KABA®

RezShield™ Multihousing Access Control

Property Administrator User Guide

Property Administrator

User Guide

_____

Table of Contents

Minimum Requirements

Server

OS – **32 Bit Windows XP PRO, Vista Business, Windows 7 Business, or Windows 2003 Server.**

(Windows 2008 Server not yet supported)

Software: NET Framework 2.0
Web Server - IIS (Internet Information Services)
Message Queuing

Backup Media: USB Memory stick
CD Writer, etc.

Network Transport Protocol: TCPIP.

Hardware: CPU – P4 or above
RAM – 1GB 2GB (recommended)
Hard Disk – 30 GB
CD ROM
USB Ports
Network Adapter
Standard Monitor

Important: The server must be on the properties network with a static IP address. Though it may not be required, a dedicated machine is recommended for optimum performance.

Workstations

OS - 32 Bit Windows XP PRO, Vista Business, Windows 7 Business

Software: IE 6.0 or above
NET Framework 2.0

Hardware: CPU – P4 or above
RAM -1GB (recommended)
Hard Disk – 30 GB
CD ROM
USB Ports
Network Adapter
Standard Monitor

Important: If there are workstations, the server must be on the property network with a static IP address. Windows Home is NOT suited for network applications.

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.
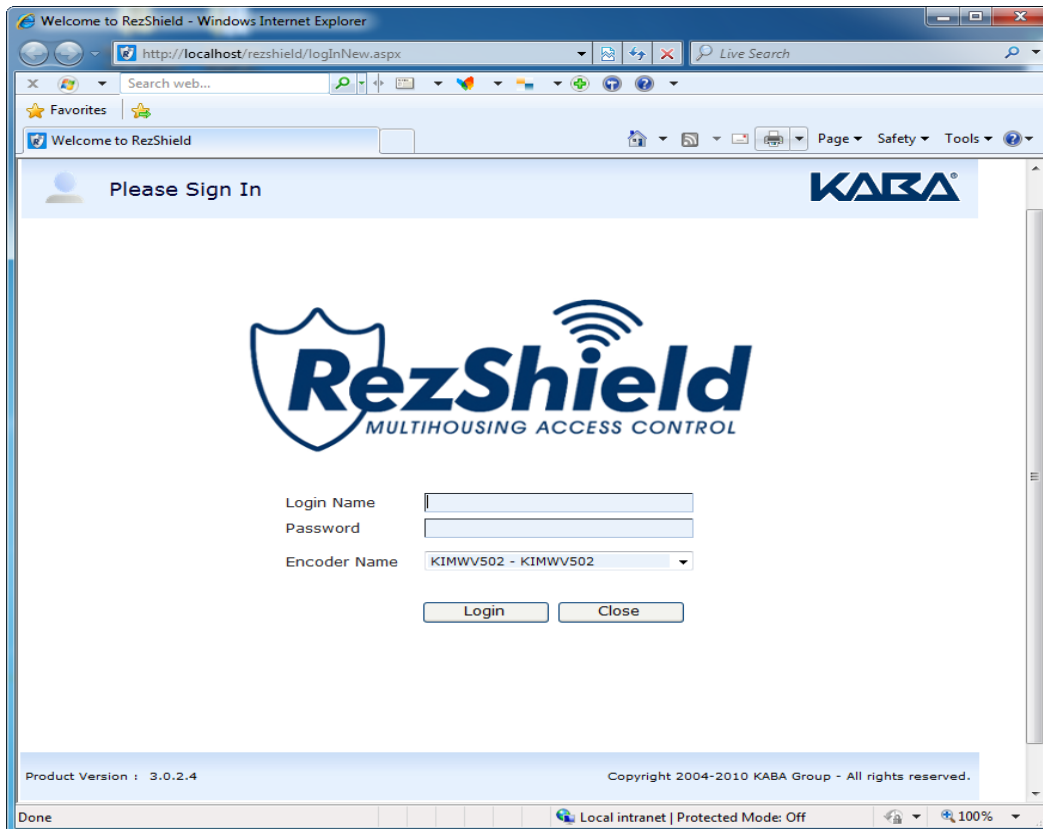
System Overview

- 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.
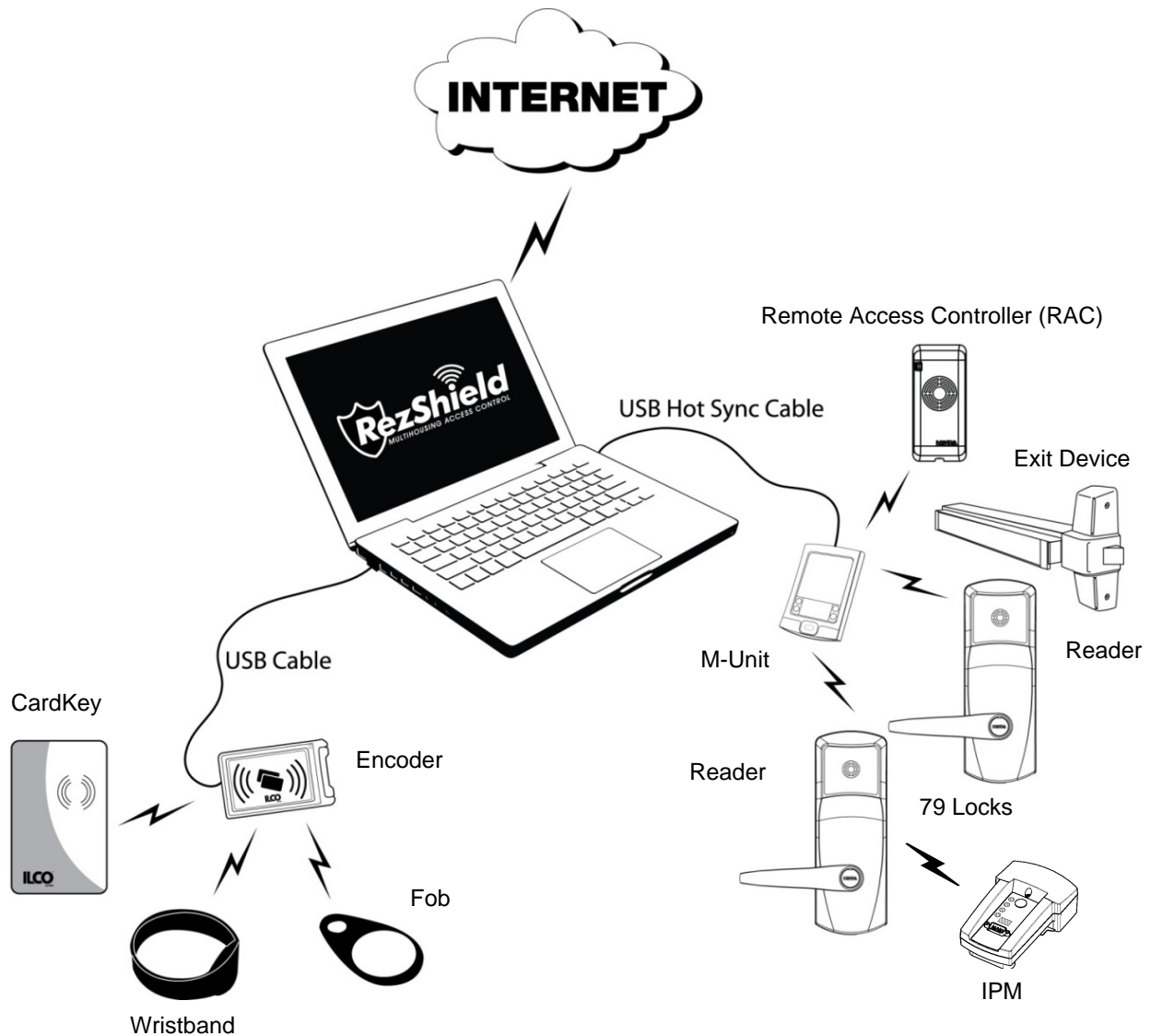
Logging on to the Application

