

ENFORCER®

SK-2612-SFSQ

Fingerprint Reader and Keypad

Manual



Features:

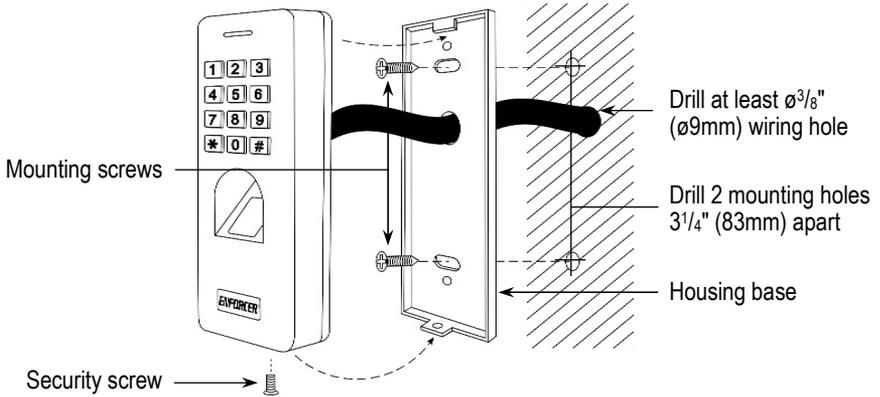
- 500DPI Optical fingerprint reader
- Up to 3,000 users (up to 1,000 fingerprint users, up to 2,000 PIN users)
- User code length 4-6 digits
- Fingerprint identification time – ≤ 1 second
- Fingerprint false acceptance rate – $\leq 0.01\%$
- Fingerprint false rejection rate – $\leq 0.1\%$
- 12VDC Operation
- Form C relay output – 2A@12VDC
- Tamper alarm output – 2.5A@12VDC
- Adjustable relay output time – 100ms~99s, or toggle
- Weatherproof – IP66
- Illuminated fingerprint reader window
- Wiegand output
- 2-Door interlock

ENFORCER Fingerprint Reader and Keypad

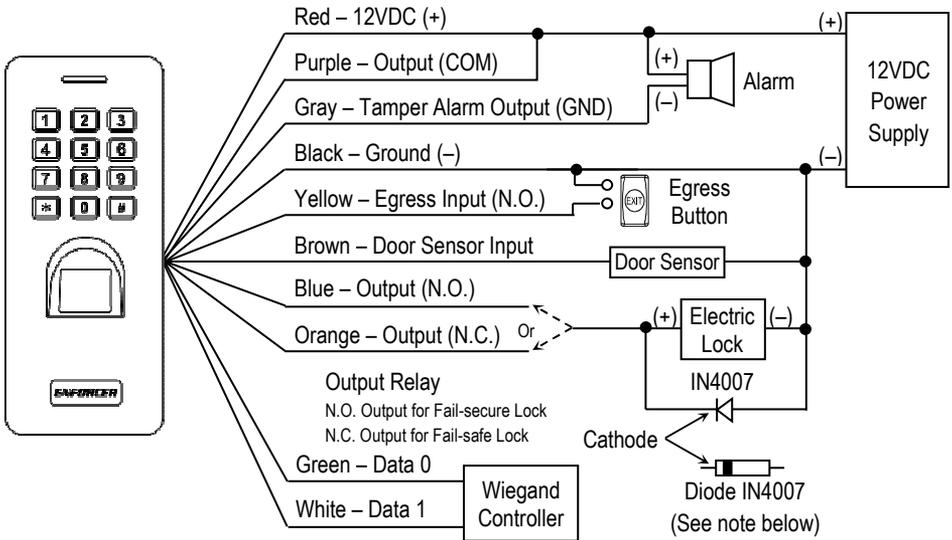
Quick Installation Guide:

This page is for installers looking to do a basic installation and programming of the fingerprint reader and keypad. For more in-depth installation and programming instructions, see "Table of Contents" on pg. 4.

Mounting Diagram:



Quick Wiring Diagram:



NOTE: For DC-powered electric strikes, connect the included diode as close as possible and in parallel with the electric strike. This absorbs possible electromagnetic interference to prevent operation of the strike from damaging the fingerprint reader/keypad. Do not connect a diode when using electromagnetic locks or with AC powered strikes.

