ENFORCER®

Bluetooth® Access Controllers

Installation Manual and Administrator Guide

No Codes to Remember
Intuitive, visual, app-based programming and management, up to 1,000 users, device options, etc.

No Cloud, No Internet Exposure
All data secured on device, set and monitored by the administrator

More Than Access
Can control doors, gates, lighting, machinery, etc.

Multiple User Types
Permanent, scheduled, temporary, number of times

Output Modes
Timed relock (1~1,800s), remain unlocked, remain locked, toggle, customizable for each users

Individual User Customization
Individually customizable output mode and time

Authorized User Monitor
Displays total number of users to guard against unauthorized additions

Multiple Ways to Open a Door or Device
Keypad*, proximity card/fob, or app

Hold Open (Passage)
Hold door open with code, card, or app (customizable)

Secure, Integrated Bluetooth
Passcode protected, AES128 encryption

Unlimited Devices
Access/manage an unlimited number of devices with one app

Easy Backup and Restore
For off-device storage, restoration, and replication of devices

Intuitive Device and User Names
Front Door, Finance Office, John Smith, Jane Doe, etc.

Downloadable Audit Trail
Last 1,000 events, searchable by user and event type

Multilingual App Interface
English, Spanish, French, Portuguese, German, Russian, Vietnamese, and Chinese (Traditional or Simplified)

*Depending on device

SLI™ SECO-LARM®

Introduction:

ENFORCER Bluetooth Access Controllers use fully integrated Bluetooth® wireless technology for streamlined setup and management as well as easy user access.

Table of Contents:

Introduction: **2**
Getting Started: **3**
Installation: **4**
Mounting *4*
Typical Wiring Diagram *4*
Bluetooth Post-Mount Keypad Wiring Diagram *5*
Sample Applications *6*
LED Indicators and Device Sounds: **8**
LED Indicators *8*
Keypad Sounds and LEDs *8*
IMPORTANT NOTES: **8**
Understanding the *SL Access* Home Screen: **9**
Logging In to Your Device: **10**
Understanding the ADMIN Setup Screen: **11**
Changing the ADMIN Passcode: **13**
Adding an ADMIN Proximity Card: **14**
Changing the Device Name: **15**
Settings to Enable/Disable: **16**
Enable/Disable the Door Sensor *16*
Enable/Disable the Key Sounds *16*
Global Output Mode: **17**
Setting the Output Mode (Global) *17*
Setting the Time for Timed Relock Mode: *18*
Understanding the Toggle Mode: **18**
Door Hold Open (Passage) **19**
Administrator *19*
User *19*
Business Hours **19**
Wrong Code/Card Lockout: **20**
Setting the Number of Wrong Codes/Cards *20*
Setting the Wrong-Code/Card Lockout Time *21*
Tamper Alarm: **22**
Enable and Select the Tamper Alarm Time *22*
Select the Tamper Alarm Sensitivity *23*
Auto Proximity Unlock: **24**
Setting the Auto Proximity Range *24*
Enable Auto Proximity Unlock *25*
Settings Screen Miscellaneous Items: **26**
Managing Users: **27**
Adding Users *27*
Viewing, Changing Settings, and Deleting a User *29*
Setting User Access Type *30*
Setting User Access Type – Visitors *31*
Setting User Access Type – Scheduled *32*
Setting a Custom Output Mode for a User *33*
Searching/Filtering Users *35*
Other User Management *36*
Exporting Users *37*
Importing Users *38*
User Import Error Message *39*
Understanding User Files *40*
The Audit Trail: **41**
Viewing the Audit Trail *41*
Searching / Filtering the Audit Trail *42*
Saving / Exporting the Audit Trail *42*
Clearing the Audit Trail *43*
Understanding the Audit Trail *43*
Backing Up Device Settings: **45**
Back Up Device Settings *45*
Restoring Device Settings or Replicating to Another Device: **46**
Restore or Replicate Device Settings *46*
Resetting the Device: **47**
Resetting Only the ADMIN Passcode *47*
Resetting the Device to Factory Default *47*
Editing an Exported User File on a Computer **48**
Instructions to Users: **53**
Firmware Version Updates: **53**
Troubleshooting: **54**
Accessories Available from SECO-LARM: **55**

Getting Started:

To complete the installation and setup, in addition to the device's box contents, you will also need:

1. A drill with a $^{5}/_{16}$" (8mm) drill bit and a larger drill bit and/or hole saw for the wiring hole
2. A bit driver for the security screw (included)
3. A Phillips head screwdriver
4. Needle-nose pliers
5. A smartphone with Bluetooth® wireless technology (iOS 11.0 and above, Android 5.0 and above)
6. The *SL Access*™ app, downloadable from the iOS App Store or Google Play Store

Download the *SL Access*™ app from the corresponding store for your phone.

NOTES:

a. Be sure to set your smartphone to automatically download app updates so that you always have the latest version of the app.
b. The app will appear in your device's default language if that language is available (currently English, Spanish, French, Portuguese, Russian, German, Vietnamese, and Traditional and Simplified Chinese), otherwise, it will default to English.
c. ENFORCER *Bluetooth*® Access Devices use EEPROM memory. Stored data is unaffected by power outages.
d. Page references within the text of this manual are all cross-reference links which will take you to the page indicated.

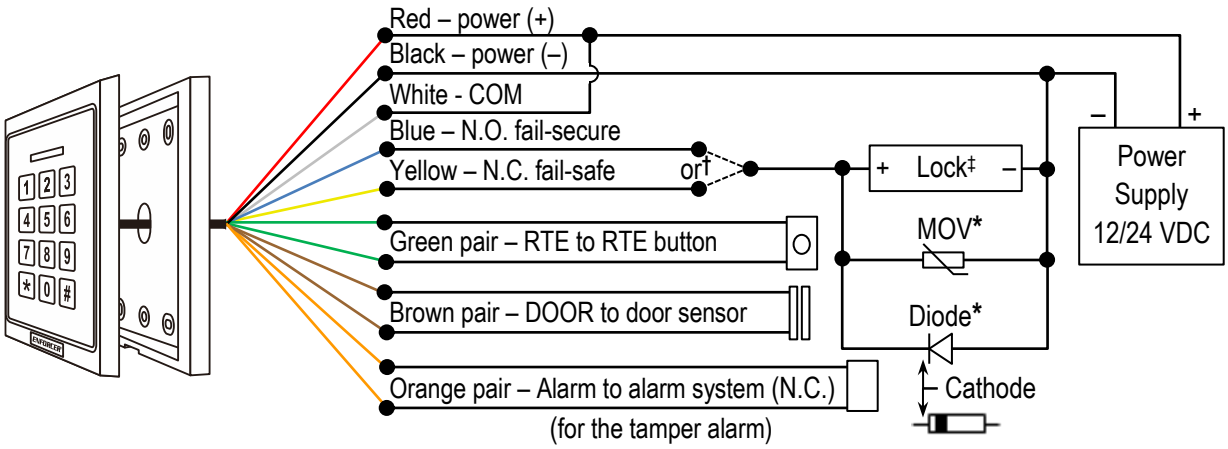
Installation:

Mounting

Follow the mounting instructions included in the *Product Specifications* (or *Additional Information*) included with your particular product. Crimp connectors are included for connecting the wires (except SK-B941-PQ).

Typical Wiring Diagram

Pictured below is the Single-Gang Keypad, but the installation and wiring for all models are the same. However, since the Post-Mount Gate Keypads have a terminal block instead of colored wires, see a separate wiring diagram on the next page showing the terminal locations. See *Sample Applications* beginning on pg. 6 for specific wiring instructions and warnings.



IMPORTANT NOTES:

*To protect the relay, you must install the enclosed diode—with the cathode (striped end) toward the positive side—for DC powered locks ***or*** install the varistor (MOV) for AC powered locks and for electromagnetic locks ***unless*** *your lock has a diode/MOV built in* (all SECO-LARM electromagnetic locks have built-in protection). Do not install both diode and MOV. Failure to use these as directed will void the warranty.

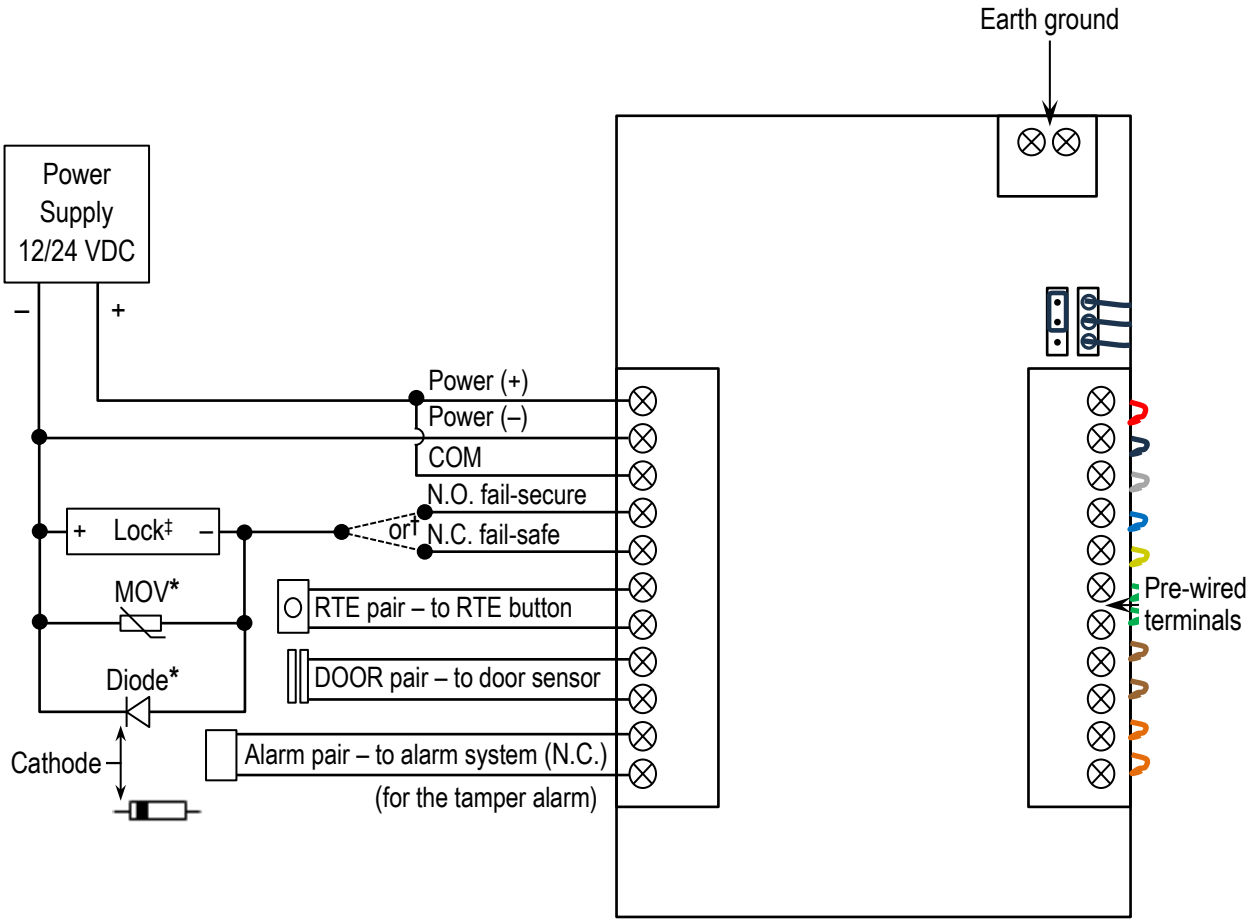
†Use the blue wire for fail-secure applications and the yellow wire for fail-safe applications. Use electrical tape to insulate the end of any unused wire.

‡AC powered locks *cannot exceed* 24VAC. For locks exceeding 24VAC, use an external relay module. Current cannot exceed 0.3A@125VAC. For AC powered locks, avoid any situation that leaves the lock continually activated for a long period of time. See *Basic Wiring to an AC Powered Lock* on pg. 7 for detailed wiring instructions.

Installation (Continued):

Bluetooth Post-Mount Keypad Wiring Diagram

Pictured below is the wiring overview for the Post-Mount Gate Keypads. See *Sample Applications* beginning on pg. 6 for specific wiring instructions and warnings.



IMPORTANT NOTES:

*To protect the relay, you must install the enclosed diode—with the cathode (striped end) toward the positive side—for DC powered locks ***or*** install the varistor (MOV) for AC powered locks and for electromagnetic locks ***unless*** *your lock has a diode/MOV built in* (all SECO-LARM electromagnetic locks have built-in protection). Do not install both diode and MOV. Failure to use these as directed will void the warranty.

†Use the N.O. terminal for fail-secure applications and the N.C. terminal for fail-safe applications.

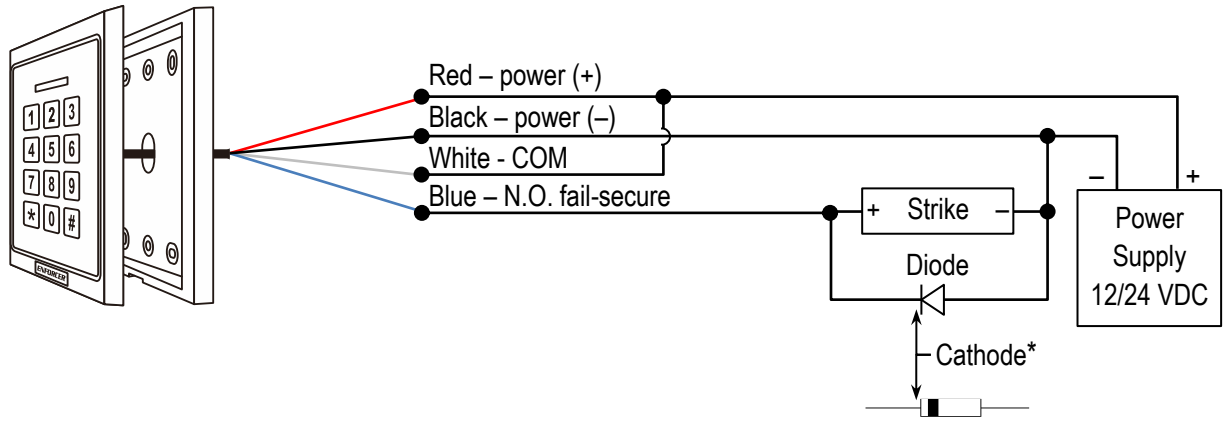
‡AC powered locks *cannot exceed* 24VAC. For locks exceeding 24VAC, use an external relay module. Current cannot exceed 0.3A@125VAC. For AC powered locks, avoid any situation that leaves the lock continually activated for a long period of time. See *Basic Wiring to an AC Powered Lock* on pg. 7 for detailed wiring instructions.

Installation (Continued):

Sample Applications

In the diagrams for each sample application, the SK-B141-PQ is pictured but the wiring is the same for all models.