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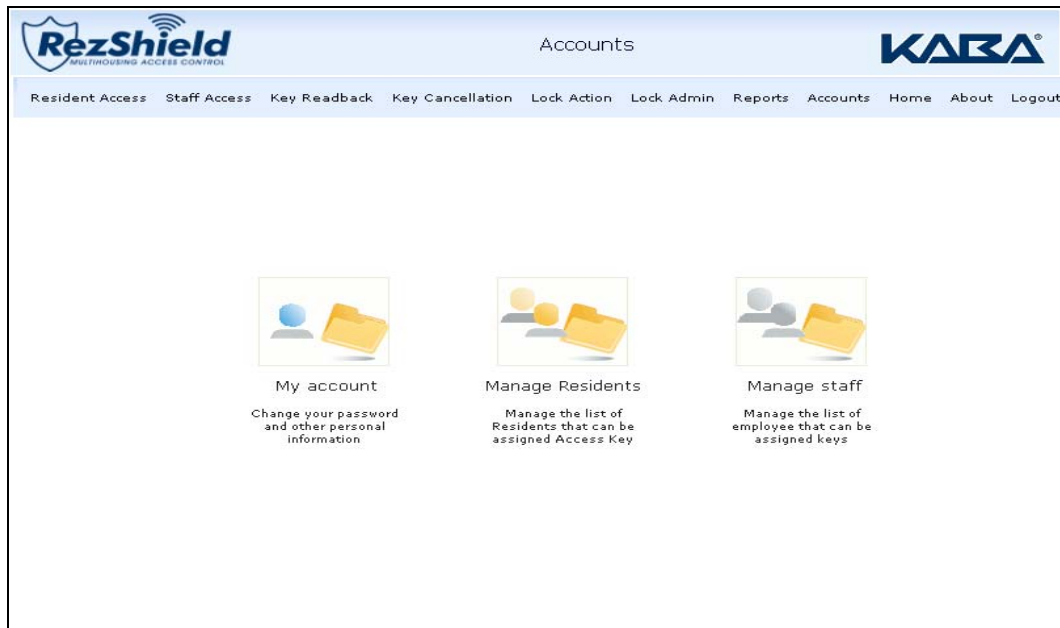
This is the section where you register and maintain the database listings of all residents and staff that have been issued key access to units and amenities on the property.

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
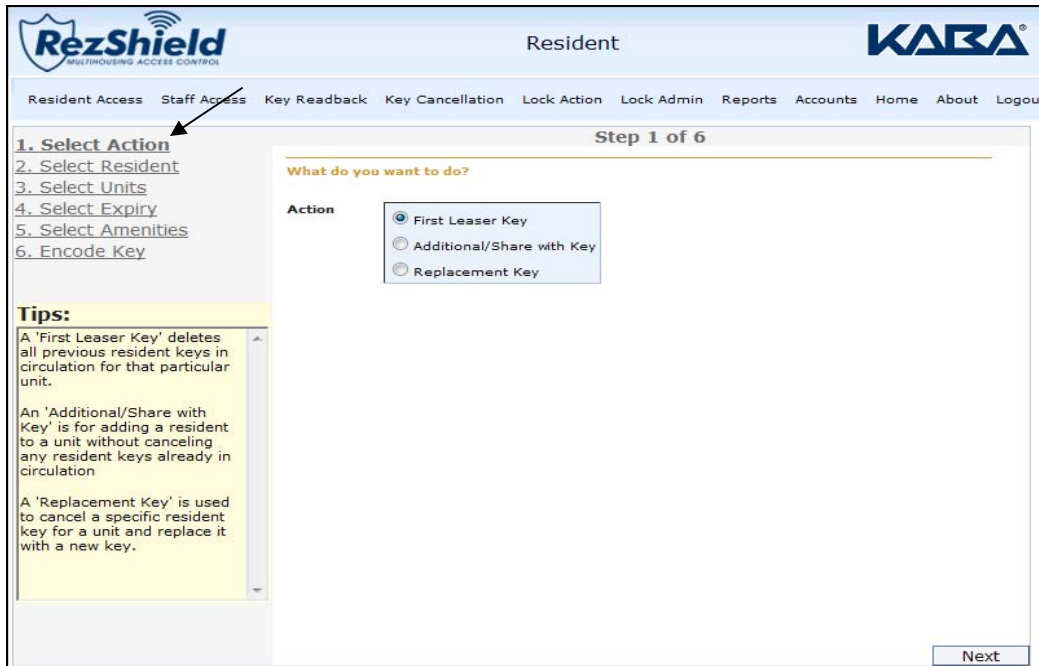
1. At the Select Action screen, choose the key type you are going to create then click **Next**.
Note: The "Tips" provide an explanation of the different key types/access options that can be created.
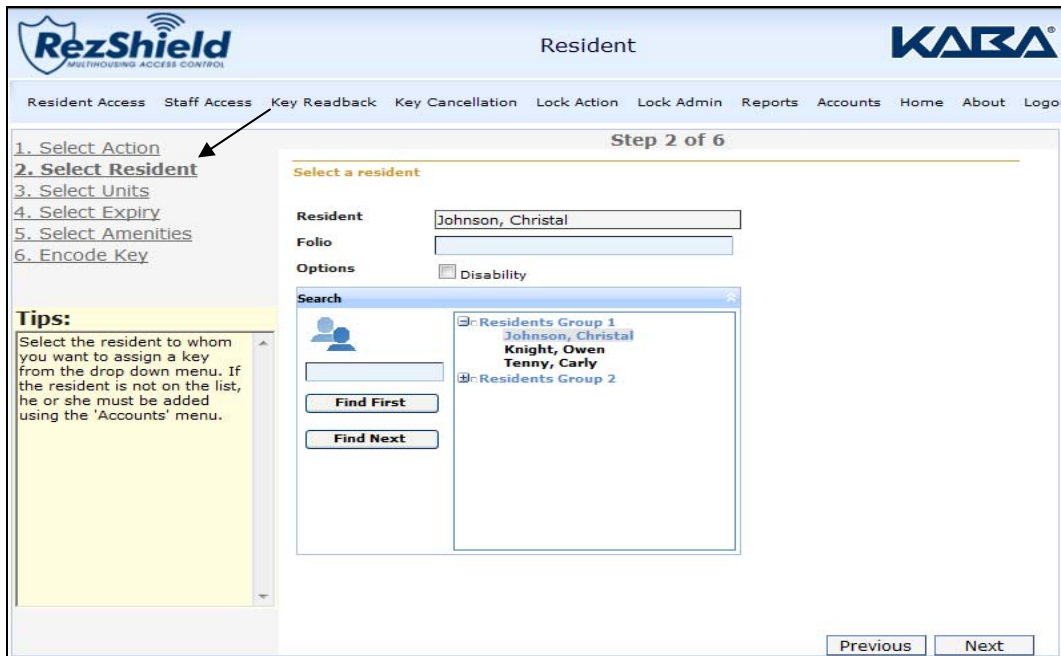
2. At the Select Resident screen, select the resident to whom you want to assign the key and click **Next**.
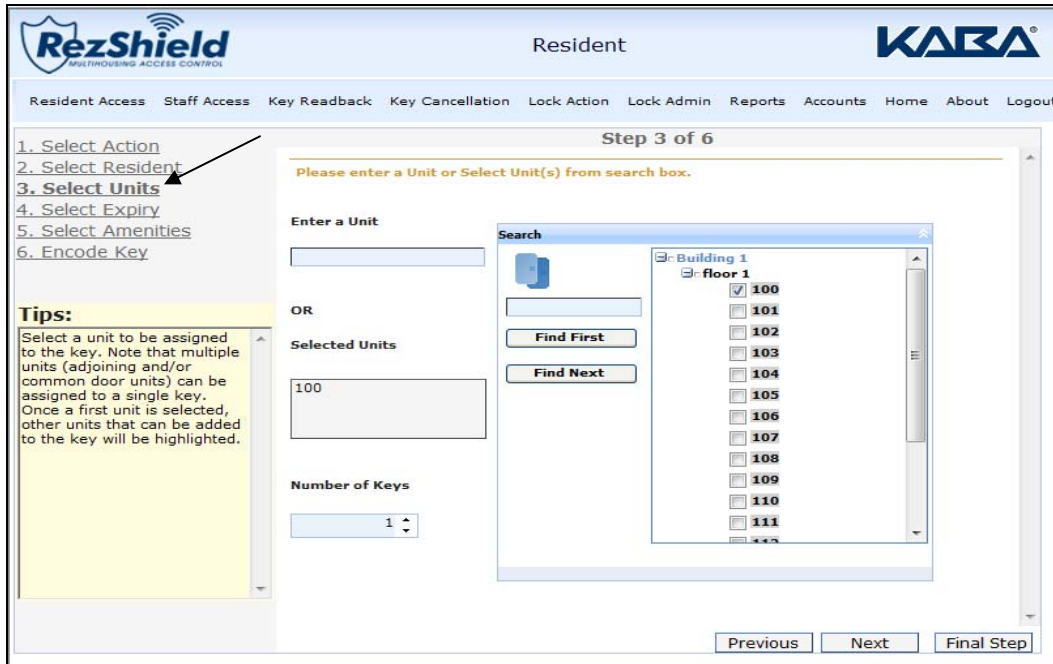
3. At the Select Units screen, select the Unit Number to which the key will be assigned.
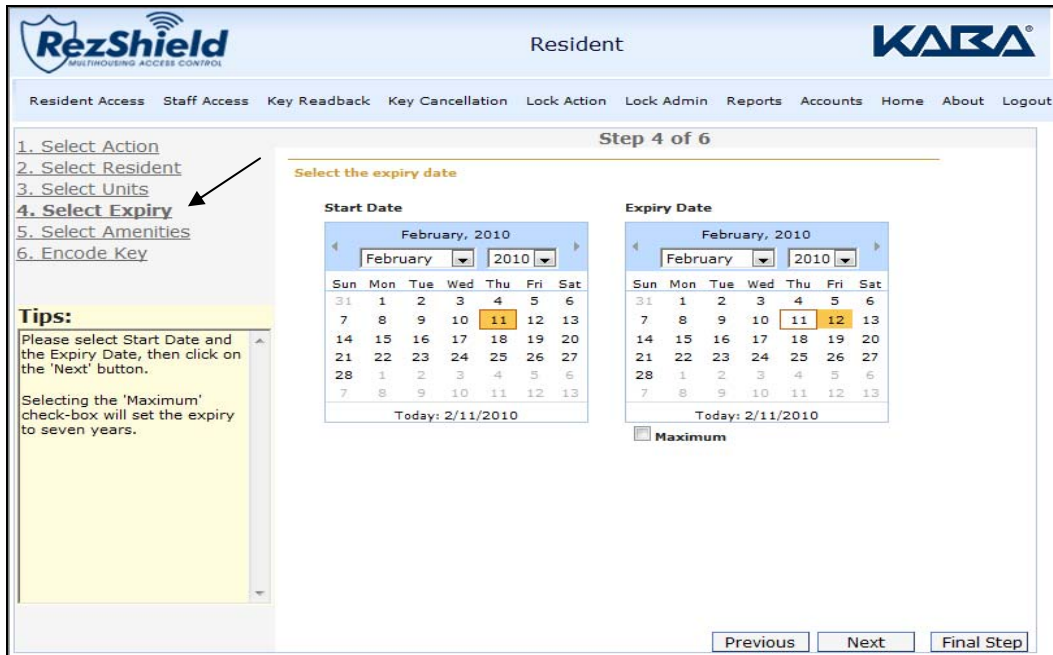
4. Next use the calendars to assign a Start Date and Expiry Date for the key. Click **Next**.