Quick Programming Guide:**Programming Tips:**

- Master programming code (6 digits) should be programmed before any other programming.
- A steady red LED indicates that fingerprint reader/keypad is in standby mode. A flashing red LED indicates that fingerprint reader/keypad is in base programming mode. A steady orange LED indicates the unit is in function programming mode.

Programming Instructions:

Follow the instructions below if the following covers your needs:

- A new master programming code.
- Setting one user fingerprint and one user code.
- A door-unlocked time of 3-seconds after the output is activated.

1. Enter programming mode:

* 1 2 3 4 5 6 #

NOTE: 1 2 3 4 5 6 is the factory default master programming code. A new master programming code (6 digits) should be set the first time you enter programming mode. There is no master programming fingerprint.

2. Set the master programming code (6 digits):

0 x x x x x x # x x x x x x #

NOTE: x x x x x x is the new master programming code and must be entered twice.

3. Set a user fingerprint to operate the output (unlock the door):

1 3 # U U

NOTES:

- 3 # chooses fingerprint user ID #3 of 998 possible fingerprint users (1~998). (Omit 3 # to use auto ID to assign the first available user ID.)
- U is the new user fingerprint (must be presented twice to set).

4. Set a user code to operate the output (unlock the door):

1 1 0 0 1 # 4 5 8 7 #

NOTES:

- 1 1 0 0 1 # chooses user code ID #1001 of 2998 possible user codes (1001~2998).
- 4 5 8 7 is the new user code for user ID #1001 (4~6 digits).

5. Set the output time (skip this step if the default value of 5 seconds is acceptable):

3 3 #

NOTE: 3 sets the output delay time for 3 seconds.

6. Exit programming mode:

*

ENFORCER Fingerprint Reader and Keypad

Table of Contents:

Quick Installation Guide:	2	Programming User Fingerprints:	11~13
Mounting Diagram:	2	Programming User Codes:	14
Quick Wiring Diagram:	2	Deleting User Fingerprints or User Codes:	15~16
Quick Programming Guide:	3	Programming Output Mode and Time:	16~17
Table of Contents:	4	Programming Access Mode / Security Level:	17~18
Features:	4	Programming Keypad Sounds/Notifications:	18~19
Specifications:	4	Programming the External Alarm Output:	19
Overview:	5	Programming Door Propped-Open / Forced-Open Detection:	20
Parts List:	5	Programming the Wrong-Code Lockout/Alarm:	21
LED Indicators and Device Sounds:	5	Wiegand Pass-Through Connection Diagram:	22
Important Notes:	5	Programming Wiegand Pass-Through Operation:	22~24
Installation:	6	Setting Up an Interlock System with Two Keypads:	24~25
Wiring Chart:	6	Resetting the Fingerprint Reader/Keypad:	25
Sample Application:	7	Installer Notes:	26
Getting Ready to Program:	7-9	User Operation of the Fingerprint Reader/Keypad:	27
Programming Master Add/Delete Fingerprints:	9-10	Troubleshooting:	28
Programming Format and Default Values:	10	Warranty:	28
Programming the Master Programming Code:	10		
Programming Super User Codes/Fingerprints:	11		

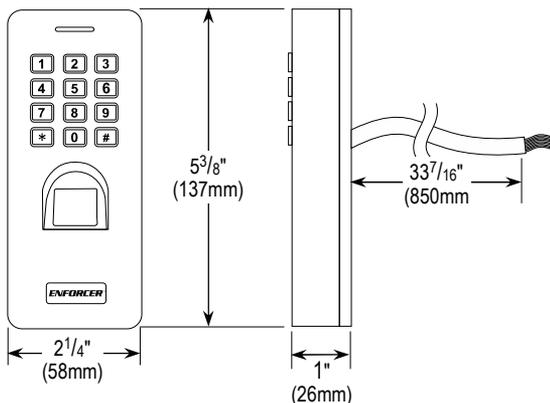
Features:

