



BEYOND SECURITY



RezShield™ Multihousing Access Control

Property Administrator User Guide

Property Administrator User Guide

Table of Contents

RezShield™ System Requirements	2
Features of the RezShield™ System	3
RezShield™ System Overview	4
Logging on to the Application	5
RezShield™ Main Screen	6
Accounts	7 - 9
Resident Access	10 - 12
Staff Access	13 - 16
Key Readback	17
Key Cancellation	18 - 19
Lock Actions	20 - 21
Lock Administration	22 – 23
Reports	24 - 28
RezShield™ Operator Levels	29 - 33
Keycard Types	34 - 36
Glossary	37
Notes	38

Minimum Requirements

1. **SERVER: (Must be a dedicated machine)**

OS: Vista Business, Windows 7 & 8 Pro, Windows Server 2008 & 2012 (32/64 bits)

Windows: Features: Pre-installed
NET Framework 2/4
Web Server - IIS (Internet Information Services)
MSMQ (Microsoft Message Queuing)

Backup Media: USB Memory stick
CD Writer

Hardware: CPU – Dual Core or above
RAM – 8GB (Recommended)
HARD DISK – 250 GB (Recommended)
CD ROM
Serial Port (For Serial PMS Only)
USB Ports
NETWORK ADAPTER
STANDARD MONITOR

The server must be on the hotel network with a static IP address or server name recognized by DNS.
N.B For more than 5 workstations, Windows Server 2008 or 2012 OS is required.

2. **WORKSTATIONS (minimum)**

OS: Vista Business, Windows 7 Pro, Windows 8

Software: IE 6.0 or above
NET Framework 2.0

Hardware: CPU – dual core or above (recommended)
RAM - 4GB (recommended)
HARD DISK – 160 GB (recommended)
CD ROM
USB Ports
NETWORK ADAPTER
STANDARD MONITOR

IMPORTANT NOTICE:

'Home Edition' OS is not suited for Atlas.

For further information

lodging-tech@kaba.com or call 1-877-468-3555 and select Technical Support

Features of the RezShield™ System

The Kaba RezShield™ System (also called the system in this booklet) uses electronic locks that work with electronic credentials instead of mechanical keys. Credentials are available in three different forms: keycards, fobs, or wristbands. RezShield software is the tool that is used to enter and encode information on residents and staff credential when their unit is assigned. These credentials work just like keys, giving residents secure access to their rooms when positioned in front of the reader on the lock. They can be customized when made to also provide r access to other amenities such as exercise room, parking, etc. The flexibility of the system enables residents to carry just one keycard for gaining access to all of these property features in addition to their own unit.

For the Property Administrator (or User), when using this system - instead of handing the residents a metal key - they simply program a new credential for each resident with the additional options and property features that they are entitled to use.

The new credential contains a unique, encrypted code that opens only the locks that the resident is entitled to use.

As soon as this new credential is used in the lock by the resident, all previous resident-level credentials for that lock are cancelled.

This leads to a high level of security, equivalent to re-keying the lock for every resident.

Every use of the RezShield PC or access to a lock is audited.

Each employee must enter a valid password to allow them to make or read a keycard and this information goes into the audit trail. The audit trail reveals the date and time, the identity of the user, and the operations performed.

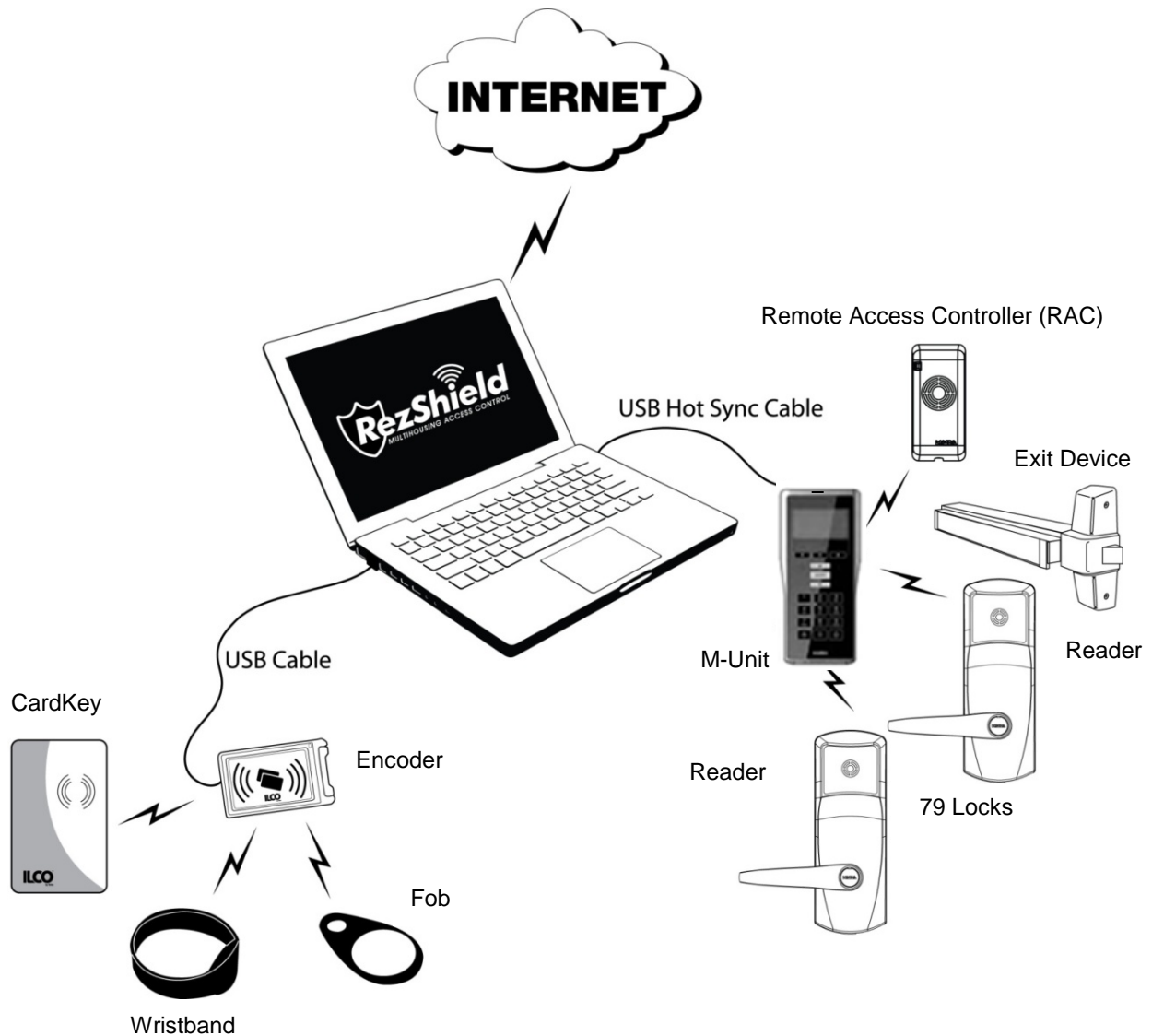
Property Administrators should NEVER give their password to anyone and never make inappropriate use of any PC, lock, or keycard. They must always log off the RezShield system after they finish using it, so no one else is able to make keycards with their password.

Screen Size – If the RezShield Web application fills the whole screen it is in Kiosk mode. This mode can be activated or de-activated in the system set-up application.

Screen Toggle – When using several applications at the same time (For example: RezShield web application, Monitoring Manager, and System Setup) you can cycle through all the open screens by using the “Alt + Tab” when you get to the icon of the application screen you want to see.

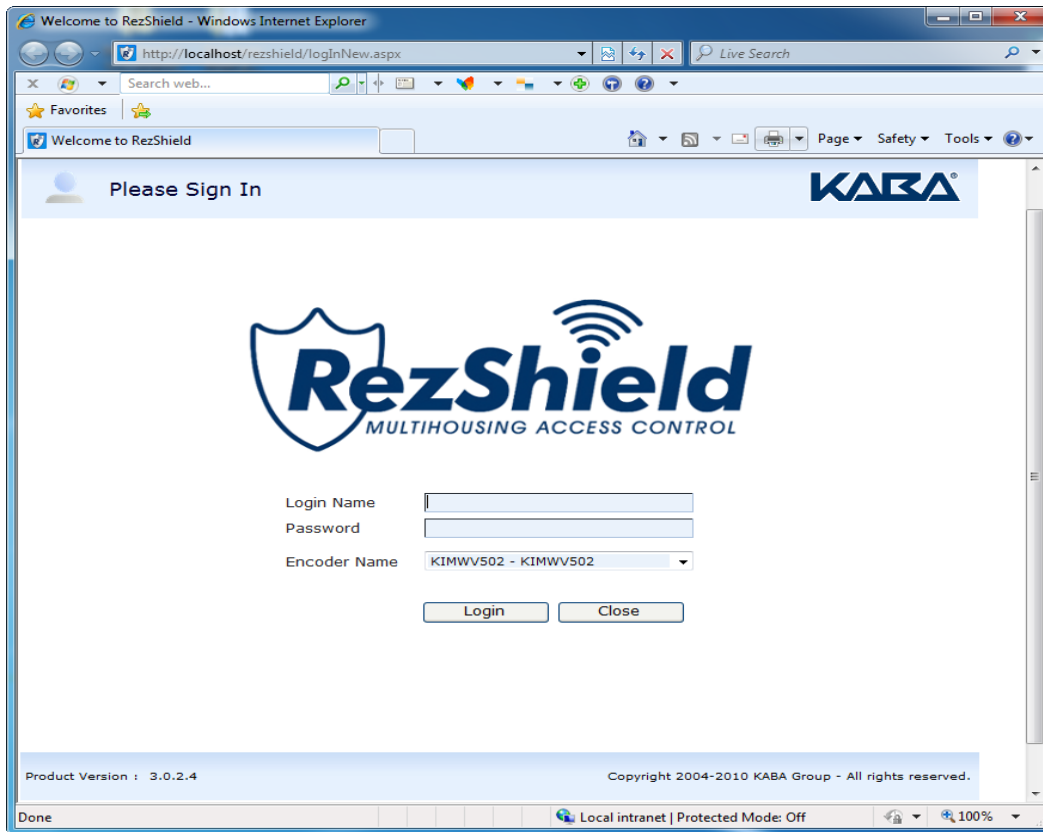
System Overview

- RezShield™ can be installed on a PC anywhere on the property (in a security or management office).
- Credentials can be made using the encoder with a USB connection.
- Remote diagnostics and maintenance on the RezShield™ server is possible via the Internet connection.
- Locks and remote access controllers are programmed and audited using a Maintenance Unit.



Logging on to the Application

Important: Ensure that your name has been entered into the system at the Administrator level by your management and that there is an activated encoder for your PC.



1. Enter **Login Name** and **Password**.
2. Encoder name is already configured when the RezShield software is loaded onto your PC.
3. Click on **Login**.
4. The **Welcome to RezShield** screen will appear.