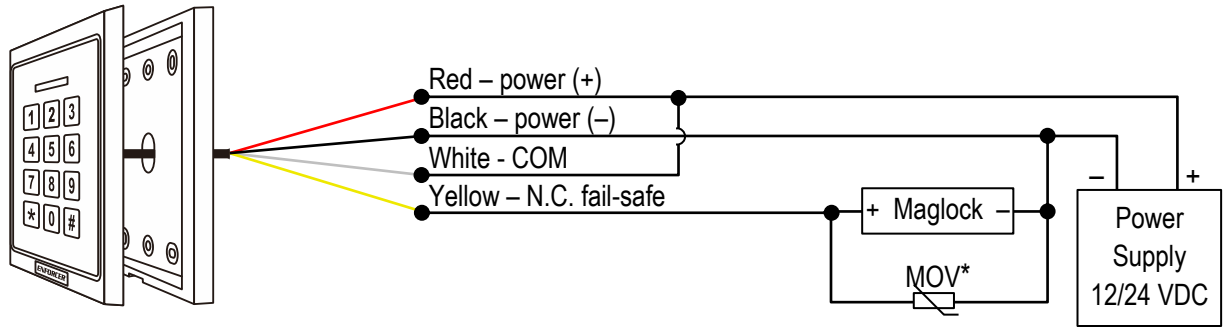
Basic Wiring to a Fail-Secure Door Strike



IMPORTANT NOTES:

*To protect the relay, you must install the enclosed diode—with the cathode (striped end) toward the positive side—for DC powered locks ***unless*** *your lock has a diode built in*. Failure to install as directed will void the warranty.

Basic Wiring to a Fail-Safe Maglock



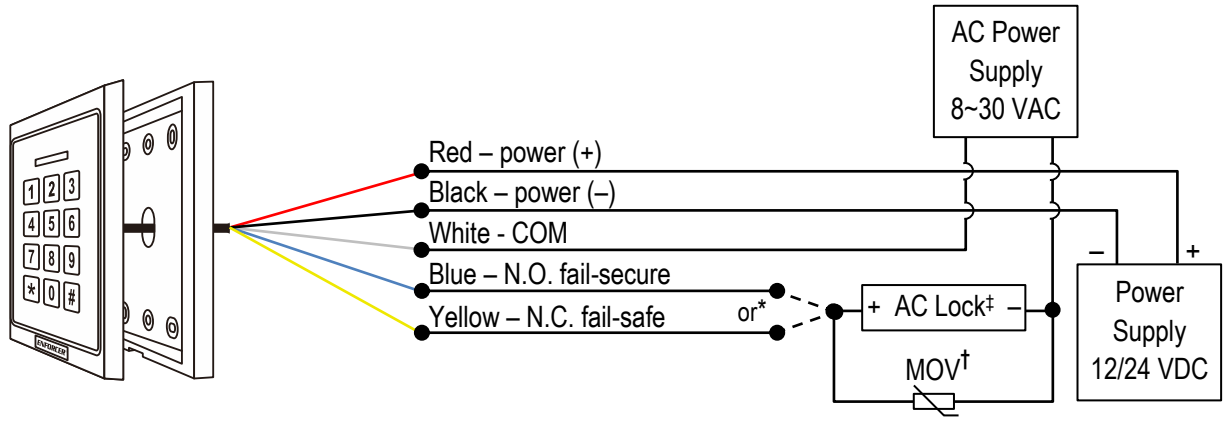
IMPORTANT NOTES:

*To protect the relay, you must install the enclosed varistor (MOV) for electromagnetic locks ***unless*** *your lock has a MOV built in* (all SECO-LARM electromagnetic locks have built-in protection and do not need this MOV). Failure to install as directed will void the warranty.

Installation (Continued):

Sample Applications (Continued):

Basic Wiring to an AC Powered Lock



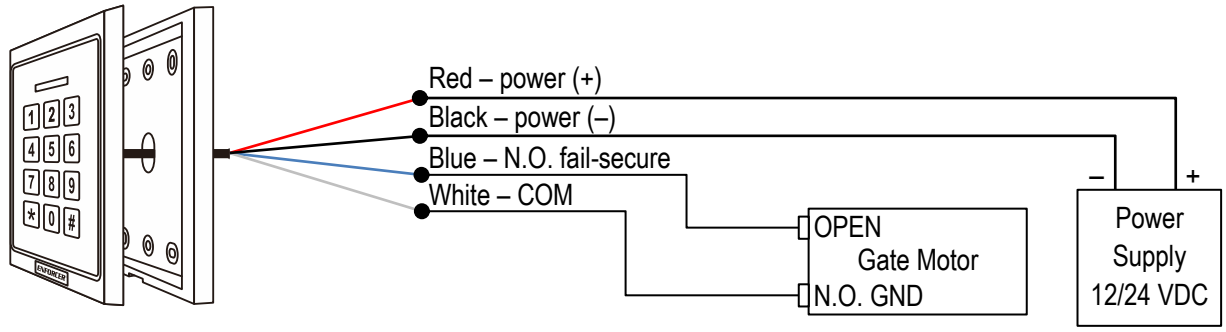
IMPORTANT NOTES:

*Use the blue wire (N.O. terminal) for fail-secure applications and the yellow wire (N.C. terminal) for fail-safe applications. Use electrical tape to insulate the end of any unused wire.

†To protect the relay, you must install the enclosed varistor (MOV) for AC powered locks ***unless*** *your lock has a diode/MOV built in*. Failure to install as directed will void the warranty.

‡AC powered locks **cannot exceed** 24VAC. For locks exceeding 24VAC, use an external relay module. Current draw cannot exceed 0.3A@125VAC. Avoid any situation that leaves the lock continually activated for a long period of time.

Basic Wiring to a Gate Operator



LED Indicators and Device Sounds:

LED Indicators

	Green LED	Blue LED	Red LED
Steady	Output activated, door always unlocked on, or toggle unlocked activated	Powered on, Standby	Invalid access attempt or door always locked activated
Flashing		ADMIN settings opened*	

*Flashing blue when ADMIN settings is opened overrides other LED indicators

Keypad Sounds and LEDs

Status	Sounds*	LED
In programming mode	–	Steady ON
Successful key entry	1 Beep	ON for relock duration
Successful code/card entry	1 Beeps	ON for relock duration
Unsuccessful code/card entry	3 Beeps	1 Flash
Wrong code lockout	3 Beeps	1-Second flashes red/blue for lockout duration

*Keypad sounds can be programmed ON or OFF (see pg. 16) but output sounds will remain activated.

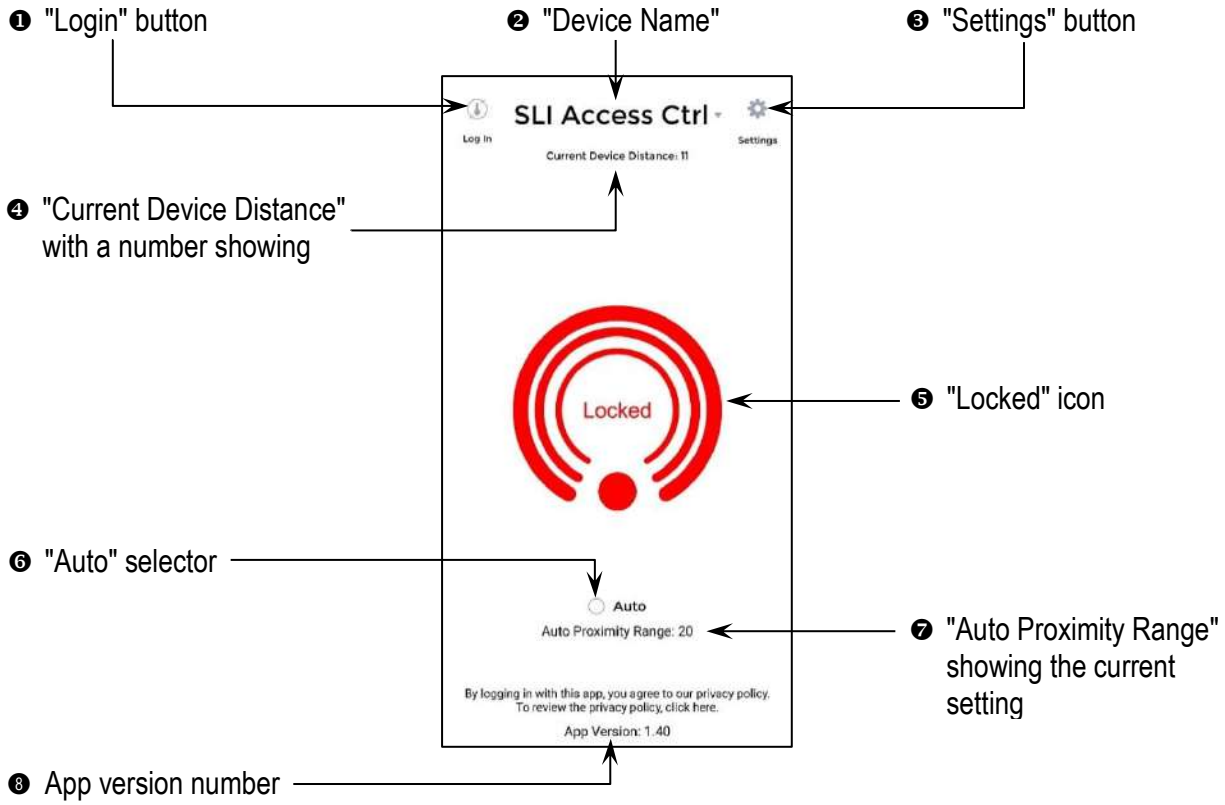
IMPORTANT NOTES:

IF USING THE KEYPAD WITH A MECHANICALLY OPERATED DOOR OR GATE, MOUNT THE KEYPAD AT LEAST 15' (5m) FROM THE DOOR OR GATE TO PREVENT USERS FROM BEING CRUSHED OR PINNED. FAILURE TO DO SO MAY RESULT IN SERIOUS INJURY OR DEATH.

1. Always disconnect power before servicing the keypad. Do not apply power until all connection wiring is completed.
2. The keypad must be properly grounded. Use a minimum 22AWG wire connected to the common ground output. Failure to do so may damage the keypad.
3. Allow at least 2ft (60cm) between this and any other keypads to avoid interference.
4. All wiring and programming should be done by a professional installer to reduce the risk of improper installation.
5. The *SL Access App User Manual* for this keypad is downloadable from the product page at www.seco-larm.com.
6. Be sure to store this manual in a safe place for future reference.

Understanding the *SL Access* Home Screen:

After you have downloaded the *SL Access* app (see pg. 3), click on the icon to open the app.



NOTES:

a. On opening the app, you may get a message asking you to enable Bluetooth. Bluetooth must be enabled to use the app and the device must be in range.

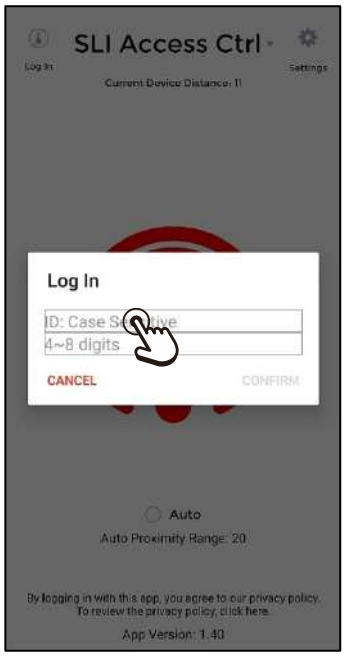
b. Pairing is not needed for *Bluetooth* LE devices. Nearby compatible devices will automatically show in the *Device Name* dropdown.

c. You may see the word "Searching…" at the top of the screen (see right). *Bluetooth* has a limited range of about 60 feet (20m) under ideal conditions but will be much less in practice. Move closer to the device, but if "Searching…" continues to show you may need to exit and reopen the app.

Logging In to Your Device:

You will need to log in as the administrator to set up the device.

1. From a position near the device, click "Login" at the top left of the home screen.
2. Type "ADMIN" (case sensitive) in the ID section.
3. Type the factory default ADMIN passcode "12345" as the passcode and click "Confirm."

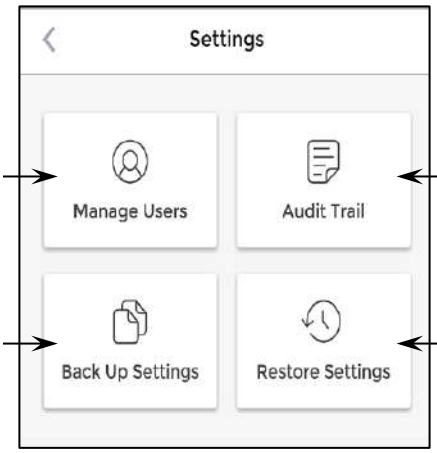


NOTES:

a. If more than one device is in range, you may need to choose the correct device from the device name dropdown at the top of the screen.
b. The administrator's ID is ADMIN and cannot be changed.
c. There is only one ADMIN account. Though the passcode can be given to more than one person if needed, it is recommended that you limit it to one person, if possible, to avoid confusion.
d. Though the ADMIN can log in using any phone, it is recommended that you perform backups, exports, and downloads from the same phone to avoid duplication and confusion about which phone has the latest versions.
e. The factory default passcode should be changed from the "Settings" page immediately for better security (see pg. 13).
f. Users will use the same app and will log in in the same manner and these screens will look the same. However, their functionality will be limited (see pg. 53).
g. Even after logging in, the home screen icon will not change to show that you are now logged in.
h. When you log in on a phone, your credentials are saved to that phone so that you don't have to keep logging in each time. However, if you log in using another phone, the first phone may have to log in again. Only one phone can be remembered at a time.
i. You cannot "log out" because Bluetooth LE only connects briefly when a signal is sent. Only logging in from another phone will cause the first to be "forgotten."

Understanding the ADMIN Setup Screen:

From the Home Screen, click on the "Settings" icon in the top right corner to open the settings. At the top you'll note 4 function buttons above a list of device settings. These will be described on the pages noted beside each button.



Manage Users (pg. 27)
Add and manage users
Export and import user lists

Audit Trail (pg. 41)
Download the audit trail or delete the current trail

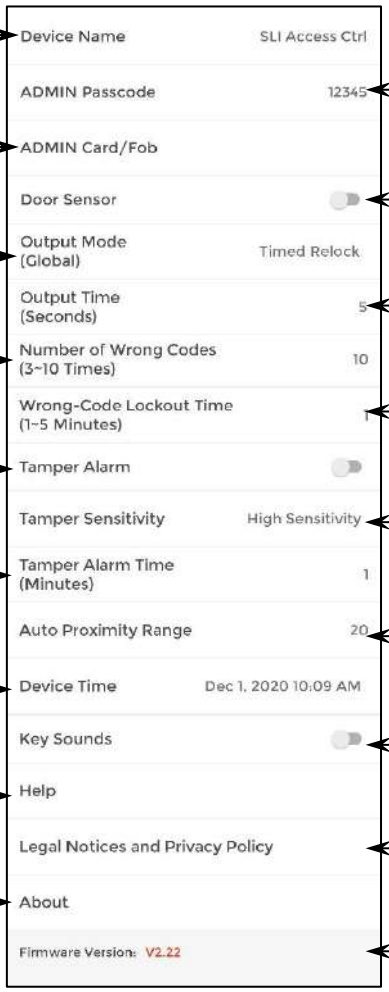
Back Up Settings (pg. 45)
Back up device settings for archive, restoration, or replication

Restore Settings (pg. 46)
Restore device settings or replicate from another device

NOTES:

a. This settings screen is available only when logged in as the ADMIN. For the User Settings screen, see pg. 53.
b. While the ADMIN settings screen is open, due to a limitation with *Bluetooth LE*, users will not be able to access the device using the app (the keypad, proximity reader, and egress button will still function normally).
c. When finished, return to the home screen before leaving the app. If you close the app before leaving the Settings screen, it may remain connected to the device rendering it inaccessible to users via app until it automatically disconnects (around 2 minutes).