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.
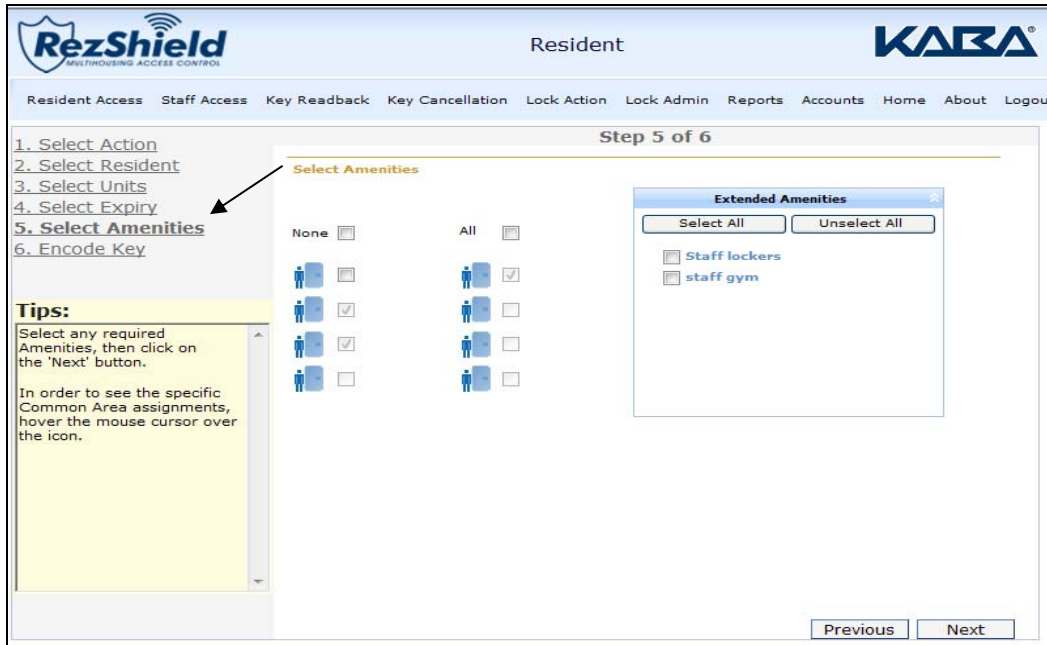
5. At the Select Amenities screen you may assign additional access points to the key. For example: dining hall, exercise room, parking or other extended amenities access.
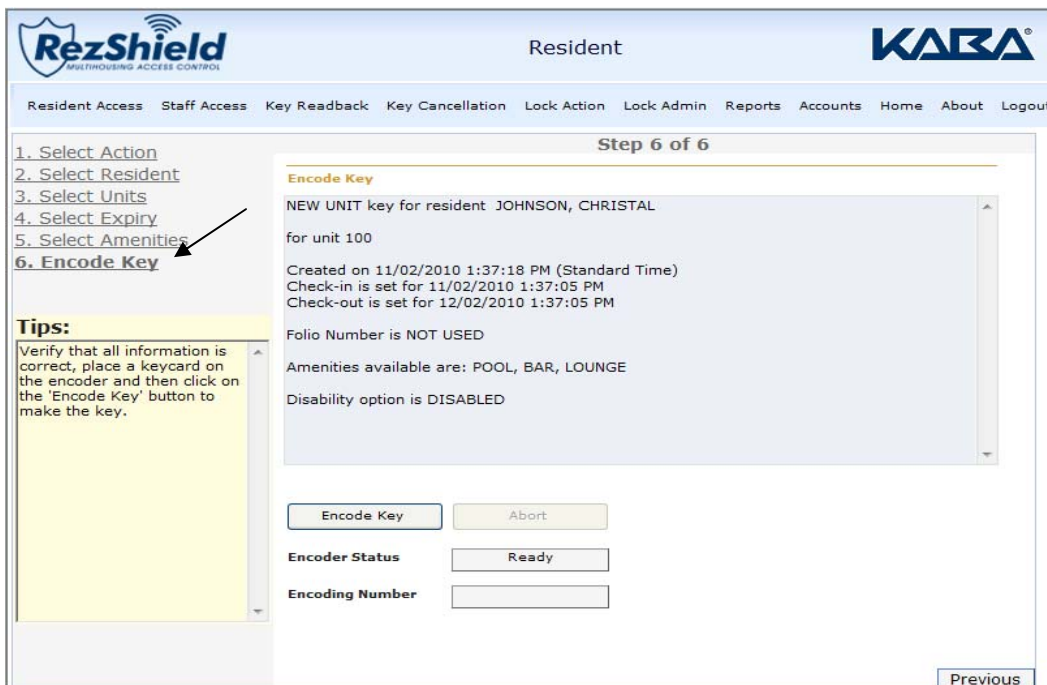
6. Now place the key onto the encoder and click **Encode Key** to program it.