- 12VDC Operation
- Up to 1,000 fingerprint users (1~1000)
- Up to 2,000 user codes (1001~3000)
- Output: Form C relay, 2A@12VDC max.
- Output can be programmed to activate for up to 99 seconds or toggle
- Tamper alarm output: Transistor ground, 2.5A@12VDC max.
- Fingerprint reader window illuminates when finger is present
- EEPROM Memory protects programmed information in case of power loss
- All features programmed directly from the fingerprint reader/keypad: No need for an external programmer
- Egress input lets users exit the premises without a fingerprint or keying in a code
- 500DPI Optical fingerprint reader
- Fingerprint identification time – ≤1 second
- Fingerprint false acceptance rate – ≤0.01%
- Fingerprint false rejection rate – ≤0.1%
- Weatherproof – IP66
- Wiegand output
- 2-Door interlock

Specifications:

Operating voltage		12VDC
Current draw	Standby	45mA@12VDC
	Active	200mA@12VDC (max.)
Outputs	Form C	2A@12VDC
	Tamper alarm	2.5A@12VDC
Egress input		N.O. Ground
Door sensor input		N.C. Ground
Enclosure material		Zinc alloy
Operating temperature		-22°~140° F (-30°~60° C)
Operating humidity		20~90%
Dimensions		2 ¹ / ₄ "x5 ³ / ₈ "x1" (58x137x26 mm)
Weight		14.2-oz (400g)

Overview:



Parts List:

1x Fingerprint reader and keypad	1x Security wrench	1x Diode
2x Mounting screws	2x Mounting screw anchors	1x Manual

LED Indicators and Device Sounds:

Status	Sounds	LED
In standby mode	--	Red steady
In base programming mode	1 Beep	Red flashing
In function programming mode	1 Beep	Orange steady
Exit programming mode	1 Beep	Red steady
Successful operation	1 Beep	Green steady
Unsuccessful operation	3 Fast beeps	
Notification output	Rapid beeping*	Red flashing rapidly

*De-activate the notification or alarm by presenting a valid user fingerprint or by entering a valid user code.

Important Notes:

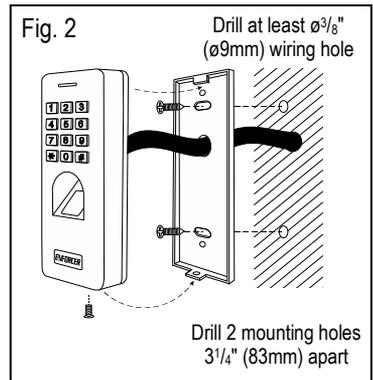
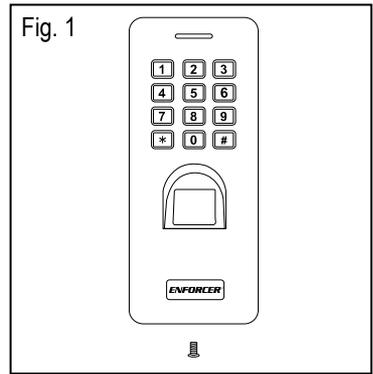
IF USING THE FINGERPRINT READER/KEYPAD WITH A MECHANICALLY OPERATED DOOR OR GATE, MOUNT THE UNIT AT LEAST 15' (5m) FROM THE DOOR OR GATE TO PREVENT USERS FROM BEING CRUSHED OR PINNED. FAILURE TO DO SO MAY RESULT IN SERIOUS INJURY OR DEATH.

1. Always disconnect power before servicing the fingerprint reader/keypad. Do not apply power until all connection wiring is completed.
2. The fingerprint reader/keypad must be properly grounded. Use a minimum 22AWG wire connected to the common ground wire. Failure to do so may damage the unit.
3. All wiring and programming should be done by a professional installer to reduce the risk of improper installation.
4. The user's operating guide for this fingerprint reader/keypad is located on pg. 27 of this manual. Be sure to store this manual in a safe place for future reference.