Welcome to RezShield

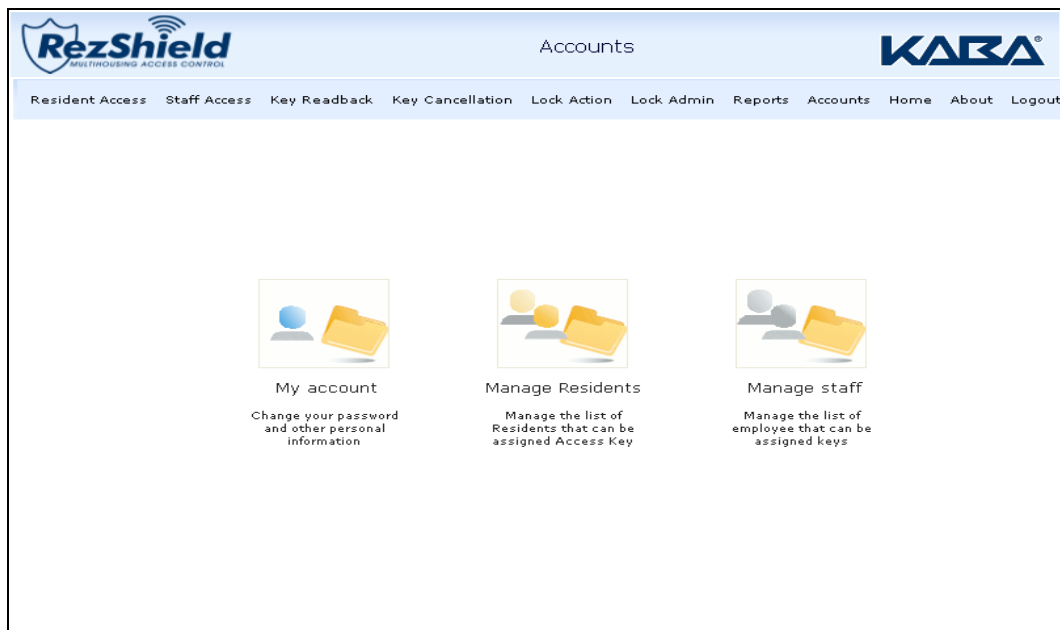
The **Welcome to RezShield** screen lists all of the functions that can be selected and used by the Property Administrator. It features a step-by-step process for each function with graphic prompts and “Tips” to guide you through the following operations:

- ✓ Accounts
- ✓ Resident Access
- ✓ Staff Access
- ✓ Key Readback
- ✓ Key Cancellation
- ✓ Lock Action
- ✓ Lock Administration
- ✓ Reports



1. Accounts

Before you can begin programming key access or using the other features of this software, you will need to set up accounts and complete the necessary information for My Account, Manage Residents, and/or Manage Staff.



This is the section where you register and maintain the database listings of all residents and staff that have been issued key access to units and amenities on the property.

My Account

This allows you to set up your login name and password. Complete the necessary fields and click **Save**.

Manage Residents

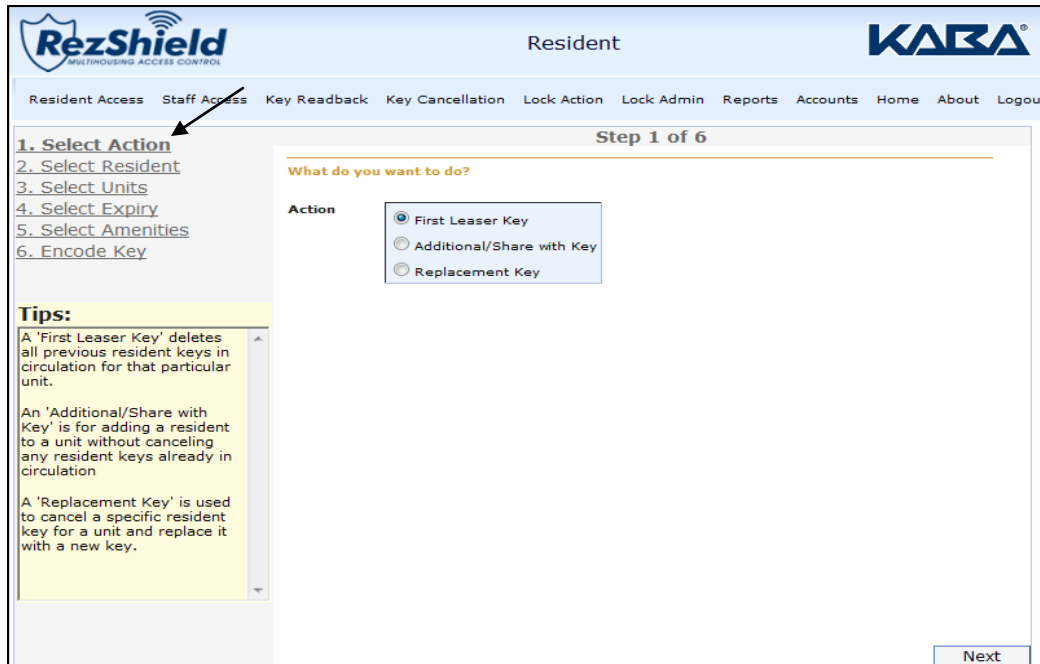
1. The Manage Residents option enables you to add new residents or edit information on an existing resident. Select from the Add a new Resident or Edit an existing Resident button and click **Next**.

2. Complete the necessary fields and click **Save**.

Manage Staff

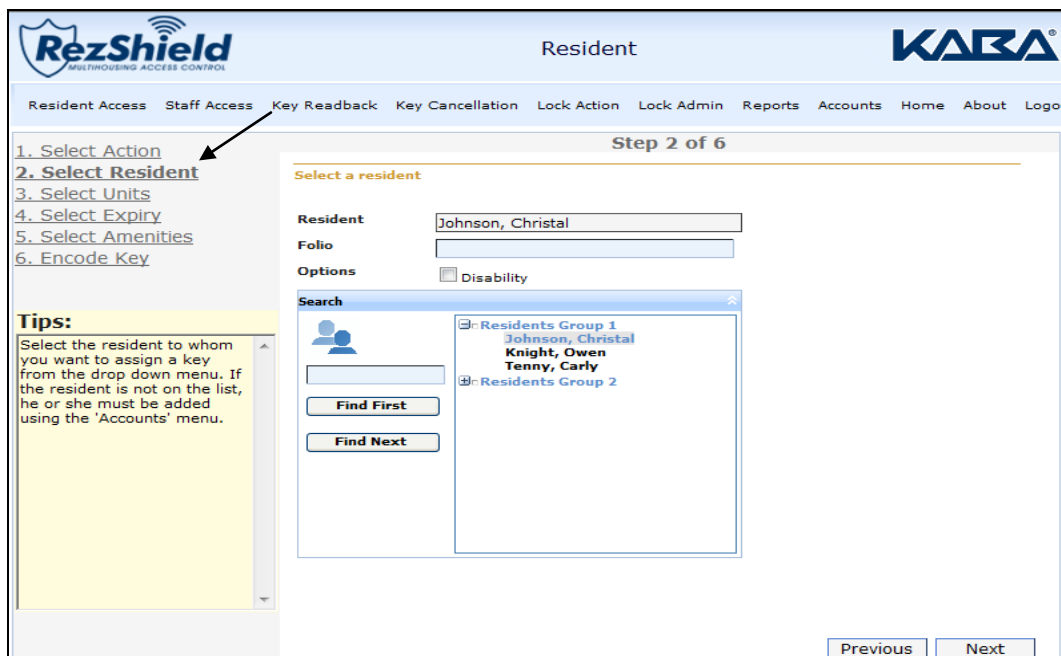
1. The Manage Staff option enables you to manage your staff information the same way you manage your resident information. The same steps apply.

2. Resident Access

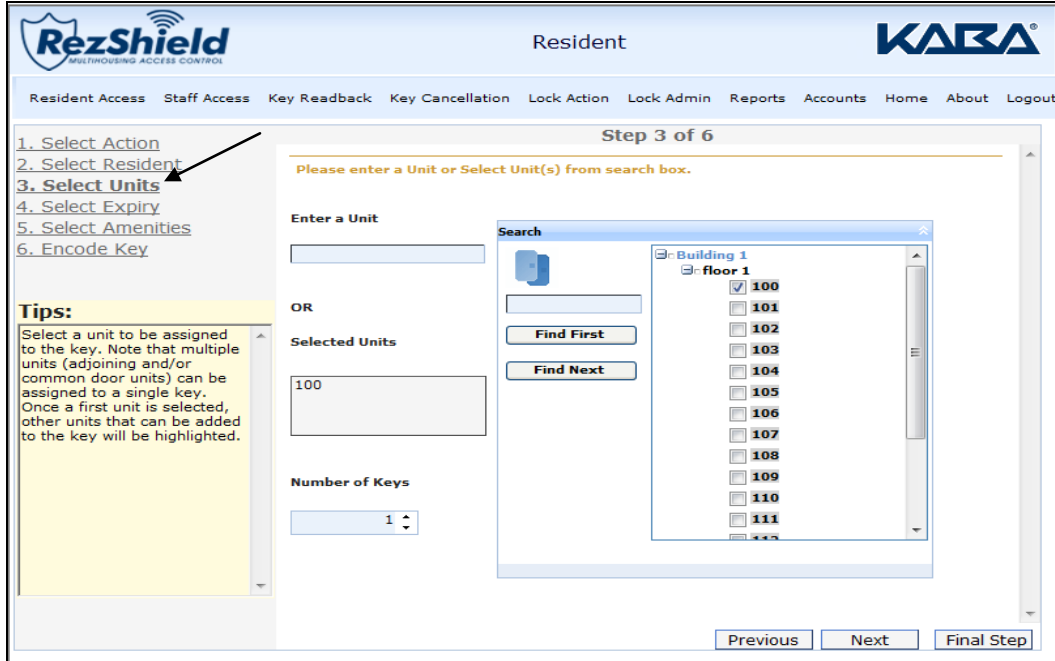


1. At the Select Action screen, choose the key type you are going to create then click **Next**.

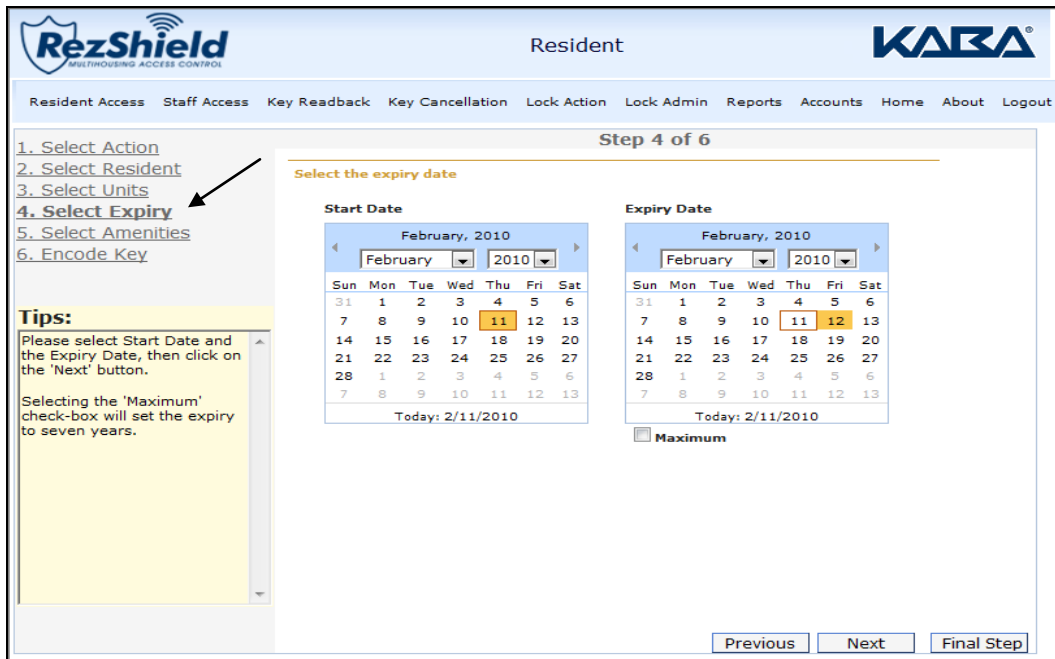
Note: The “Tips” provide an explanation of the different key types/access options that can be created.