Understanding the *SL Access* ADMIN Setup Screen (Continued):



Device Name (pg. 15)
Rename the device

ADMIN Card/Fob (pg. 14)
Add ADMIN proximity card/fob*

Output Mode (Global) (pg. 17)
Set the global output mode

Number of Wrong Codes (pg. 20)
Set number of wrong codes before temporarily locking out the device

Tamper Alarm (pg. 22)
Enable/disable the tamper alarm (default - enabled)

Tamper Alarm Time (pg. 22)
Set the duration of the tamper alarm (default – 255 minutes)

Device Time (pg. 26)
View the device's date and time

Help (pg. 26)
Go to the SECO-LARM help page

About (pg. 26)
About this app

ADMIN Passcode (pg. 13)
Factory default – 12345. Please change immediately.

Door Sensor (pg. 16)
Enable/disable the door sensor input

Output Time (pg. 18)
Set the length of time before relocking for Timed Relock Output Mode

Wrong-Code Lockout Time (pg. 21)
Set the locked out duration after too many wrong codes

Tamper Sensitivity (pg. 23)
Set the sensitivity of the tamper alarm vibration sensor

Auto Proximity Range (pg. 24)
Set the relative range for the "Auto" setting†

Key Sounds (pg. 16)
Enable/disable the key sounds‡

Legal and Privacy (pg. 26)
Visit the SECO-LARM website for legal notices and our privacy policy

Firmware Version (pg. 53)
The connected device's firmware version

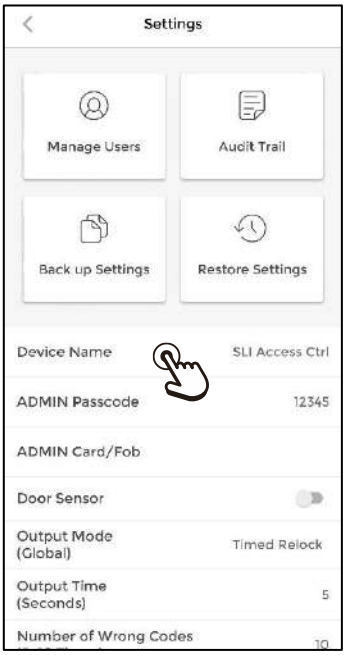
*For devices with a proximity reader

†The *Auto Proximity Range* refers to the App's *Auto Unlock* and is unrelated to proximity cards/fobs

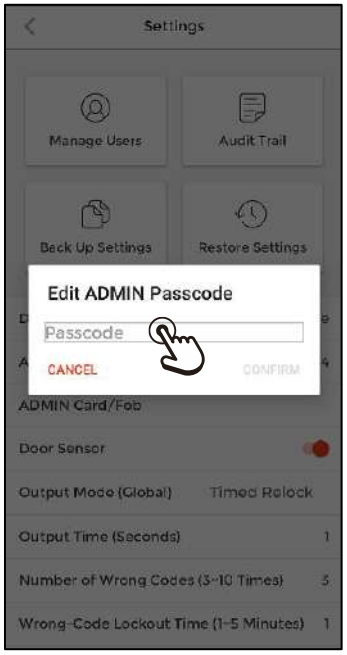
‡For keypads only

Changing the ADMIN Passcode:

For security, it is important that you immediately change the ADMIN passcode immediately on installation. In addition, if the eventual administrator is a different person from the installer, or when the administrator changes, it is important to change the passcode again. The passcode may be 4~8 digits.



Click on ADMIN Passcode



Select the *Passcode* box

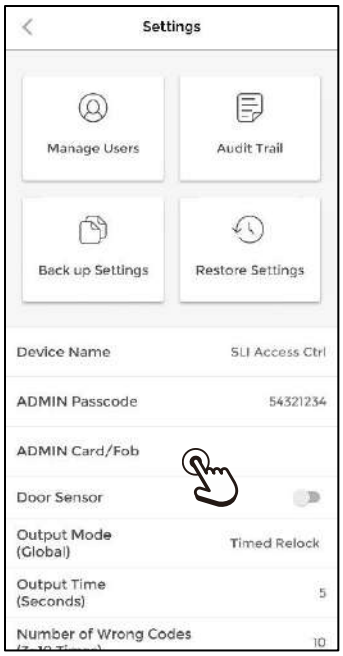
Type the new code (4~8 digits) and click *Confirm*

NOTES:

a. The passcode should be something you can easily remember but which is unlikely to be guessed by others. If you forget your password, see pg. 47 for reset instructions.
b. The ADMIN passcode can also be used like a common user to trigger the access device.
c. There is only one ADMIN account. The ADMIN passcode can be given to more than one person, but only one can access the device at the same time.
d. If the ADMIN forgets the passcode, the device can be reset to factory default and a new passcode can be set (see pg. 47).
e. If the ADMIN resigns, they should be asked to delete the app from their phone so that any downloaded data will also be removed from their phone. The ADMIN passcode should then be changed by the new ADMIN.
f. If the ADMIN's phone is replaced, be sure to reset the old phone to erase all data.
g. If the ADMIN's phone is lost, the data is secure as long as the phone is secured, but it is recommended that you change the ADMIN passcode and remotely erase the phone (see your phone manufacturer's instructions).

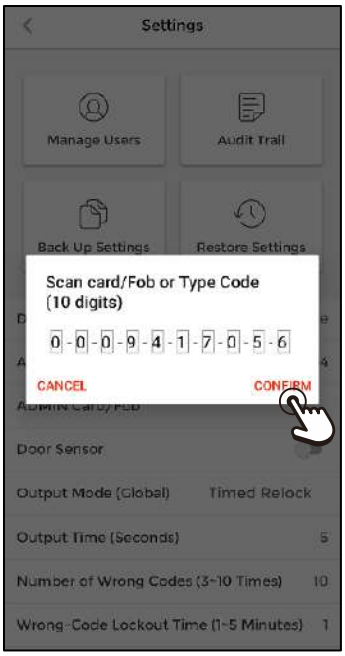
Adding an ADMIN Proximity Card:

If your device includes a proximity reader, the ADMIN can also use a proximity card/fob to log in. Assign a proximity card/fob to the ADMIN as follows.



Click on ADMIN Card/Fob

Scan the card/fob on the device or…



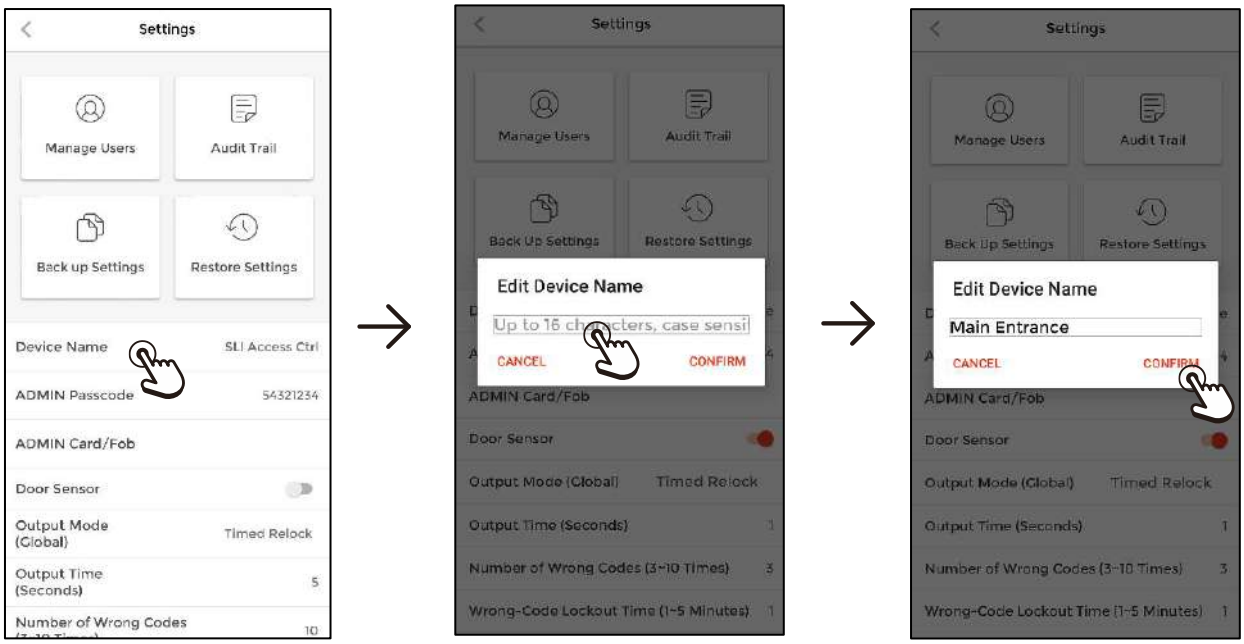
… type the card's code in the popup and click *Confirm*

NOTES:

a. Like the ADMIN passcode, the ADMIN proximity card/fob can also be used to trigger the access control device as a regular user.
b. To delete an ADMIN's card/fob, click *ADMIN Card/Fob* and then delete the number from the popup box.

Changing the Device Name:

You can give your access control device a name that can be easily recognized by users and is distinguishable from other nearby devices.



Click on Device Name

Select the Device Name's entry box

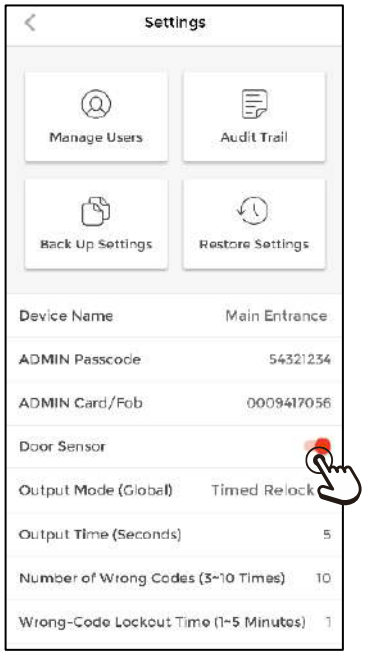
Type the new name and click *Confirm*

NOTE: The device name can be up to 16 characters including spaces (or 16 bytes for some languages).

Settings to Enable/Disable:

There are two settings that can be enabled (disabled by default).

Enable/Disable the Door Sensor

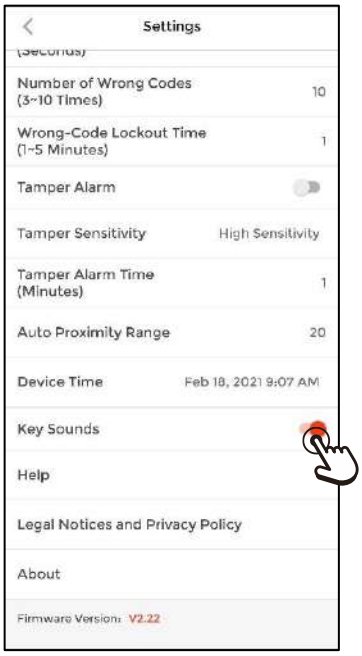


Enable the door sensor* for a warning when the door is held open longer than the set relock time (see pg. 18) or if the door is forced open. Note that the device cannot distinguish between a door forced open and a door that is held open beyond its relock time.

In either of these cases a built-in buzzer will sound until the door is closed.

*Requires either a magnetic contact installed at the door or a door lock with a built-in sensor.

Enable/Disable the Key Sounds



Enable the key sounds for an audible indicator when the keys are pressed.†

Disable them for a quieter environment.

Disabling the key sounds does not disable other warning sounds.

†For keypads only

Global Output Mode:

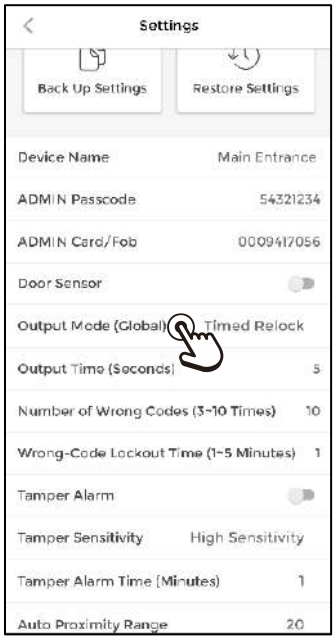
There are 4 global output modes:

1. **Timed Relock** – when triggered, the door will unlock and, after a set time, will relock
2. **Remain Unlocked** – for times when you want to have free access
3. **Remain Locked** – for times when you do not want any user access.
4. **Toggle** – will change the current state of the device, will unlock if locked and lock if unlocked.

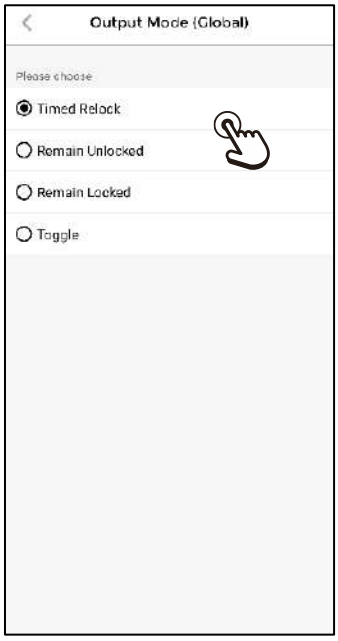
NOTE: The *Toggle* mode overrides other *Output Modes* (see pg. 18 for details).

The default output mode is *Timed Relock* and the time is programmable (default – 5 seconds, see "Setting the Time for *Timed Relock* Mode below).

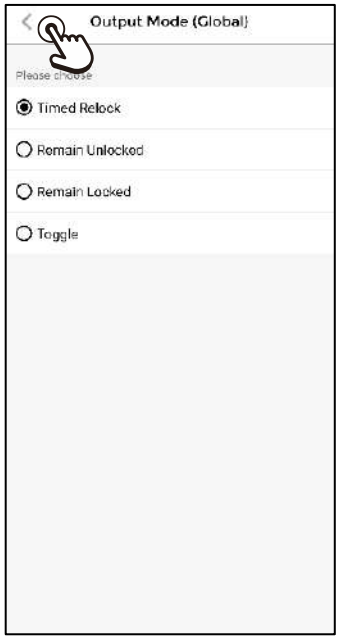
Setting the Output Mode (Global)



Click on Output Mode (Global)



Select the desired global output mode



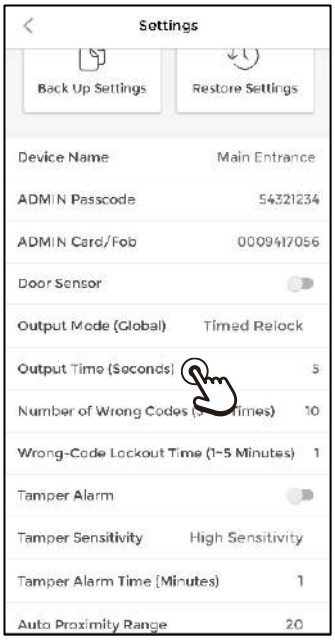
Click on the back arrow or the backup button (Android)

NOTES:

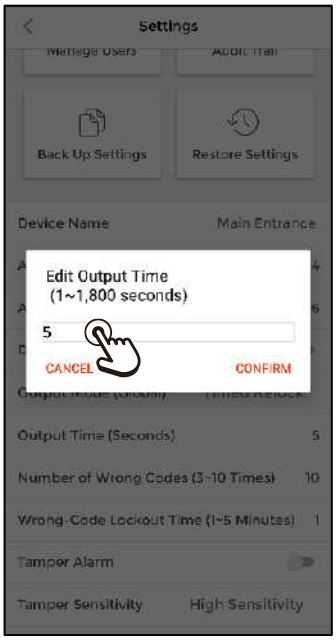
a. The global output mode will become the default mode for all users. However, the ADMIN can assign a different mode to certain users (see pg. 33).
b. *Remain Unlocked* and *Remain Locked* are only available to the ADMIN and will immediately unlock or lock the door. Other users do not have this option and their actions will not override this setting. A normal user can still use their normal access mode which will be recorded in the Audit Trail but will not change the door's locked or unlocked status.

