Intelligent Key Cabinet (IKC) iFOB Configuration

System Manual & Installation Guide

medeco
ASSA ABLOY

Experience a safer
and more open world

Table of Contents

First Time User Recommendations

medeco
ASSA ABLOY

Experience a safer and more open world

For the best user experience possible, we strongly suggest scheduling a training session with Medeco Tech Services before proceeding.

To schedule a session call 800-839-3157 (option 2) to speak with one of our specialists.

Checklist

Before we begin, please make sure you have the following:

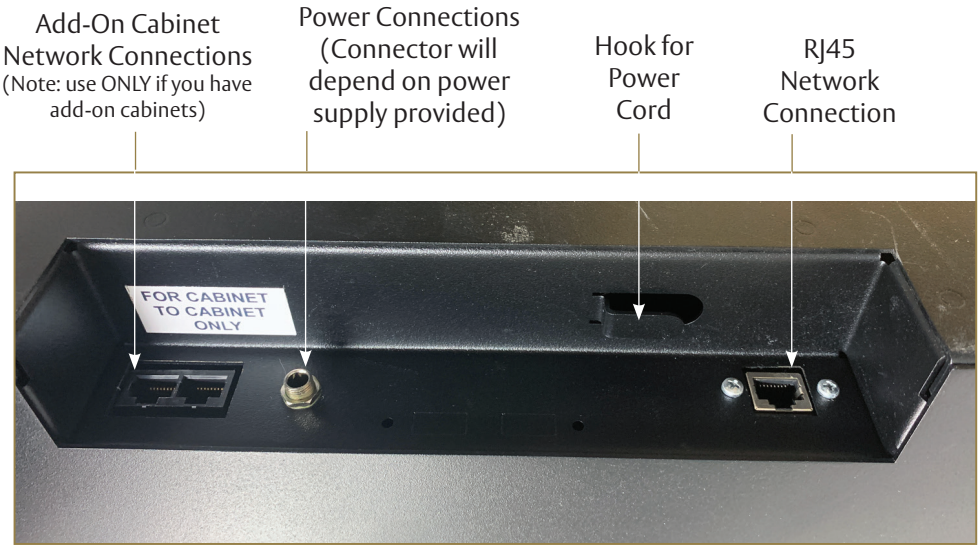
- ❑ **Cabinet w/power supply** – arrived in good condition with no damage. Report any damage or missing parts immediately to Medeco Customer Care at 800-548-8472
- ❑ **Stand (optional)** – if cabinet is ordered with a stand, the unit should arrive already mounted to the stand.
- ❑ **Medeco High Security override cylinder with mechanical keys (2), Mechanical key card, and key port alignment tool** (shown on next page) –The keys are used as a mechanical bypass to open the cabinet door if power is lost. These keys are part of the Medeco key control carded program. You must present this card to an authorized Medeco dealer in order to get new keys made. **Please keep these in a safe location**.
  - We include a small alignment tool for the charging ports. In rare instances a port can be set out of alignment. As a result a key cannot be returned until it is re-aligned. This tools resolves the issue quickly.
- ❑ **Emergency Key removal tool** (shown on next page) – If cabinet power is lost, this device can be used to power individual ports to remove a key/keys. This tool should be stored in a safe location.
- ❑ **Connection** - It's recommended that you have a hardwired LAN network connection. However, the iFOB unit also supports WiFi.
- ❑ **IKC Elite Software** - Use of the IKC Elite web-based software will require a PC/laptop with internet/intranet access (depending on hosting method.

Backup Power supply – if you require a battery backup you can purchase one of the following from your authorized reseller, or electronic reseller/supply store:

- **APC BE425M**
- **APC BE650G1**

Checklist

Mechanical keys and Key removal tool, port alignment tool

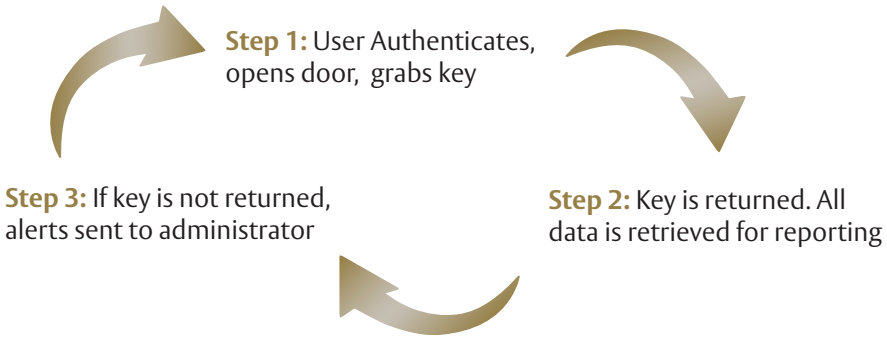


Emergency Key Removal Tool
(4 AA batteries included)

Overview

Thank you for your purchase & we hope you enjoy your new Medeco IKC Solution. You have taken an important step in securing access to keys and other assets that help run your facility as well as increasing accountability of all users.

Just as a reminder, the Medeco Intelligent Key Cabinet (IKC) is a key management system ideal for keys that require a high level of security and accountability. A complete storage and control solution, the IKC is an electronically controlled steel cabinet that restricts access to keys, and can only be opened by authorized personnel using PIN, Biometric Fingerprint, or Prox Card authentication (optional). The IKC electronically keeps a record of key removals and returns - by whom and when. Exclusive iFob technology allows storage of all types of keys.



Quick Start

Select the area for installation of your Main Cabinet (vs Add-on cabinet)

The Main Cabinet contains the touchscreen and other authentication devices necessary to access your keys. The Add-on cabinets need to be installed in an area near the Main unit.

- ❑ Mount Cabinet:
  - If your unit was not ordered on a stand, identify the optimum wall location for mounting. If necessary, please reference the Hardware Installation section in this guide.
- ❑ Power Cabinet:
  - Using the included power supply connect one end to the cabinet (barrel connector) and the other to a wall outlet that is not currently in use. Once power is applied the IKC should boot up to the Windows 10 desktop.
- ❑ Connect Network:
  - To administer the Elite cabinet application or pull reports, the Cabinet must be connected to your local intranet or Internet depending on your hosting method. (See Connections Page)

IKC Installation Instructions

Safety

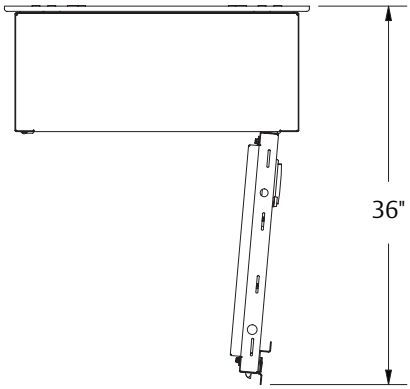
1. Read these instructions thoroughly before attempting to install or operate the equipment.
2. Keep these instructions.
3. Heed ALL Warnings, Notes, and Cautions
4. Do not use equipment near water.
5. Do not block any ventilation openings.
6. To avoid risk of electric shock, do not disassemble any part 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 plus 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

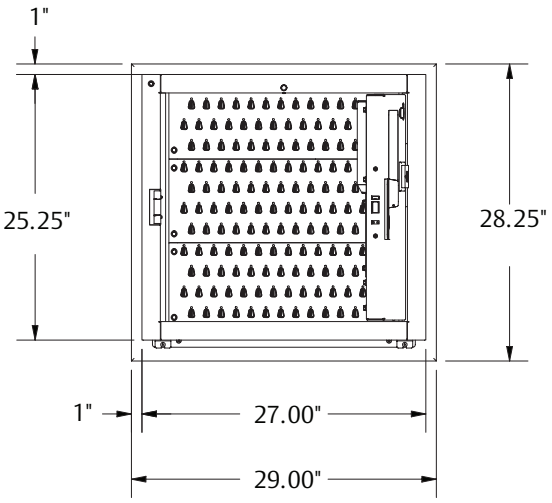
1. If you believe your system requires service, contact Medeco® Support.
2. To clean the biometric lens, place a strip of transparent tape (i.e. Scotch) on the lens and peel off. Repeat as required. NEVER USE ANY TYPE OF CLEANER OR FLUID & NEVER WIPE WITH ANY TYPE OF CLOTH OR PAPER.
3. To clean the cabinet(s):
    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 Medeco® 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.

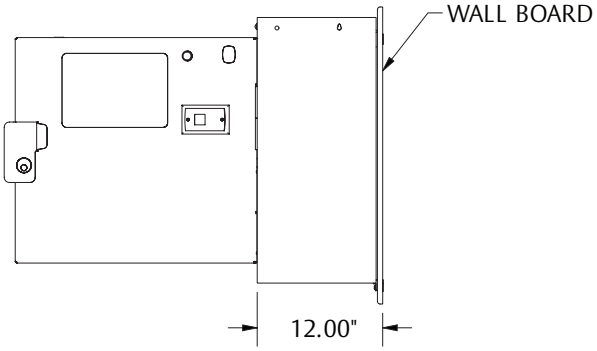
Cabinet Wall Mounting

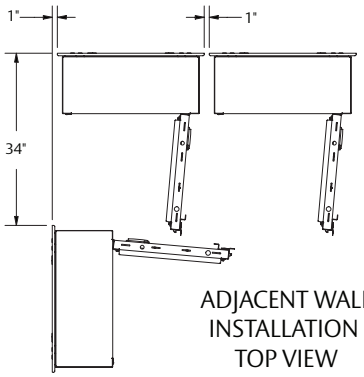
64 Port Standard Size Cabinet



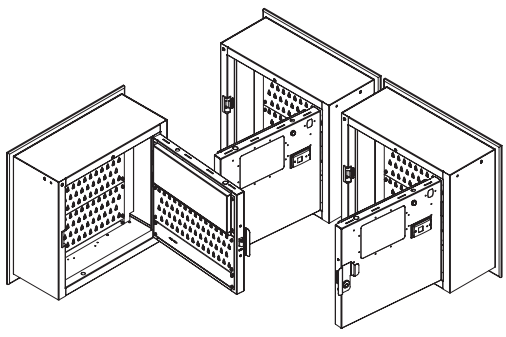
NOTE:
1. For multiple cabinets leave 1" between wall boards. The maximum distance between cabinets is not to exceed 5'.
2. AC mains must be within 48" of the cabinet and preferably on the same wall.
3. Ethernet connections must be within 48" of the main cabinet with controller; if a multiple cabinet system; and perferabily 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. Local ethernet cable is supplied by customer.
5. The mounting height of the cabinet is 67" from the floor to the top of the cabinet.
6. If this cabinet is mounted above a desk or table, allow at least 3" between the desk or table and the bottom of the cabinet.





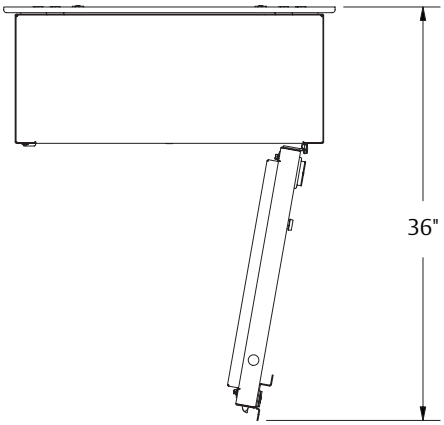


ADJACENT WALL
INSTALLATION
TOP VIEW

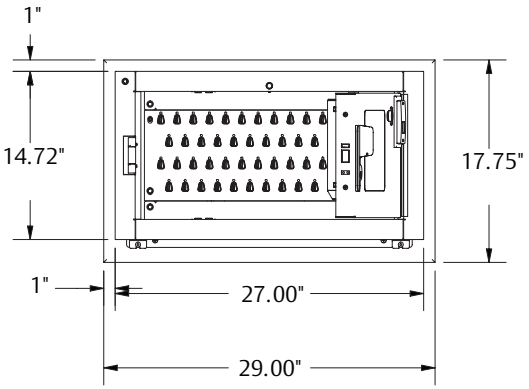


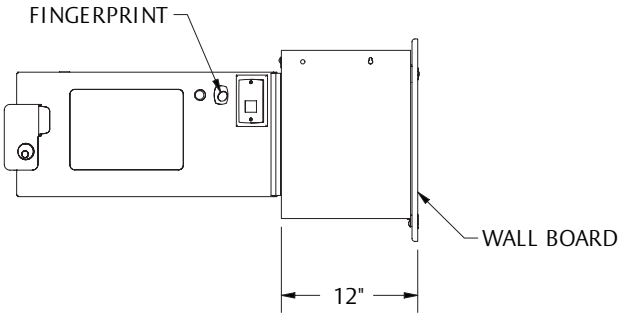
Cabinet Wall Mounting (cont.)