3. Staff Access
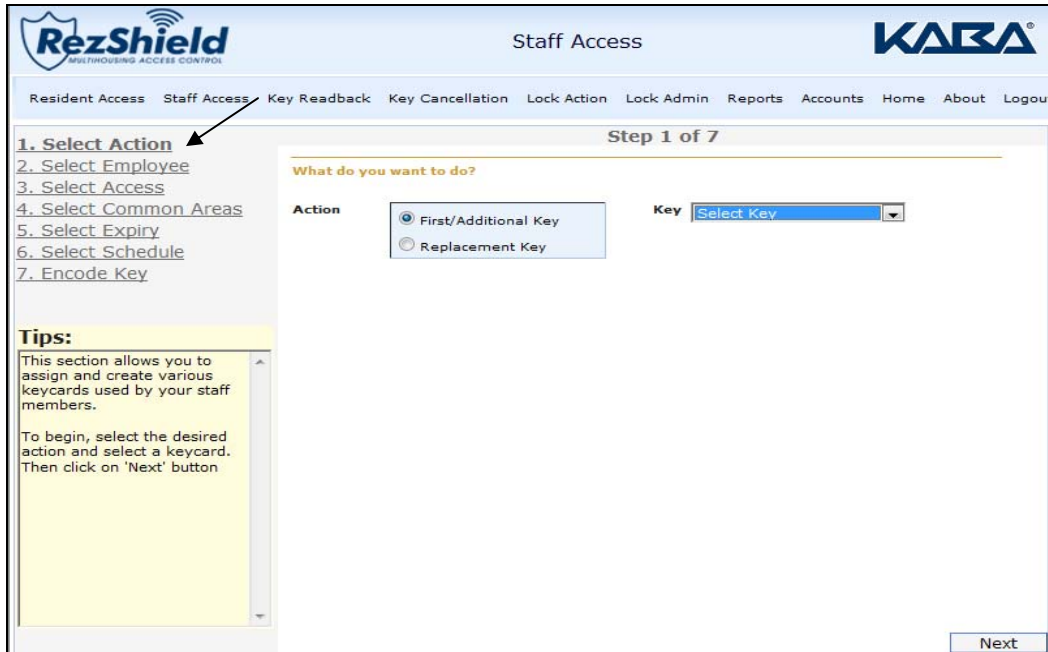
1. At the Select Action screen, click on the type of key you want to create. Next choose Select Key from the dropdown menu and then click **Next**.
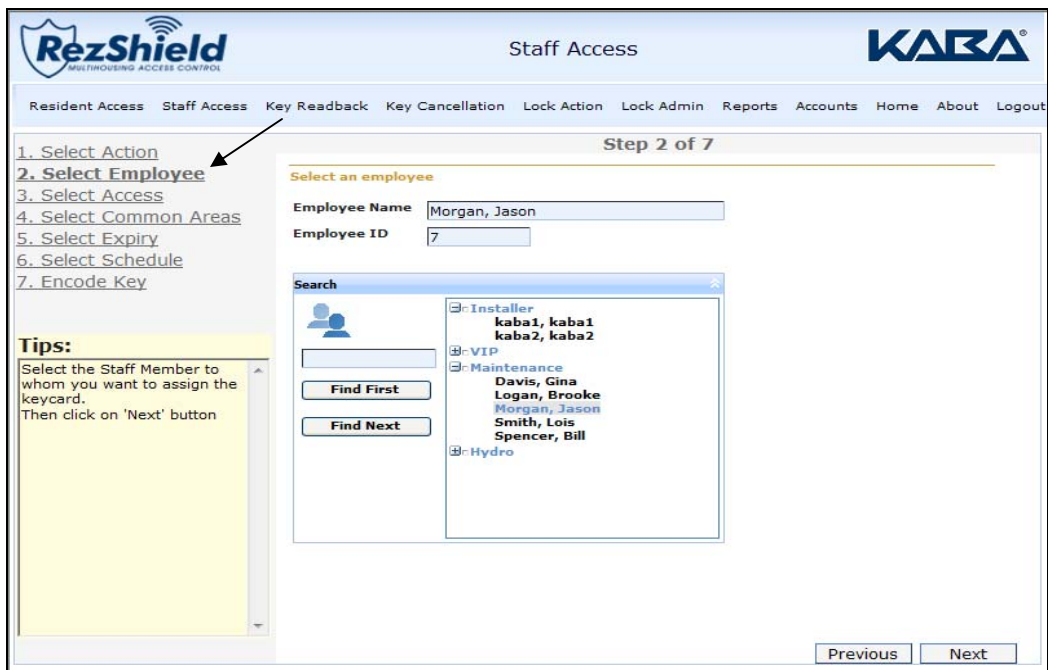
2. At the Select Employee screen, choose the employee or supplier for whom to create the key.
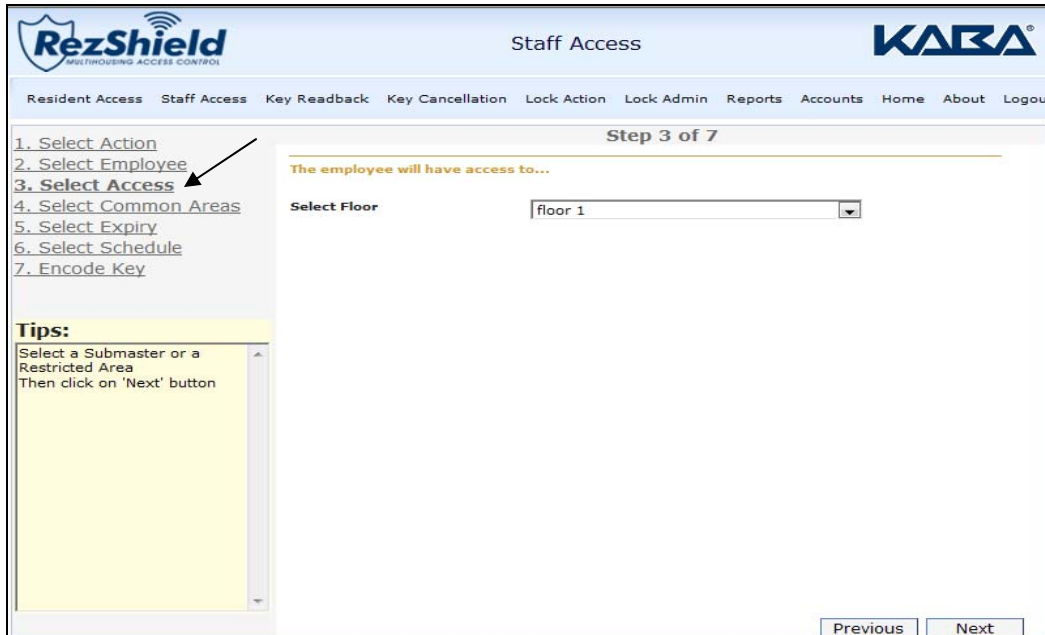
3. The Select Floor dropdown allows you to choose the floor(s) to which the employee will have access.
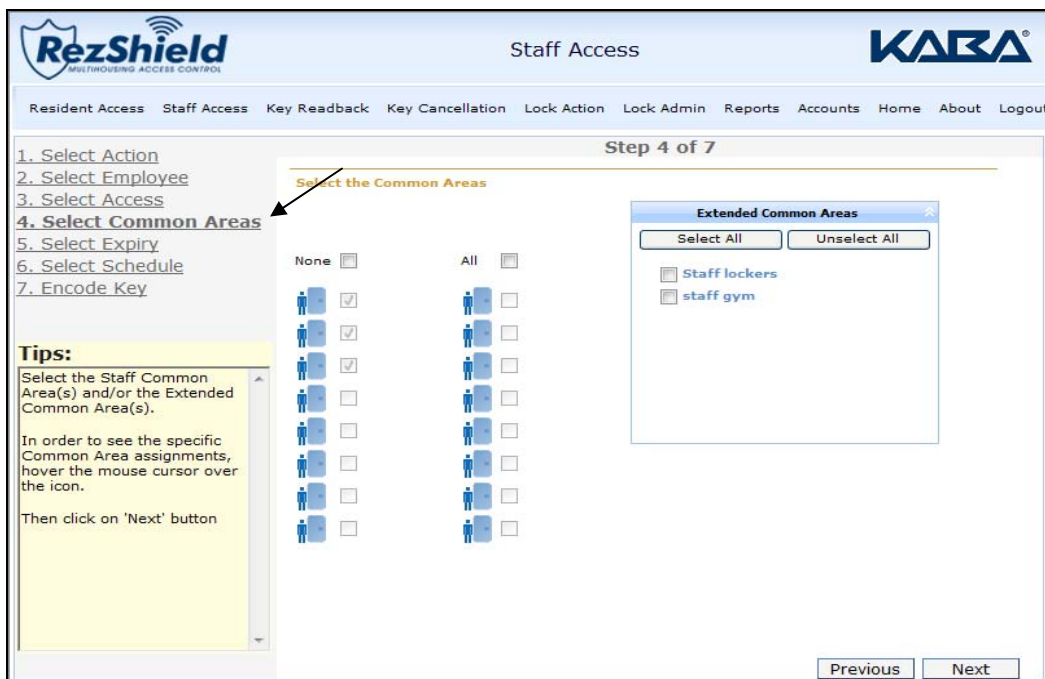
4. At the Select Amenities screen you may assign additional access points to the key. For example: dining hall, exercise room, parking or other extended amenities access.