ENFORCER Fingerprint Reader and Keypad

Installation:

1. Find a suitable location to mount the fingerprint reader/keypad. Install it at a height at which most users will be able to easily operate the unit.
2. Using the included security wrench, unscrew the security screws located on the bottom of the fingerprint reader/keypad (Fig. 1).
3. Carefully remove the fingerprint reader/keypad from the housing base, sliding the keypad slightly upwards.
4. Using the housing base as a template, mark the holes needed for the wiring and mounting screws and drill needed holes. Ensure that the wiring hole is large enough to allow the wiring to be pushed in without crimping.
5. Run wiring through the wall to the wiring hole cut in the wall
6. Thread the wiring through the center of the fingerprint reader/keypad's base.
7. Install the base using the included mounting screws and mounting screw anchors (if necessary). Ensure the correct orientation as shown in Fig. 2.
8. Connect the wires to the fingerprint reader/keypad according to "Wiring Chart" below.
9. Finish assembly by reattaching the fingerprint reader/keypad to the base and securing with the security screw.

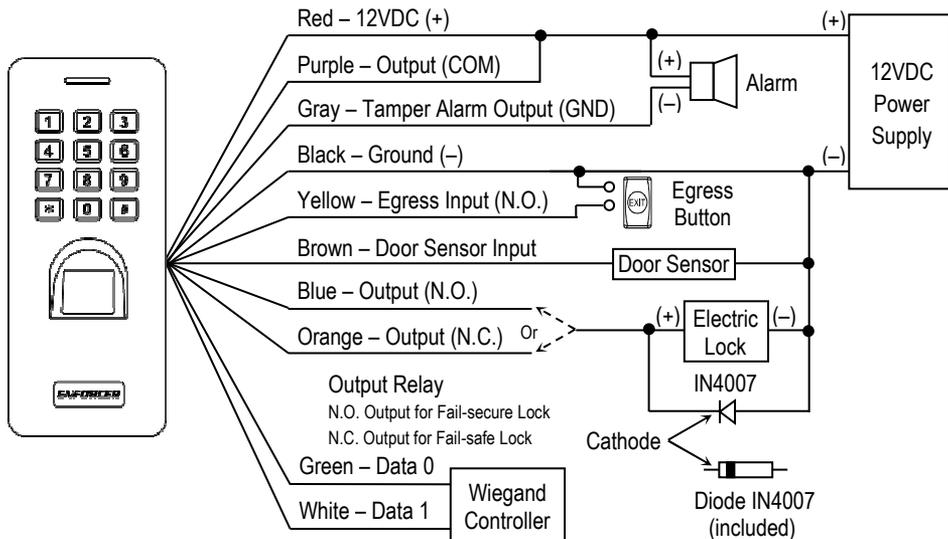


NOTE: For weatherproof installation, add a bead of silicone sealant around the base where it meets the wall.

Wiring Chart:

Connection Wires		
Color	Function	Description
Red	Power (+)	Connect to +12VDC power supply
Black	Ground (-)	Connect to Ground
Yellow	Egress Input	N.O. Pushbutton contact to ground. Press button to activate the output
Brown	Door Sensor	Connect to a magnetic contact or door sensor
Blue	Output N.O.	NO/NC/COM, relay output, max. 2A@12VDC
Purple	Output COM	
Orange	Output N.C.	
Gray	Alarm Output	Transistor ground output, max. 2.5A@12VDC. Switches to ground (-) when tamper switch activated.
Green	Data 0	Wiegand controller
White	Data 1	Wiegand controller

Sample Application:



NOTE: For DC-powered electric strikes, connect the included diode as close as possible and in parallel with the electric strike. This absorbs possible electromagnetic interference to prevent operation of the strike from damaging the fingerprint reader/keypad. Do not connect a diode when using electromagnetic locks or with AC powered strikes.

Getting Ready to Program:

The fingerprint reader/keypad can be set to be activated by users using either a keypad user code or a fingerprint. All fingerprints and user codes must have a unique User ID (between 1 and 3000). User IDs may be specifically selected or, for fingerprints, may be either specifically selected or automatically assigned. It is important to record all User IDs for future management tasks

Keypad code:

There are three types of keypad codes:

- **Master programming code** – Used only for entering programming mode. The initial master programming code is disabled after setting the new master programming code. The master programming code is 6 digits in length and there can be only one master programming code per keypad.
- **Super user code** – 2 Super user codes (user IDs 2999 and 3000) can be assigned to toggle between allowing and disallowing user access. When user access is disallowed, the doors will remain locked and not respond to other users' fingerprints or user codes.
- **User codes** – Up to 1998 user codes (user IDs 1001~2998) can be assigned. User codes are used to activate the relay.