2. At the Select Resident screen, select the resident to whom you want to assign the key and click **Next**.

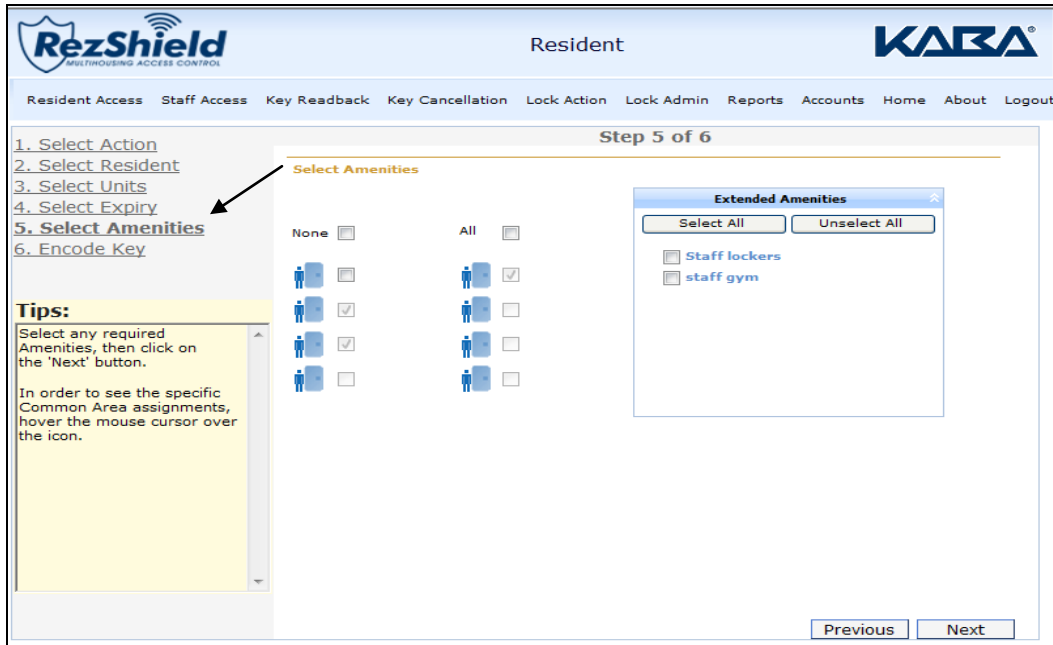


3. At the Select Units screen, select the Unit Number to which the key will be assigned.

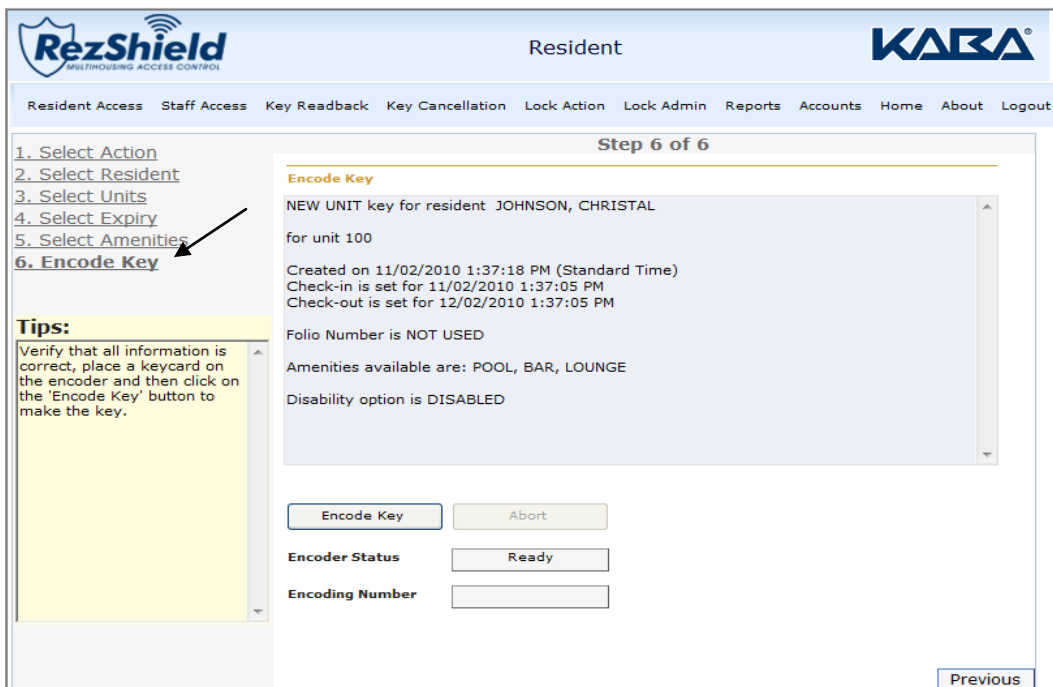


4. Next use the calendars to assign a Start Date and Expiry Date for the key. Click **Next**.

Note: Assigning a Start Date and Expiry Date helps you control the period for which a key is valid. A key will not work outside its Expiry Date.

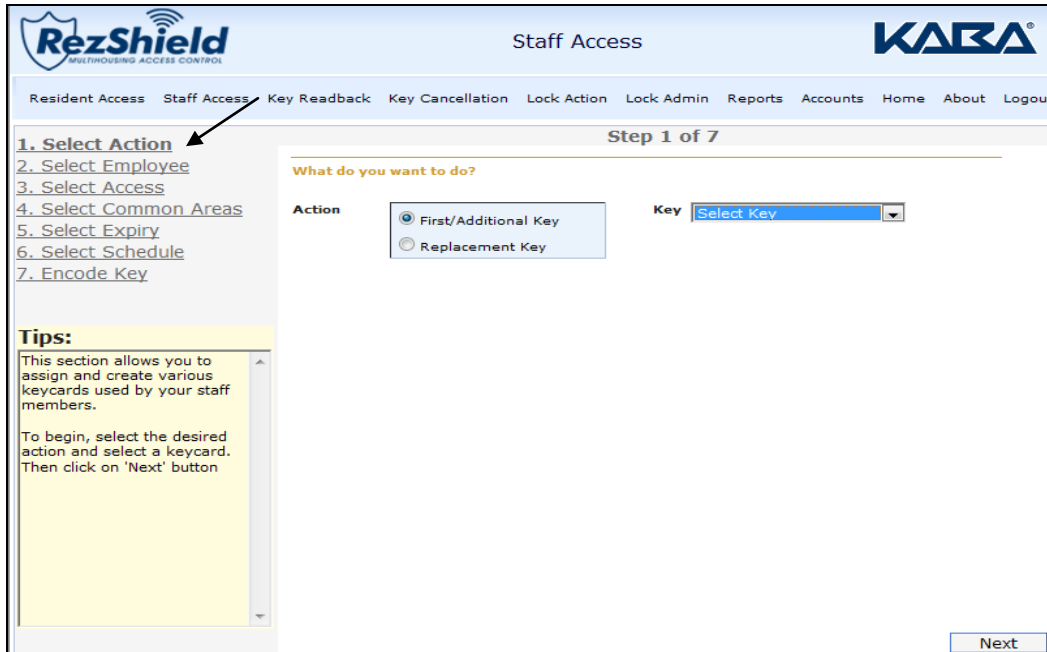


5. At the Select Amenities screen you may assign additional access points to the key. For example: dining hall, exercise room, parking or other extended amenities access.