Global Output Mode (Continued):

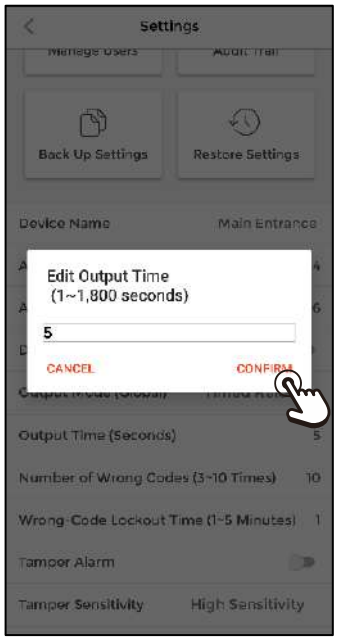
Setting the Time for *Timed Relock* Mode:



Click on Output Time (Seconds)



Enter the desired relock time from 1~1,800 seconds



Click *Confirm* to set the time

NOTE: As with the global output mode, the ADMIN can assign a different relock time to certain users (see pg. 33).

Understanding the Toggle Mode:

Because the *Toggle* Mode overrides other *Output Modes,* it is important to understand how it works.

1. If the device is unlocked using the *Toggle Output Mode* (whether set globally or individually), another user set to the same mode will then relock the device. The same is also true in reverse.
2. If the device is unlocked using the *Toggle Output Mode* (whether set globally or individually), another user set to *Timed Relock* will not have any effect on the unlocked state, however their entry will still be recorded in the *Audit Trail*. This is useful for a business where a manager might be set to *Toggle* to open or close the business to the public, but still wants the employees to use the access control device (whether using the app, keypad, or card/fob) in order to have a record of entry.
3. If the device is later locked using *Toggle Output Mode* (whether set globally or individually), other users will be granted or denied access depending on their individual settings.
4. The *Toggle Output Mode* is also useful for turning machinery or other devices on or off for a longer, undetermined period of time.

Door Hold Open (Passage)

There are several ways that you can use to hold a door/gate open.

Administrator

The ADMIN may set the *Output Mode (Global)* to *Remain Unlocked*. In that case, the device will immediately unlock and remain unlocked. The device LED will turn green to indicate that the door is unlocked (see pg. 17).

If other users use the app, keypad, or card, the event will be recorded in the audit trail, but will have no effect on the device, which will remain unlocked until the administrator again changes the *Output Mode (Global)* setting. Note that only the ADMIN will be able to relock the door/gate by returning the *Output Mode (Global)* to its normal setting

User

The ADMIN can allow individual users to hold open with the app, keypad, or card. To do this, the Administrator can set an individual user's *Output Mode* to *Toggle* under their *Output Mode* setting (see pg. 33) to allow them to hold open and relock it again later.

When a user "holds open," this action will be reported in the *Audit Trail*. While a device is held open, if another user whose *Output Mode* is not *Toggle* uses the app, keypad, or card on the device, it will have no effect on the device but will be recorded in the *Audit Trail*.

Note that the app gives lots of flexibility in handling this. The hold open privilege can be given to an individual user or multiple users. Or the ADMIN can give a second login to a particular user. For example, *John* could be set to *Timed Relock*, but also be given a second UserID such as *John – Hold*. Or a UserID called *Hold Open* could be set up and the passcode for that shared with several users, allowing them to use the keypad passcode to hold open and relock later or login as *Hold Open* to use the app to do the same thing.

Business Hours

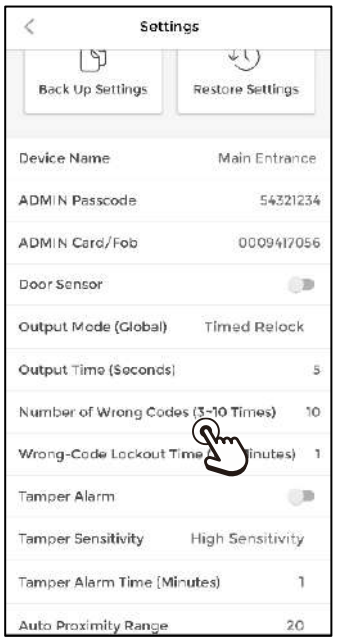
Business hours can also be handled in a similar manner as above. The ADMIN can set the *Output Mode (Global)* to *Remain Unlocked*. In that case, the device will immediately unlock and remain unlocked. The device LED will turn green to indicate that the door is unlocked (see pg. 17). Note that only the ADMIN will be able to relock the door.

An easier way would be to handle it in a similar way as the "Door Hold Open" described above. A separate UserID could be set up (maybe called *Toggle* or *Business Hours*) with the *Output Mode* set to *Toggle* to unlock the door for business and relock it again at closing time. Other employees set to *Timed Relock* could still enter the business before business hours to prepare for opening.

Wrong Code/Card Lockout:

If a user enters too many wrong codes or swipes too many unregistered cards, the device will temporarily be unavailable for use. The ADMIN can set the number of wrong codes/cards before lockout and the length of time the device will locked out.

Setting the Number of Wrong Codes/Cards



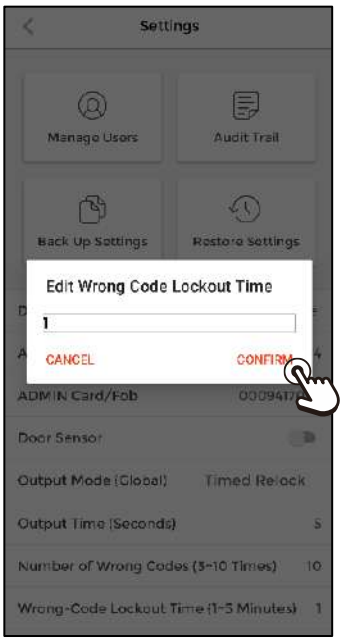
Click on Number of Wrong Codes

Enter the number of wrong codes (3~10) for lockout and click *Confirm*

Wrong Code/Card Lockout (Continued):

Setting the Wrong-Code/Card Lockout Time

Click Wrong-Code Lockout Time



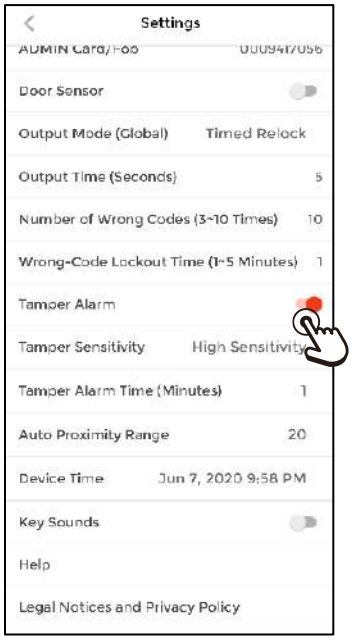
Enter the desired time (1~5 minutes) for the device to lockout and click *Confirm*

NOTE: During the lockout time, the ADMIN can interrupt the lockout with the app, but not with the keypad or card.

Tamper Alarm:

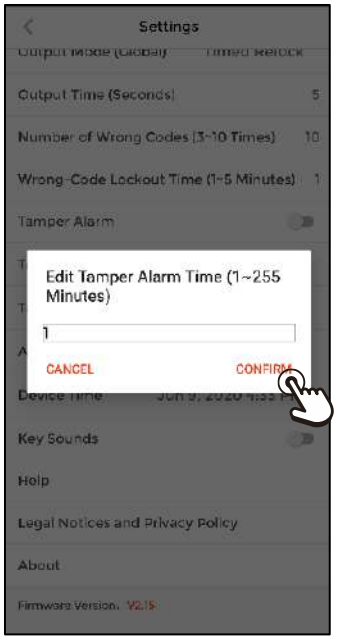
The access controller uses a 3-axis accelerometer to detect vibrations indicative of possible tampering. The ADMIN can enable/disable the tamper alarm, adjust the sensitivity, and set the duration of the alarm.

Enable and Select the Tamper Alarm Time



Click on the *Tamper Alarm* enable button

Select Tamper Alarm Time



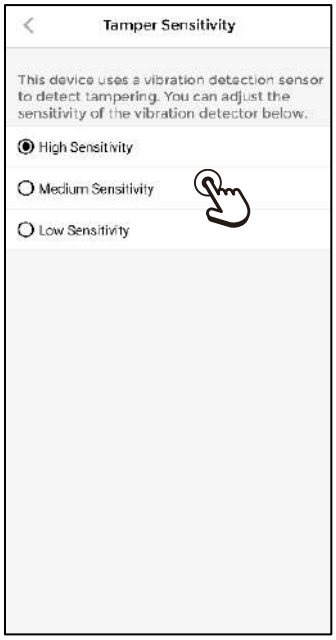
Enter the desired time (1~255 minutes) and click *Confirm*

NOTE: The tamper alarm will sound an internal buzzer and will output to an external alarm if connected. It will continue until the time expires or until the ADMIN disables the tamper alarm in the app. The tamper alarm can be immediately re-enabled for continued protection.

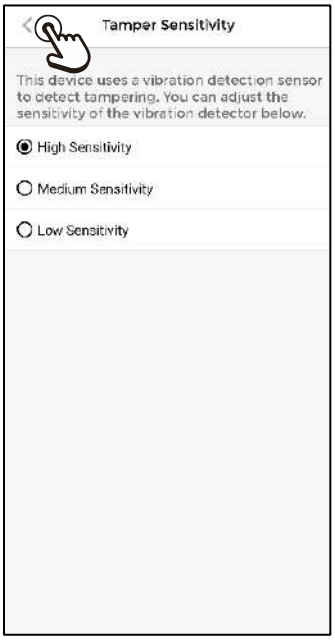
Tamper Alarm (Continued):

Select the Tamper Alarm Sensitivity

Click on Tamper Sensitivity



Select the desired level of sensitivity



Click the back arrow or the back button (Android)

NOTES:

a. The tamper alarm uses a 3-way accelerometer to detect vibration or movement which could indicate possible tampering. The default setting is "High Sensitivity" meaning that a smaller vibration or movement will set off the alarm. Low Sensitivity means that the level of vibration or movement must be much greater to set off the alarm.
b. Vibration can vary depending on the mounting surface. You may need to experiment with different settings if you find that there are too many false alarms.

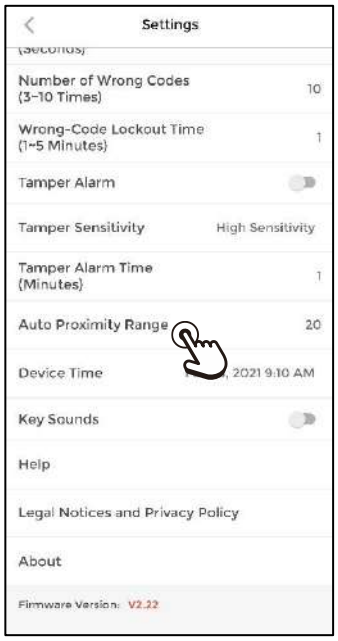
Auto Proximity Unlock:

The *Auto* setting at the bottom of the home screen allows you to unlock the door when your phone gets close to the device. This can be convenient when your hands are full. However, there are several things to note about this feature.

1. The app must be loaded and the screen on for the *Auto Proximity Unlock* to work. Therefore, it should be enabled only when needed and just before approaching the door so that the screen doesn't timeout.
2. The settings for this only apply to the device in use and therefore is enabled/disabled for each individual user. The ADMIN settings for this apply only to the ADMIN and individual users can adjust their own settings.
3. This feature depends on the Bluetooth signal strength which can vary greatly depending on the environment and the particular phone's Bluetooth radio. Therefore, you must first set the Auto Proximity Range for the particular phone and environment.
4. The *Current Device Distance* is a relative number based on the relative signal strength and will vary from phone to phone. It is not a specific distance measurement.

Setting the Auto Proximity Range

Bring your phone within the approximate range where you wish to the device to be triggered. Click on the *Settings* icon.

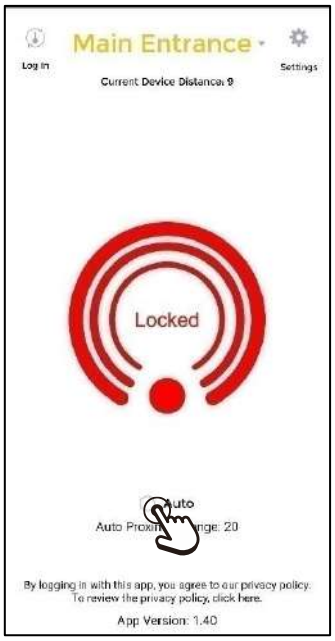


On the settings page, select the *Auto Proximity Range.*

Note that the *Current Device Distance* is also shown on this screen. Use the slider to adjust your *Auto Proximity Range* to a number that closely matches the *Current Device Distance*.

Auto Proximity Unlock (Continued):

Enable Auto Proximity Unlock



Click the radio button next to *Auto* to enable or to disable.

NOTE: You cannot open the *Settings* screen when *Auto* is enabled. You must first disable *Auto* on the home screen to enter *Settings.*

Settings Screen Miscellaneous Items:

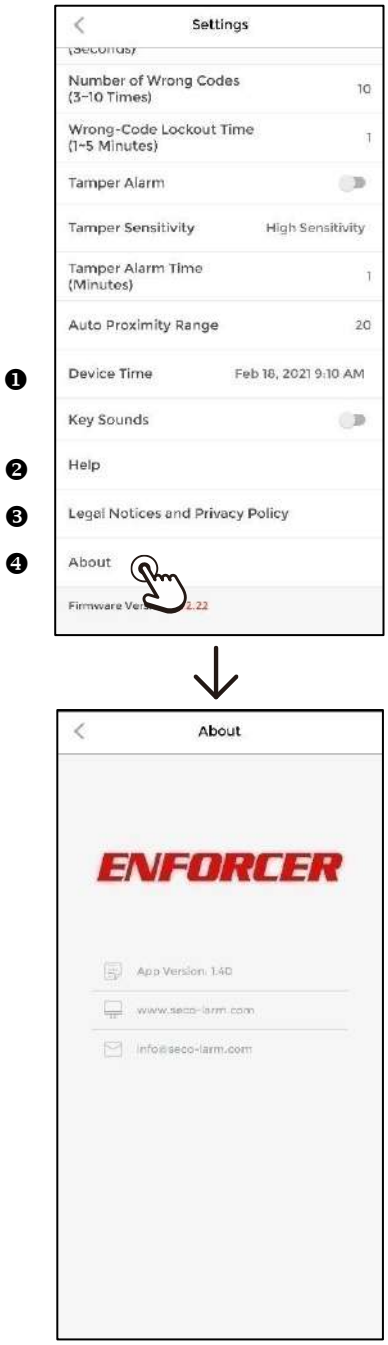
❶ **Device Time** – The device date and time synchronizes with the date and time of the ADMIN phone each time the ADMIN opens the settings page, thus keeping the device date and time up to date. There is no manual date/time setting.

NOTE: The device has no internet connection and cannot automatically adjust for Daylight Savings Time. The ADMIN will need to connect to the device and open the Settings page, which will automatically set the device to the correct date and time.

❷ **Help** – Selecting *Help* will take you to the SECO-LARM website. Use the search box to find the product page for further help. If you can't find the information you need there, go to the Support page to contact SECO-LARM.

❸ **Legal Notices and Privacy Policy** – Clicking this link takes you to the corresponding page on SECO-LARM's website.

