................................................................................................................................................... 4
  - Edit Users ..................................................................................................................................................... 6
  - Delete Users.................................................................................................................................................. 6
  - Import Users.................................................................................................................................................. 6
- Manage Assets.......................................................................................................................................................... 7
  - Installing Fob Reader Drivers ........................................................................................................................ 7
  - Importing Assets ........................................................................................................................................... 7
  - Adding Assets ................................................................................................................................................ 8
  - Deleting Assets ............................................................................................................................................ 11
- Access Groups .......................................................................................................................................................... 12
  - Create Access Group.................................................................................................................................... 12
  - Configure/Edit Access Groups ...................................................................................................................... 13
- Asset Attributes ...................................................................................................................................................... 14
- Reporting ............................................................................................................................................................ 15
- Settings .................................................................................................................................................................. 15
  - Alerts ............................................................................................................................................................ 15
  - Email ............................................................................................................................................................ 16
  - Issue Reasons ............................................................................................................................................. 16
- Support .................................................................................................................................................................. 17

**WARNING**: It is very important to clean the lens of the fingerprint device frequently using transparent tape ONLY (i.e., Scotch tape). Press on and peel off to remove oils, dirt, etc. Repeat as necessary.
Connect to the Management Console

NOTE:
1. Your system will arrive with a Default Admin administrative profile installed. The PIN is 1234. Use this to log into the Management Console to begin key system administration.
2. The Management Console may be opened in IE, Edge, Chrome, etc. However, the fob reader is compatible with IE only.

WARNING: Once you have created your own Admin profile, DELETE the Default Admin user!

Connect to the Management Console from a PC on the same network by opening Internet Explorer and entering the IP address of the key system in the URL bar. The IP address is displayed on the kiosk screen (eg. 192.168.25.15).

NOTE: Primary WS (Web Service) and Primary DB (Data Base) should always indicate Connected.
The Dashboard

The **Dashboard** is the Home Screen of the **Management Console**. It provides an “at a glance” view of the status of the key system. The menus located at the top of the **Management Console** 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 display lists the last 10 transactions and warranty expiration information.

![Dashboard Image](image-url)

**Figure 1: The Dashboard**
Manage Users – Edit, Audit, User Change Log

Admin vs. User – Know the Difference

<table>
<thead>
<tr>
<th>ADMINs:</th>
<th>USERS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Can access the KEYper® Management Console</td>
<td>• Cannot access the KEYper® Management Console</td>
</tr>
<tr>
<td>• Override all Access Group restrictions</td>
<td>• Adhere to assigned Access Group restrictions</td>
</tr>
<tr>
<td>• Have Access to the Admin functions of the kiosk</td>
<td>• Can only Check In, Check Out and Identify assets at the kiosk</td>
</tr>
</tbody>
</table>

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 quickly find a particular User.

1. Add New User
   a. In the upper right of the Users List page (fig. 2), click the “Add” button.
b. Fill in the Users information (** indicates required field)
   i. First Name**
   ii. Last Name**
   iii. Description (i.e. position title)
   iv. Password** (Numeric only, 6-digit minimum)
   v. Role** Admin or User
   vi. Access Web Reports – if marked True this feature allows a User to log into the Management Console and access Reports only.
   vii. Access Web Assets – if marked True this feature allows a User to log into the Management Console and access Assets only (Add, Delete, Edit).
   viii. Email Address (For Email Alerts)
   ix. Phone Number (For SMS Alerts)
   x. Carrier (For SMS Alerts)
      1. If desired carrier is not listed, contact KEYper® to see about adding it as a selection.
   xi. Prox or Swipe ID – for systems incorporating either a proximity card reader or a magnetic strip card reader. If the number is known, it may be entered at the time the User is added to the system. Primarily, this field will be auto-filled when the User’s card is read during Device Enrollment.
   xii. 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 users have been entered into the system, a User’s Access Group membership must be edited through the user’s profile or by editing individual Access Groups.
2. Edit a User
   a. From the main User List page, find the User you wish to modify in the list of Users.
      i. 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.
   b. Click the Edit button to the right of the desired user.
   c. Make adjustments and click Save.