32 Port Mini Cabinet



NOTE:
1. AC mains must be within 48" of the cabinet and preferably on the same wall.
2. Ethernet connection must be within 48" 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. Local ethernet cable is supplied by customer.
4. The mounting height of the cabinet is 67" from the floor to the top of the cabinet.
5. If this cabinet is mounted above a desk or table, allow at least 3" between the desk or table and the bottom of the cabinet.





Installation of Wall Mounted System

CAUTION: A Certified Professional should install Wall mounts. We recommend a wall board, which is sold separate. Cabinets are heavy. NEVER attempt to install or remove a cabinet without proper assistance.

Before mounting, we suggest you check to ensure the location is compliant with Americans Disabilities Act (ADA) regulations.

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 (200lbs for small cabinets).
2. Install so top of mount is 67" from the floor.
3. Minimum of 24" clearance required above wall mount.
4. Minimum of 1" space required between adjacent wall mounts and/or walls.

NOTE: Hardware securing the upper area of the mount to wall requires placement between 1" and 5" from top of mount, avoiding the metal, upper, cabinet mount bracket. The 2" mark is preferred (figure 6).

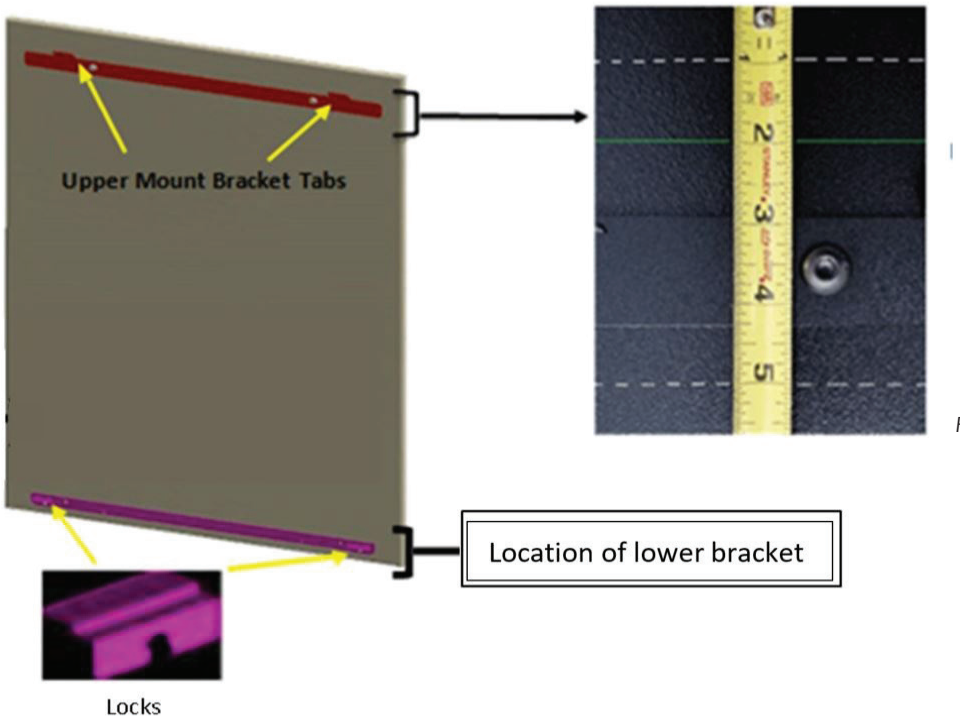


Figure 6

Wall mounts, which are ordered separately, are available with the upper and lower cabinet mounting brackets installed. Two (2) cabinet locks attach to the lower bracket. The tool for the screws straps 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.

Installation of Wall Mounted System (cont.)

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. 7).

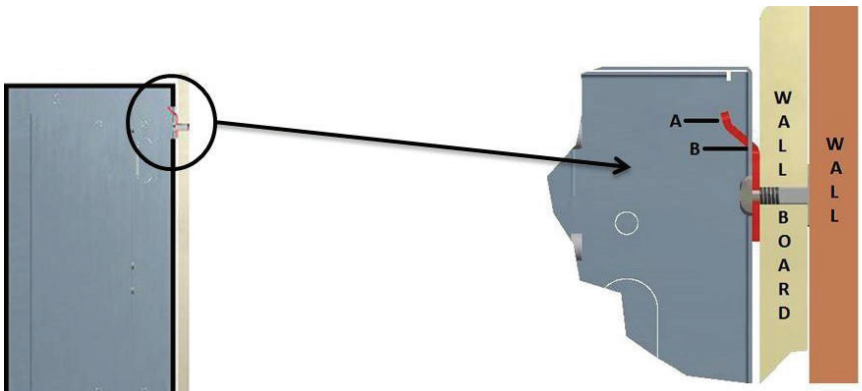


Fig.1
A – Upper Mount Bracket
B – Slot in cabinet back

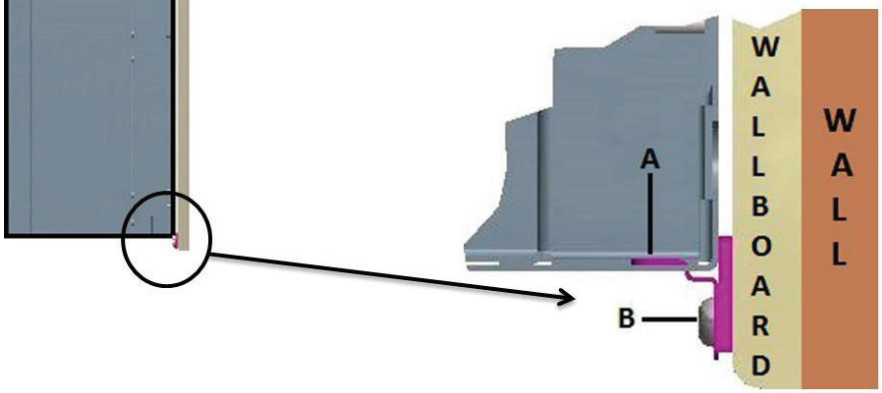


Figure 7

A - Cabinet Lock
B - Button Head Allen Screw

Installation of Optional 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.**

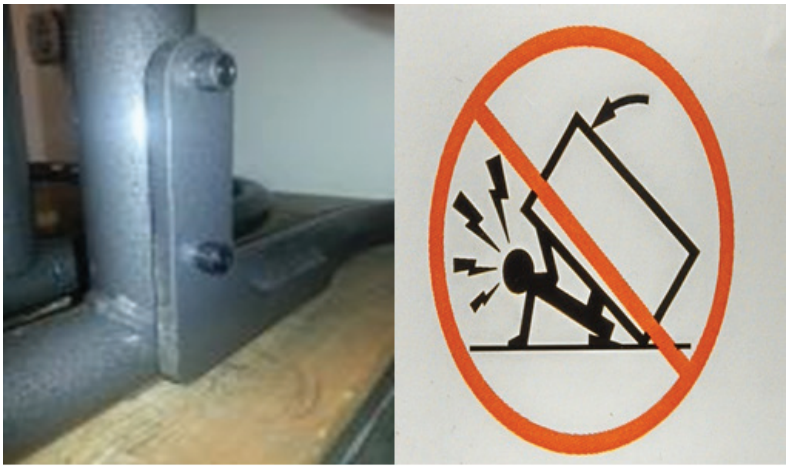


Figure 8: Detachment of rear stand foot

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 9: Wall brackets included in accessories box

Connections

Power-Up & Connect to your network

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

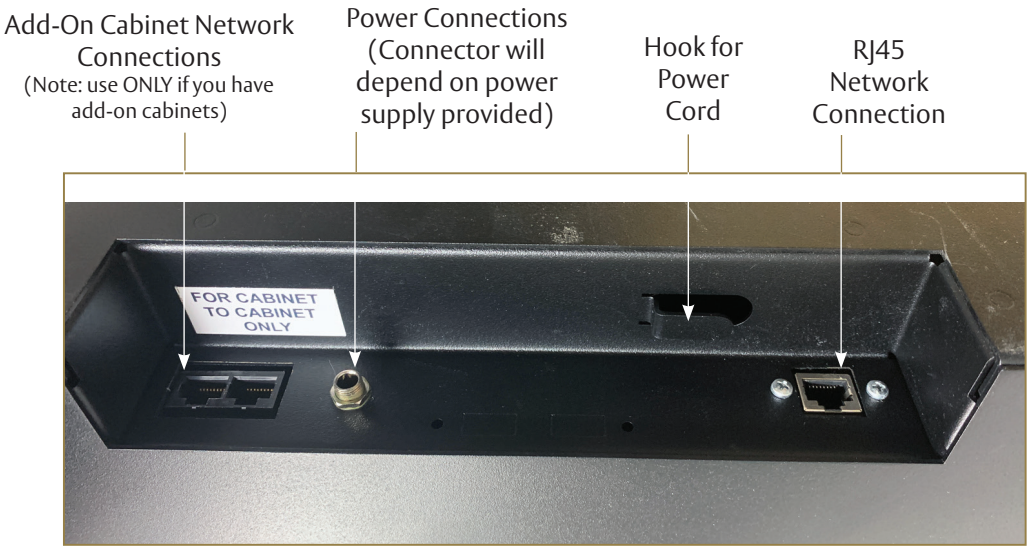


Figure 10: External Connections, Bottom Center of the Rear Panel of the Cabinet

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 10). Medeco recommends your IT department configure the system to have Static IP information prior to setting your IP Address Setting. To configure your system IP Address Setting for accessing the Elite Web Admin application please follow the steps below:
   a) Use PIN 1234 to login to the Kiosk (if 1234 does not work, your XT Web users have already synced to the cabinet database and any 'Admin' level user account PIN may be used)
   b) Click on the gear icon labeled 'Admin' at the bottom left of the screen. Then click on the power button icon at the bottom right of the screen to exit the application
   c) You are now at the Desktop and will have access to configure your IP Address Setting
   d) Navigate to 192.168.10.1 using a web browser on the desktop
   e) Log into the router with the username/password configured specifically for your system (obtainable from Medeco support)
   f) Navigate to System > Status > WAN > WAN IP to see what IP address the router is associated to on your network
   g) Call Medeco support to edit your IP Address Setting on the cabinet to allow the IP address to show on the kiosk login page
   h) Double tap the Elite Kiosk icon on the desktop to restart the Medeco® software.
   i) Contact Medeco Support with questions and for assistance if required.
   j) To connect to the key system from a PC on the same network, please refer to page 2 of the Web Administration Guide.

   Optionally:
   - You may choose to enable WiFi by following steps a-c above to navigate to the desktop where your IT will have access to configure your WiFi connection.
   - You may choose to display the WAN MAC address of the router on the login screen of the kiosk by following steps a-e above and navigating to System > Status > Information > WAN MAC Address then contacting Medeco support to edit your WAN MAC Address Setting on the cabinet.

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.

Connections (cont.)

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 10).

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 Input: 100-240VAC, 50/60Hz, 1.3A; Output: 12V, 6.67A, 90W Max. We recommend that you connect the system to battery backup and/or surge protection devices.