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

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.
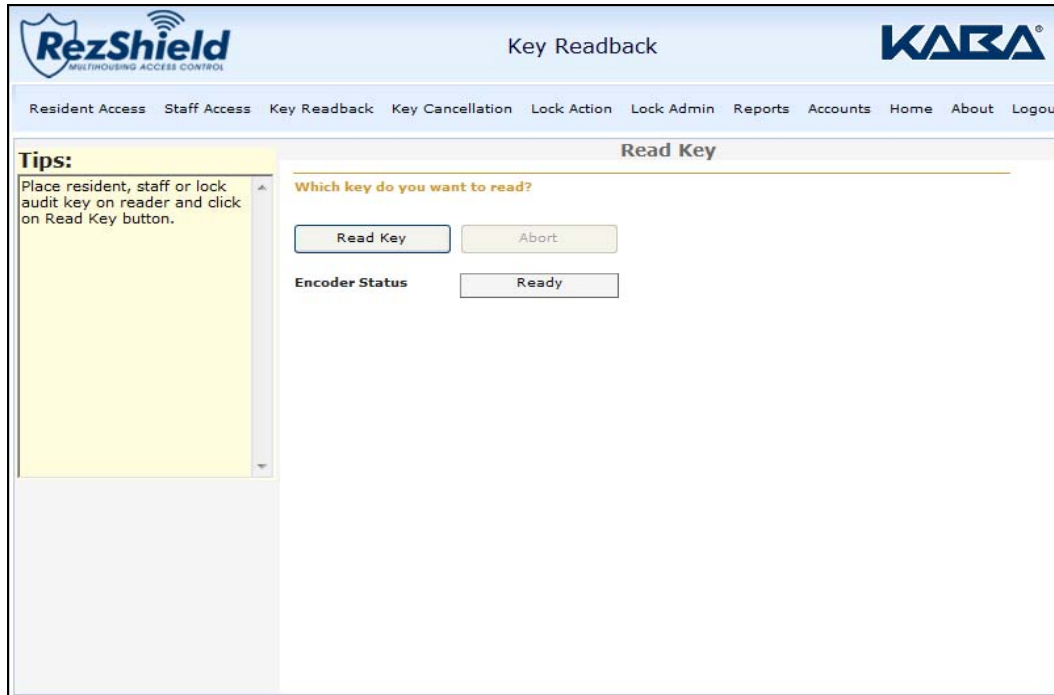
RezShield
MULTIHOUSING ACCESS CONTROL   Staff Access   KABA®

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

Step 7 of 7

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

Tips:
Click on 'Encode' to encode the key

Encode Key

DUPLICATE FLOOR key for employee MORGAN, JASON

for floor FLOOR 1

Created on 11/02/2010 1:46:36 PM (Standard Time)
Expiry is set for 11/02/2011 1:45:18 PM