Both types of user codes may be 4~6 digits in length, but the master code must be 6 digits.

Getting Ready to Program (Continued):

Fingerprints:

There are three types of fingerprint entries:

- Master add/delete fingerprints – 2 Master fingerprints can be assigned as master fingerprints which are only used for conveniently adding/deleting user fingerprints. The first master fingerprint programmed is for adding user fingerprints and the second is for deleting user fingerprints (see "Programming the Master Add/Delete Fingerprints," pgs. 9~10). Master add/delete fingerprints **are not** used to enter programming mode.
- Super user fingerprints – 2 Super user fingerprints (user IDs 999 and 1000) can be assigned to toggle between allowing and disallowing user access. When user access is disallowed, the doors will remain locked and not respond to other users' fingerprints or user codes.
- User fingerprints – Up to 998 fingerprints (user IDs 1~998) can be assigned as user fingerprints. User fingerprints are used to activate the relay.

Security Levels:

There are four possible security levels (see "Programming the Access Mode / Security Level," pgs. 17~18):

- User code only – A user must use a user code for access (see "Programming User Codes," pg. 14).
- Fingerprint only – A user must use a fingerprint for access (see "Programming User Fingerprints," pgs. 11~13).
- Either user code or fingerprint – A user may use either a user code or a fingerprint for access (see pgs. 11~14).
- Multiple user codes or fingerprints – Multiple (2~9) user codes/fingerprints are required for access. Any combination of user codes or fingerprints in any order up to the set number must be used with no more than 5 seconds between each code/fingerprint. No particular user code/fingerprint can be repeated. This could be used for extremely secure areas requiring authentication by more than one person or requiring one person to either use both a user code and a fingerprint or multiple fingerprints/user codes (by assigning more than one user ID to that person, see pgs. 11~14).

NOTES for Multiple User Codes or Fingerprints:

- If the same user fingerprint/code is repeated, the device will return to standby without triggering the output.
- In multiple user code/fingerprint mode, the interval between each user code/fingerprint must not exceed 5 seconds, otherwise, the device will return to standby.

Getting Ready to Program (Continued):

Enter and Exit Base Programming Mode:

All programming of the fingerprint reader/keypad is done from base programming mode.

1. Enter base programming mode using the master programming code:

One beep will sound, the LED will flash red to indicate the unit is in base programming mode. From there you may press a function code to enter function programming mode (the LED will change to steady orange).

NOTE:      is the master programming code.       is the default master programming code (see "Programming the Master Programming Code," pg. 10). The LED will flash red to indicate the keypad is in base programming mode.

2. Exit programming mode:

Press the  key or wait 25 seconds to exit automatically.

NOTES:

- **DO NOT DISCONNECT THE FINGERPRINT READER/KEYPAD FROM POWER WHILE IN PROGRAMMING MODE.** Disconnecting the unit while in programming mode may cause a memory error.
- The flashing red LED indicates that the unit is in base programming mode and will turn to steady orange when you press one of the programming function codes. If you are unsure which function you are in, press the  key to return to base programming mode (flashing red LED) and then press the number of the function to proceed (steady orange LED).
- Except for adding or deleting users with the master add/delete fingerprints, for all programming functions, the fingerprint reader/keypad must first be in base programming mode.

Programming Master Add/Delete Fingerprints:

Two master add/delete fingerprints are used only to conveniently add or delete user fingerprints. The first master fingerprint added will be the master add fingerprint, used for adding a new fingerprint user, and the second will be the master delete fingerprint, used for deleting a fingerprint user. The master add/delete fingerprints **are not** used to enter programming mode and **do not** serve as user fingerprints activating the output. To program the master add/delete fingerprints:

1. Power the reader/keypad off.
2. While holding down the egress button, power the keypad on. When you hear two beeps, release the egress button. The LED should change to orange. You must complete the process within 30 seconds of this point.
3. Program the master add fingerprint by pressing a finger against the reader and repeat.
4. Program the master delete fingerprint by pressing a different finger against the reader and repeat.
5. After 30 seconds, the keypad/reader will exit programming mode and the LED will return to steady red, or you can press the  key to exit immediately.