3. Deleting a User (Deleting a user does not remove the user’s history from the database.)
   a. Find the user you wish to delete in the list of users.
   b. Click the Delete button to the right of the desired user.
   c. Confirm that you wish to delete the user.

4. Importing a User List (figs. 4-6)
   a. A group or list of users can be imported into the system. Except for biometric registration, this eliminates the individual addition of users.
   b. The file must be saved in .CSV format. (Comma Separated Value)
   c. The User info in the CSV file must be in the format shown in figure 4.

   NOTE: A minimum 4-digit number is required in the Prox column.

<table>
<thead>
<tr>
<th>First</th>
<th>Last</th>
<th>Description (job title)</th>
<th>PIN</th>
<th>Role (Admin or User)</th>
<th>Prox</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adam</td>
<td>Smart</td>
<td>Sales</td>
<td>4321</td>
<td>User</td>
<td>4321</td>
</tr>
<tr>
<td>Jane</td>
<td>Smith</td>
<td>Controller</td>
<td>5923</td>
<td>Admin</td>
<td>5923</td>
</tr>
<tr>
<td>Tom</td>
<td>Jones</td>
<td>Maintenance</td>
<td>7894</td>
<td>User</td>
<td>7894</td>
</tr>
</tbody>
</table>

Fig. 4 User Import Format

NOTE: Column headers (row 1) are for reference only, and must be deleted prior to import.

d. In the upper right of the Users screen (fig. 5), select Import.
   e. Browse to the user file you have created, select the file and click the Import button.
   f. If the file is created and formatted correctly, you will see all of the users in the user screen.

User Change Log (Manage Users > User ChangeLog)

This date searchable database displays information regarding changes to the User database. The information displayed includes the type of change, the date of the change, and the name of the user making the change.
**Manage Assets** – Edit Assets, Assets with Attributes, Audit Assets, Asset Change Log

---

**Loading Fob Reader Drivers**

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

When the **Asset** menu is selected after logging into the **Management Console** for the first time, look for a pop-up on the screen requesting an **Active X** control be installed. Depending on the operating system, browser, network restrictions, etc., the **Active X** prompt may not appear. If it does, install the control.

Also, you may see a pop-up referring to **intranet** settings not being configured. Select the option to turn intranet settings on.

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

![Identify Asset](image)

**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 experience difficulty, contact KEYper® Support.

---

**Importing Assets** *(Manage Assets > Edit Assets > Import {DMS Style})*

A manual import of assets may be accomplished in one of two ways. There is the version for automotive applications, and then there is the version for everyone else. 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’s fine. What’s important is that there are (8) columns.

![Vehicle Import Format](image)

**Figure 8: Vehicle Import Format**

**NOTE:** Column headers (row 1) are for reference only and may be deleted prior to import.

Save the file as a CSV document.
From Manage Assets > Edit Assets select Import (DMS Style). Browse to the saved CSV 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 (7) columns and the asset name column is populated.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Asset Name</td>
<td>Attribute 1</td>
<td>Attribute 2</td>
<td>Attribute 3</td>
<td>Attribute 4</td>
<td>Attribute 5</td>
</tr>
<tr>
<td>2</td>
<td>1071</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2071</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3071</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 9: 6 Attributes Import Format

Save the file as a CSV document.

From Manage Assets > Edit Assets select Import (6 Attributes). Browse to the saved CSV and Import.

---

**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)

---

**Figure 10: Asset List Main Page**

1. **Adding Assets from a Blank Record** (fig. 11)
   a. Click the Add option in the upper right area of the Asset List page.
   b. Fill in the Asset Information (** Indicates Required Field).
      i. **Name** – (eg. Stock Number, Unit Number, etc.)
      ii. **Description** – (for automotive applications, the model is suggested here)
      iii. **Fob Number** – (hold fob on the Fob Reader and select Read Fob)
      iv. **Status** – not editable
      v. **Registered Type** – *always* select Registered
c. Fill in **Asset Attributes**, if desired.
   i. Select a value from the dropdown menus.
   ii. If your desired value is not in the dropdown menu, select the **Enter** option to allow manual entry of a value.

d. Select the **Access Group(s)** to which the asset will be assigned.
e. Click **Save**.