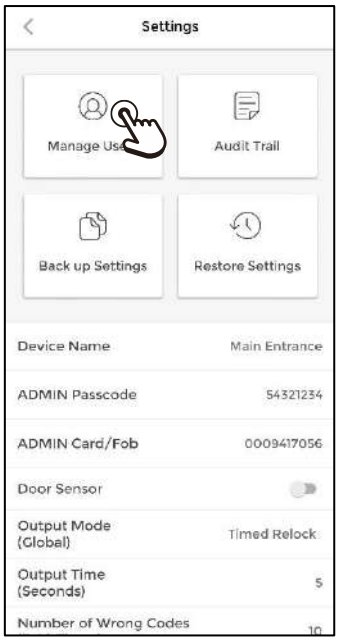
❹ **About** – Click the *About* link for the app version and links to other information.



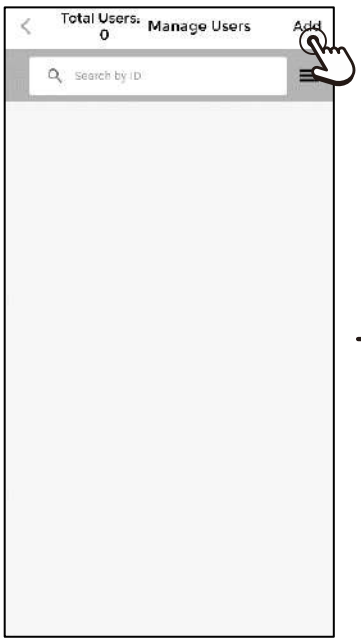
Managing Users:

Press the *Manage Users* button to add or delete users, view and edit individual user settings, and export or import user lists.

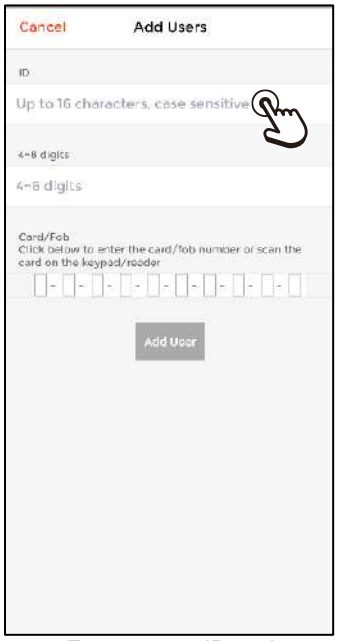
Adding Users



Click on Manage Users



To add a user, click on *Add.*

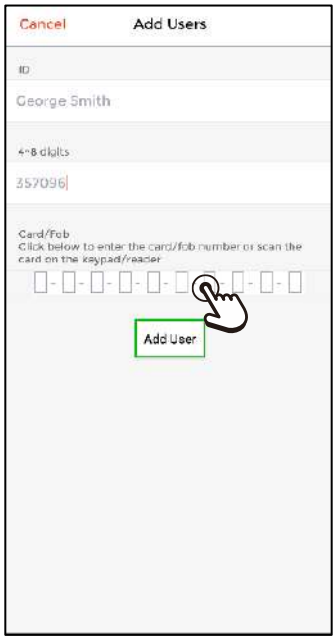


Enter a user ID and passcode and click the *Add User* button

NOTES:

a. The user ID is up to 16 characters, case sensitive, and including spaces.
b. Accented letters, numbers and foreign character sets can be used to allow the use of user's actual names.
c. Each user ID must be unique.
d. Passcodes must be 4~8 digits and are used to allow a user to log in to the app and as their keypad code.
e. Each passcode must be unique.
f. Each device supports up to 1,000 users plus the ADMIN.

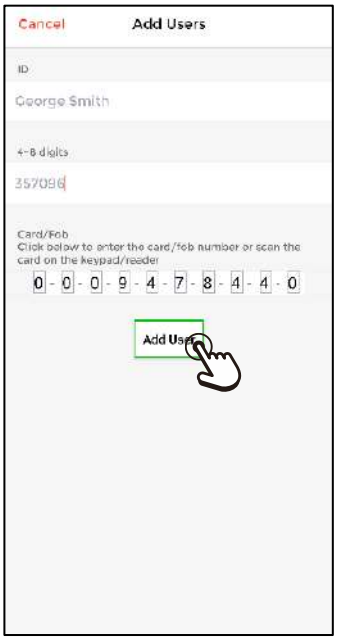
Managing Users (Continued):



To assign a proximity card* to the user, either type the card's code (if known) or…

OR

…click on the card number area and swipe a card or fob on the device.



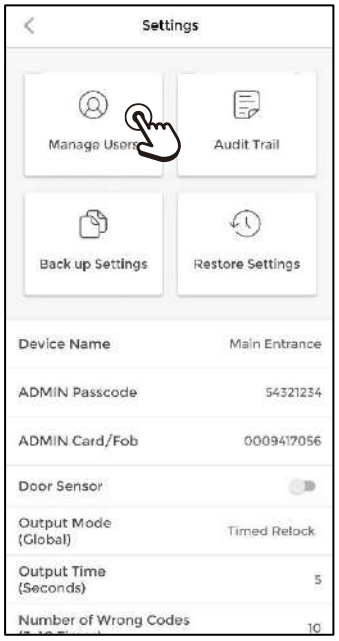
Click the *Add User* button when complete.

*Devices with a proximity reader only.

NOTE: After a user has been added, any changes made on the User Info screen will take effect immediately without needing to "save."

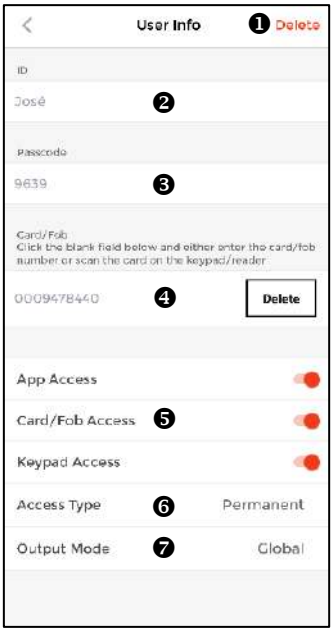
Managing Users (Continued):

Viewing, Changing Settings, and Deleting a User



Click on Manage Users.

Select a user to view, delete, or manage their settings.



❶ Delete the user.

❷ Edit the *User ID*.

❸ Edit the user's *Passcode.*

❹ Add, delete, or edit a proximity card/fob.

❺ Enable or disable an access mode – app, card/fob, keypad.

❻ Access Type (see pg. 30)

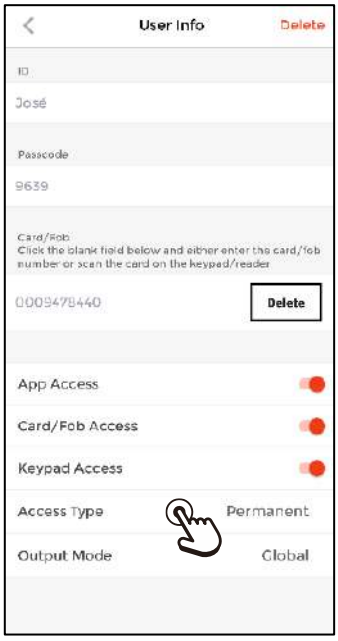
❼ Output Mode (see pg. 33)

NOTE: A popup will open to show the progress as it opens the user list. If you have a very large number of users, it may take several minutes to completely download. To start viewing the list while it is processing, click *Hide* to remove the popup.

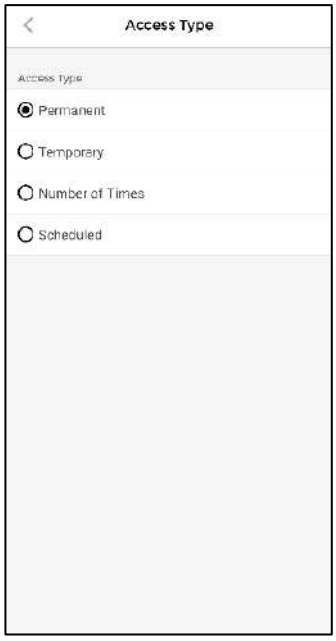
Managing Users (Continued):

Setting User Access Type

You can set each user for permanent access, scheduled access, temporary access with a start and end date/time, or to a specific number of times.



On the *User Info* screen, click on *Access Types*



Choose one of the four access types. The default is *Permanent* for which there are no further settings.

NOTES:

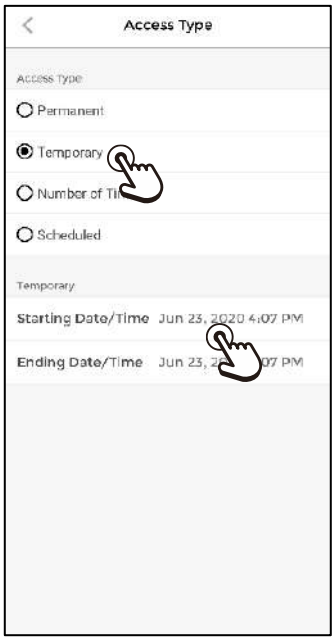
a. The default for all users is *Permanent*, so be sure to set the *Access Type* individually for any user who should have limited access.

b. Remember that the devices have no internet connection and therefore cannot adjust for Daylight Savings Time on their own. The device time is synchronized to the ADMIN phone each time they connect to the device and open the settings page. To adjust to Daylight Savings Time, the ADMIN must log in and open the *Settings* page after their phone adjusts to the new time which will then automatically adjust the device time. The device time cannot be set manually.

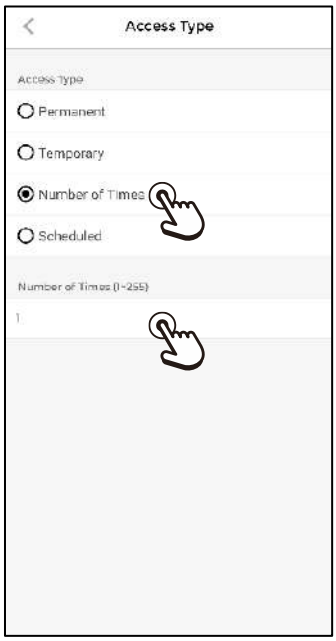
Managing Users (Continued):

Setting User Access Type – Visitors

For visitors you can easily give them temporary access, setting a starting and ending date and time. Otherwise, you can limit them to a number of entries up to 255.



Choose *Temporary* for visitors that you only wish to give short term access, from a few hours to several days. You will also need to set starting/ending dates/times.



Choose *Number of Times* to limit visitors to a certain number of times, ranging from once to 255 times. Enter the number of times in the box below.

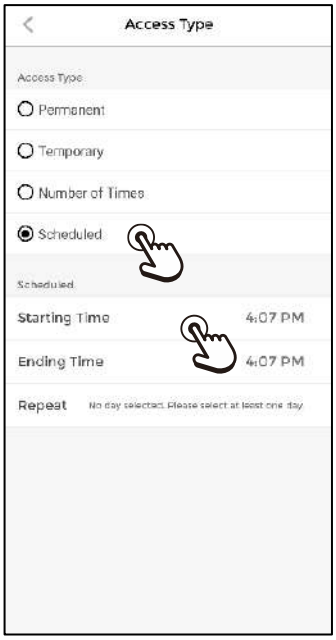
NOTES:

For the *Temporary* access type:

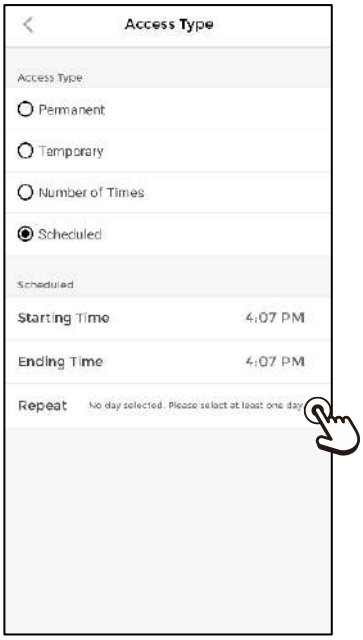
a. The ending date/time must be later than the starting date/time.
b. The time between starting and ending is continuous, so if the ending date is different, the access will include the overnight time between them.

Managing Users (Continued):

Setting User Access Type – Scheduled



On the *Access Types* screen, click on *Scheduled* and choose the time period you wish to give the user access by clicking on and setting the *Starting Time* and *Ending Time.*



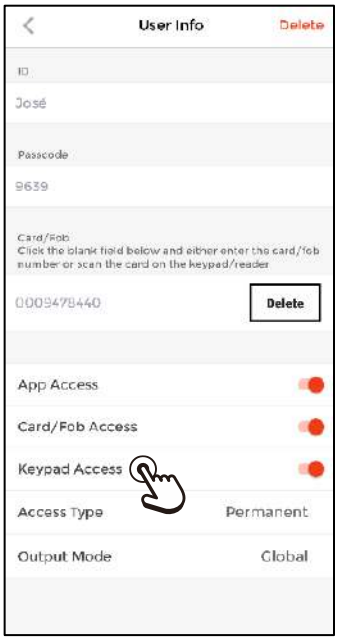
Click on *Repeat* to choose which days you wish to give the user access.

Choose any number of days and then click the back arrow or back button.

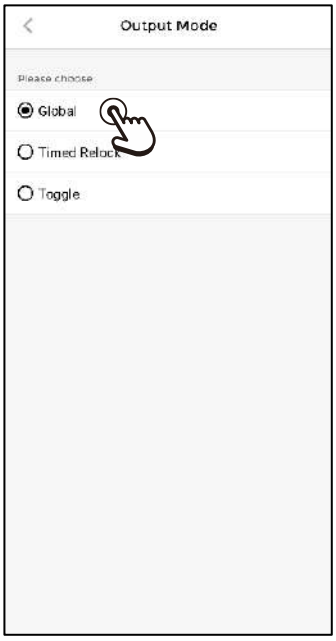
Managing Users (Continued):

Setting a Custom Output Mode for a User

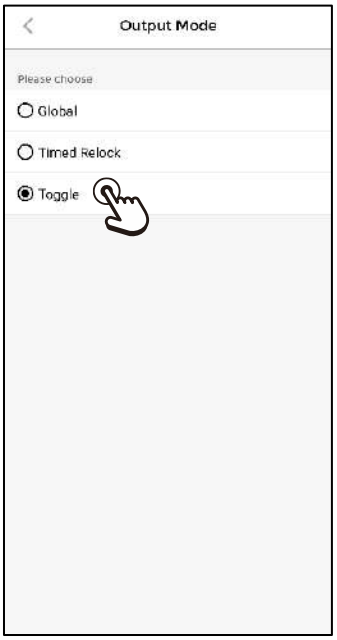
The default for every user is the *Output Mode (Global)* that the ADMIN sets on the main *Settings* screen. However, some users can be given custom *Output Mode* settings that override the global setting for that user.



On the *User Info* screen, click on *Output Mode.*



Global is the default, meaning that the user's *Output Mode* (and timing, if the global mode is set to *Timed Relock*) will follow the settings in *Output Mode (Global).*



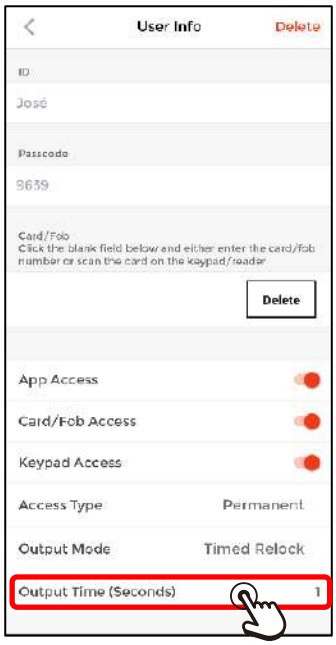
Click *Toggle* to allow this user to toggle between locked and unlocked.

NOTE: For a better understanding of the Toggle mode, please see pg. 18.