Diagram 1 – Cabinet Connections

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

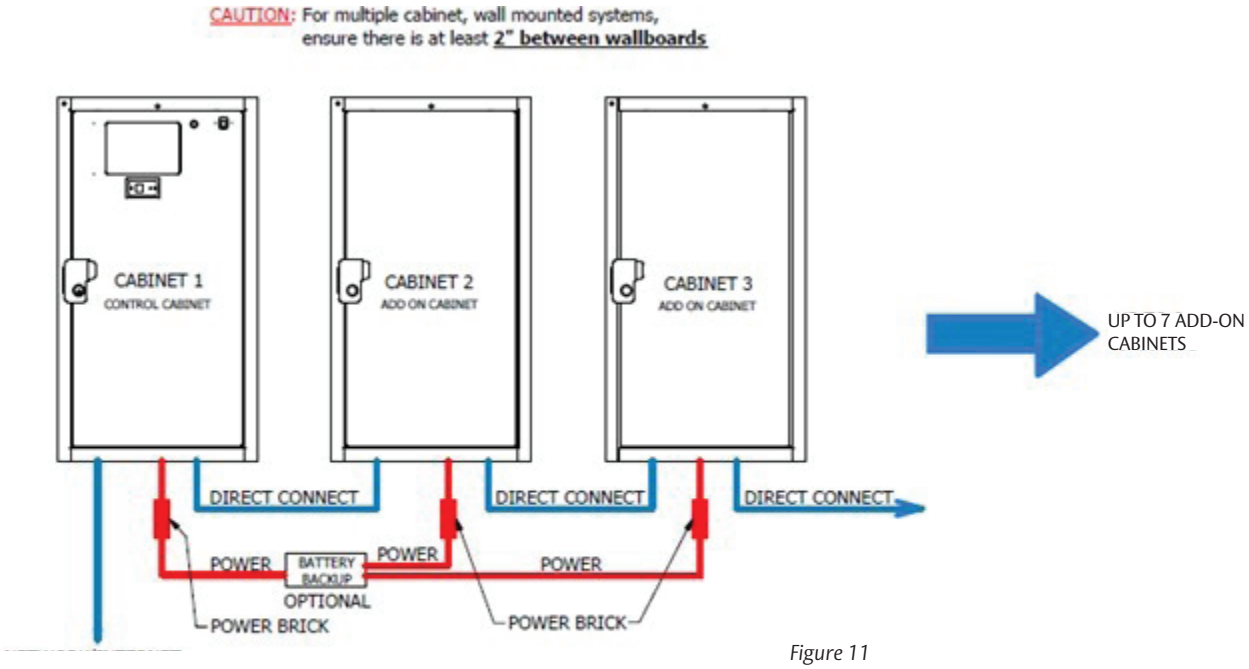


Figure 11

IKC Startup and Login

Login

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

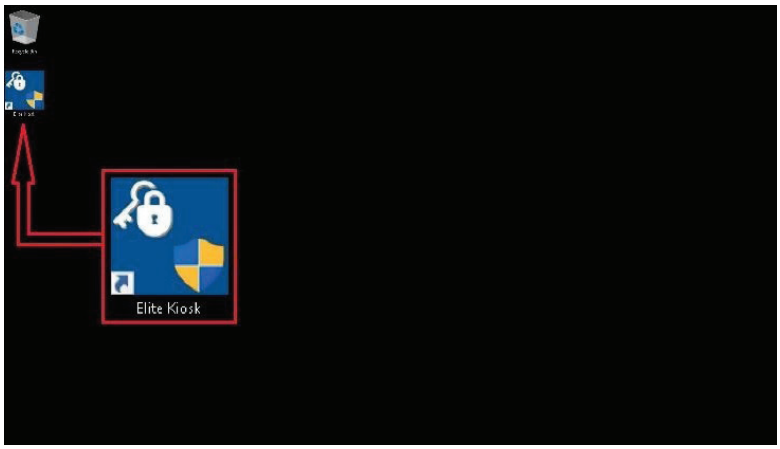


Figure 24: Desktop Icon

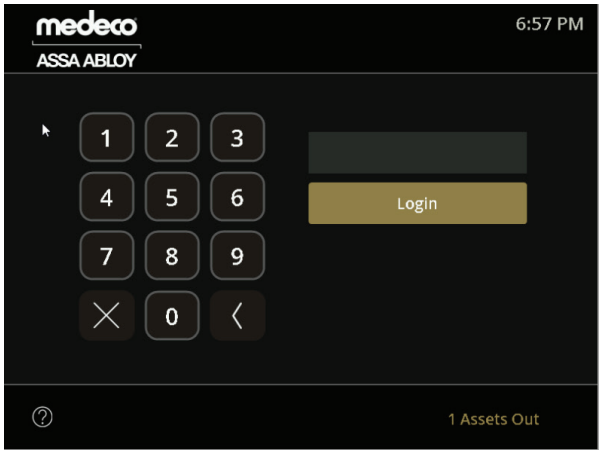


Figure 25: Login Screen

When the system is ready, you will see the login screen (figure 25). In order to view the current system status, click the question mark icon at the bottom left-hand corner. On this screen, you will see if the system can connect to the Primary Web Service (WS) and Primary Database (DB). Both of these must have the status of CONNECTED displayed on the main screen for the system to function properly.

The login screen also displays your WAN MAC address, external IP address, and WiFi adapter IP Address if configured appropriately. Please refer to the installation guide or contact Medeco support if you would like assistance in configuring these options to display.

On the bottom right of the screen (figure 25) 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.

The methods for logging into the kiosk are via Pin Code, Fingerprint, Proximity (Prox) Card, or Magnetic Stripe 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 cabinets that are not networked together, you may have to register at each one.

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

Programming at the Cabinet

After you login, you will be greeted with the options screen. The selections will vary between an Admin and a normal User. We will address this guide for Admins.

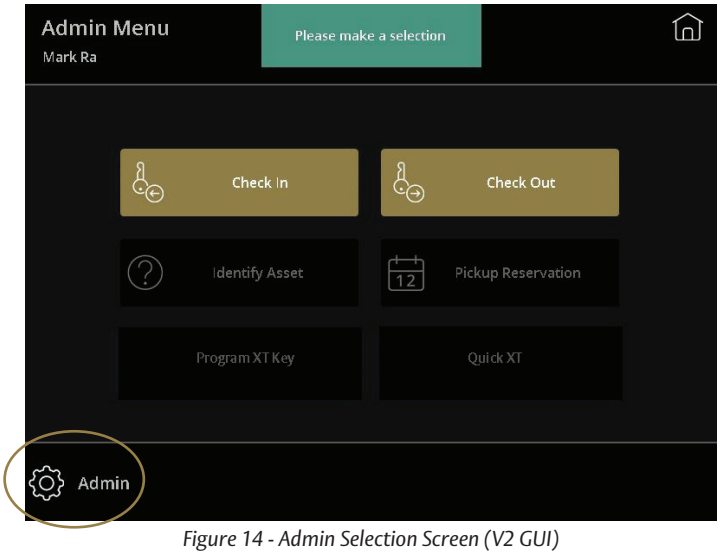


Figure 14 - Admin Selection Screen (V2 GUI)

Check In, Check Out, Program XT Key, and Quick XT

On the main screen Check In and Check Out behave the same for both Admins and Users. See the Local Management section of this Guide for more details.

Device Enrollment (aka Biometric or Prox Card Enrollment)

This is an optional feature and not required for cabinet use. However, since this is a security device, it is always recommended that you use dual-authentication (Biometric and PIN) for users to gain access to the cabinet. If that is not desired then using the fingerprint reader only is recommended. PIN codes can be easily compromised.

These buttons are available to Admins only. If using the V1 GUI the Device Enrollment feature is shown on the Admin Selection screen by default. If using V2 GUI the Admin need to press the gear icon  (bottom left).

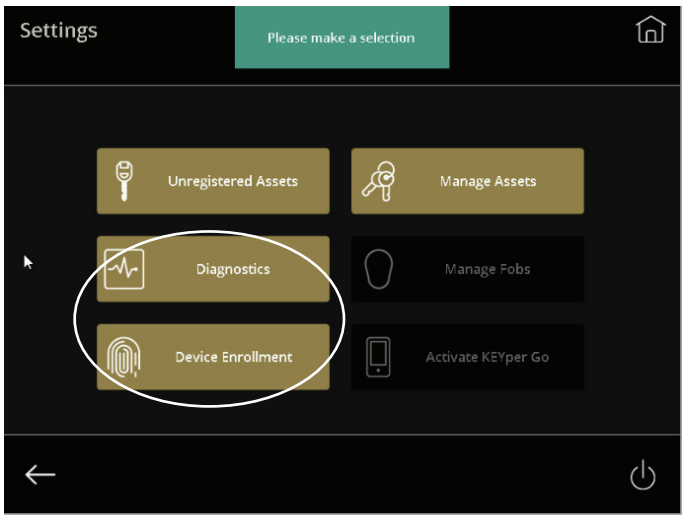


Figure 15

Fingerprint Access

To begin using the fingerprint reader for user access, you need to first register the user's fingerprints. To register user fingerprints, click the Device Enrollment if using the Original GUI or select the gear icon if using the new GUI elect a user on the Device Enrollment screen and press the Fingerprint button.

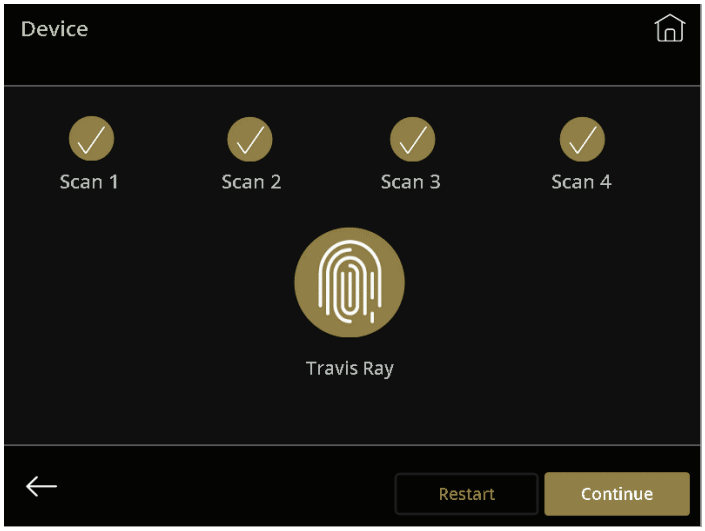


Figure 17 - Process Complete

Prox ID or Swipe ID Card Access

There are two ways to setup a user with a proximity or Magnetic Stripe access card.

1. If known, enter the proximity 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 18). Press the Prox button to bring up the screen shown in figure 19 below.