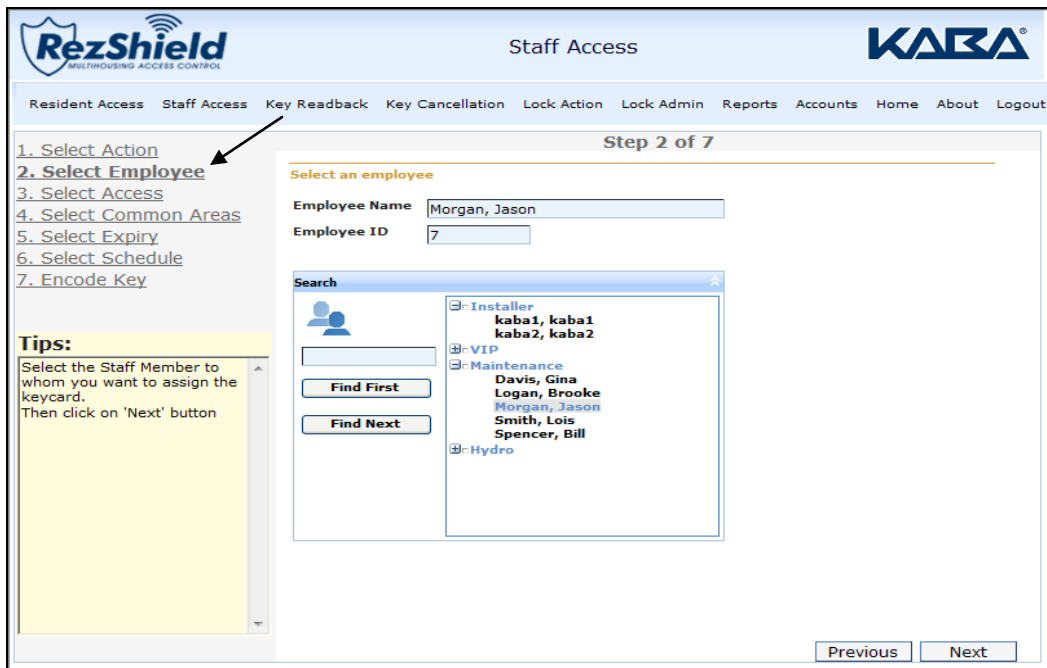


6. Now place the key onto the encoder and click **Encode Key** to program it.

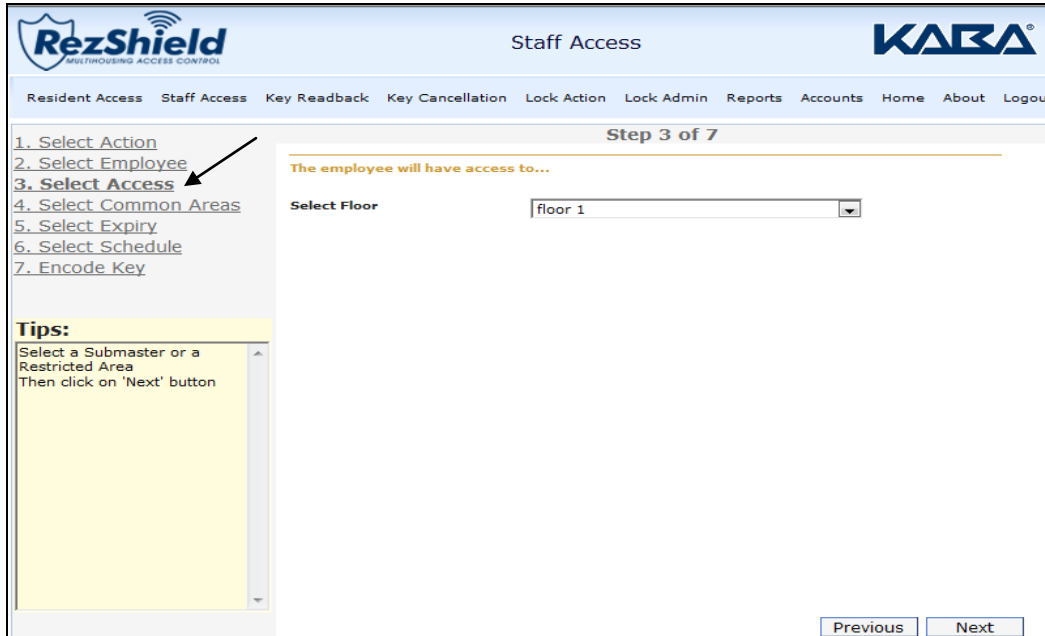
3. Staff Access



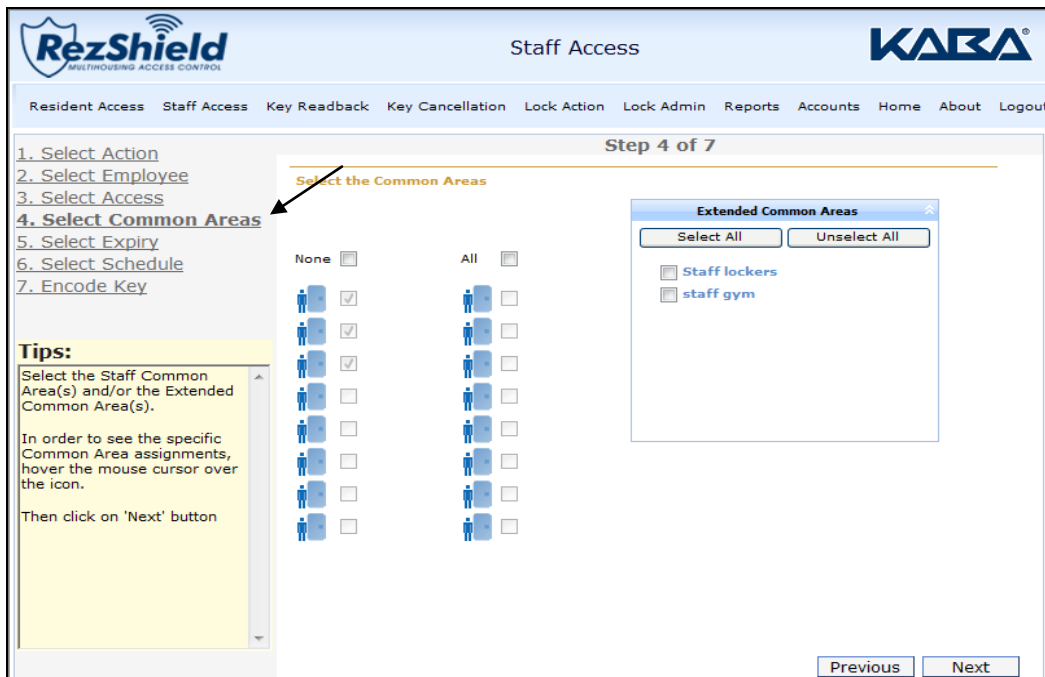
1. At the Select Action screen, click on the type of key you want to create. Next choose Select Key from the dropdown menu and then click **Next**.



2. At the Select Employee screen, choose the employee or supplier for whom to create the key.



3. The Select Floor dropdown allows you to choose the floor(s) to which the employee will have access.



4. At the Select Amenities screen you may assign additional access points to the key. For example: dining hall, exercise room, parking or other extended amenities access.

Staff Access

Resident Access Staff Access Key Readback Key Cancellation Lock Action Lock Admin Reports Accounts Home About Logout

Step 5 of 7

Select Expiration Date

February, 2010

Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6
7	8	9	10	11	12	13

Today: 2/11/2010

February, 2011

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	1	2	3	4	5
6	7	8	9	10	11	12

Today: 2/11/2010

Maximum

Previous Next

1. Select Action
2. Select Employee
3. Select Access
4. Select Common Areas
5. Select Expiry
6. Select Schedule
7. Encode Key

Tips:
Please select Start Date and the Expiry Date for the keycard
Then click on 'Next' button

5. Use the calendars to indicate the Start Date and Expiry Date for the key, then click **Next**.

Staff Access

Resident Access Staff Access Key Readback Key Cancellation Lock Action Lock Admin Reports Accounts Home About Logout

Step 6 of 7

Select a schedule

- None
- Timezone 1
- Timezone 2
- Timezone 3
- Timezone 4
- Timezone 5
- Timezone 6
- Timezone 7
- Timezone 8

Intervals	Start	End
Intrv 1	-	-
Intrv 2	-	-
Intrv 3	-	-
Intrv 4	-	-

S	M	T	W	T	F	S
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

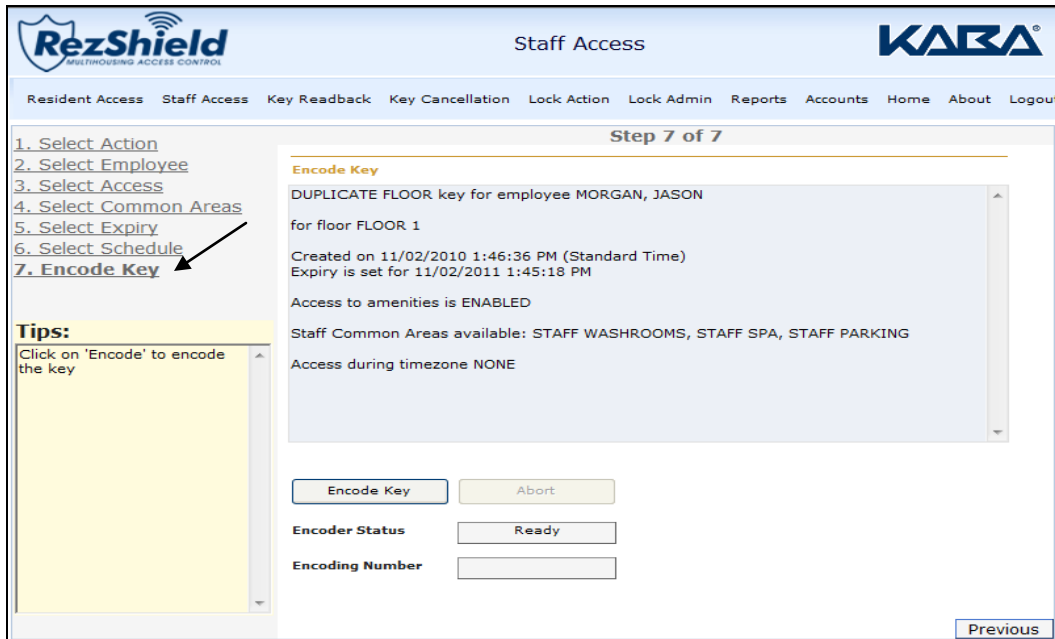
Previous Next

1. Select Action
2. Select Employee
3. Select Access
4. Select Common Areas
5. Select Expiry
6. Select Schedule
7. Encode Key

Tips:
Select the desired schedule.
Note: Leaving the selection to 'None' means that the selected Staff Member will have access at all times
Then click on 'Next' button

6. When programming staff keys the Select Schedule option allows you to selective program specified time periods when staff keys are operational. For example, staff keys may be programmed to work only from 8 a.m. to 5 a.m. daily.

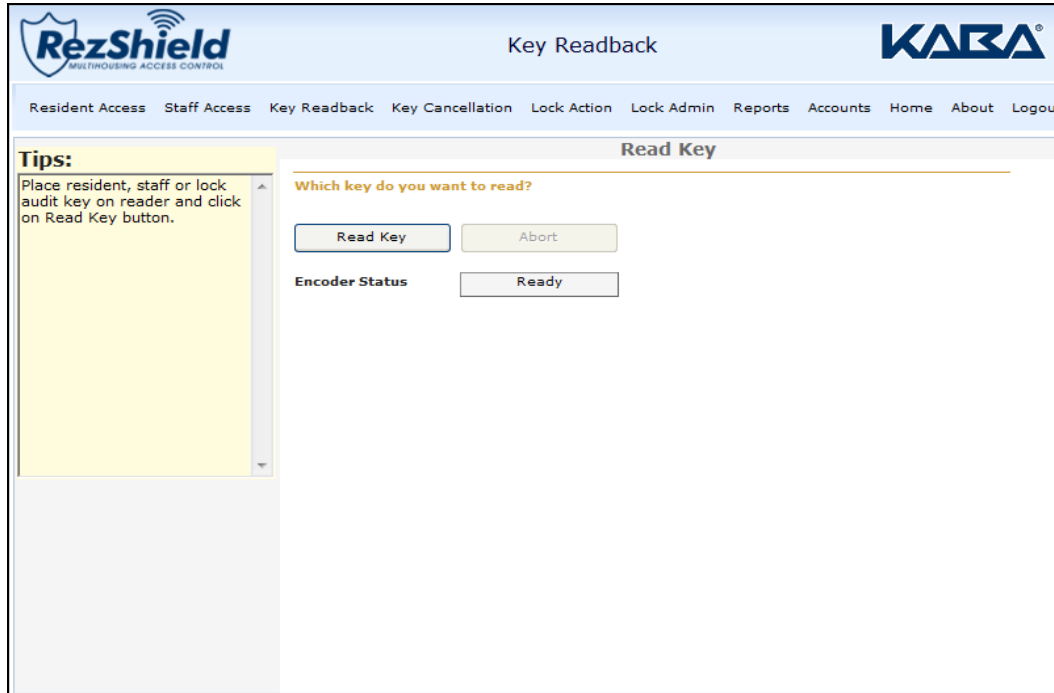
Note: The Timezone option can be customized to your requirements.



The screenshot shows the 'Staff Access' interface in the RezShield software. The top navigation bar includes 'Resident Access', 'Staff Access', 'Key Readback', 'Key Cancellation', 'Lock Action', 'Lock Admin', 'Reports', 'Accounts', 'Home', 'About', and 'Logout'. The main content area is titled 'Step 7 of 7' and 'Encode Key'. A list of steps on the left includes '1. Select Action', '2. Select Employee', '3. Select Access', '4. Select Common Areas', '5. Select Expiry', '6. Select Schedule', and '7. Encode Key', with an arrow pointing to the last step. A 'Tips' box contains the instruction: 'Click on 'Encode' to encode the key'. The main display area shows details for a 'DUPLICATE FLOOR key for employee MORGAN, JASON for floor FLOOR 1', including creation and expiry dates, access status, and available common areas. At the bottom, there are buttons for 'Encode Key' and 'Abort', and fields for 'Encoder Status' (set to 'Ready') and 'Encoding Number'. A 'Previous' button is located in the bottom right corner.