**Note:** If label printing is enabled, select **Print Asset Label**. Click **Save**. Click **Open** to be directed to the label in PDF format from where it may be printed.

2. **Adding Imported Assets**
   a. Utilizing the **Filter** feature on the main **Asset List** page (fig.10), find the unregistered **Asset**. Click the **Edit** option.
   b. Verify imported information is correct (fig. 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.

   **NOTE:** For automotive sales applications, we recommend the **Model** of the vehicle be entered into **Description** field.

c. Assign a fob to the asset (place the fob on the reader and select **Read Fob** to assign the fob to the asset).

d. Ensure **Registered Type** is set to **Registered**.

e. Select the **Access Group(s)** to which the asset will be assigned.

f. If label printing is a feature in use at your site, select **Print Asset Label**. Upon clicking **Save** you will be directed to a label in PDF format and given the option to print the label.

g. Click **Save**.
3. **Adding Unregistered Assets** – 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.
   a. Log into the key system kiosk (must be an administrator). Tap **Unregistered Assets** button. A list of all unregistered assets (unused or empty fobs) is displayed. Select as many displayed entries as needed and check out.
   b. From the **Management Console**, go to **Manage Assets**, place unregistered fob on reader and click **Identify Asset**. The page depicted in figure 13 will be brought up. Select **Edit**.
   c. Fill in the **Asset Information** (** Indicates RequiredField)**
      i. **Name** – (eg. Stock Number, Unit Number, etc.)
      ii. **Description** – (for automotive applications, the model is suggested here)
      iii. **Fob Number** – (hold fob on the **Fob Reader** and select **Read Fob**)
      iv. **Status** – not editable
      v. **Registered Type** – **always** select **Registered**
   d. Fill in **Asset Attributes**, if desired.
      i. Select a value from the dropdown menus.
ii. If your desired value is not in the dropdown menu, select the **Enter** option to allow manual entry of a value.

e. Select/Deselect the **Access Group(s)** to which the asset will be assigned.

f. If label printing is a feature in use at your site, select **Print Asset Label**. Upon clicking **Save** you will be directed to a label in PDF format and given the option to print the label.

g. Click **Save**.

![Figure 14: Add Unregistered Asset](image)

**Note:** If label printing is a feature in use at your site, select **Print Asset Label**, then **Save**. Click **Open** to be directed the label in PDF format from where it may be printed.

---

### Deleting Assets *(Manage Assets > Edit Assets)*

The procedure for deleting of assets is the same for all industries utilizing a **KEYper® Asset Management System**. 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. The fob should be placed 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.

Place the fob on the fob reader, click **Identify Asset**, then **Delete**. Alternatively, you may filter or scroll through the **Asset List** page, locate the asset, 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 > Asset 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, Audit**

There is a factory loaded default **Access Group** named, wait for it... **Default Group**.

![Access Group List](image)

**Figure 15: Edit Access Group Screen**

This facilitates rapid system configuration, making the system operational in the shortest period of time. The group may be edited, *(see pg. 9)*, but should not be deleted. Standard settings for the **Default Group** are:

1. 0 (Zero) Asset Issue Limit per user (0 = No Limit)
2. 0 (Zero) Out Duration Limit per Asset (0 = No Limit)
3. 24/7 access to remove and return Assets
4. Access to all Locations, Systems and Cabinets

---

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

a. From the **Access Group** home screen (fig.1), click the **Add** button in the upper right.

b. Fill In the desired **Name** for the access group (Eg. Managers).

c. Fill in the **Description** for the access group (Eg. 3rd Shift Manager Access). **Not a required entry**

d. Set the desired **Issue Limit** for the group. **0 indicates unlimited.**

   i. **Issue limit** – the number of keys each user in the group may have checked out of the system at any given time. (Eg. If the limit is 10, each user in the group may have up to 10 keys checked out at any given time.)

e. Set the desired out duration time limit. **0 indicates unlimited.**

   i. **Out Duration** – Once a key has been checked out past the set time limit, the assets will change from status **Out** to **Overdue**, and an alert will be sent to all recipients on the **Out Duration Exceeded Alert** list. 24 Hours, 59 Minutes is the maximum time that can be set.

f. Click the **Save** button. This will add the group into the system and will allow the final settings to be configured.