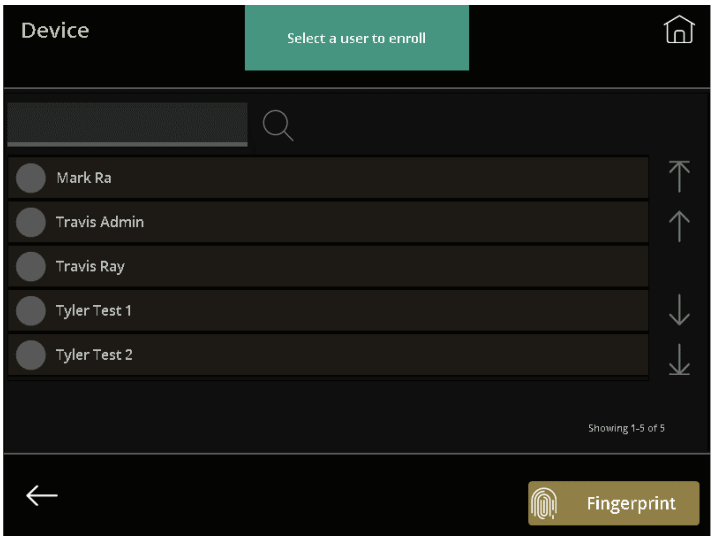


Figure 18

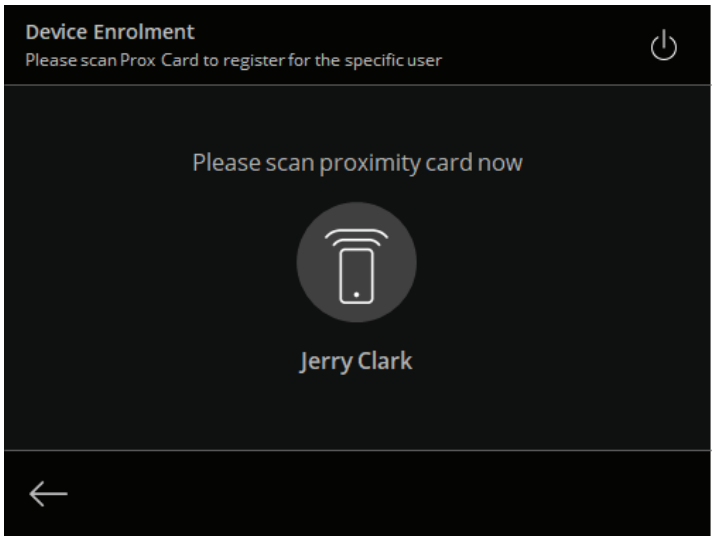


Figure 19

Diagnostics

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

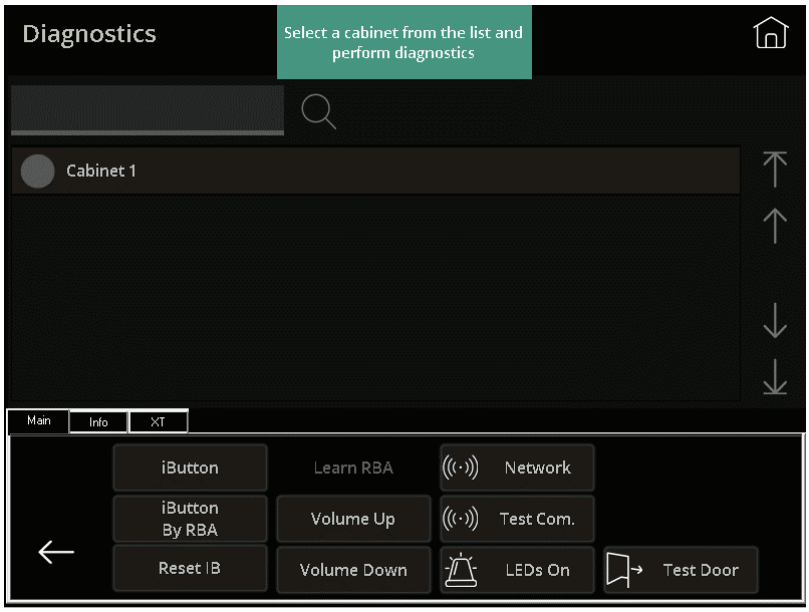


Figure 20

Manage Assets

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

Add New

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

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

Name and Asset Type (Attribute 1) are required. Description and remaining Attribute fields are optional.

See Web Admin Guide for more details.

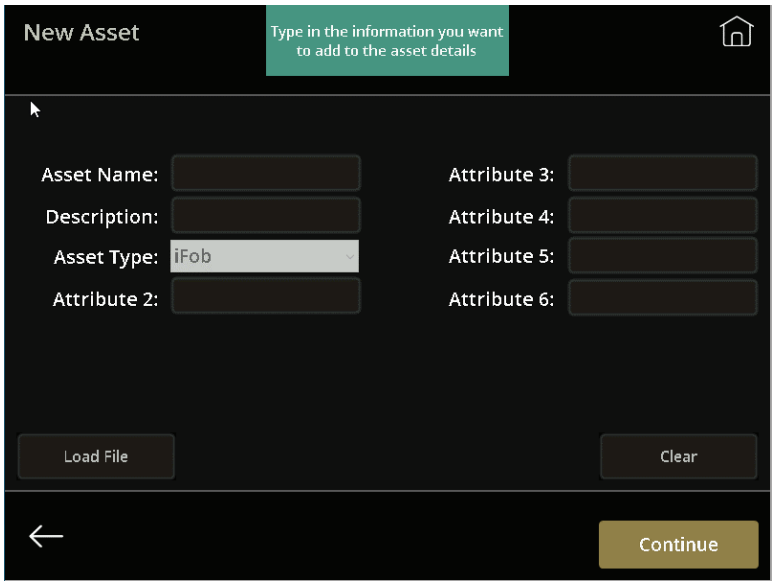


Figure 21

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.

Delete allows an admin user to delete a registered asset from the Kiosk (figure 22).

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.

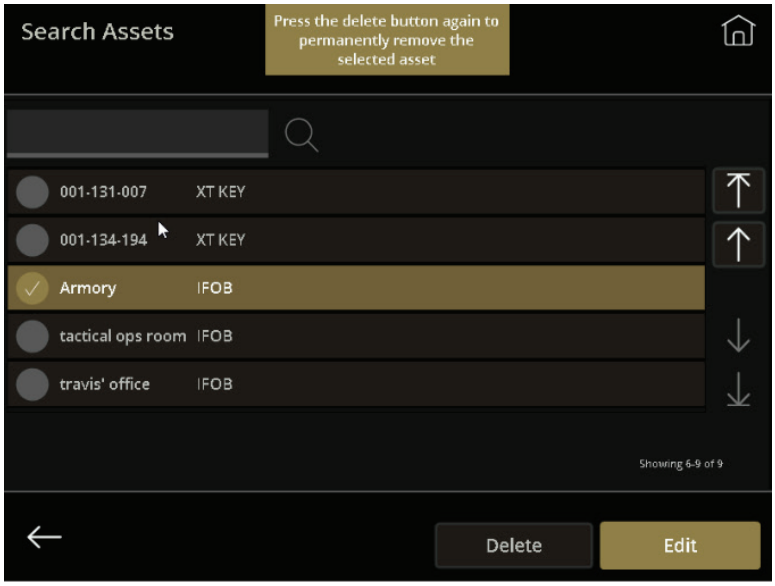


Figure 22

Exit Application

To end the program, touch the Exit Application button at the bottom right hand corner of the main admin screen. Then either restart the computer or restart the program by clicking the icon on the desktop.

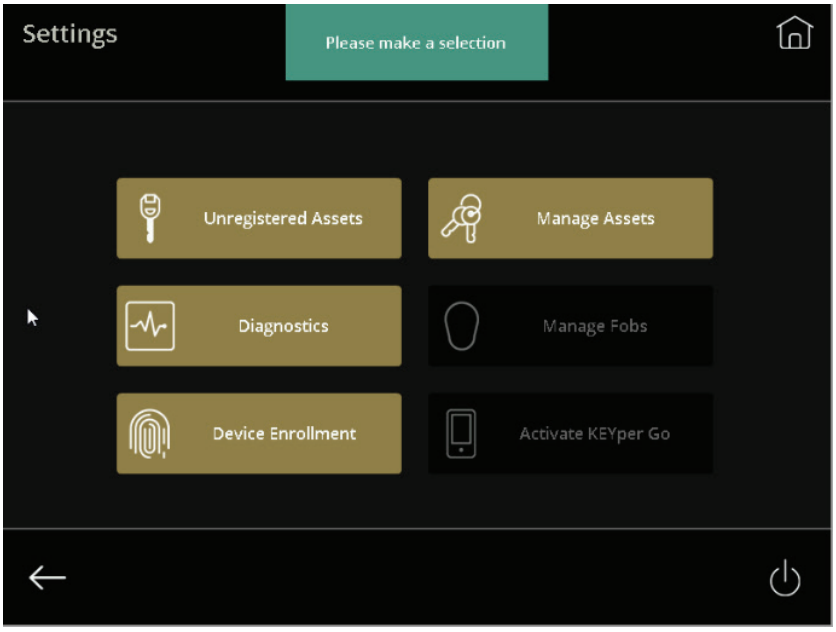


Figure 23: Exit Application Button

Check Out iFob Keys

To remove an keys from the cabinet, login and press Check Out. A screen prompting you to select the key type will display. Click the iFob Key button to continue.

Figure 26

Check Out – Searching

During the checkout process, you have three options for checking out an asset: By Name, By List or by Filter Assets.

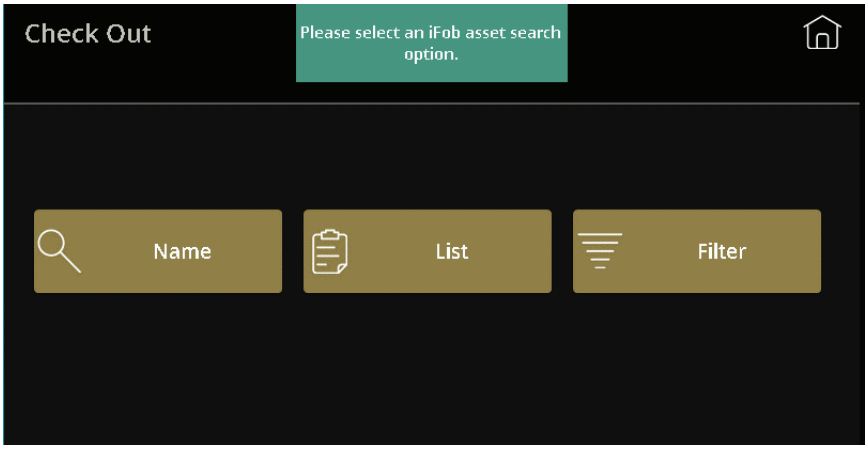


Figure 27: Check Out Screen

NOTE: 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.

Check Out iFob Keys (cont.)

Check Out by Name

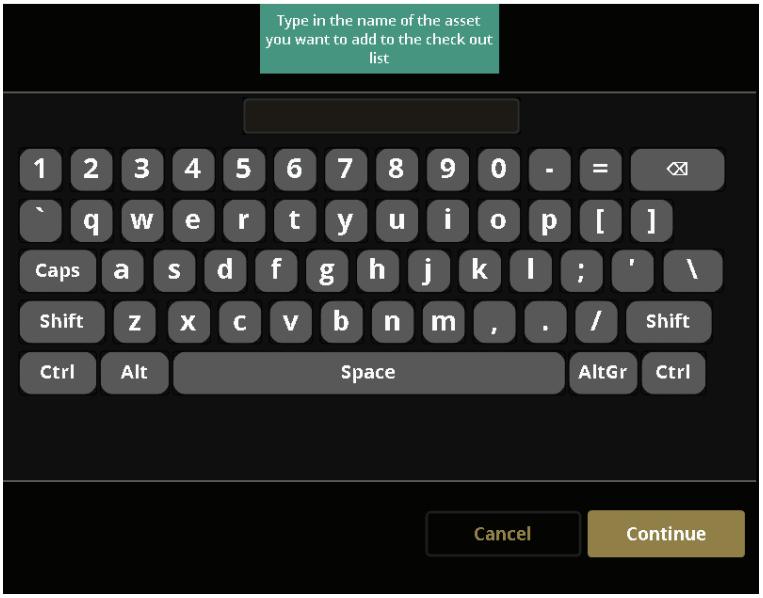
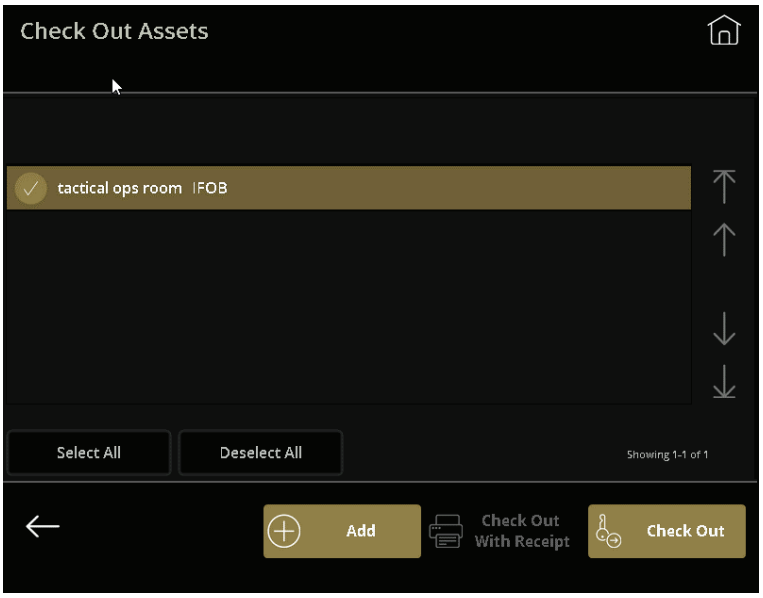


Figure 28: Check out By Name

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 28). 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 are highlighted gold. Unselected assets remain grayed out. 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.

Figure 29: Check out By Name - asset found

Check Out iFob Keys (cont.)