Access to amenities is ENABLED

Staff Common Areas available: STAFF WASHROOMS, STAFF SPA, STAFF PARKING

Access during timezone NONE

Encode Key	Abort

Encoder Status   Ready

Encoding Number

Previous

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

4. Key Readback

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
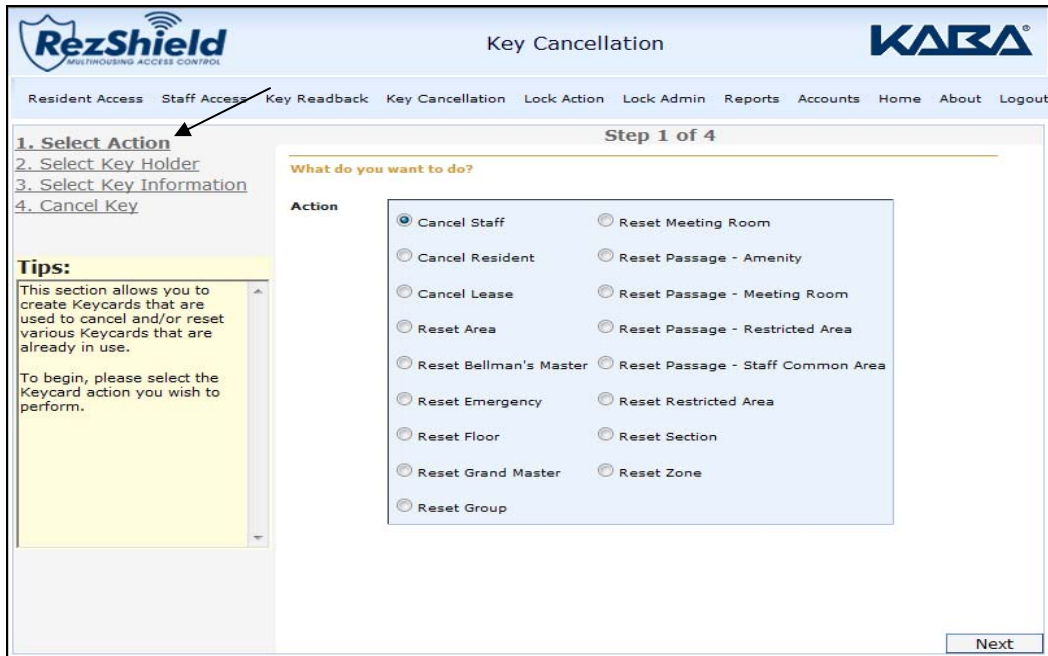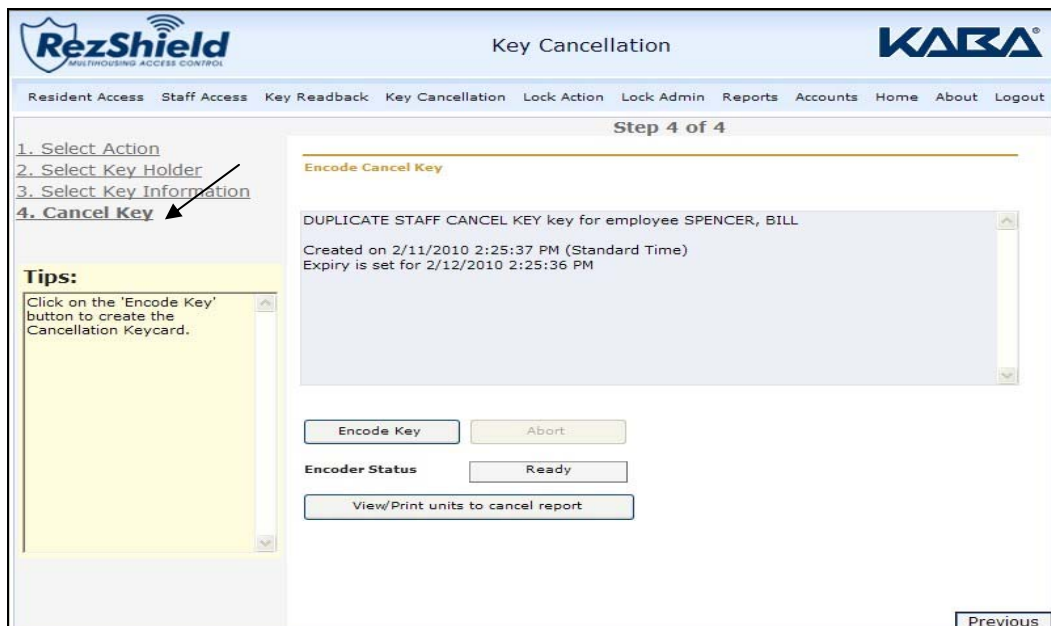
1. To cancel a key, first click on Select Action to select the key you want to cancel. Click **Next**.
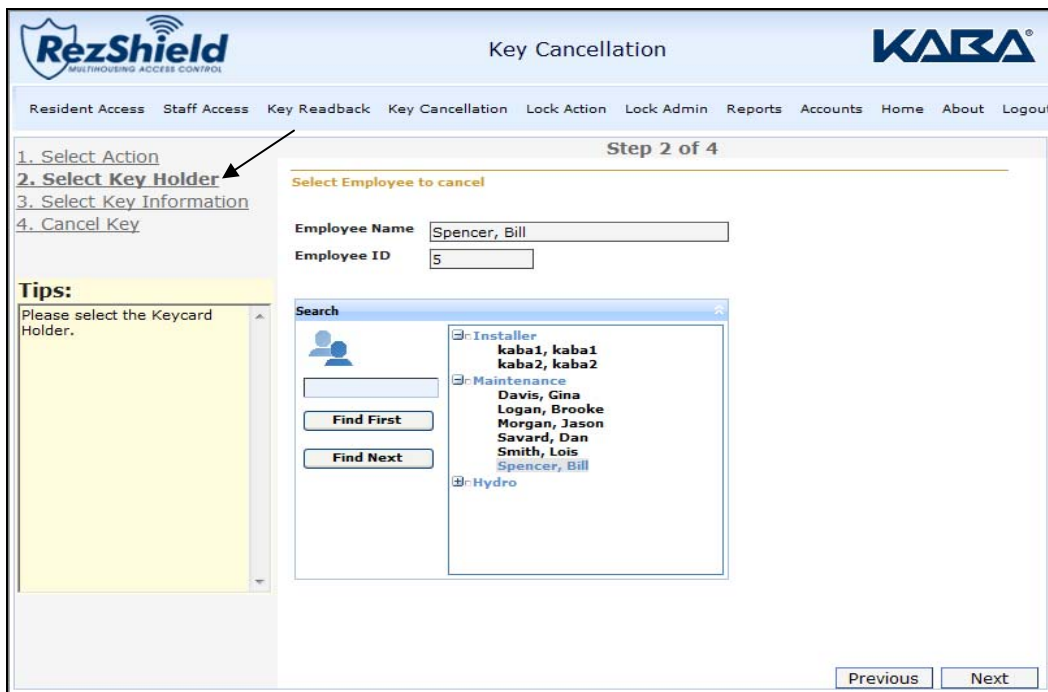
2. At the Select Key Holder screen, identify the individual to for whom the key has been programmed.