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

**User List**
- a. Click the **User List** header to expand.
- b. Select **Edit** to see the list of all users in the system.
- c. Choose **Select All**, or the check box for each user to be assigned to this group.
- d. Click **Select**, then **Close**.

**Asset List**
- a. Click the **Asset List** header to expand.
- b. Select **Edit** to see the list of all assets in the system.
- c. Choose **Select All**, or the check box next to all assets that are to be assigned to this group.
- d. Click **Select**, then **Close**.

**Physical Access List**
- a. Click the **Physical Access List** header to expand.
- b. The **System Map** will be displayed.
- c. Select the check box next to all **Locations**, **Systems** and **Cabinets** that are to be assigned to this group.
- d. Click the **Update** button.

![Figure 16: Access Group Physical Access List](image)

Once you've completed all the above steps, your **Access Group** has been successfully created.


This date searchable database displays information regarding changes to the **Access Groups**. The information displayed includes the type of change (Add, Delete, Update), 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. (eg. Stock #, Make, Model, Unit #, Building #)

All **Asset Attribute** databases are empty by default configuration. They may be populated manually (see below), by **Asset Import** (pg. 6) and “on-the-fly” (pg. 7-c.ii).

**NOTE:** Assigning attributes to assets is required if the **Filter Assets** method of check out at the Kiosk is to be utilized.

There are two types of attributes:

1. **Collections (limit 6)**
   - These are attributes that will be stored in a group. These values may apply to many different assets (eg. Make, Model, Floor, Building).

2. **Single Value Attributes (limit 1)**
   - These attributes are associated only with the record it is assigned to. These would not be assigned to more than one key (eg. VIN numbers, KeyCodes).

**NOTE:** **Attribute Names** can be customized to meet your preferences. This must be done with the assistance of an authorized KEYper® Technician.

**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, add and delete values. (You cannot delete a value once it has been assigned to a record.)

---

**Fig 17: Attributes for Automotive Applications**

Notice in **Attribute Collection**, for automotive applications, that **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** (fig. 19).

**Fig. 18: Attributes for Other Applications**

---

**Figure 19: Edit Attributes**
**Reporting**

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

1. **Asset Transactions Report**
   a. Provides real time reporting on **User/Asset** transactions.
   b. **Asset Transactions** can be filtered to search for desired data.
   c. Filters available for searching:
      i. User
      ii. Asset
      iii. System (Networked Systems)
      iv. Cabinet (Multi-Cabinet Systems)
      v. Date Range

   **NOTE**: Any combination of these filters may be used to filter specific events.

2. **Assets by Status**
   a. Provides the current **Status**, (In, Out, or Overdue) of all assets in the system.
   b. Select **Assets by Status** from the **Reports** menu.
   c. Set any filters to view desired data.
   d. Filters available for searching
      i. Status – In, Out and Overdue
      ii. System
      iii. Cabinet
      iv. Individual Asset Name

3. **Report Builder** – Create customized reports.

4. **View Kiosk Photos** (if system is camera equipped and enabled) – A snapshot is taken with every successful and unsuccessful login. The view provides information about each login and the ability to view and/or print photos.

5. **Web Login Audit Report** – Provides a list of key system **Administrative** login/login attempts for a specific date or specified time period.

**Settings**

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

1. **Alert Settings** *(Settings > Alert Settings)*

   There are 6 different alerts that will trigger an email and/or SMS alert from the KEYper® System. Any **User** that is configured in the system can receive these alerts. Phone number, phone service carrier, and email addresses are configured 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**, then **Close**.
a. **Illegal Asset Removal** – an asset has been removed without following the proper checkout procedure.
b. **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**
c. **Door Open** – a user has opened a door to the system and failed to close it within the allotted time allowed.
d. **Incorrect Fob Location** – an asset has been returned to the wrong position in the system
e. **Nightly Reports** – a report of assets in ‘Out’ status as of the time the alert is sent
f. **System Maintenance** – used by KEYper® tech support

2. **Email Settings (Settings > Email Settings)**
   a. Email settings are configured to allow alerts to be sent out from the KEYper® System via email.
   b. The KEYper® System does not receive emails, it only sends.
   c. The KEYper® System comes with a default SMTP server, user name and password that can be used in most instances. Certain network security protocols will not allow the default settings to forward emails, and in this case the end user must provide SMTP Server and Authentication information.
   d. 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 is received.
   e. If the test message is not received you will need to contact your IT to have the default SMTP settings changed. Contact KEYper® Support if assistance is required.