Along the bottom of the screen are four (4) icons: 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.

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 icons 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.

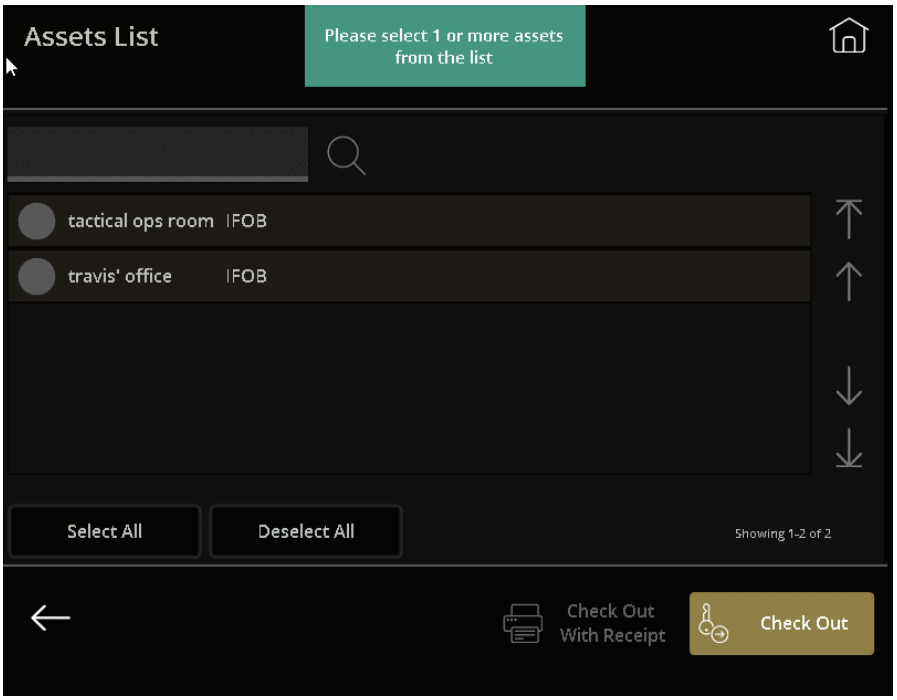


Figure 30

Check Out – Filter Assets

Use Filter Assets to search for assets by attributes.

Check Out iFob Keys (cont.)

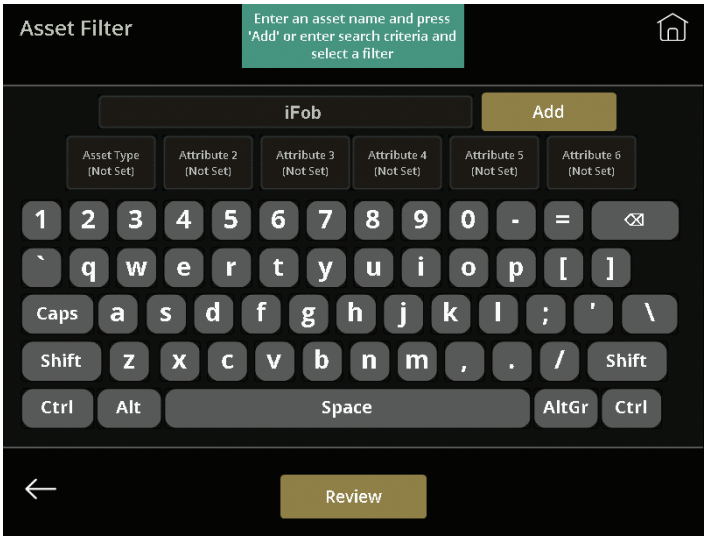


Figure 31: Filter Screen

To search for assets by filtering attributes, enter an attribute value, then press the applicable filter button. For example, enter an asset type ('iFob' or 'XT Key'), then press the 'Asset Type' filter button.

Figure 32: Filter Screen

Now the 'Asset Type' filter button says "iFob" and the green message box indicates the filter narrowed the total to two (2) assets (figure 32).

Check Out iFob Keys (cont.)

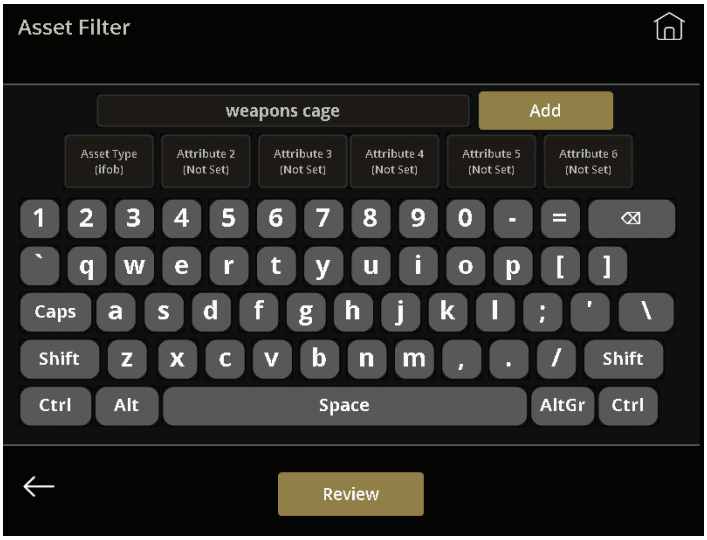


Figure 33: Filter Screen

Continuing the example, the 'Asset Type' is filtered on "iFob" and before the Review button is pressed, the 'Attribute 2' is filtered on "weapons cage" (figure 33).

Figure 34: Filter Screen

Now in figure 34, the green message box indicates the narrowing of the list to one (1) asset.

Check Out iFob Keys (cont.)

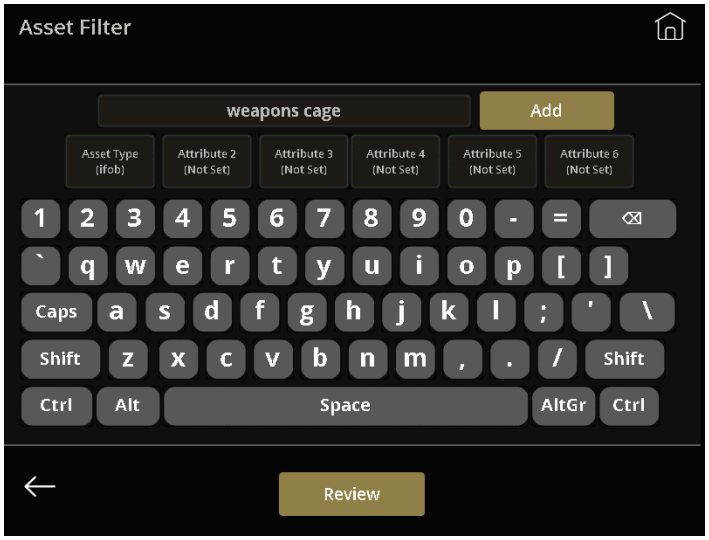


Figure 35: Filter Screen

Pressing Review shows the filtered asset (figure 35).

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.

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.

Check In iFob Key

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 asset into any illuminated socket. Close the door. Logout occurs when you close the door.

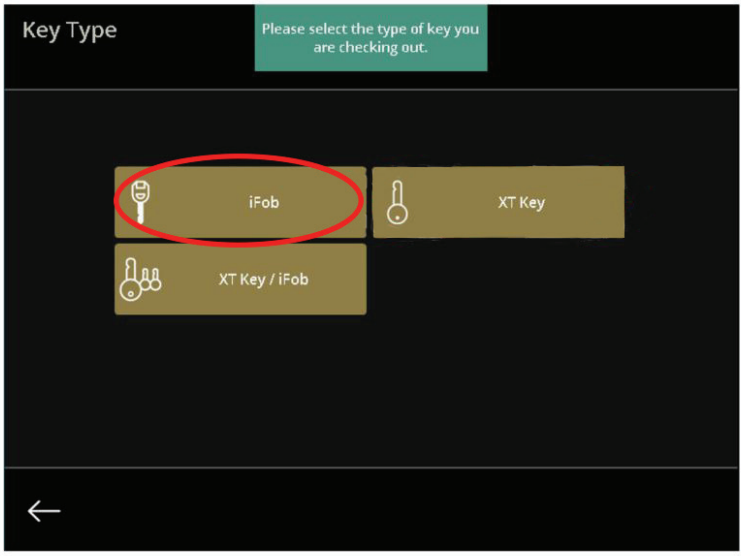


Figure 39

Asset Not Locked In

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).

Check In iFob Key (cont.)

Multi-Cabinet Check In

Login and press check in. Choose one or more cabinets from the Cabinet Selection Screen (figure 40). 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 one at a time. Logout occurs when you close the last cabinet door that was selected or when the open door timeout expires subsequent to a cabinet door unlocking but not being physically opened by the user.

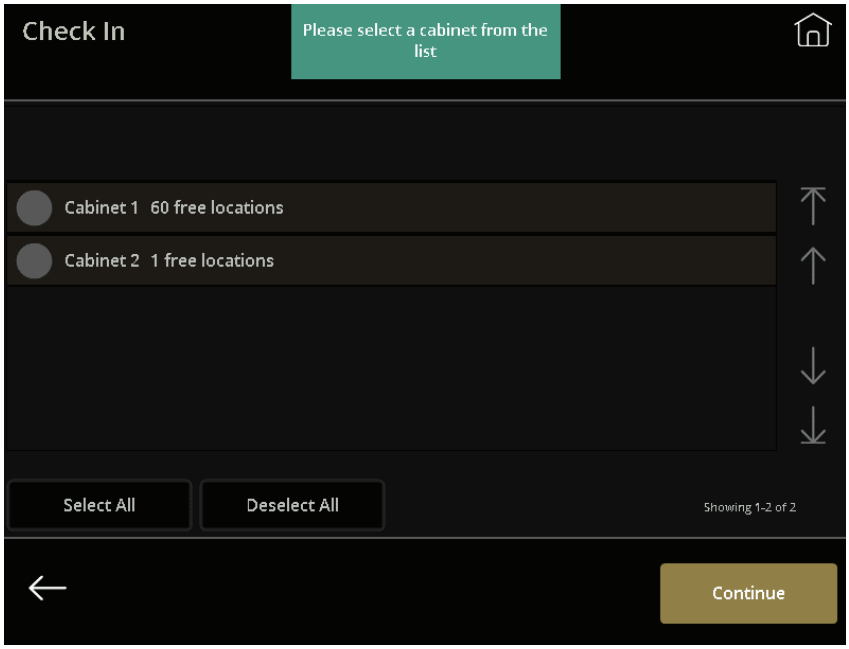


Figure 40

IKC Remote Management

Programming from the Web Application

- If a hardwire connection is available, you may use a Wi-Fi connection to connect to the Remote Management Web Admin app. You must set this up through the Win10 OS that is installed on the cabinet before attempting this connection.
- Once a Wi-Fi connection is established you can open the 'Elite Kiosk' application located on the desktop by double-clicking.
  - To determine the Wi-Fi IP address simply click the ? on the bottom left of the screen. Enter the IP address shown on the screen under "IP Addresses" into your web browser on a PC that is attached to the same network

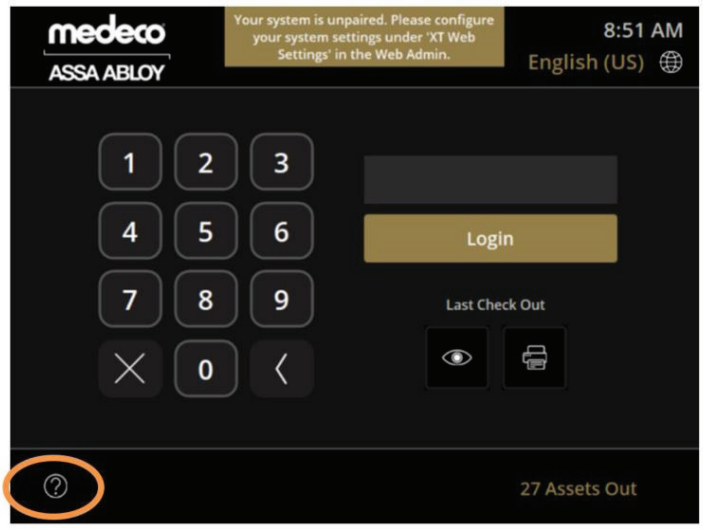


Figure 41

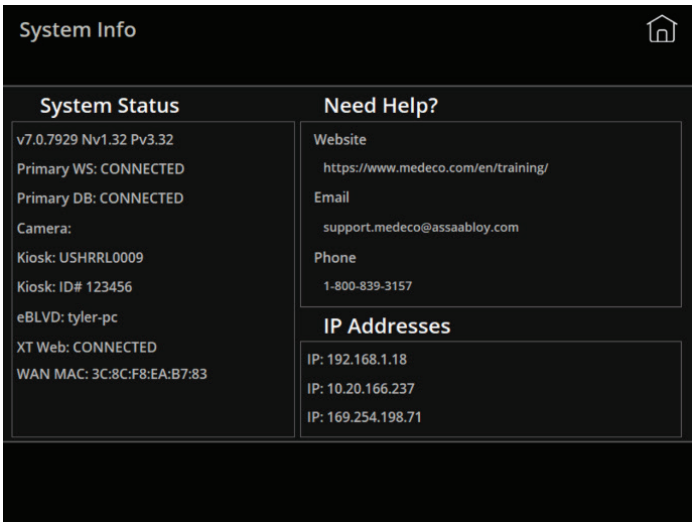


Figure 42

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.