ENFORCER Fingerprint Reader and Keypad

Programming the Master Add/Delete Fingerprints (Continued):

NOTE: Programming the master add/delete fingerprints also resets the keypad to factory default. Though all user information is retained, the master code will return to the default 123456, and other settings will return to the default. Because of this, if you desire to use the master add/delete fingerprints, it is best to program them before programming any other settings.

Programming Format and Default Values:

In this manual, the format used for programming the keypad is as follows:

- A single-digit (\boxed{x}) FUNCTION CODE to tell the keypad what is being programmed.
- A varying number of digits (\boxed{x}) to represent the parameters of that FUNCTION.
- The $\boxed{\#}$ key to confirm programming of the FUNCTION and exit to base programming mode.
- The $\boxed{*}$ key to exit programming mode and return to standby mode.

The following is a list of the different programming functions:

Function Code*	Parameters	Default Functions and Values	Page #
0	Master programming code	Default 123456, code length 6 digits	10
1	Add user codes/fingerprints	No default, must be programmed	11~14
2	Delete user codes/fingerprints	No default, must be programmed	15~16
3	Output mode/time	Momentary 5 seconds	16~17
4	Access mode / security level	Either user code or fingerprints	17~18
5	Wrong-code lockout / external alarm	Lockout disabled, alarm enabled 1 minute	19, 21
6	Keypad sounds / interlock system / door propped-open/forced-open notification	Sounds enabled, interlock disabled, door open notification disabled	18~20, 24~25
7	Set device ID for Wiegand controller	0	22~23
8	Set Wiegand output bits/format	Output bits 26, output bits 4	23~24

*Press the function code only to enter the programming mode for that function. It should not be repeated between each parameter.

Programming the Master Programming Code:

The master programming code is used to enter programming mode. The master programming code does not serve as a user code to activate the keypad output.

1. Make sure the keypad is in base programming mode (see "Enter and Exit Base Programming Mode," pg. 9).
2. Enter the new master programming code (6 digits):
 $\boxed{0}$ \boxed{x} \boxed{x} \boxed{x} \boxed{x} \boxed{x} \boxed{x} $\boxed{\#}$ \boxed{x} \boxed{x} \boxed{x} \boxed{x} \boxed{x} \boxed{x} $\boxed{\#}$ (where "X" is the new master programming code)
3. Exit programming mode:
Press the $\boxed{*}$ key or wait 25 seconds to exit automatically.

Programming Super User Codes/Fingerprints:

Four super users (2 fingerprints, 2 codes) may be used to toggle the reader between disabling and re-enabling user access. Super user codes/fingerprints are not used to gain entry.

- When the reader is in normal access mode, present a super user fingerprint or enter a super user code to disable access to all users. The device will beep once and the LED indicator will flash red four times to indicate that user access has been disabled. No user fingerprint/code will be able to trigger the device.
- Presenting a super user fingerprint or entering a super user code again will re-enable user access. The device will beep once and the LED indication will flash green four times to indicate that user access has been enabled. The door remains locked, but user access is enabled for all users.

Super user codes/fingerprints are programmed in the same way as other user codes/fingerprints, but must be assigned the specific IDs of 999 or 1000 for super user fingerprints and 2999 or 3000 for super user codes. See "Programming User Fingerprints" on pgs. 11~13 and "Programming User Codes" on pg. 14.

Programming User Fingerprints:

There are several ways to program user fingerprints.

With Auto ID:

Auto ID allows the device to assign the user fingerprint to the first available fingerprint user ID in numerical order (IDs 1~998). When programming user fingerprints with auto ID, use the following formula after entering base programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

[1] [U] [U] – After a short beep, you may continue to add users consecutively without repeating the function code **[1]**

[1] – Add Users function code (LED will change to steady orange)

[U] – User's fingerprint

NOTES:

- To delete user fingerprints when the user to be deleted is not present, you will need to know the particular user ID of that person. Therefore, it is important that you record all user IDs as they are entered. In this case, if you have already previously added any fingerprint users, you will need to have a record in order to see which IDs are blank.
- **[U][U]** represents the user fingerprint, which must be presented twice. The unit will beep once and the LED will flash green once to indicate that the fingerprints were read successfully.
- Additional users may be entered in succession without repeating the function code **[1]**.
- Exit programming mode by pressing the **[*]** key after all programming is completed. One beep will sound and the LED will return to steady red. After 25 seconds of inactivity, the keypad will automatically exit programming mode and return to standby.