7. Finally, place the key onto the encoder and click **Encode Key** to program it.

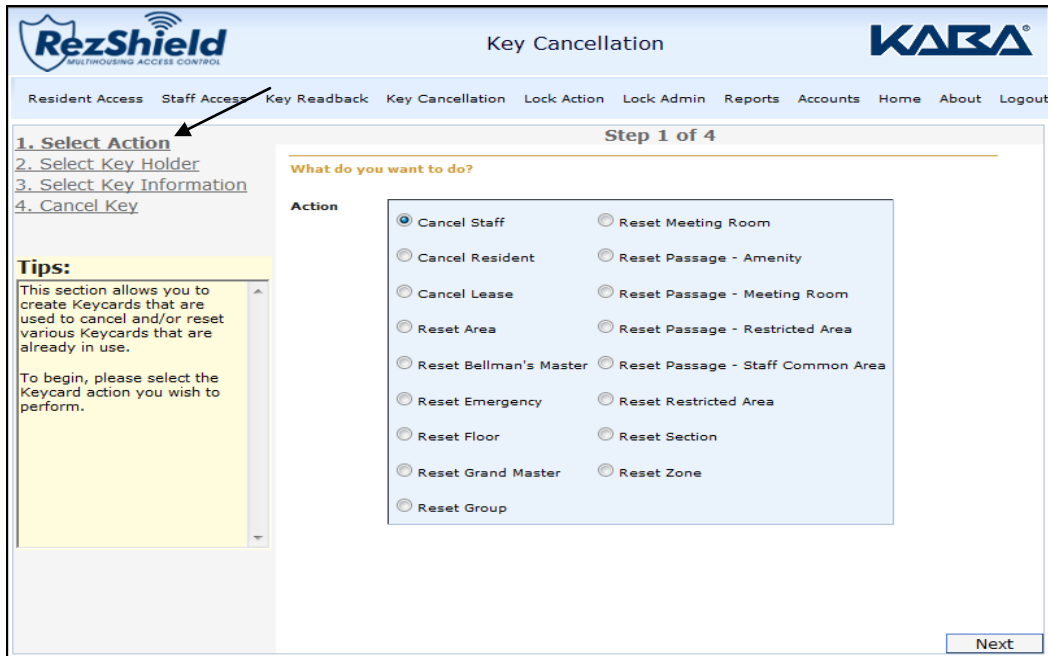
4. Key Readback



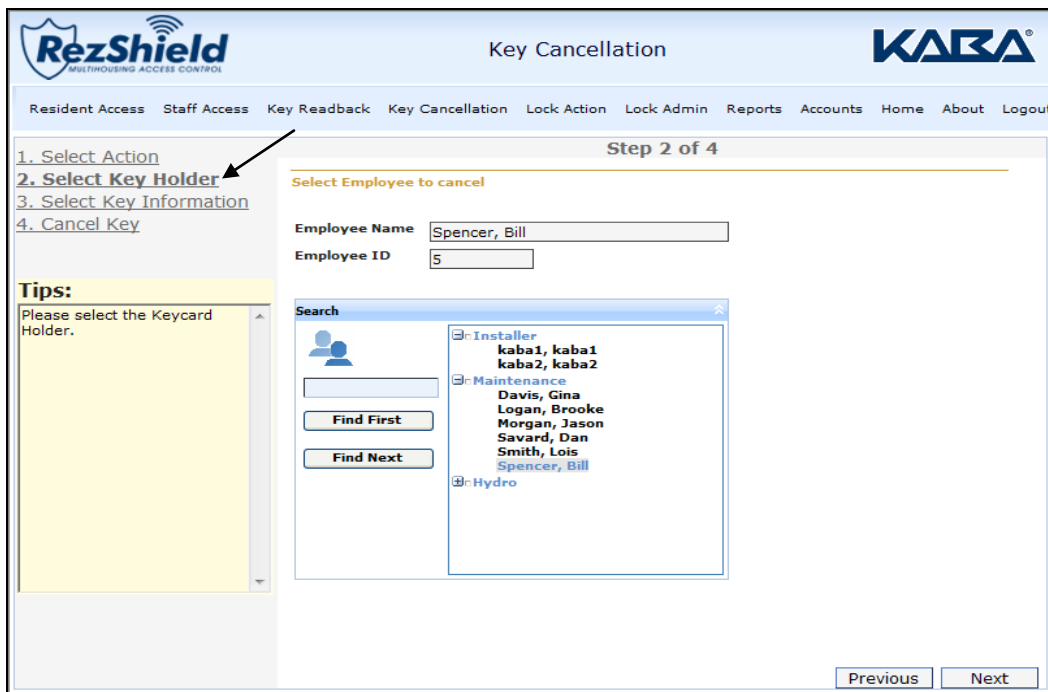
The screenshot shows the 'Key Readback' interface in the RezShield software. At the top, there is a navigation bar with the RezShield logo on the left, the title 'Key Readback' in the center, and the KABA logo on the right. Below the navigation bar is a menu with the following items: Resident Access, Staff Access, Key Readback (highlighted), Key Cancellation, Lock Action, Lock Admin, Reports, Accounts, Home, About, and Logout. The main content area is titled 'Read Key' and contains a 'Tips' section on the left with the text: 'Place resident, staff or lock audit key on reader and click on Read Key button.' To the right of the tips, there is a question 'Which key do you want to read?' followed by two buttons: 'Read Key' and 'Abort'. Below this, there is an 'Encoder Status' section with a 'Ready' button.

The *Key Readback* feature will help identify a particular key and how it was programmed. When reading a Resident key, certain Staff keys, or an Audit key an audit trail will be displayed.

5. Key Cancellation



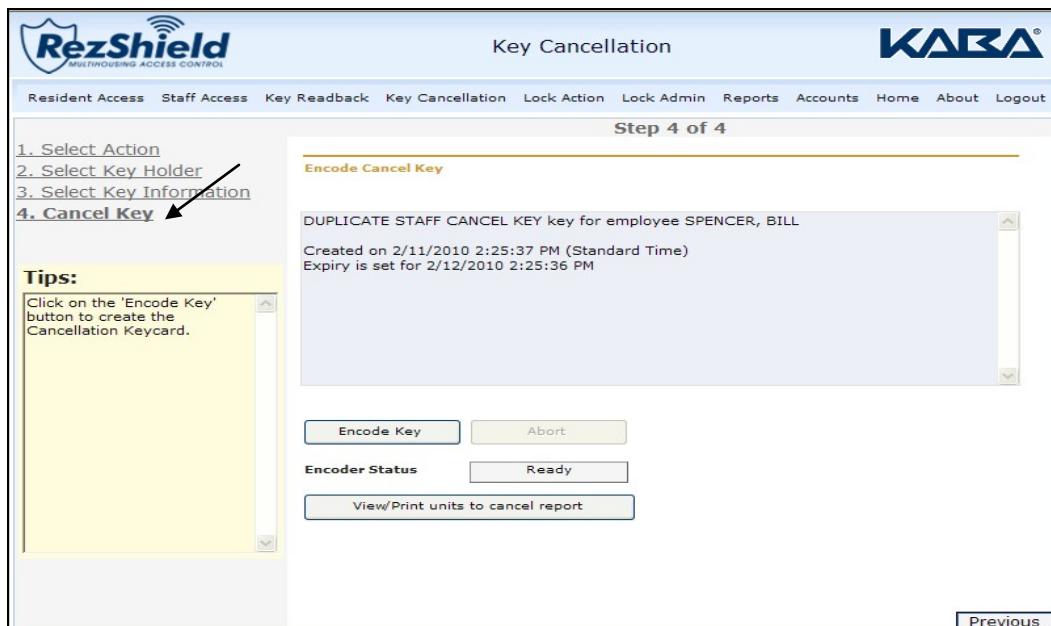
1. To cancel a key, first click on Select Action to select the key you want to cancel. Click **Next**.



2. At the Select Key Holder screen, identify the individual to for whom the key has been programmed.

NOTE: Depending on the Key chosen, all steps may not be required.

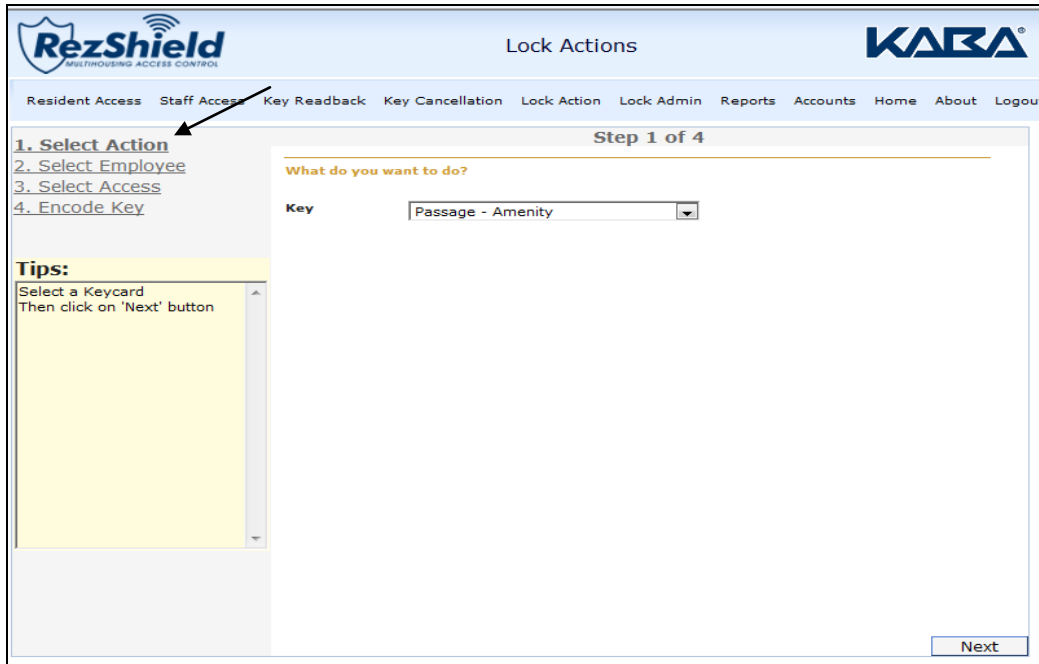
3. Select Key Information.