- **Warning:** Once you have created your own Admin profile, the Default Admin User will automatically be deleted and the default PIN of 1234 will no longer work or be assignable.
  - Each unit is shipped with an internal router that contains a password for access.
  - In order to determine the IP address for the Web Admin connection Medeco will need to provide you with this password.

Notes:
The Web Admin GUI (displayed in your Web browser) for remote Management and the cabinet GUI (displayed on the cabinet touchscreen) for Local Management are different. In this section we will cover the Web Admin GUI for Remote Management.

In order to access the Web Admin GUI from your browser we will need to determine the IP address of your cabinet.

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.

Programming from the Web Application

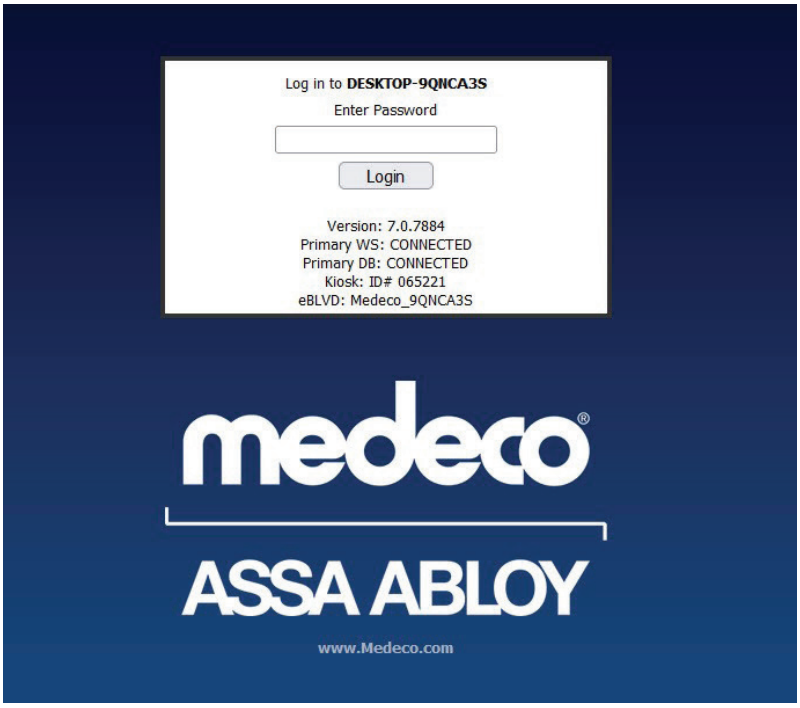


Figure 43

"Log in to" - Shows the name of the system hosting the Web Admin software

Password Box - User will enter their PIN/Password to access the Web Admin here. The default Admin PIN is 1234. Once you have created your own Admin profile, the Default Admin User will automatically be deleted and the default PIN of 1234 will no longer work or be assignable.

Login - Will log in the user using the entered PIN/Password

Version - Current version of the Elite software. We use this to help determine if a software upgrade may be necessary to resolve a particular issue the customer is having.

Primary WS - Determines whether the primary web service is connected. If this shows as anything other than CONNECTED, there may be a network issue or other problem which needs to be resolved.

Primary DB - Determines whether the primary database connection is established. If this shows as anything other than CONNECTED, there may be a network or configuration issue which needs to be addressed.

Kiosk ID - Used by Customer Support to identify the customer's system and aid in resolution of any issues they may be experiencing.

eBLVD - The name of the system on eBLVD which is used by Customer Support to log in the customer's system and troubleshoot any issues.

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 – Assets that are in the database, but do not have details such as name/description assigned to them. Clicking this button provides a current Assets List view, filtered by asset type Unregistered.
- The grid view lists the last 10 transactions.
- The Command Center is shown as an option and is not active by default. Please contact your Medeco representative for additional information.

Figure 44: Dashboard Screen with last 10 transactions displayed

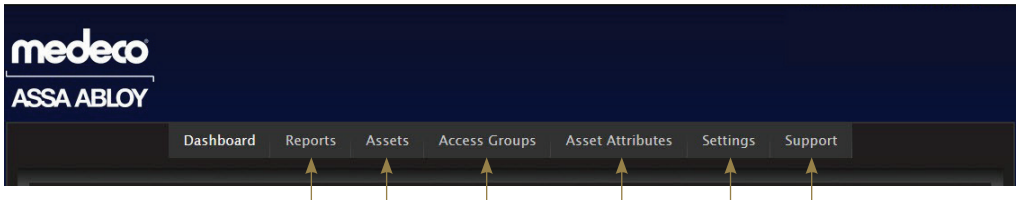


Figure 45

In addition to the stock reports, you are also able to access 'Report Builder' from this drop down, which allows you to create custom reports of your choosing.

12 different reports are available from this drop-down

Used for describing the assets contained in the cabinet.

Access Groups are used to configure when a User can access the cabinet

Asset Attributes allows you to add additional descriptions to the assets in the cabinet.

Settings are used to customize your system. Some more advanced or sensitive settings are password protected.

Several support resources are available.

Manage Users – Edit, User Change Log

Admin vs. User – Know the Difference

ADMINS:	USERS:
Can access the Medeco® Web Admin Site	Cannot access the Medeco® Web Admin Site
Override all Access Group restrictions	Adhere to assigned Access Group restrictions
Have Access to the Admin functions of the kiosk	Can only Check In, Check Out, and Identify assets at the kiosk

It is recommended that after adding 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.

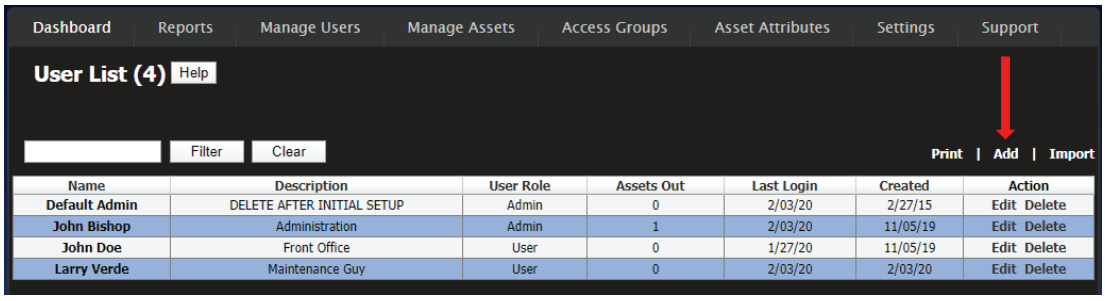


Figure 2: User List

- Fill in the information on the Add New User page (figure 3) ** Indicates Required Field
  - 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)

Manage Users – Edit, User Change Log (cont.)

- Phone Number (For SMS Alerts)
- Carrier (For SMS alerts. If desired carrier is not listed, contact Medeco® Support)
- 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.

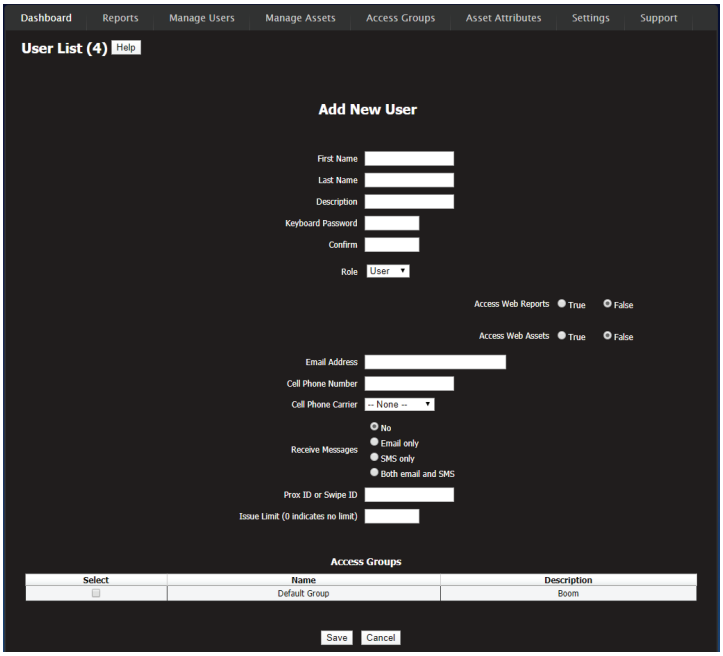


Figure 3: Add New User Page

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.

Manage Users – Edit, User Change Log (cont.)

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: A unique PIN and Prox number must be included for the import. The import will fail if the data is not unique. Unused data can be deleted from the user profile once imported, if desired.*

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
Adam	Smart	Sales	4321	User	4321
Jane	Smith	Controller	5923	Admin	5923
Tom	Jones	Maintenance	7894	User	7894

Figure 4: User Import Format

- In the upper right of the Users screen, select Import (figure 5).
- Browse to the user file you have created, select the file and click the Import button (figure 6).
- If the file format is correct, you will see all of the users in the user grid view.

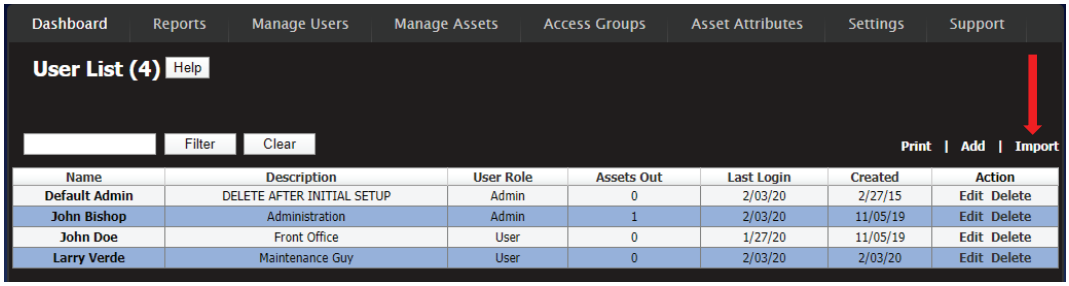


Figure 5: Import User Button

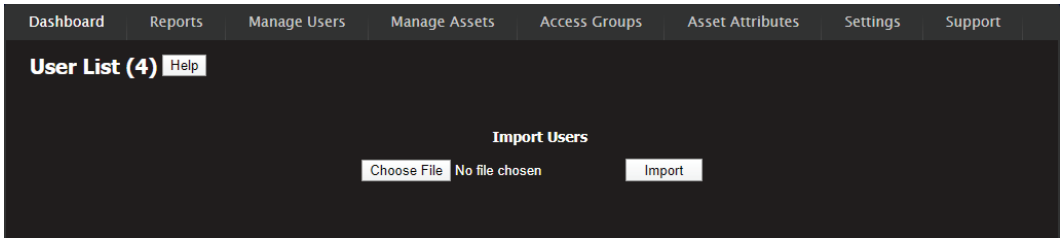


Figure 6: Import User Screen

User Change Log (Manage Users > User Change Log)

This date searchable report 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

Importing Assets

- A manual import of assets is possible.
- This feature is especially useful during initial key system installation, as it facilitates rapid asset registration by populating the Asset Attribute databases.
- From Manage Assets > Edit Assets select Import (6 Attributes). If this option is not available on the main Asset List page, contact Medeco® Support.
- It is very important to make any changes to the Attribute names before adding assets to the system.
  - It is NOT POSSIBLE to change the name of Attribute 1 - 'Asset Type'. Contact Medeco® Support for assistance editing any of the other Attribute Names (Attribute 2, Attribute 3, Attribute 4, Attribute 5, Attribute 6).
- Figure 7 illustrates the required format for Import (6 Attributes) style of importing.
  - If there is no data in the attribute columns, it is not a problem; just be sure there are (8) columns with the 'Asset Name' column and 'Asset Type' column populated.
  - Column headers (row 1) are for reference only, removal is required prior to import.
- Save the file as a .CSV document.