3. **Issue Reasons (Settings > Issue Reasons)**
   a. To enable **Issue Reasons** for any system, click the desired **System** (i.e. KEYPER-SYSTEMS), check the **Enable Issue Reasons** box and select **IRL** from the dropdown menu.

![Figure 20: Enabling Issue Reasons](image)

**NOTE**: System Structure and System Settings may only be accessed by KEYper® Support
Support

Under the Support menu you will find the following links:

1. Email Support – send support questions directly to KEYper® Support
2. How To Videos – link to tutorials on the KEYper® website
3. Remote Support – opens a web page that will allow KEYper® Support to connect to your PC
4. System Manual – link the system user guide
5. Shop at KEYper® Systems – a direct link to the online KEYper® store where supplies and accessories may be purchased
6. Zebra Printer Drivers – provides label printer drivers for installation
 Elite Series Kiosk Operation Guide
This Guide explains Kiosk features and operation for system Administrators (Admins) and Users.

**NOTE:** The word “Admin” is short for Administrator. In this manual Admin refers to the person or persons at your company that have been assigned to manage the KEYper® Systems Asset Management System.

**Contents**

- **Administrator Login** .................................................................................................................................................................................. 2
- **Device Enrollment** .................................................................................................................................................................................... 3
- **Proximity (Prox) Card or Magnetic Strip Card Enrollment** .................................................................................................................. 3
- **Fingerprint Enrollment** ............................................................................................................................................................................... 4
- **Unregistered Assets** .................................................................................................................................................................................. 5
- **User Login** ................................................................................................................................................................................................. 6
- **Check In** ........................................................................................................................................................................................................ 6
- **Identify Asset** ..................................................................................................................................................................................................... 7
- **Check Out** ........................................................................................................................................................................................................ 7
WARNING: It is very important to clean the lens of the fingerprint device frequently using transparent tape ONLY (i.e. Scotch tape). Press on and peel off to remove oils, dirt, etc. Repeat as necessary.

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

![KS icon](image)

**Administrator Login**

The methods for logging into the Kiosk are via **Pin Code, Proximity (Prox) Card, Magnetic Strip Card** or **Fingerprint**. Depending on how your system is factory configured, as the Admin, you will enroll User’s with appropriate access type(s). See **Device Enrollment** on page 3.

As Administrator, after logging in, the screen will display 2 rows of buttons as shown in figure 1.

**NOTE:** Users only see the top row.

![Figure 1](image)

**Check In, Identify Asset, Check Out**

The top row of buttons (Check In, Identify Asset, and Check Out) behave the same for both Admins and Users.

**Device Enrollment, Unregistered Assets, Diagnostics, Exit Application**

This row of buttons is available to Admins only.
Device Enrollment - Configuring Access for Users (Admins only)

Prox ID or Swipe ID Card Access (Login > Device Enrollment)

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 page 6 of the Management Console section.

2. Use the Device Enrollment feature of the Kiosk.

Log into the Kiosk as an Admin. Press Device Enrollment. As shown in figure 2, select a user from the list or use the Search button to locate the user. Press the Prox button.

![Device Enrollment Interface](image)

When the Prox Scan screen appears, 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 will be used for login.
**Fingerprint Enrollment**

To register user’s fingerprint, select a user on the Device Enrollment screen and press the Fingerprint button.

When touched, the fingerprint reader light will briefly turn red. To achieve consistent printing, press the pad of any finger on the reader lens, covering as much of the lens as possible. Press flatly and firmly for about one second. Four (4) good scans of the same finger are required for successful enrollment. Press the Continue button to save the scan (fig. 4). Select the next User and repeat the process.
**Unregistered Assets (Admins only)**

An **Unregistered Asset** is defined as 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** in your **Management Console** indicates there are **Unregistered Assets** in your system, log into the Kiosk, select the **Unregistered Assets** button, highlight the entries and **Check Out**.