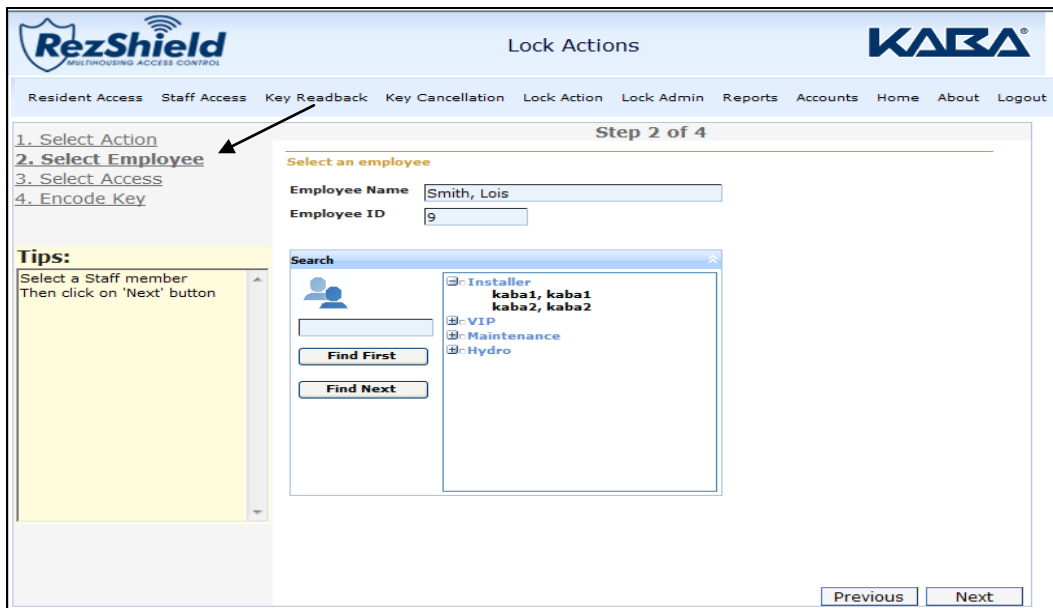
The screenshot shows the 'Key Cancellation' page in the RezShield web interface. The page title is 'Key Cancellation' and it features the KABA logo. A navigation menu includes: Resident Access, Staff Access, Key Readback, Key Cancellation, Lock Action, Lock Admin, Reports, Accounts, Home, About, and Logout. The current step is 'Step 4 of 4'. On the left, a list of steps is shown: 1. Select Action, 2. Select Key Holder, 3. Select Key Information, and 4. Cancel Key. An arrow points to step 4. Below the list is a 'Tips:' section with a scrollable area containing the text: 'Click on the 'Encode Key' button to create the Cancellation Keycard.' The main content area is titled 'Encode Cancel Key' and contains a scrollable text box with the following information: 'DUPLICATE STAFF CANCEL KEY key for employee SPENCER, BILL', 'Created on 2/11/2010 2:25:37 PM (Standard Time)', and 'Expiry is set for 2/12/2010 2:25:36 PM'. Below the text box are three buttons: 'Encode Key', 'Abort', and 'Encoder Status'. The 'Encoder Status' button is currently set to 'Ready'. At the bottom of the page is a 'View/Print units to cancel report' button and a 'Previous' button in the bottom right corner.

4. Place the key on the encoder and click **Encode Key** to cancel the key.

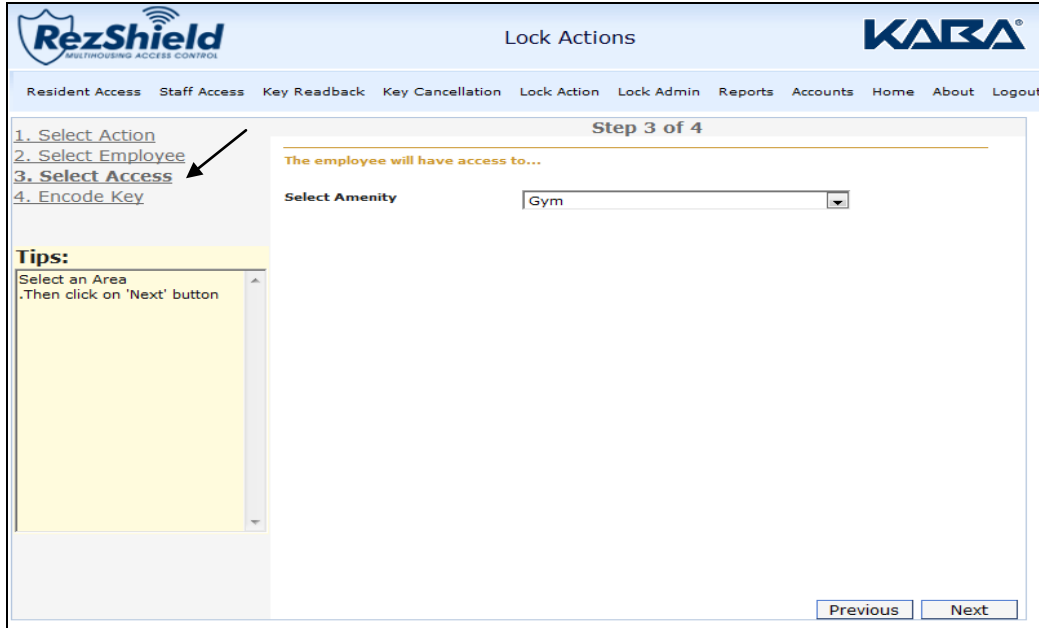
6. Lock Actions



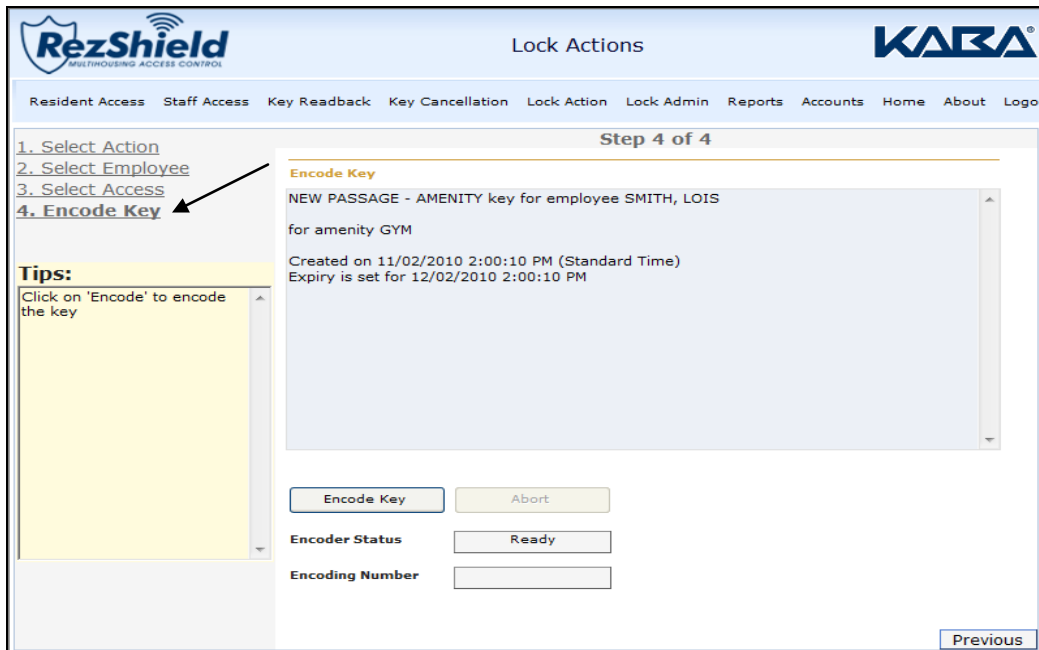
1. At the Select Action screen, select the type of key you want to create. Click **Next**.



2. Then Select Employee and click **Next**.

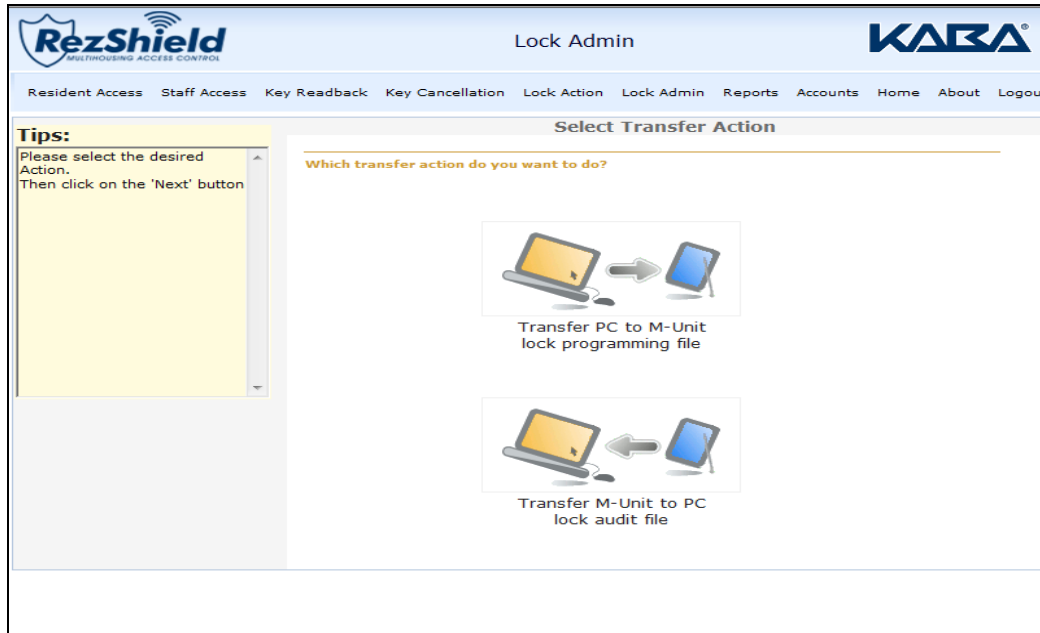


3. Select the access type for the key and click **Next**.



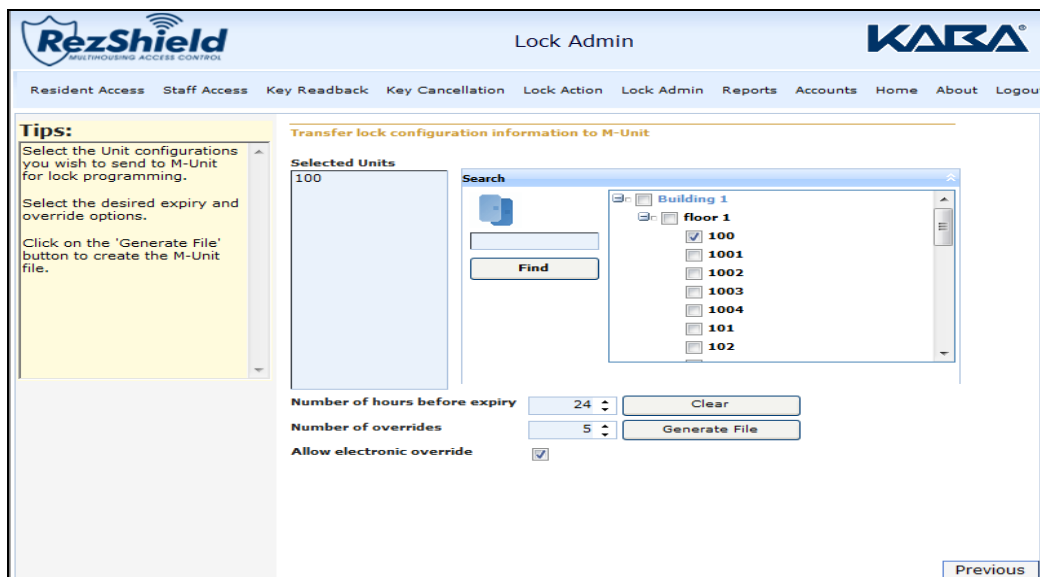
4. Place the key on the encoder and click **Encode Key** to cancel the key.