Asset Name	Description	Asset Type	Attribute 2	Attribute 3	Attribute 4	Attribute 5	Attribute 6
1071		iFob Key					
2071		Control Key					
3071		User Key					

Figure 7: 6 Attributes Import Format

Adding Assets

There are two methods for adding assets:

1. Web Admin Registration (using "empty" iFobs stored in cabinet(s))
2. Kiosk Registration (See Medeco Kiosk Administration Guide)

Web Admin Registration

This method is for systems where unused iFobs (no keys connected and/or 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 asset with a Registered Type of 'Unregistered' and click Edit (figure 8).
- The 'Update Asset Information' page will display (figure 9).
- Edit the Asset Information (** Indicates Required Field)
  - Name**
  - Description – (customizable and used to describe/reference the asset)
  - Serial Number** – DO NOT EDIT (must remain the same as it was read by the system hardware)
  - Status – not editable
  - Registered Type** – always switch to 'Registered' (figure 9)
- Fill in Asset Attributes (Attribute 1** - 'Asset Type' is required).
  - 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.

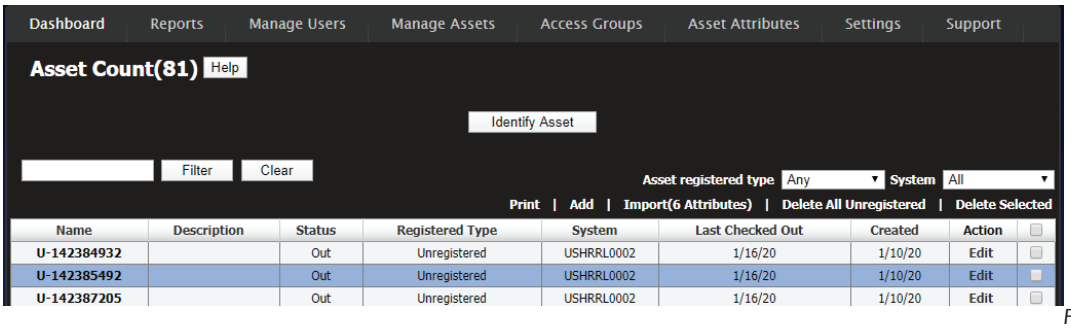


Figure 8: Edit Unregistered Asset

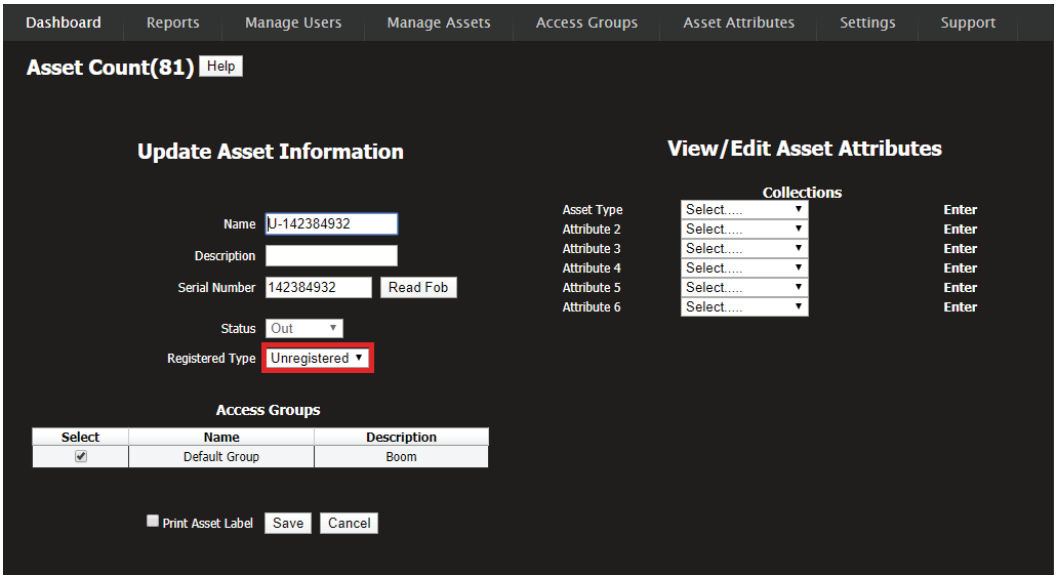


Figure 9: Register Asset

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

Deleting Assets

A system administrator, or a user with proper permissions, will "disassociate" the iFob from the database, thereby making the iFob ready for a new registration. Filter or scroll through the Asset List page, locate the asset, check the adjacent box and select Delete.

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 report 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

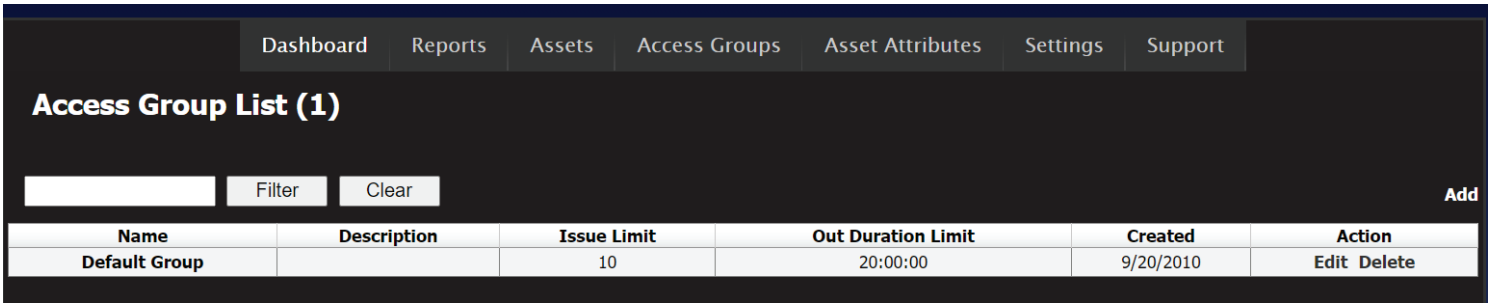


Figure 49: Edit Access Group Screen

The factory-loaded default Access Group is named Default Group. You may edit the default group, but you are unable to 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

- From the Access Group home screen > click the Add button in the upper right (figure 49).
- 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

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.

Access Groups (cont.)

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.

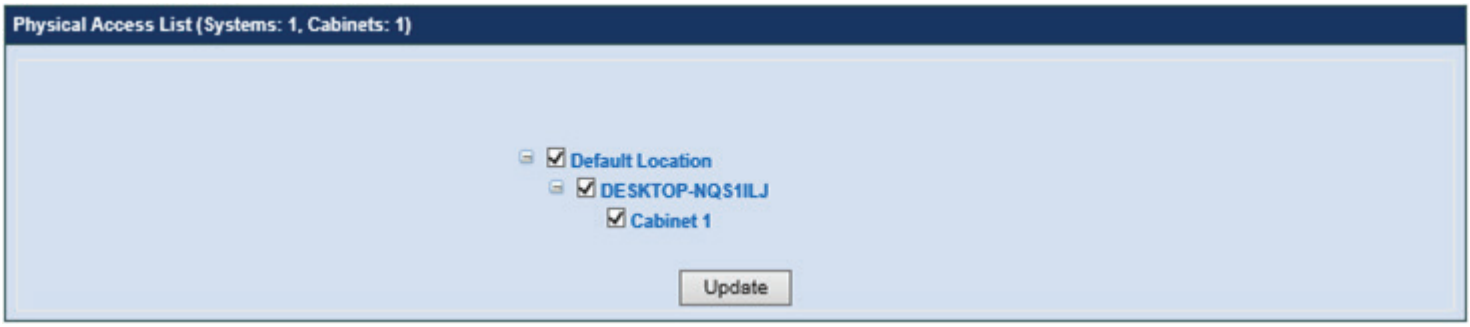


Figure 50: Access Group Physical Access List

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 report 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. Room #, Department, Model, Unit #, Building #, etc.).

All Asset Attributes except Attribute 1 - 'Asset Type' are empty by default configuration. They may be populated manually (see below), by Asset Import, or by Asset Edit.

Notes:
- *Assigning attributes to assets is necessary if using the Filter Assets method of check out at the Kiosk.*
- *Attribute Names are customizable to meet your preferences but requires the assistance of Medeco® 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).

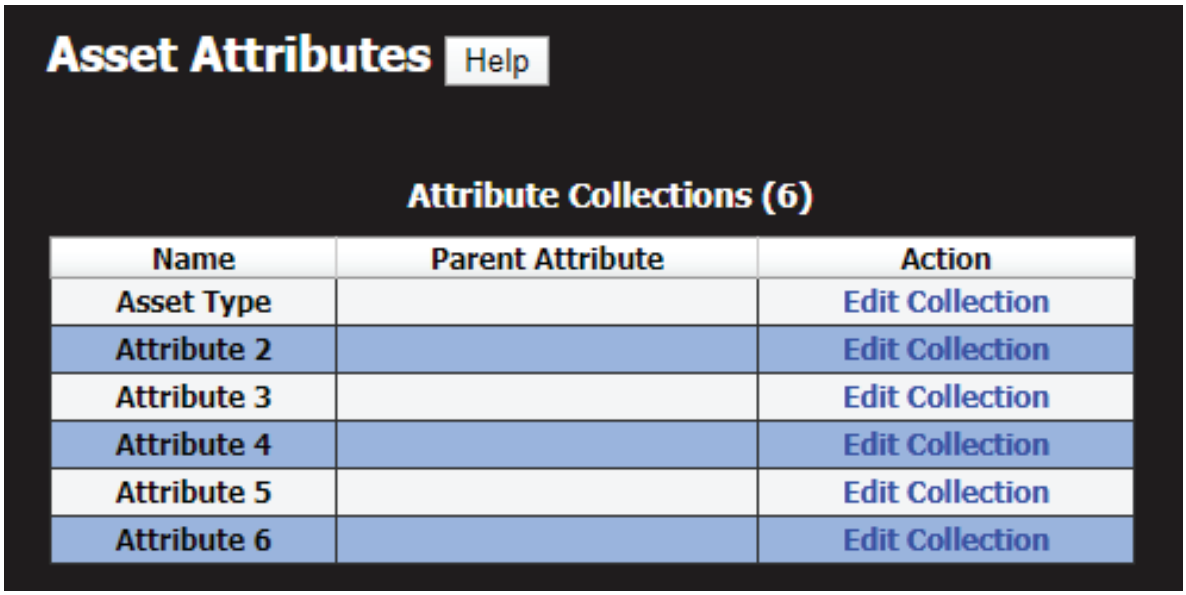


Figure 51: Attributes

Reports

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

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 systems equipped with cloud based backup, a map of key locations saves to the cloud.
  - Access your cloud map by clicking the Key Map button on the right hand side (figure 52).