<div style="border:1px solid #000; padding:20px;">

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

</div>

3. Select Key Information.

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

6. Lock Actions
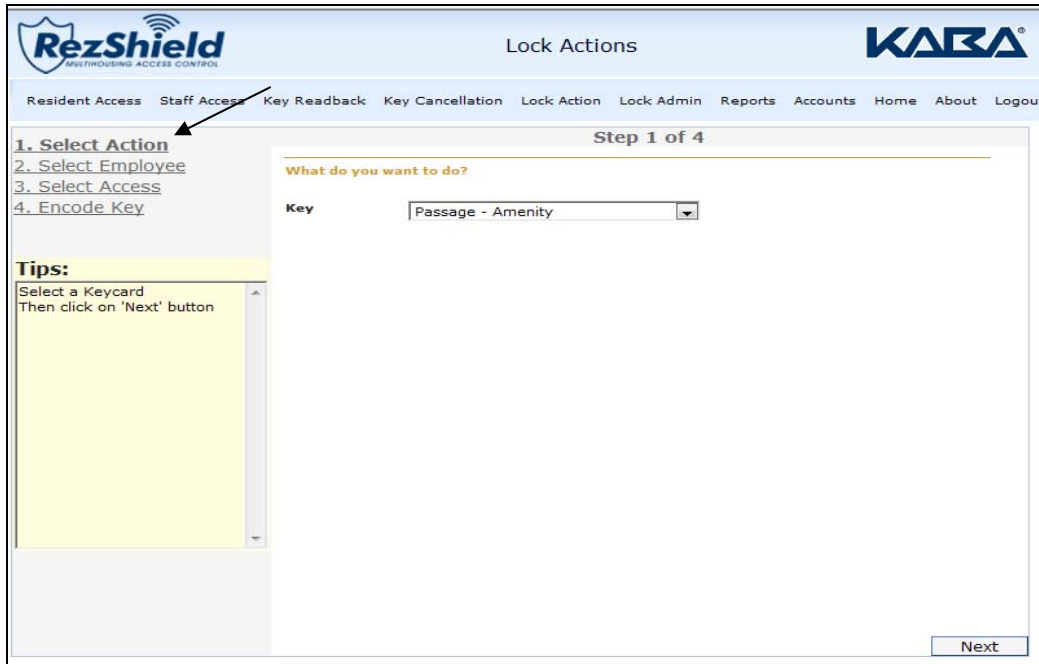
1. At the Select Action screen, select the type of key you want to create. Click **Next**.
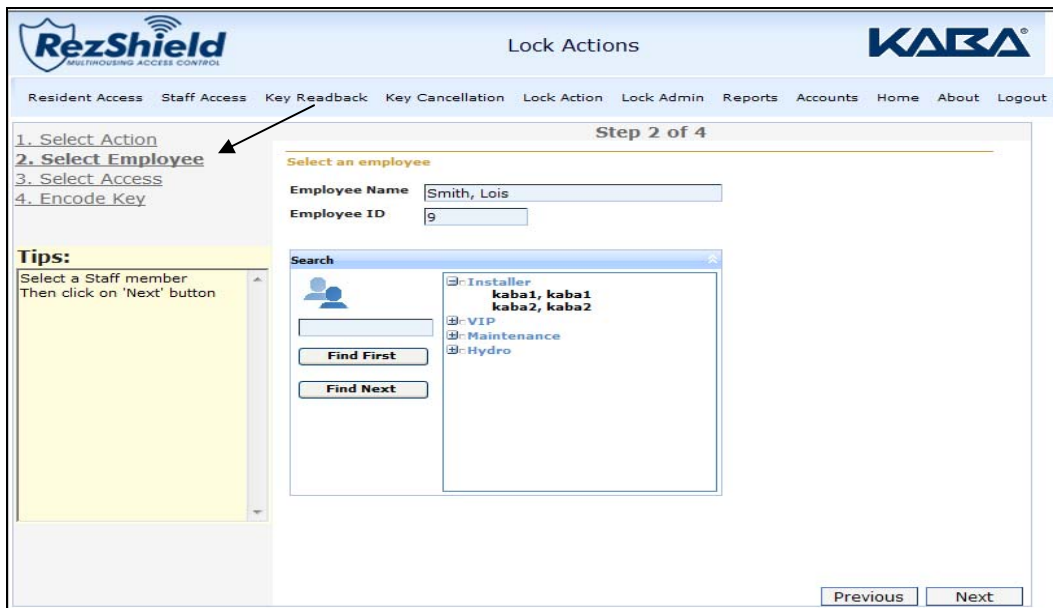
2. Then Select Employee and click **Next**.
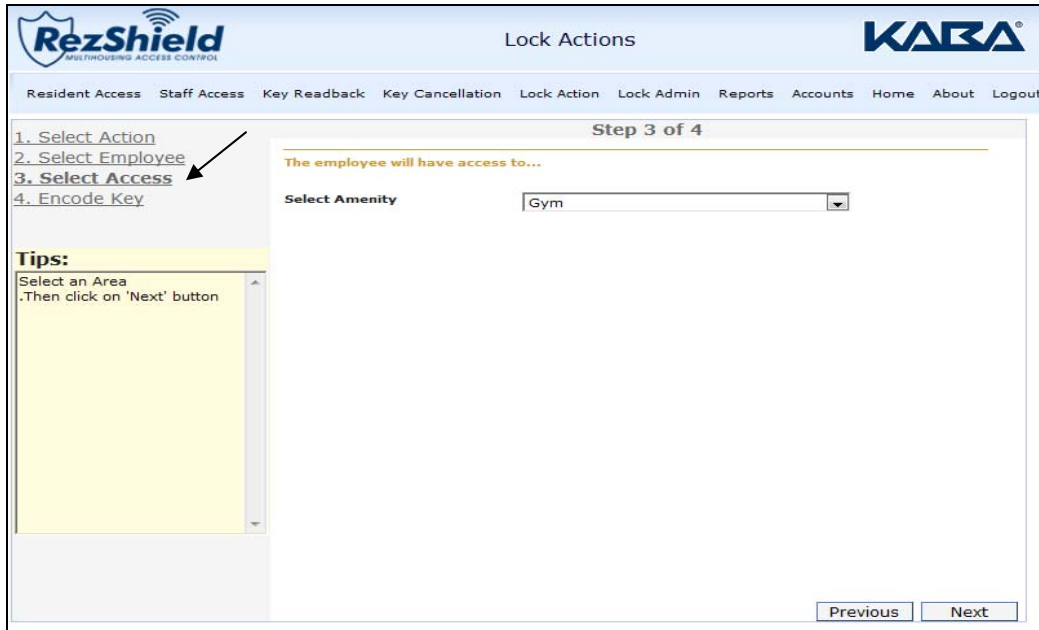
3. Select the access type for the key and click **Next**.
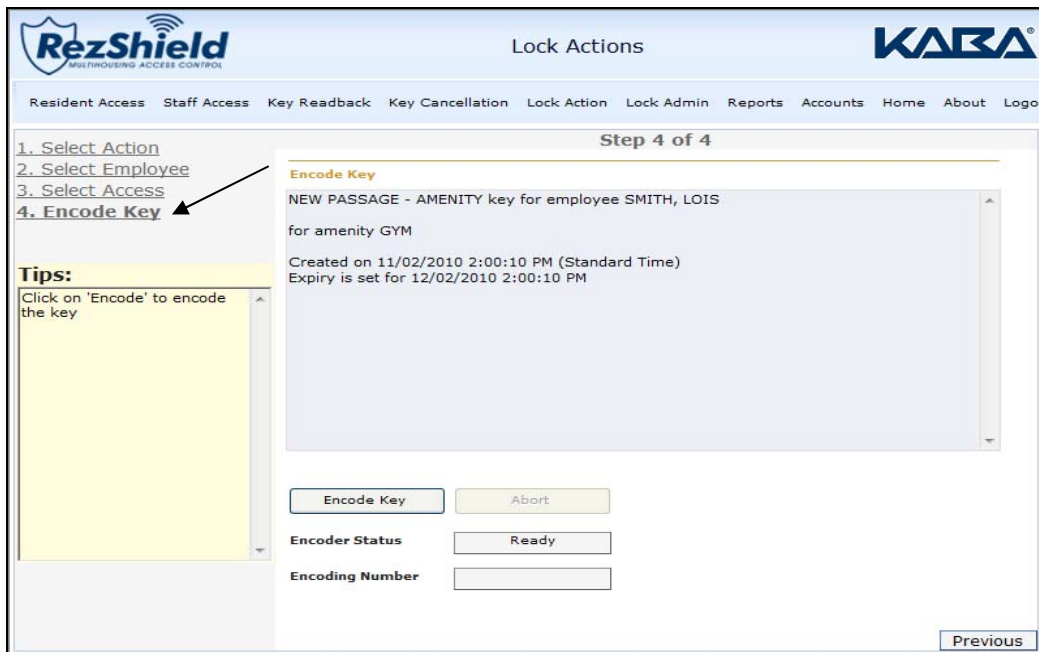
4. Place the key on the encoder and click **Encode Key** to cancel the key.

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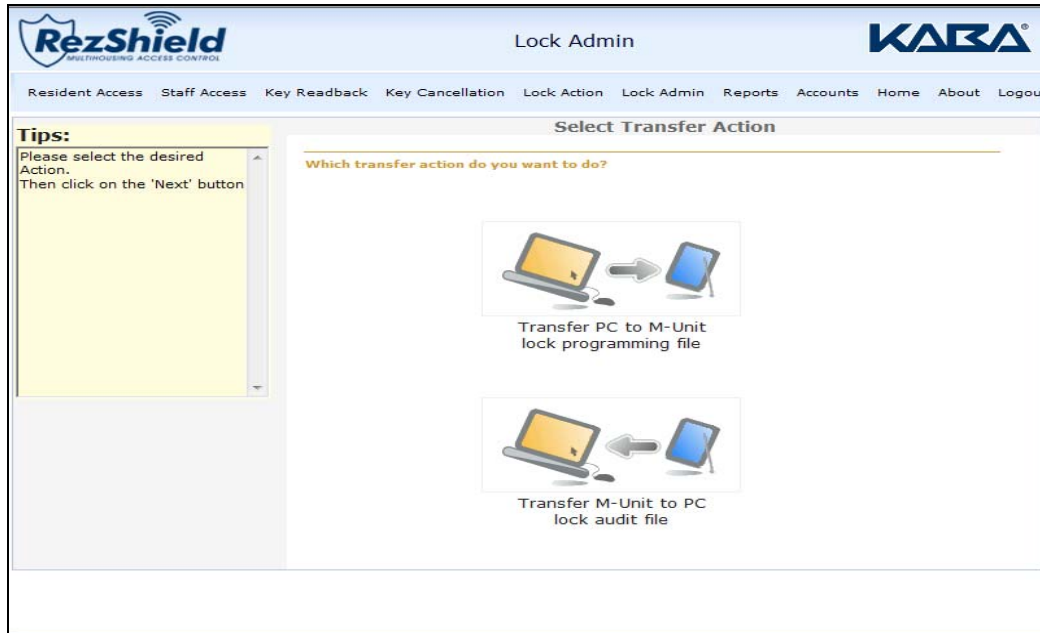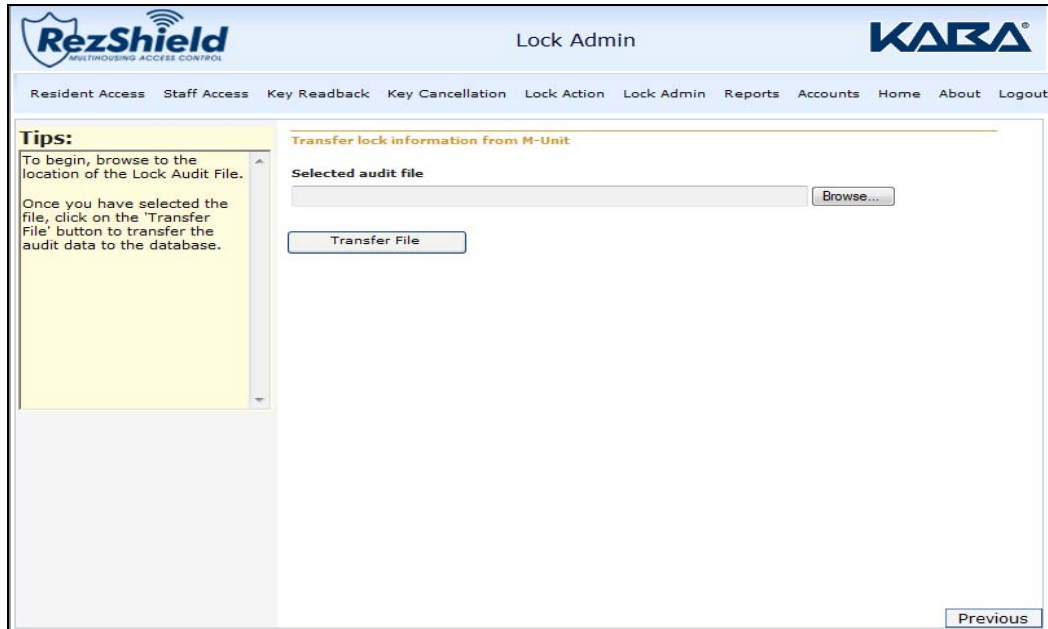
1. Select Transfer Action by clicking on the appropriate icon for the action you wish to perform.