7. Lock Administration

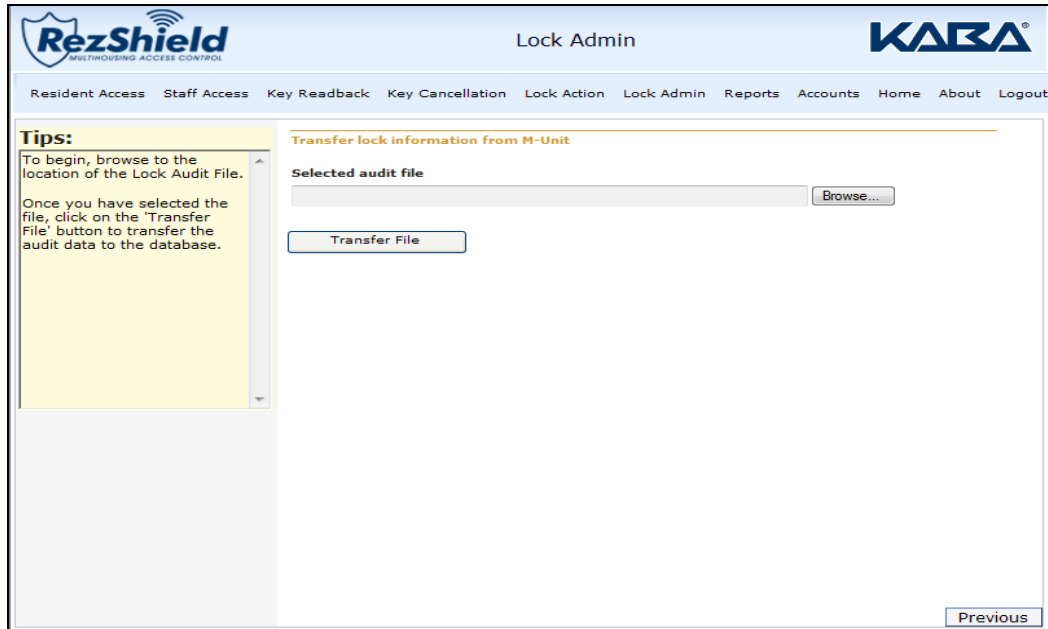


1. Select Transfer Action by clicking on the appropriate icon for the action you wish to perform.

Transferring Lock Configuration to the M-Unit



1. In the right hand box under the Search option, select the floor and unit to be transferred to the lock configuration.
2. The selected information will be displayed on the left side of the search box. Click **Generate File**.



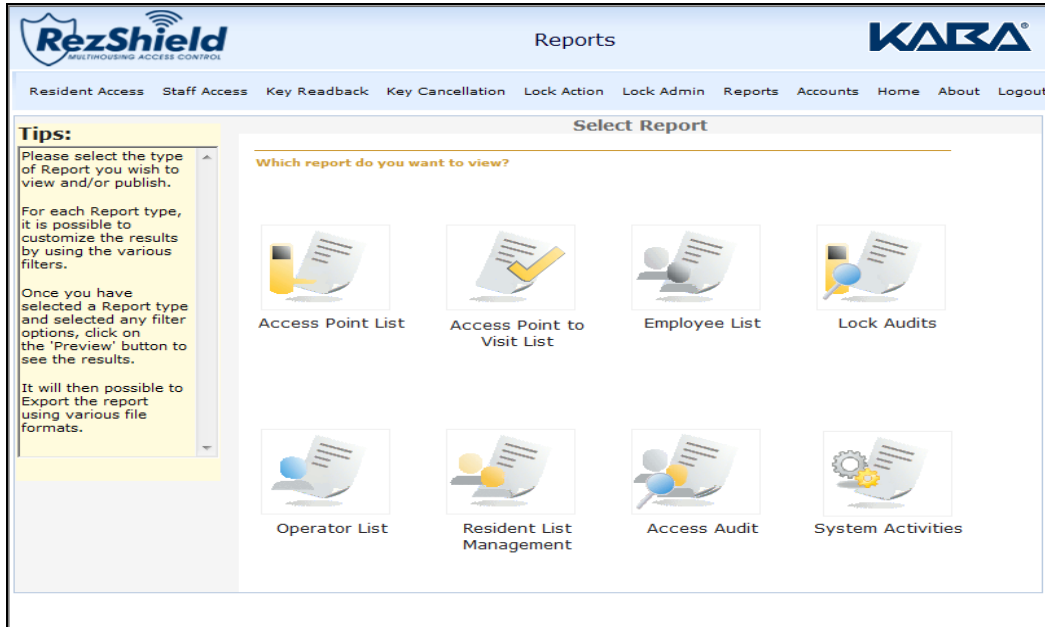
The screenshot shows the 'Lock Admin' page in the RezShield web interface. The page has a light blue header with the RezShield logo on the left, 'Lock Admin' in the center, and the KABA logo on the right. Below the header is a navigation menu with links: Resident Access, Staff Access, Key Readback, Key Cancellation, Lock Action, Lock Admin, Reports, Accounts, Home, About, and Logout. The main content area is divided into two sections. On the left is a yellow 'Tips' box with the following text: 'To begin, browse to the location of the Lock Audit File. Once you have selected the file, click on the "Transfer File" button to transfer the audit data to the database.' On the right is a section titled 'Transfer lock information from M-Unit'. It contains a 'Selected audit file' label, a text input field, a 'Browse...' button, and a 'Transfer File' button. At the bottom right of the main content area is a 'Previous' button.

3. Click Transfer to save the file to the M-Unit folder. Perform a Hotsync* to send the file to the M-Unit.
4. Lock configuration information has been successfully transferred to the M-Unit.

**Refer to Glossary for definition.*

8. Reports

RezShield provides a variety of reports for reference and audit purposes. Three of the most common reports are: *Access Point*, *Lock Audits*, and *Operator List*.



Access Point



1. Determine the criteria for the report. Click to select it and press **Preview**.

KABA Access Point List Thursday, February 11, 2010
2:09 PM
 Maple Residences

Parameters selected for this report:
 Access Point Type: Resident Unit

Page 1 of 2

Access Point Name	Access Point Type	Area	Floor	Group	Section	Zone
200	Resident Unit	Area Two	floor 2	Group 2	Section 2	
201	Resident Unit	Area Two	floor 2	Group 2	Section 2	
202	Resident Unit	Area Two	floor 2	Group 2	Section 2	
203	Resident Unit	Area Two	floor 2	Group 2	Section 2	
204	Resident Unit	Area Two	floor 2	Group 2	Section 2	
205	Resident Unit	Area Two	floor 2	Group 2	Section 2	
111	Resident Unit		floor 1			
112	Resident Unit		floor 1			
113	Resident Unit		floor 1			
114	Resident Unit		floor 1			
115	Resident Unit		floor 1			
116	Resident Unit		floor 1			
100	Resident Unit		floor 1			
101	Resident Unit		floor 1			
102	Resident Unit		floor 1			
103	Resident Unit		floor 1			
104	Resident Unit		floor 1			
105	Resident Unit		floor 1			
106	Resident Unit		floor 1			
107	Resident Unit		floor 1			
108	Resident Unit		floor 1			
109	Resident Unit		floor 1			
110	Resident Unit		floor 1			

2. The Access Point list preview information displays a report which can also be exported and printed.

Lock Audits

Reports
KABA

[Resident Access](#)
[Staff Access](#)
[Key Readback](#)
[Key Cancellation](#)
[Lock Action](#)
[Lock Admin](#)
[Reports](#)
[Accounts](#)
[Home](#)
[About](#)
[Logout](#)

Lock Audits - Select Dates

Tips:

Please select the report criteria.

Start Date

February, 2010

February 2010

Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6
7	8	9	10	11	12	13

Today: 2/12/2010

End Date

February, 2010

February 2010

Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6
7	8	9	10	11	12	13

Today: 2/12/2010

1. Select the Start Date and End Date for the criteria.

M3550 ©Kaba Ilco Inc., all rights reserved.

Rev. 9/14

Pg. 25

Reports

Resident Access Staff Access Key Readback Key Cancellation Lock Action Lock Admin Reports Accounts Home About Logout

Lock Audits - Select Employee

Start date: 02/11/2010 09:24:00 AM End date: 02/12/2010 09:24:59 AM

Select Employee

Search

- Installer
 - kaba1, kaba1
 - kaba2, kaba2
- Maintenance
 - Davis, Gina
 - Logan, Brooke
 - Morgan, Jason
 - Savard, Dan
 - Smith, Lois
 - Spencer, Bill
- Hydro

Find First Find Next

Previous Next

2. Find and select the employee key for your report criteria.

Reports

Resident Access Staff Access Key Readback Key Cancellation Lock Action Lock Admin Reports Accounts Home About Logout

Lock Audits - Select Unit

Start date: 02/11/2010 09:24:00 AM End date: 02/12/2010 09:24:59 AM

Employee: [Empty field]

Select Unit

Search

- Building 1
 - floor 1
 - floor 2
 - 200
 - 201
 - 202
 - 203
 - 204
 - 205
 - Bar
 - Pool
 - Spa
 - staff gym
 - staff lockers

Find First Find Next

Previous Next

3. Select the Floor and Unit.

Reports

Resident Access
Staff Access
Key Readback
Key Cancellation
Lock Action
Lock Admin
Reports
Accounts
Home
About
Logout

Lock Audits - Select Key Holder

Tips:

Please select the report criteria.

Start date

End date

Employee

Selected Unit

Select Key Holder

Search
x

- [-] Residents Group 1
 - Johnson, Christal
 - Knight, Owen**
 - Tenny, Carly
- [-] Residents Group 2
 - Barr, Patrick
 - Greene, Donna
 - Vierra, Carlos

4. Select the person who is assigned the key in question, then click **Preview**.

Lock Audits

G40 Demo for sales reps, training

Wednesday, February 17, 2010
3:16 PM

Parameters selected for this report:

From Date/Time: 02/01/2010 03:16:00 PM To Date/Time: 02/17/2010 03:16:59 PM

Operator Name: <A/> Room Name: <A/>

Keycard Holder: <A/>

* ST = Standard Time

Page 1 of 4

Date/Time	Keycard Type	Keycard Holder	Encoded by	Creation Date/Time	ID-Seq
<div style="border: 1px solid #ccc; padding: 5px; font-size: x-small;"> <p>Room Name: 100</p> <p>Room Type: Resident Unit</p> <p>Lock Type: RFID 79M/T/L/X/S</p> <p>Floor: Floor 01</p> <p>Area: -</p> <p>Group: -</p> <p>Section: -</p> <p>Zone: -</p> <p>LCB/Firmware: 11.00/1.14</p> <p>Battery Level: 4.24</p> <p>Audit Date/Time: 2/17/2010 3:15 PM</p> <p>Auditor: Savard, Daniel</p> <p>Audit Source: MUnit</p> </div>					
2/17/2010 3:14 PM	Programming	Davis, Gina	Savard, Daniel	02/17/2010 03:06 PM	26
2/17/2010 3:14 PM	Unlocked from Outside	-	-	N/A	0
2/17/2010 3:14 PM	Grand Master	Logan, Brooke	Savard, Daniel	02/17/2010 03:12 PM	30
2/17/2010 3:14 PM	Locked from Outside	-	-	N/A	0
2/17/2010 3:14 PM	Resident	Aston, Ned	Savard, Daniel	02/17/2010 03:13 PM	210
2/17/2010 3:14 PM	Unlocked from Outside	-	-	N/A	0

5. The Preview shows the report information, which can be exported and printed.

Operator List

1. Determine what level of operators are to be listed, then click **Preview**.

Operator	Login Name	Access Level
Savard, Dan	1	KABA Tech Support
Logan, Brooke	4	Access Control Administrator
kaba1, kaba1	kaba1	KABA Tech Support
kaba2, kaba2	kaba2	KABA Tech Support

3. The Preview shows the report information, which can be exported and printed.

RezShield™ Operator Levels

RESIDENT SERVICE ATTENDANT	RESIDENT SERVICES MANAGER	MAINTENANCE ENGINEERING	SERVICE	IT ADMIN	MASTER	ACCESS CONTROL ADMIN	KABA TECHNICAL SUPPORT

Resident Services Attendant

The RSA works at the front desk and deals primarily with registering and making Resident keys and reading back resident keys. Grants access to screens of the RSA level tasks.