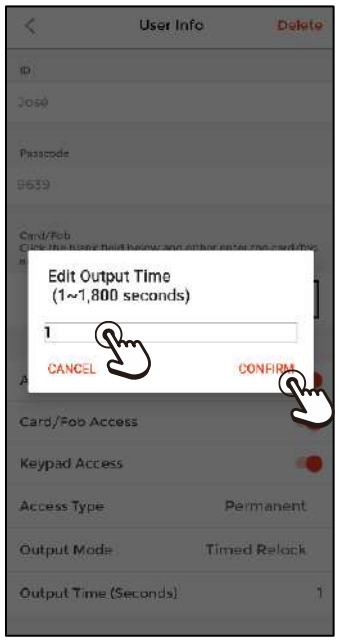
Managing Users (Continued):

Setting a Custom Output Mode for a User (Continued)

Click *Timed Relock* override the *Output Mode (Global)* or to give the user a different *Output Time* setting if the global mode is *Timed Relock.*



If you choose *Timed Relock,* when you return to the *User Info* screen, you will see an additional line for *Output Time.* Click on this to set the time before relock.



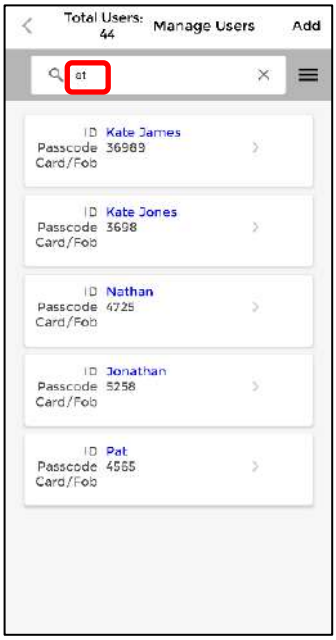
Enter the desired number of seconds (1~1,800 seconds) and click *Confirm.*

Managing Users (Continued):

From the *Manage Users* screen, you can see a list of all users and can also search/filter users, delete users, and export or import users.

Searching/Filtering Users

Click the *Search* box to filter a list of users or find a user.



Type any series of characters to find a particular user or group of users with those consecutive characters.

Click on the three bars in the top right corner for other options—import a user list, export this user list, or delete all users.

Managing Users (Continued):

Other User Management

Clicking on the three bars in the top right corner allows you to perform other user management tasks. You can import a user list, export this user list, or delete all users.

NOTES:

a. ***Import*** allows you to import a user list previously exported from this device or another device.
b. ***Export*** allows you to export these users as a backup or to replicate (import) to another device.
c. ***Delete All*** will delete all users from this device.
d. To delete individual users, you must open that user's *User Info* screen (see pg. 29) or swipe left on the user you wish to delete.

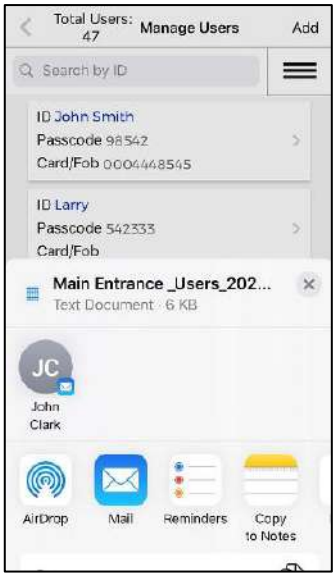
Managing Users (Continued):

Exporting Users

Click on the three bars in the top right corner and choose *Export* and wait for the export to complete.

Android

OR



iOS

A popup will appear shortly, allowing you to share or send it to an additional location in addition to saving it to the phone's app data folder. If you don't wish to do so, simply click anywhere above the popup and the file will only be saved on this phone.

NOTES:

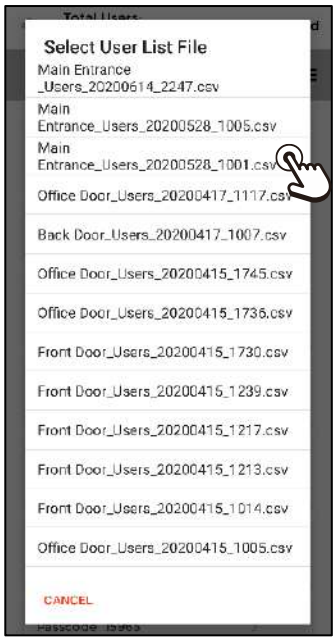
a. For very large user files, the export may take several minutes to process.
b. It is recommended that user file exports be performed on the same phone to avoid duplication and confusion as to which file has the latest changes.
c. The exported file is in a special .CSV format which can be read by any spreadsheet for easy review of user's settings and permissions.
d. Sharing or sending the exported to another allows you to have a backup off your phone or to share it with another phone for replication.
e. For longer lists the user list file can be edited in a computer spreadsheet and reimported, however great care must be taken in the process to avoid data corruption (see pg. 48).
f. For more information on user files, see pg. 40.

Managing Users (Continued):

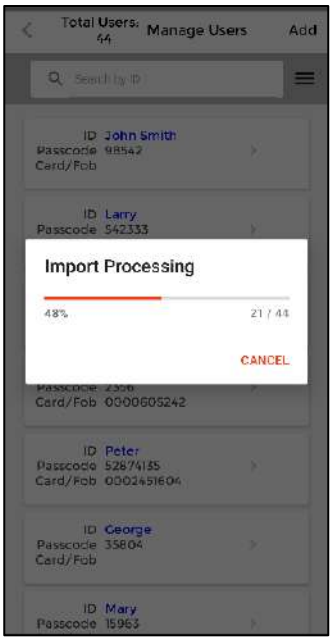
Importing Users

You can import any user list that is in the app data folder on your phone.

Click on the three bars in the top right and choose *Import*.



From the list of valid user files, choose the list to import.



Wait as you see the Import Processing popup.

NOTES:

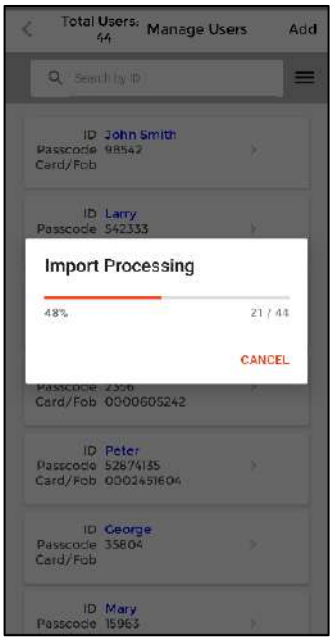
a. The *Select User List* File screen will show all lists in the app data folder on your current phone. You can choose any file exported from any device.

b. Very large user lists may take several minutes to import. Although you can cancel while the import is processing, doing so will not cancel any users already imported and will result in an incomplete list.

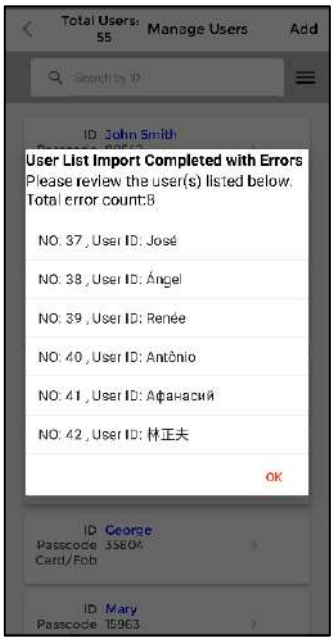
c. Importing a user file will not overwrite existing users. It will only add any users that do not exist in the current file (see the import logic process for users that exist in both files on pg. 40). To replace all users, first *Delete All* (see pg. 36) and then import.

Managing Users (Continued):

User Import Error Message



Wait as you see the Import Processing popup.



Issues encountered in merging are listed as above.

NOTE: If an error message appears after the import is complete as shown above, the users listed in the error message were *not* merged to the device because of conflicting data (see the import logic process for users that exist in both files on pg. 40). View the names on the file you were trying to import and make sure that no passcodes or proximity cards are the same as already existing users (see *Understanding User Files*, pg. 40).

Managing Users (Continued):

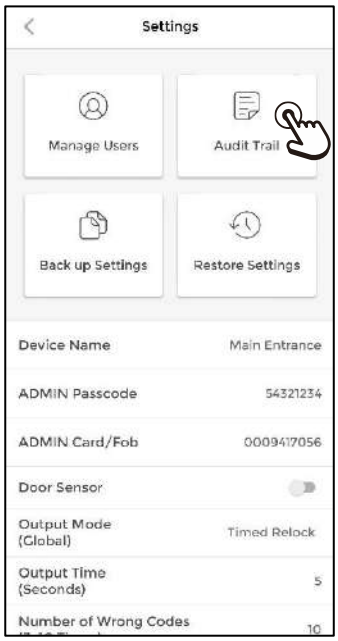
Understanding User Files

1. Exported user filenames will follow the format: "Device Name_Users_Date_Time.csv" where the date is shown YYYYMMDD, and the time is in 24-hour (military) format without the colon. For example, the exported user filename for the device named "Main Entrance" exported on June 14, 2020, at 10:47PM would be: *Main Entrance_Users_20200614_2247.csv*.
2. Exported files are saved in your phone's app data folder, though you can also share them to other locations using email or various messaging apps or by saving them to a synchronized folder such as *My iPhone*, *Google Drive*, *Dropbox*, etc.
3. You can only directly import files saved to your phone's app data folder. To import a file from elsewhere, you will need to move it to your phone's app data folder (see below).
4. Each time you export a user list, a new file is created on the phone. These files cannot be deleted from within the *SL Access* app. To delete old files, connect your phone to your computer with a USB cable and view the folders within your computer's File Manager for Android phones. For iOS phones, use the MacOS Finder on an Apple computer or iTunes on Windows computers.
5. When importing a user file on a device that already has users, the existing file is not overwritten, and no users are deleted. Instead, the lists will be merged according to the following the logic process.
   a. For users with *identical User IDs*, the import will overwrite the existing data.
   b. If two different users have the same passcode and/or the same proximity code, the existing user with that data will not be overwritten, and an error message will be generated.
   c. A new User ID will result in a new user added to the list.
   d. No users will be deleted.
6. Exported user files are saved as special .CSV files. They can be viewed in any spreadsheet, but if you want to edit them and import them again, they must be imported into a spreadsheet (not opened) in a special format and following a special procedure. For more information, see pg. 48, or visit the device product page at www.seco-larm.com.
7. File names for devices named in a right-to-left language (such as Arabic) will not display correctly onscreen unless the phone's language setting is also a right-to-left language.

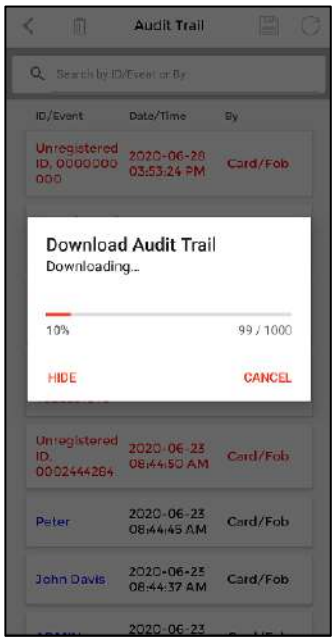
The Audit Trail:

The device will keep a record of all events, including entries, egress button presses, rejected access, door forced/propped-open alarms, tamper alarms, toggle on/off, and activation of *Door Remain Unlocked* or *Locked*. These are saved to an audit trail which can be downloaded and saved to your phone and to an external location.

Viewing the Audit Trail



Click the *Audit Trail* button on the ADMIN settings screen.



A popup shows the download progress. Click *Hide* to view the more recent records while the download is in progress

Click the circular *Refresh* icon to reload the audit trail.

NOTE: Viewing the Audit Trail ***does not save it*** to your phone. See the following page to save and/or export the Audit Trail.

The Audit Trail (Continued):

Searching / Filtering the Audit Trail

You can use the search box to filter the *Audit Trail* to show any series of characters from either the *ID/Event* column or the *By* column simply by typing the characters you are searching for.

The list will continue to filter in real time as you type any additional characters.

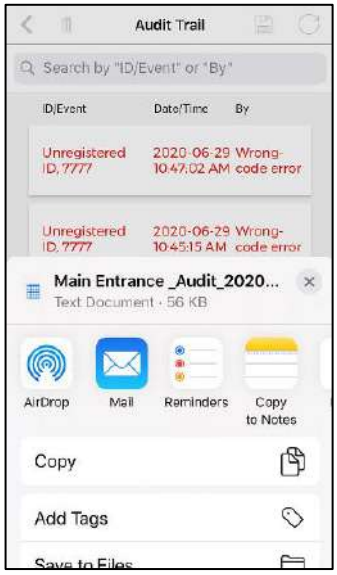
Note that in the example left, typing "lo" shows *Car**lo**s*, *Toggle **lo**cked*, and *Toggle un**lo**cked* in the *ID/Event* column and *Remain **lo**cked activated* in the *By* column.

Saving / Exporting the Audit Trail

Click the *Disk* icon to save and/or export the Audit Trail.

Android

OR

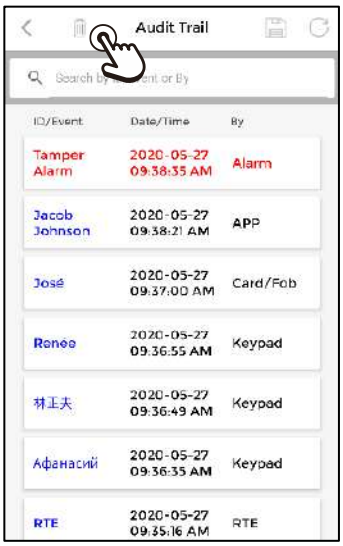


iOS

A popup will appear allowing you to share or send to an additional location in addition to the phone's app data folder. If you don't wish to do so, simply click anywhere above the popup and the file will only be saved on this phone.

The Audit Trail (Continued):

Clearing the Audit Trail

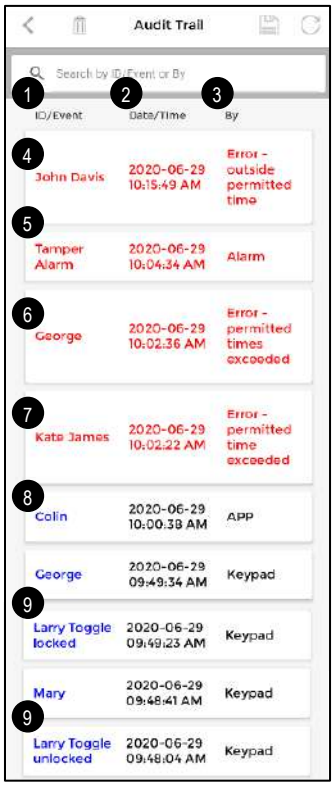


After saving and exporting the *Audit Trail* for archive, you may want to clear the *Audit Trail* to start afresh.

To clear the current *Audit Trail* from the device, simply press the trash can icon at the top of the page.

NOTE: Pressing the trash can icon does not delete any *Audit Trail* file that you have saved to your phone or exported to another location. It only deletes the records from the current *Audit Trail* to allow you to start over with the records cleared.