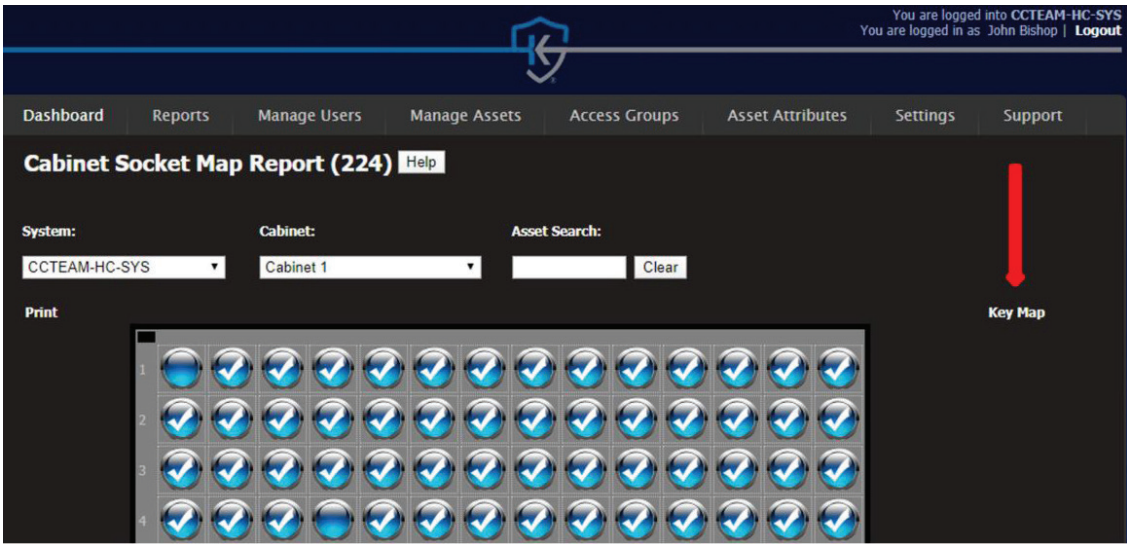


Figure 52: Cabinet Socket Map Report

Report Builder

- Create Customized reports with email and spreadsheet export 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. Photos are also taken when an alarm is set off by illegal activity (illegal key removal, door opening, etc.)

Reports (cont.)

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.

Settings

Some settings are password protected and only Medeco® Support can access these menus. The following items fall under the accessible Settings menu.

Alert Settings (Settings > Alert Settings)

- There are eight different alerts that will trigger an email and/or SMS alert from the Medeco® 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 - an asset inside the cabinet is 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 Medeco® Support. These alarms include the Door Open Alarm, Illegal Asset Removal Alarm, Asset Not Locked In, and an alarm that triggers when the Kiosk experiences an unexpected Power Loss. A speaker inside the cabinet plays a siren sound when alarming.

Email Settings (Settings > Email Settings)

- Configure email settings to allow your Medeco® System to send out email alerts.
- The Medeco® System does not receive emails, it only sends.
- The Medeco® 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 Medeco® 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 Medeco Support if assistance is required.

Issue Reasons (Settings > Issue Reasons)

- To enable Issue Reasons for any system, click the desired System (i.e. USHRRL0002), check the Enable Issue Reasons box and select IRL from the dropdown menu (figure 53).

Settings (cont.)

Figure 53: Enabling Issue Reasons

Note: System Structure and System Settings are only accessible by Medeco Support

Under the Support menu, you will find the following links

- Support Website – send support questions directly to Medeco® Support
- FAQs – link to support documents addressing frequently asked questions
- Remote Support – opens a webpage that will allow Medeco® Support to connect to your PC
- System Manual – link to the system user guide

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 55 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.

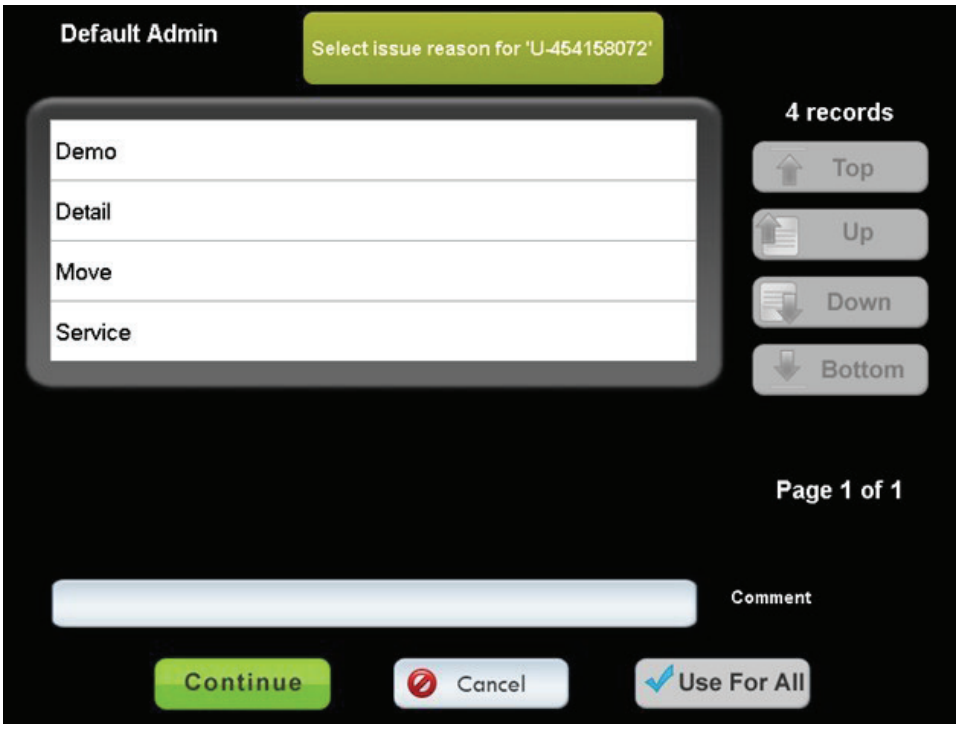


Figure 55: Issue Reason Screen

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 white 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 two Checkout buttons. 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 56).

Optional Features (cont.)

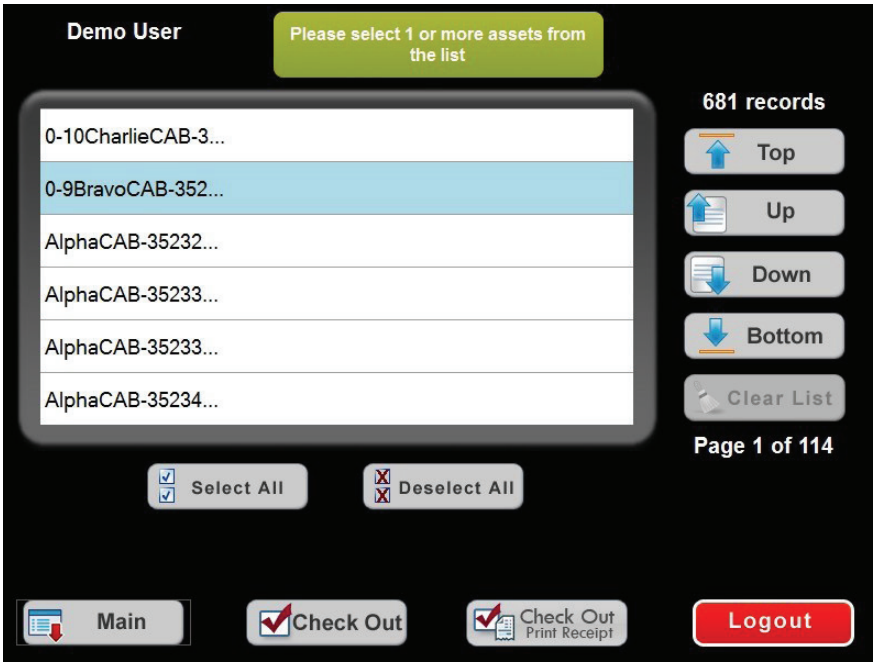
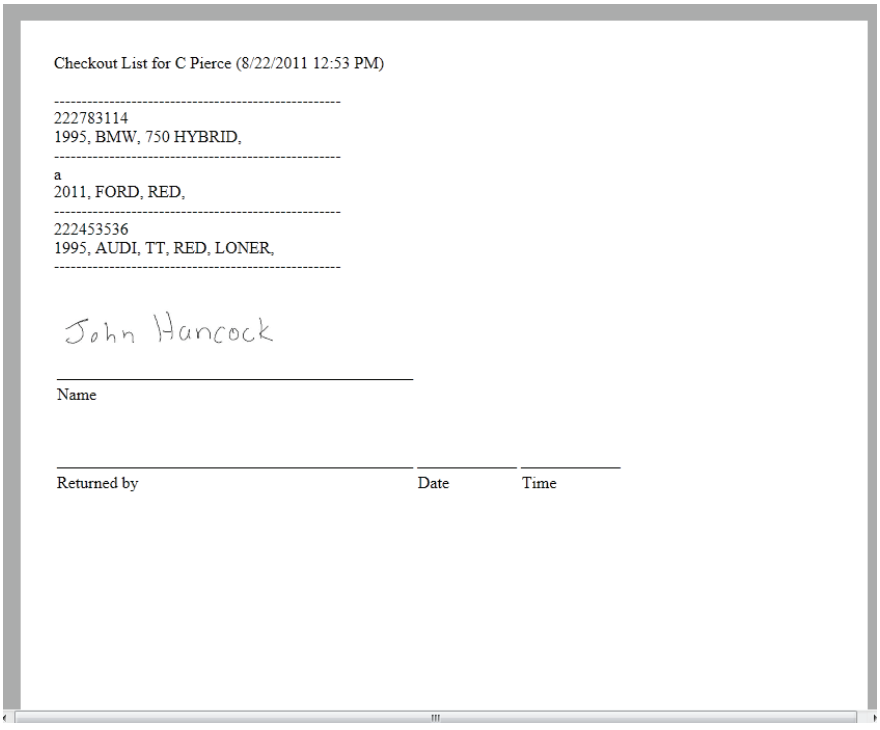


Figure 56: Print Receipt Checkout Button



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

222783114
1995, BMW, 750 HYBRID,

---

a
2011, FORD, RED,

222453536
1995, AUDI, TT, RED, LONER,

John Hancock

Name

Returned by Date Time

Figure 57: Sample Receipt

Biometric Policy

Medeco ("Medeco Security Locks") has instituted the following policy related to any finger-sensor or biometric data that Medeco may possess, if any, as a result of Medeco's customers' and customers' employees' and/or other individuals who are provided access to the Medeco devices ("User" or "Users") and/or use of Medeco products and services and whose data is transmitted or disclosed to Medeco by its customers. Medeco'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 Medeco devices utilize a finger-sensor which may be considered to collect biometric data.

Collection, Storage, Use, And Transmission Of Biometric Data

Medeco'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. Medeco's customers shall obtain written authorization from each User of Medeco devices to collect, capture, receive or otherwise obtain, possess, store, use, and/or transmit biometric data prior to the collection of such data. Specifically, Medeco 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 Medeco's customers and/or Medeco;
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 Medeco's customers and/or Medeco; 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 Medeco customers and/or by Medeco.

Medeco and/or its vendors may receive, store, use and/or transmit any biometric data solely for access to Medeco devices and keys stored therein. Neither Medeco 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 Medeco devices and services.

Retention Schedule

Medeco will retain any client's employee's or User's biometric data in Medeco's possession, if any, until the customer notifies Medeco that it has terminated the employee or User or discontinued their access to the Medeco devices. When Medeco 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 Medeco devices; or (3) the User requests in writing that his/her data be deleted. Medeco'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 Medeco or (ii) within three (3) years after the customer informs Medeco that its last interaction with User has occurred.

Biometric Data Storage

Medeco and/or its vendors shall use the reasonable standard of care in Medeco'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 Medeco stores, transmits, and protects other personal information of Users.

The ASSA ABLOY Group is the global leader in access solutions. Every day, we help billions of people experience a more open world.

ASSA ABLOY Opening Solutions leads the development within door openings and products for access solutions in homes, businesses and institutions. Our offering includes doors, frames, door and window hardware, mechanical and smart locks, access control and service.

Medeco U.S.
3625 Alleghany Drive
P.O. Box 3075
Salem, Virginia 24153-0330
Customer Service
1-877-633-3261
www.medeco.com

Medeco Canada
160 Four Valley Drive
Vaughan, Ontario, L4K 4T9
Customer Service
1-888-633-3264

2020.012 - 07/25