Follow the same procedure if you are storing unused fobs in the system, and retrieve them as needed to add new assets to the system.

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

![Keyper Default](image)

**Diagnostics (Admins only)**

You will not really need to be in this area unless you are on the phone with KEYper® Support.

**Exit Application (Admins only)**

To end the program, touch the Exit Application button. Then either restart the computer, or restart the program by clicking the ![icon](image) icon on the desktop.
**User Login**

**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 your numbers by pressing “C” for Clear.

**Proximity (Prox) or Magnetic Strip Card Access**
Swipe your card over the card reader and you will be logged in.

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

**Fingerprint Access**
Simply touch your finger to the fingerprint reader and you will be logged in. 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 log in. If your company has more than one kiosk system, you may have to register at each one.

**Unable to Log In**
Common reasons are:
- Incorrect PIN entered
- Fingerprint lens is dirty/clouded (contact KEYper® Support)
- Log in at the current time of day or day of week is not allowed
- Account disabled by admin

**Check In**

**Single Cabinet Check In**
To return a key to the cabinet, log in and press **Check In** and the door will unlock. Open the door and insert the key fob into any lighted holder. Close the door. You will be logged out when you close the door.

**Multi-Cabinet Check In**
Log in and press **Check In**. Choose one or more cabinets from the **Cabinet Selection Screen**. The wait screen will appear and the door on the first cabinet will unlock. Open the door and insert the key fob into any lit fob holder. Close the door. If additional cabinets were selected, the next cabinet will unlock, and so forth. You will be logged out when you close the last door.

![Figure 6: Multi-cabinet Check In](image-url)
**Identify Asset**

To get information on a fob in your possession, log into the kiosk and press the *Identify Asset* button the main screen. Once on the *Identify Asset* screen, hold the fob against the fob reader on the kiosk, and press the *Read* button. The screen will display information about that fob.

![Figure 7: Identify Asset](image)

**Check Out**

To check out an asset, log into the kiosk, or if already logged in, press the *Main* button. Press the *Check Out* button. You will have 4 options for checking out an asset: *By Name*, *By List*, by VIN or by *Filter Assets*.

![Figure 8: Check Out Screen](image)

**NOTE:** Regardless of the Check-out method used, if *Issue Reasons* has been activated on the system you will be required to choose an issue reason for each asset being checked out of the system. The *Issue Reason* screen will appear when an asset has been selected, then highlighted, for check out.
Check Out by Name (figures 9-10)

NOTE: For automotive applications, NAME usually equals Stock Number.

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

Press Check Out by Name, enter the complete Asset Name and press the Continue button.

If the name is found, it is shown in the list (fig. 10). You can press the Check Out button now or press Add to return to the keyboard screen and add additional assets to your list. If the asset is not found, a message will appear at the top of the screen indicating this fact.

If the asset has been checked out by another user, the message will identify the user.

Fig. 9

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.

Fig. 10

Be sure to select the assets you want to check out. Assets that are selected will have a blue background. Assets with a white background are not selected. 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.

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 log you out.
Check Out by List (figure 11)

Pressing Check Out by List will display a list of all assets currently in the cabinet(s) that you are allowed to access, which is based on your Access Group restrictions. Press each record (row) you wish to checkout. The asset name will always be shown first, to the left side of the list. If the administrator has added more information for an asset, it will be shown. Examples are Year, Make, Model, Exterior Color, Interior Color, Type, and VIN.

Press Select All and all records will be selected, even if there are many pages. Likewise, Deselect All will deselect every record that was selected.

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 is shown 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.
Check Out – Filter Assets (figures 12-13)

Filter Assets is used 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. Partial attribute values may be entered (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.

Filtering Example: Enter “2012” and press the Year attribute button. The Year field is now set to 2012, and the number of Assets in the cabinet with a matching attribute is displayed.

Enter “Red” and press the Ext. Color attribute button. The number of Assets meeting both Year & Ext. Color filter criteria is displayed. Continue to filter as desired.

Press Review to see a list of Assets meeting the search criteria. You may either Check Out or start over.

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 2 or more cabinets are attached to the Kiosk, 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 will not unlock until the first cabinet has been opened and closed. The 3rd will not unlock until the 2nd has been opened and closed, and so on.

Log Out

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