Understanding the Audit Trail



1. The *ID/Event* column shows the user name, if valid, and/or a description of the event recorded.
2. The audit trail is sorted by date/time with the most recent events at the top. The format of the date and time will depend on your phone's settings.
3. The *By* column shows the method used or error messages.
4. For scheduled users (see pg. 29), if they attempt to access the device outside of their permitted time range, you will see "Error – outside permitted time" in the *By* column.
5. If the tamper alarm has been triggered, it will show in the *By* column.
6. For users limited to a number of entries (see pg. 29), if they attempt to access the device after they have exhausted their limit, you will see "Error – permitted times exceeded" in the *By* column.
7. For temporary users limited to a certain time period (see pg. 29), if they attempt to access the device beyond their permitted time, you will see "Error – permitted time exceeded" in the *By* column.
8. The method used to gain entry will be shown in the *By* column (APP, Keypad, Card/Fob).
9. When a user with *Output Mode* set to *Toggle* (see pg. 33) accesses the device, the toggle will be recorded along with the action, "unlocked" or "locked."

The Audit Trail (Continued):

Understanding the Audit Trail (Continued)

10. If anyone who is not a registered user tries to access the device, this will be recorded as "Unregistered ID" and if a card/fob is used, the code number of the card/fob will be recorded. If the keypad was used, the passcode that the user tried will be recorded (see notes below).
11. If a user who is not permitted to use either the APP, keypad, or card/fob (see pg. 29) tries to use that method, the message "Error – keypad use restricted" (or APP or card/fob) will show.
12. If someone forces the door open, or if the door is left open beyond the set relock time, a "Door forced open" message will appear. The device cannot distinguish between the two events. Note that this requires a connection to a door sensor.
13. Any press of the egress button will also be reported as "RTE", but the device will not be able to determine who used the egress button

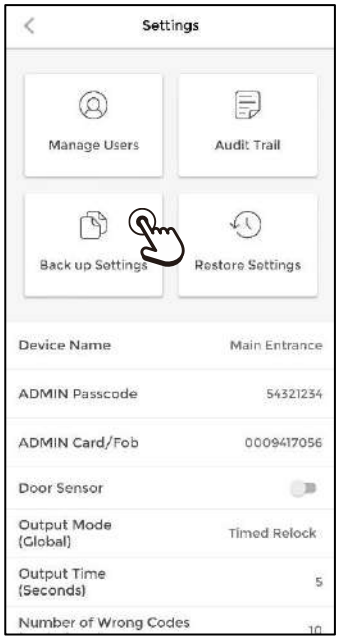
NOTES:

a. During the audit trail download, the device will be inaccessible to users, except for the Egress button (which will always be available for safety reasons). However, egress button presses during the audit trail download will not be recorded to the audit trail.
b. The audit trail saves the last 1,000 events. When it reaches that number, the oldest events will be overwritten. To keep a permanent record, download the trail regularly before it reaches 1,000 events and then clear the current audit trail on the device for a fresh start.
c. Messages that may require the ADMIN's particular notice will be in red.
d. When downloading the audit trail, the file will be saved to the phone's app data folder, but can also be saved to an additional location or shared via another app.
e. The audit trail is a .CSV file and can be opened in a spreadsheet program on a computer for easier viewing. The filename format is "Device name_Audit_Date_Time.csv" where the date is written as YYYYMMDD and the date is in 24-hour (military time) format, so a file for the Main Entrance device created on June 30, 2020, at 4:00 PM would be named: *Main Entrance _Audit_20200630_1600.csv*.
f. Each time you download the audit trail, a new file is created on the phone. These files cannot be deleted from within the SL Access app. To delete old files, connect your phone to your computer and use your computer's file manager, the MacOS Finder (on Apple computers), or iTunes (on Windows computers).
g. Passcodes are limited to no more than 8 digits. Should a person enter more than 8 digits before the # sign, this will be recorded as an unauthorized user but only the last 7 digits of the passcode, preceded by an asterisk, will be recorded. For example, if the passcode *1234567890#* is entered (10 digits), the audit trail will record this as *Unregistered ID *4567890*.

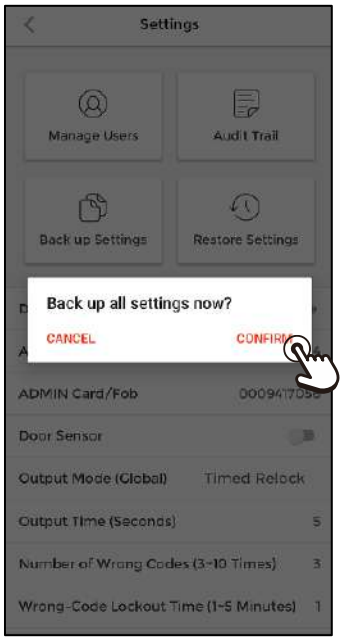
Backing Up Device Settings:

A device's settings can be backed up for future restoration. This does not back up or restore any user data, only the device settings including the ADMIN passcode and proximity card. On Android devices, the backup file can be moved off the phone for off-site backup and can also be used to duplicate the settings to another device (not available on iOS).

Back Up Device Settings



Click the *Backup Settings* button on the ADMIN settings screen.



A popup appears asking for confirmation. Click *Confirm* to accept.

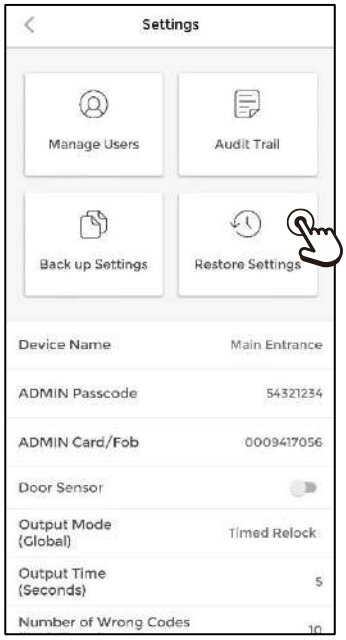
A popup shows the backup completed. Click *OK*.

NOTES:

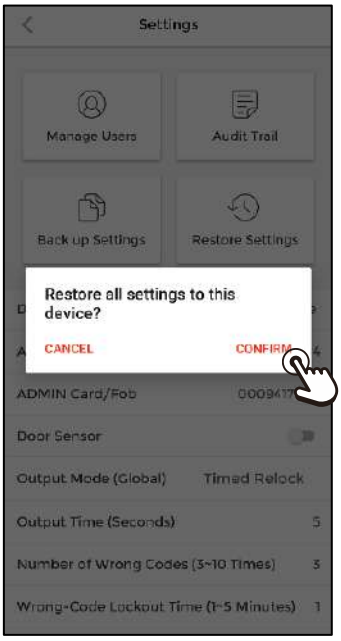
a. Your phone will only keep one backup file per device at any time. Each time you back up a device, the previous backup is overwritten.
b. If you have multiple devices, each device will have a separate backup file and other device backups will remain.
c. The backup file will be stored in the phone's app data folder on Android devices. On iOS devices, it is saved in the app's program folder which is not user accessible.
d. The filename format is "Device Name_Backup.bp" so for the Main Entrance, the filename would be: *Main Entrance_Backup.bp*.

Restoring Device Settings or Replicating to Another Device:

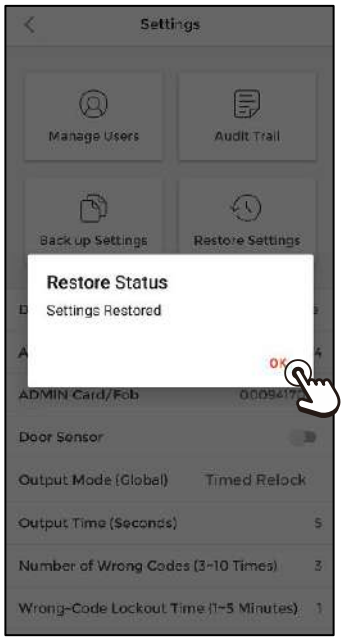
Restore or Replicate Device Settings



Click the *Restore Settings* button on the ADMIN settings screen.



A popup appears asking for confirmation. Click *Confirm* to accept.



A popup shows the restore completed. Click *OK*.

NOTES:

a. Your phone will restore from the backup file with the same device name as your device.
b. To replicate settings to another device, connect your Android phone to a computer's USB port to find the backup file that you wish to use, copy the file, and rename it so that it begins with the receiving device's device name.
c. Be careful when renaming the file to only change the device name and make sure that it is spelled and capitalized correctly.
d. Replication can only be done on an Android phone.

HINT: Another option for replication (which can also work on iOS) is to temporarily give the second device the same name as the first, then use *Restore Settings* on the second device. After the restore is complete, rename the second device to a more suitable name.

Resetting the Device:

There are two stages in resetting the device, depending on what you want to reset.

Resetting Only the ADMIN Passcode

1. Power the device off, remove the security screw, and detach the unit from the base.
2. On the back of the device is a set of jumper pins (see diagrams below). The jumper should be on pins 1 and 2.
3. Move the jumper to the reset pins 2 and 3.
4. Power up the device and wait for 5 seconds. After you hear a short beep, the ADMIN password is reset to 12345.
5. Remove power, restore the jumper to pins 1 and 2, reinstall, and power on the device.

Jumper Pins

1 2 3
Normal
(default)
Pins 1 and 2

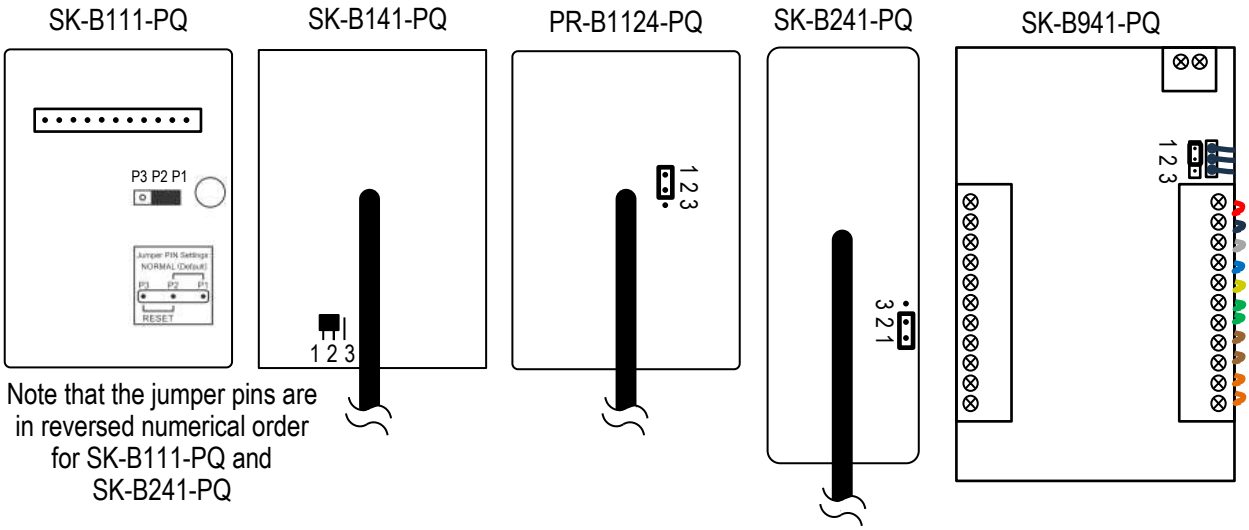
1 2 3
Reset
Pins 2 and 3

Resetting the Device to Factory Default

To reset the device to factory default, removing the user list and audit trail and clearing all settings:

6. Follow the above steps 1~4 but continue to wait another 5 seconds after hearing the first short beep.
7. You will then hear 1 long beep, indicating that a full reset is now being started to return the keypad/reader to factory default.
8. Keep waiting until you hear 1 short beep. At this point, a full reset has been completed.
9. Remove power, restore the jumper to pins 1 and 2, reinstall, and power on the device.

Jumper Pin Locations



Note that the jumper pins are in reversed numerical order for SK-B111-PQ and SK-B241-PQ

NOTES:

a. If your device firmware version is 2.21, resetting the device to factory default will not reset the device name. The device name will remain as you had previously set it.
b. If your device firmware is 2.22 or later, resetting the device to factory default will also reset the device name.
c. For information about updating firmware, see pg. 53.

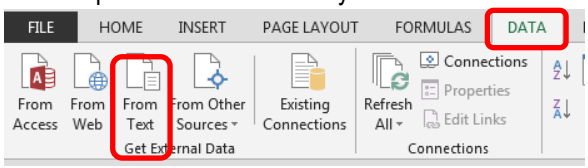
Editing an Exported User File on a Computer

For very large user lists where you need to make multiple changes, it may be more convenient to edit the files on a computer. However, you must follow the editing steps very carefully. This feature is for advanced users and assumes that you know how to use a spreadsheet program and get the files from your phone to a computer and back again.

NOTE: Some spreadsheet programs, even though they allow you to import a UTF-8 CSV file, do not allow you to save in that format. Standalone versions of Excel 2016 and later and Office 365 versions do allow you to save in UTF-8 CSV file formats, but earlier versions do not. If you have a spreadsheet version which does not support this, there are some workarounds that you can find on various help websites.

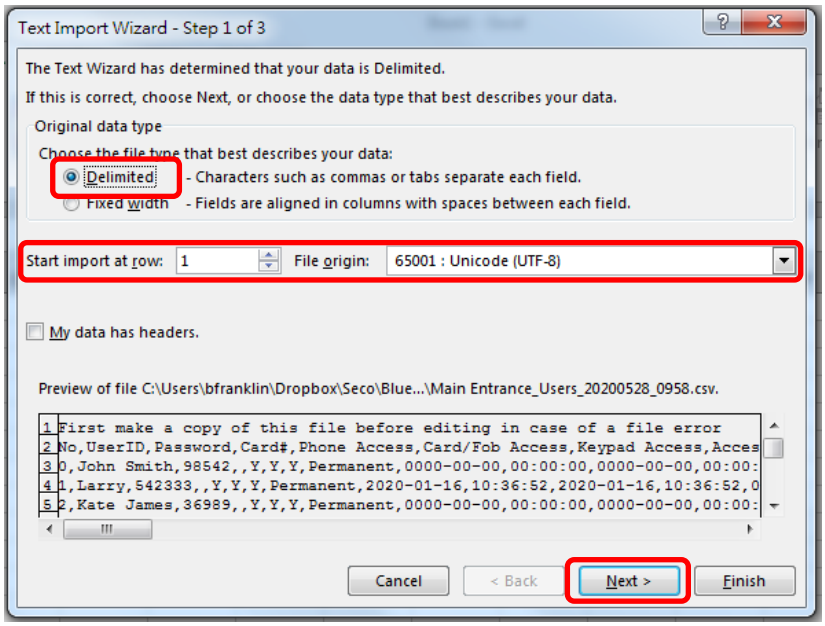
Open a new, blank spreadsheet in your chosen program. The following photos use Excel as an example but other programs should have similar options.

1. Do not open the user file directly. Instead use the data import feature and import as a text file.



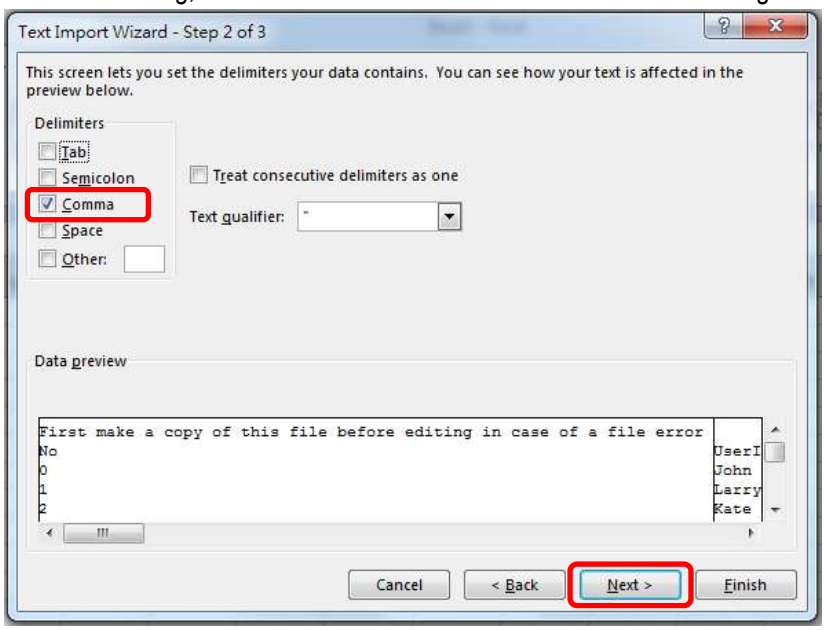
2. From the dialog box that opens, navigate to the correct folder, choose your user file, and click on "Import."