RSA Functions Available

Resident Access	Staff Access	Key Readback	Cancel Key	Lock Action	Lock Admin	Reports	Accounts
Make all types of Resident keys	No	Readback all types of Resident keys	No	Make Battery Test key	No	No	Able to change their own password and other information

Resident Services Manager

The RSM supervises the Front Desk activities. Grants access to all the same functions as the RSA. Additionally, under *Lock Action*, this level grants rights to Make Passage and Reset Passage keycards for Meeting Rooms and amenities as well as Battery Test Keycards. In addition, staff access to meeting rooms is also available by using the Meeting Room and Reset Meeting keycards which do not provide access to amenities and do not activate Passage. Under *Reports*, accesses System activities Report for Keycard Encoding and Keycard Verification operation types.

RSA Functions Available

Resident Access	Staff Access	Key Readback	Cancel Key	Lock Action	Lock Admin	Reports	Accounts
Make all types of Resident keys	No	Readback all types of Resident keys	Cancel all types of Resident keys	Make Battery Test Key, make Passage and Reset Passage keys for Amenties, Staff common area, Restricted area, Meeting room	No	System Activities report for Key Encoding and Key Verification	Able to change their own password and other information and also Add Residents

Maintenance / Engineering

The Maintenance person for the property is responsible mainly for programming and auditing locks. This Operator level grants access to all the functions related to programming/auditing locks, including the creation of Initialization and Programming keycards.

Maintenance Functions Available

Resident Access	Staff Access	Key Readback	Cancel Key	Lock Action	Lock Admin	Reports	Accounts
No	No	Only readback cancel keys	Make all types of Cancel and Rest Keys	Make all types of Lock action keys	Create and Transfer Lock files and Audit Files	All reports	Able to change their own password and other information

Services

The Service level allows only the creation of the Services access key. This key permits Service access to all rooms (except Restricted Areas, Common Areas and Locked Out rooms) on a particular time shift. Under the *Staff* menu, it grants access only to Make and Verify keycard menu.

Service Functions Available

Resident Access	Staff Access	Key Readback	Cancel Key	Lock Action	Lock Admin	Reports	Accounts
No	Make Only Services key	Readback Services key and Cancel Service Key	Can Only make Reset Service Key	No	No	No	Able to change their own password and other information

IT Administrator

Refer to *Network & Hardware Setup, PK3065 02/06*.

IT Administrator can only access Network and Hardware Setup. They can add and remove Encoders and IPM's.

Master

Grants access to **all functions of RezShield™**. Intended for the highest level of user System Administrator/Property Configuration.

Master Functions Available

Resident Access	Staff Access	Key Readback	Cancel Key	Lock Action	Lock Admin	Reports	Accounts
Make all types of Resident keys	Make all types of Staff keys	Readback all types of Resident and Staff Access Keys	Make all types of Cancel and Rest Keys	Make all types of Lock action keys	Create and Transfer Lock files and Audit Files	All reports	Able to change their information, add/edit residents and staff

Access Control Administrator

Grants access to **all functions of RezShield™**. This level grants you COMPLETE SYSTEM RIGHTS. Intended for the highest level of user System Administrator/Property Configuration.

Access Control Administrator Functions Available

Resident Access	Staff Access	Key Readback	Cancel Key	Lock Action	Lock Admin	Reports	Accounts
Make all types of Resident keys	Make all types of Staff keys	Readback all types of Resident and Staff Access Keys	Make all types of Cancel and Rest Keys	Make all types of Lock action keys.	Create and Transfer Lock files and Audit Files	All reports	Able to change their information, add/edit residents and staff

KABA Technical Support

This level is only available to KABA technical support personnel for troubleshooting advanced configuration and application issues.

List of Keycard Types & Functions

Adjoining Suite

Keycards for a combination of up to 15 individual units or rooms, within a *15 room number range*. All the encoded keycards work in all the locks of the suite.

Area

A submaster level keycard. The Submaster levels (Section, Floor, Group, Zone and Area) are used for access by staff (e.g. management, maintenance workers, laundry, etc.)

Battery Test

Prompts a low battery indicator in locks where the battery is below acceptable voltage. Battery Test keycard does not give access to the door.

Common Door Suite

Suites with a common door where the rooms inside (up to eight inner doors) can be rented separately or together. Each keycard opens the common door and at least one and up to eight inner doors.

Emergency

The Emergency keycard can open ANY door in ANY situation, if the lock is working properly; overrides deadbolt or privacy lock, as well as Unit, Property and Salesman's Lockouts.

Floor

A submaster level keycard granting access to the units on a floor or floors. The Submaster levels (Section, Floor, Group, Zone and Area) are used for access by staff (e.g. management, maintenance workers, laundry, etc.)

Grand Master

Opens every unit and room on the property, except Restricted Areas or rooms that have been locked out using the deadbolt or privacy lock, the Salesman's Lockout, Unit Lockout or Property Lockout. The Grand Master keycard opens all Common Area/Amenity doors.

Group

A submaster level keycard. The Submaster levels (Section, Floor, Group, Zone and Area) are used for access by staff (e.g. management, maintenance workers, laundry, etc.)

Group Lockout

Locks out a group of units according to the Group submaster address in the lock. Group addresses are usually assigned according to the duties of each building supervisor. Group lockout is used after inspecting a unit after a resident has moved out and after the unit has been cleaned, so that the previous resident cannot enter.

Initialization

Initializes the lock during a first-time installation, or after an interruption of battery power (e.g. during a battery replacement, or whenever the battery power is temporarily disconnected).

Meeting Room

Provides access to meeting room with passage mode not available. The keycard does not provide access to Amenities and is valid for a period of 24 hours by default. This keycard is used for access by staff.

Meeting Room Reset

Used to invalidate any circulating Meeting Room keycard for a specific meeting room door. Keycards encoded before the Reset keycard was encoded will not work in the locks.

One-Shot

Opens a specific room only once, for use by maintenance or an external vendor, contractor, etc.

Passage

Puts the lock in Passage mode, in which a keycard is no longer required to open the door. Passage mode is removed by re-inserting the Passage keycard. Typically, rooms such as Staff Common Areas/Amenities and Meeting rooms are appropriate for the use of Passage mode. Temporary or rented units should *not* be put in Passage mode.

Passage Mode Reset

Used to invalidate any circulating Passage keycards for a specific door. Does not cause the lock to revert to normal mode from Passage mode. Keycards encoded before the Reset keycard was encoded will not work in the locks.

Programming

Prepares the lock for communication with the M-Unit.

Property Lockout

Locks out all but the Emergency keycard. The locks remain locked-out until unlocked by a Property Unlock keycard.

Property Restart

Used to set or change the Property Code when installing the RezShield™ system, or if a severe security problem has occurred.

Property Unlock

Unlocks any unit locked by the Property Lockout or Unit Lockout keycard.

Resident

Gives residents access to specified room/s with specified options for defined time period.

Resident Reset

Invalidate the corresponding Unit entry keycard. The Reset keycard must be inserted in all locks leading to the specified resident unit. Entry keycards encoded before the Reset keycard was encoded will not work in the lock. Keycards encoded before the Reset keycard was encoded will not work in the locks.

Restricted Area

This keycard is intended for rooms that do not fit into the normal master-keyed structure e.g. GM office, computer room, liquor storage areas. Locks programmed as Restricted Area doors accept only two types of entry keycards: Restricted Area and Emergency.

Section

A Submaster level (Section, Floor, Group, Zone and Area) are used for access by staff (e.g. housekeepers and housekeeper managers, maintenance workers, laundry, room service, etc.)

Service Master

Opens any guest room on the property, except for rooms that have been locked out using the deadbolt or Salesman's Lockout as many times as required

Test Lock

Used by the lock installers to access Units and rooms during the installation of the locks. Test Lock keycards do not work after a lock has been programmed.

Unit Lockout

Locks out all but the Emergency keycard. The Room Lockout keycard is valid for a specified room. The lock remains locked-out until unlocked by a Unit or Property Unlock keycard.

Unit Unlock

Unlocks a specified unit locked-out by a Unit Lockout keycard.

Zone

A Submaster levels (Section, Floor, Group, Zone and Area) are used for access by staff (e.g. management, maintenance workers, laundry, etc.)

Lock Audit

Emergency Reset

Passage – Amenity

Passage – Meeting Room

Passage – Staff Common Area

Glossary

Access Point	Points of entry and exit such as Resident Room, Gym, Garage, Door etc.
Audit Trail	Audit trail determines which keycard was used, when an access occurred, who owned the keycard at the time of access and what action was performed. Use-history stored in the lock's non-volatile memory. Displayed in the RezShield software in order of most recent event.
Credential	Keycard, fob, or wristband programmed to store access information and grant entry for a designated period of time.
Disability Option	Changes the time delay during which the door is unlocked after a valid resident level keycard is presented to the lock. The time delay changes from 4 seconds to 15 seconds, to assist residents who may have difficulty turning the handle.
Encoder	The device used to write information on the keycard (encode) or to read information from the keycard (audit).
Encryption	All the data that is written on the keycards is encrypted and can only be read by the RezShield software. Also each Resident property will have its own encrypted code to prohibit keycards of working from one property to another.
Hotsync	A transfer or back-up of data between a hand-held unit and a desktop computer through a serial port or USB connection.
IPM	The Infrared Programming Module sits over the reader on the door lock to receive data transmitted from the M-Unit. The infrared receiver and transmitter on the M-Unit are aligned with the IrDA window (the small red glass window) on the IPM and data is transmitted from the M-Unit to the lock via the IPM or from the lock to the M-Unit via the IPM – in the case of an audit.
MIFARE	Type of technology used for contactless smart card systems. MIFARE is compliant with the international ISO 14443 Type A standard.
M-Unit	A handheld computer containing the RezShield M-Unit software downloaded from the CD. The M-Unit is used to program and audit locks and card readers.
RAC	Remote access controller is the device to secure common access and perimeter doors such as access to elevators, parking, and other electrically- operated doors –as well as doors requiring an electric strike or electromagnetic lock.
RFID	Radio frequency identification - RezShield uses wireless RFID technology to encode keycards via a contactless encoder. The 79 lock uses RFID keycards and credentials.

Notes