Transferring Lock Configuration to the M-Unit
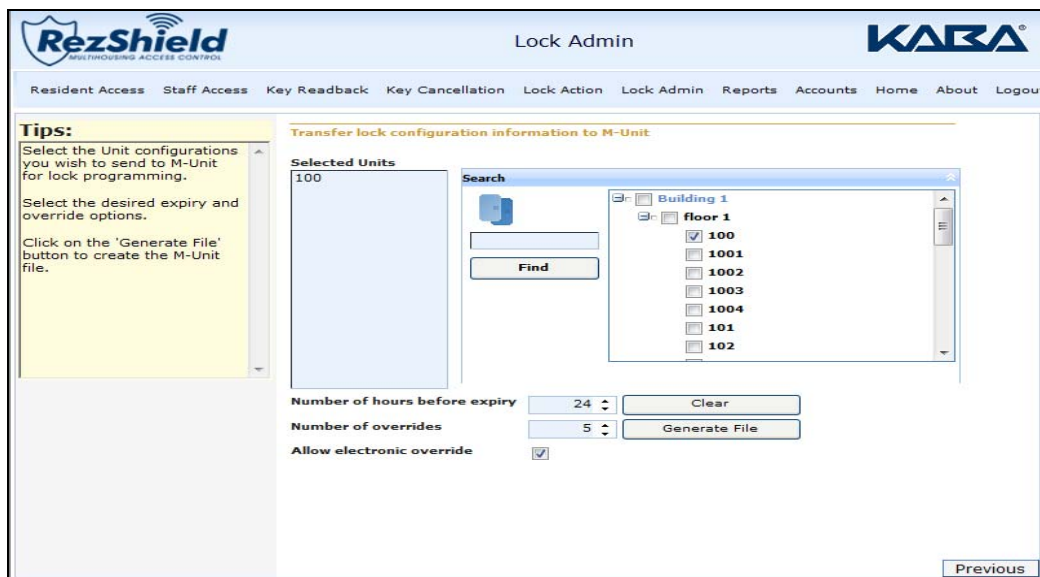
1. In the right hand box under the Search option, select the floor and unit to be transferred to the lock configuration.

2. The selected information will be displayed on the left side of the search box. Click **Generate File**.

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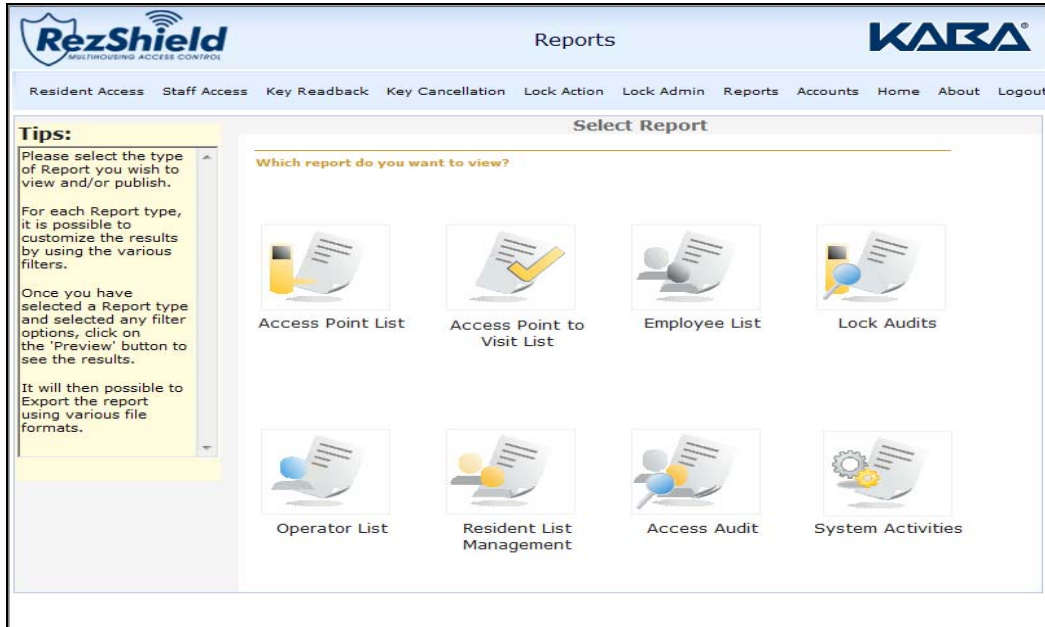
Access Point
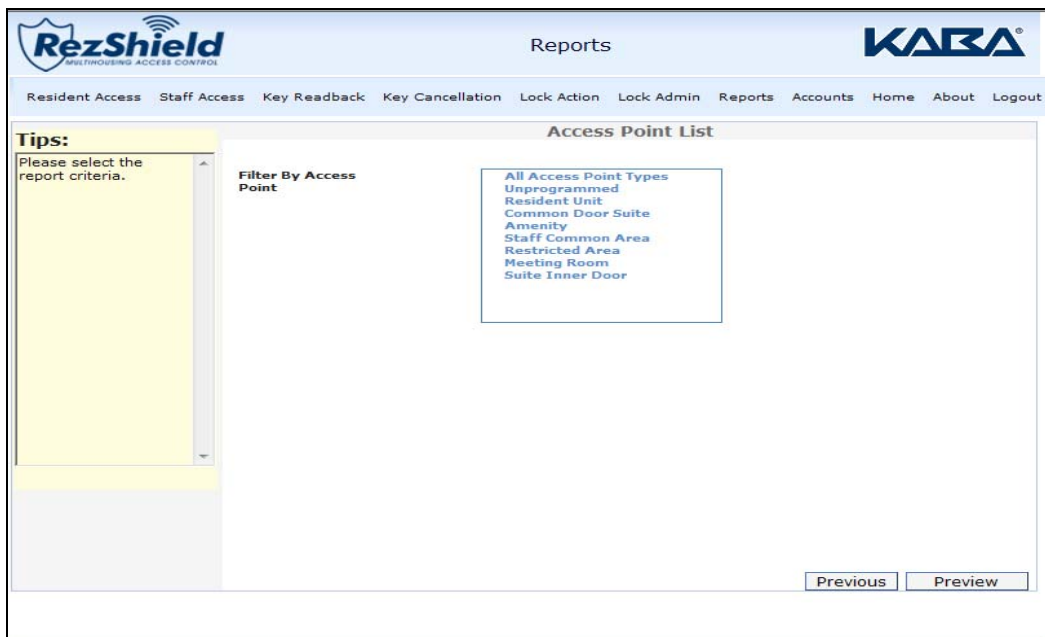
1. Determine the criteria for the report. Click to select it and press **Preview**.

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

Lock Audits

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

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

3. Select the Floor and Unit.

.

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

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**.

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

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

KABA ®