3. In the next dialog, choose "Delimited," "Start at row 1," and for the "File origin," choose "65001 : Unicode (UTF-8)" and click "Next."

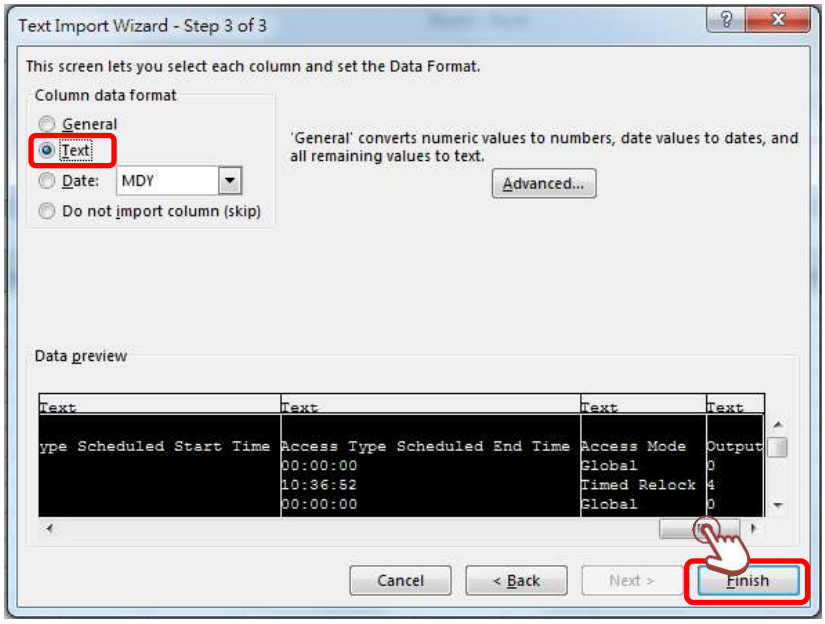


Editing an Exported User File on a Computer: (Continued)

4. In the next dialog, choose "Comma" as the delimiter and ensure nothing else is checked. Click the "Next" button.

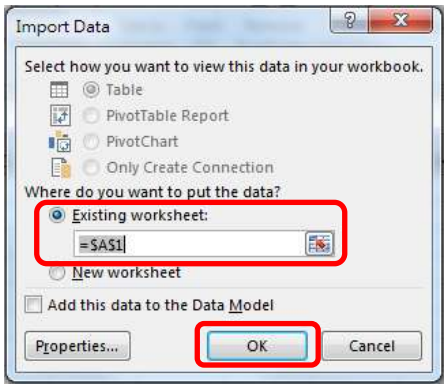


5. In the next dialog box, click on the horizontal scroll button and drag to the right so that the last field is showing. Holding down the shift key, click on the last field. All the fields should now be highlighted. Choose "Text" as the "Column data format" and click the "Finish" button.



Editing an Exported User File on a Computer: (Continued)

6. A final dialog will pop up. Choose "Existing worksheet" and starting at "=A1" if these are not already chosen and click "OK."

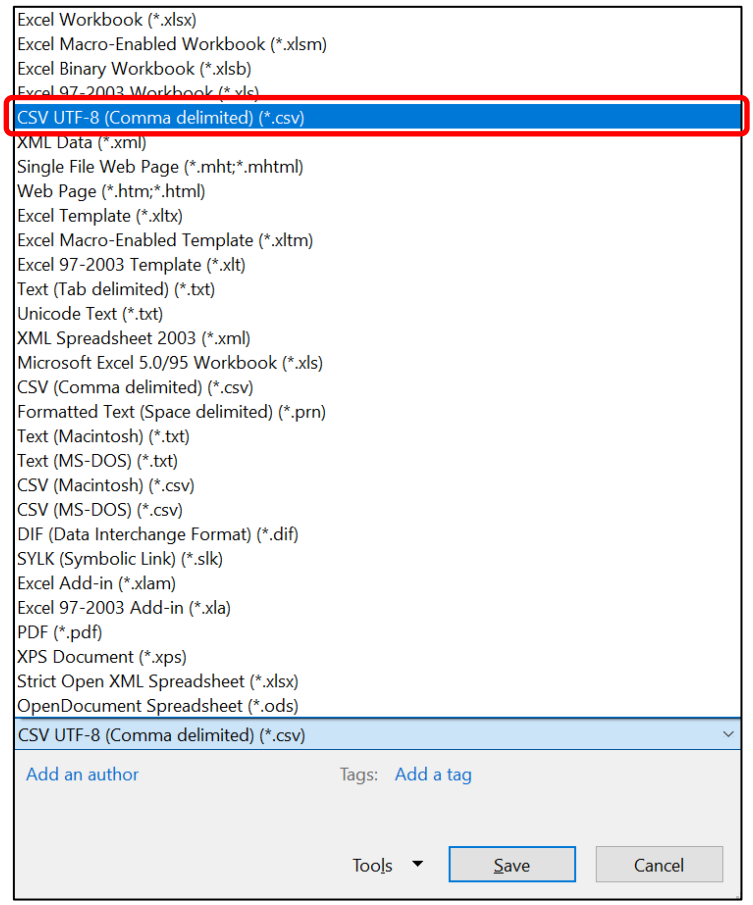


7. You can then edit the worksheet. However, you must take care not to change either the headers (Rows 1~2) or column A.

   a. For other columns, make sure that no User ID, Passcode, or Card# is duplicated.
   b. In order to avoid errors in spelling or word choice, if you change another text column such as the "Access Type" column, it is best to find another user with the same setting and copy from that user.
   c. Make sure that you use the same time (24-hour military time) and date (YYYY-MM-DD) format as you see already used for existing users and that the end date/time is after the start date/time.

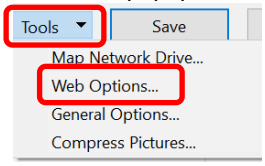
Editing an Exported User File on a Computer: (Continued)

8. When finished, use the "File, Save As" to save to the correct folder. In the popup dialog, first change the file format to "CSV UTF-8 (Comma delimited) (*.csv)" format.

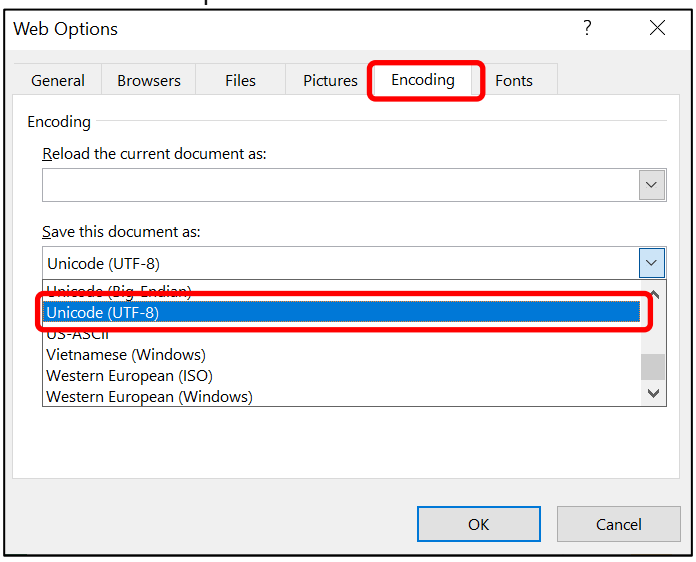


Editing an Exported User File on a Computer: (Continued)

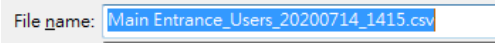
NOTE: In some versions of Excel, you may have to click on the "Tools" dropdown near the "Save" button in the "Save As" popup, click on "Web Options…,"



then click on the "Encoding" tab and then choose this format in the "Save this document as:" dropdown in order to have the option to save in this format.

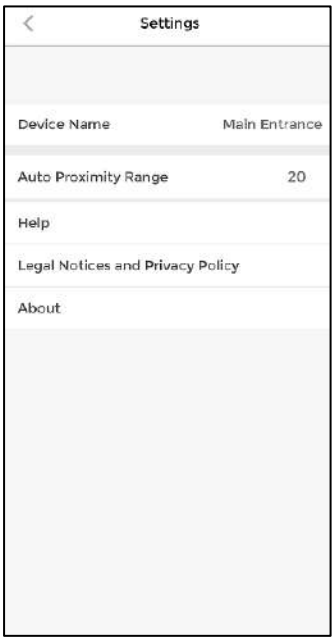


9. The filename will be a generic name such as "Book1" so you must change that to a name that your device will recognize as a user file. The easiest way is to click on the original file, but then change that datecode and/or timecode in the filename. In the following example, you can see the device name, the user file designation, then the datecode (20200714 for July 14, 2020) and timecode (1415 for 2:15PM).



10. Move that file back to the app data folder on your phone using a USB connection to your computer. It will then appear in your import list when you attempt to import a user file to the device (or any ENFORCER Bluetooth Access Control device).

Instructions to Users:



Users will use the same app to access the device, however users will not have access to any device settings and will only be able to adjust their Auto proximity range.

The user *Home* screen will look the same and they will log in with the User ID and passcode assigned by the ADMIN.

The user *Settings* screen will show the *Device Name* that they are connected to and the links as shown to the right of this paragraph. The only thing that they can adjust is the *Auto Proximity Range* for their particular phone.

The user can install the app to multiple phones. They will still need to log in with their User ID and passcode for a particular device to use the app on that device.

If not restricted by the ADMIN, the user may use the app, their passcode on the keypad, or, on devices that include a proximity reader, a proximity card/fob provided by the ADMIN.

For the ADMIN's convenience, we have placed a downloadable *User Instruction* file on each product page on SECO-LARM's website. It is a fillable PDF that you can give to users, providing them with basic instructions for downloading what they need to get started. There are blanks for their User ID, passcode, device name, device location, and effective date as well as instructions for downloading the *SL Access User Guide* and a download link for the *SL Access* app. It is designed to be filled out and either printed or sent as an email attachment along with the *SL Access User Guide*.

Firmware Version Updates:

The device you purchase will have the latest firmware update available at the time, however if there are future firmware updates available, there will be a notice on the product page of the SECO-LARM website. Download the *SL Access OTA Firmware Update Guide* for instructions on how to download and install it. Note that firmware updates can only be installed using an Android phone.

Troubleshooting:

Users can't access the device and the LED is flashing between red and blue	• The wrong-code lockout has been activated. Either wait till the set lockout time has expired, or the ADMIN can use the app to interrupt the lockout.
I no longer have the ADMIN password	• See the instructions for resetting just the ADMIN password on pg. 47.
My device doesn't show on the home screen	• Move closer to the device. • Exit and reopen the app.
I've lost the phone which I've used as ADMIN	• You can switch to any other phone and log in with your ADMIN password. However, immediately change the ADMIN password for better security. It's also recommended that you remotely erase the lost phone.
The home screen always says "Log In" even after I have logged in	• Bluetooth LE doesn't keep a permanent connection to your phone so it can't know whether you are logged in to a nearby device or not. You should normally not need to log in again if you continue to use the same device.
Another device is showing on my home screen though I am not logged in to that device	• The app will scan for and show nearby devices and the strongest signal will appear at the top of the screen. However, you will not be able to access the device unless you have the device's ADMIN passcode or a user passcode for the device.
Clicking "Settings" does not take me to the ADMIN settings	• Make sure that the device shown at the top of the home screen is a device you have credentials for. • Make sure that you have logged in as ADMIN.
I'm seeing "Door forced open" in the Audit Trail, but I know no one has forced entry	• The same message is used to indicate a door propped open. If a door is kept open longer than the set relock time, it will register as "Door forced open."
The locked icon returns to the home screen even when the door is still unlocked	• The unlocked icon only shows that a signal has been sent to unlock the door. Because Bluetooth LE only maintains the connection long enough to send an "unlock" signal, it cannot know when the door is relocked.
A user is not able to unlock the door	• Ensure that the user is logged in with the correct user ID and passcode. • Ensure that the user is within the time scheduled or the number of times limit. • If scheduled or temporary, make sure that the time settings, including for AM and PM, are correct.
I can't find the settings backup file on my iOS phone	• The settings backup file is not accessible on iOS devices.

Accessories Available from SECO-LARM:

Proximity Cards

PR-K1S1-A

Proximity Key Fobs

PR-K1K1-AQ

California Proposition 65 Warning: These products may contain chemicals which are known to the State of California to cause cancer and birth defects or other reproductive harm. For more information, go to www.P65Warnings.ca.gov.

The *Bluetooth*® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by SECO-LARM is under license. Other trademarks and trade names are those of their respective owners.

IMPORTANT WARNING: For a weather-resistant installation, ensure that the unit is properly sealed where the housing base meets the wall so that no moisture can reach the wiring. Incorrect mounting may lead to exposure to rain or moisture which could cause a dangerous electric shock, damage the device, and void the warranty. Users and installers are responsible for ensuring that this product is properly installed and sealed.

IMPORTANT: Users and installers of this product are responsible for ensuring that the installation and configuration of this product complies with all national, state, and local laws and codes related to locking and egress devices. SECO-LARM will not be held responsible for the use of this product in violation of any current laws or codes.

FCC/IC COMPLIANCE STATEMENT FOR *BLUETOOTH*® MODULE **FCC ID: K7TRB8762** **IC ID: 2377ARB8762**

THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES. OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS: (1) THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE AND (2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED, INCLUDING INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION.
Notice: The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
IMPORTANT NOTE: To comply with the FCC RF exposure compliance requirements, no change to the antenna or the device is permitted. Any change to the antenna or the device could result in the device exceeding the RF exposure requirements and void user's authority to operate the device.
This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

WARRANTY: This SECO-LARM product is warranted against defects in material and workmanship while used in normal service for one (1) year from the date of sale to the original customer. SECO-LARM's obligation is limited to the repair or replacement of any defective part if the unit is returned, transportation prepaid, to SECO-LARM. This Warranty is void if damage is caused by or attributed to acts of God, physical or electrical misuse or abuse, neglect, repair or alteration, improper or abnormal usage, or faulty installation, or if for any other reason SECO-LARM determines that such equipment is not operating properly as a result of causes other than defects in material and workmanship. The sole obligation of SECO-LARM and the purchaser's exclusive remedy, shall be limited to the replacement or repair only, at SECO-LARM's option. In no event shall SECO-LARM be liable for any special, collateral, incidental, or consequential personal or property damage of any kind to the purchaser or anyone else.

NOTICE: The SECO-LARM policy is one of continual development and improvement. For that reason, SECO-LARM reserves the right to change specifications without notice. SECO-LARM is also not responsible for misprints. All trademarks are the property of SECO-LARM U.S.A., Inc. or their respective owners. Copyright © 2024 SECO-LARM U.S.A., Inc. All rights reserved.

SECO-LARM® U.S.A., Inc.
16842 Millikan Avenue, Irvine, CA 92606 Website: www.seco-larm.com
Phone: (949) 261-2999 | (800) 662-0800 Email: sales@seco-larm.com

MI_SKPR-Bxxx-xQ_240313.docx