ENFORCER Fingerprint Reader and Keypad

Programming User Fingerprints (Continued):

With Specific ID:

Specific ID allows the programmer to assign the user fingerprint to a particular fingerprint user ID (any unused fingerprint user ID between 1 and 998 for common users; 999 or 1000 for super user fingerprints). When programming user fingerprints with specific ID, use the following formula after entering programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

1 **A A A A** **#** **U U** – After a short beep, you may continue to add users by repeating these steps, but without repeating the function code **1**.

1 – Add Users function code (LED will change to steady orange)

A – **1** to **10000** – 998 unique fingerprint user IDs for user fingerprints to trigger the device (and 2 super user IDs for super user fingerprints to toggle between disable and enable user access)

U – User's fingerprint

NOTES:

- Entering a User ID followed by the **#** key allows the programmer to assign a particular fingerprint user ID to the subsequent user fingerprint. If this step is omitted, the fingerprint reader/keypad will automatically assign the user fingerprint to the first available user ID.
- Each user ID must be unique and cannot be repeated for multiple user fingerprints or codes.
- **U U** represents the user fingerprint, which must be presented twice. The unit will beep once and the LED will flash green once to indicate that the fingerprints were read successfully.
- Additional users may be entered in succession without repeating the function code **1**.
- To return to base programming mode to program other functions, press the **#** key (the LED will flash red) followed by the function code for that function (LED becomes steady orange).
- Exit programming mode by pressing the ***** key after all programming is completed. One beep will sound and the LED will return to steady red. After 25 seconds of inactivity, the keypad will automatically exit programming mode and return to standby.

Examples for the Above Methods:

1. Program a user fingerprint for User ID #10:

1 **1 0** **#** **U U**

2. Program two user fingerprints for User IDs #15 and #17

1 **1 5** **#** **U U** (1st user) wait for beep, then **1** **1 7** **#** **U U** (2nd user)

3. Program a user fingerprint to an automatically assigned User ID (generally not recommended, since the User ID will be needed to delete a user when their fingerprint is not available):

1 **U U** – In this example, the reader/keypad will assign the next available User ID

Programming User Fingerprints (Continued):**NOTES:**

- The add user function key places you into this programming mode. Press the add user function key **[1]** only before adding the first user. To continue to add other users in the same session, do not repeat the add user function code **[1]**.
- **[UU]** represents the user fingerprint, which must be presented twice. The unit will beep once and the LED will flash green once to indicate that the fingerprints were read successfully.

With Master Add Fingerprint:

Using the master add fingerprint allows the programmer to quickly add user fingerprints without going into programming mode, particularly useful when adding a single user fingerprint (see "Programming the Master Add/Delete Fingerprints," pgs. 9~10). The fingerprint will be assigned to the first available fingerprint user ID in numerical order (IDs 1~998).

[A] [UU] [A]

[A] – Master Add fingerprint. The device will beep once, the green LED will flash once, then change to steady orange.

[U] – User's fingerprint

Examples Using the Master Add Fingerprint:

1. Program a user fingerprint for single user using the master add fingerprint:

[A] [UU] [A]

2. Program user fingerprints for two users using the master add fingerprint:

[A] [UU] (1st user) wait for beep, then **[UU]** (2nd user) **[A]**

NOTES:

- **[UU]** represents the user fingerprint, which must be presented twice. The unit will beep once and the LED will flash green once to indicate that the fingerprints were read successfully.
- Exit programming mode by presenting the master add fingerprint twice or by pressing the **[*]** key after all programming is completed. One beep will sound and the LED will return to steady red. After 25 seconds of inactivity, the keypad will automatically exit programming mode and return to standby.
- The master add fingerprint can only be used to add fingerprint users, not user codes.

ENFORCER Fingerprint Reader and Keypad

Programming User Codes:

User codes may be assigned to user IDs between 1001 and 2998 for common users, and 2999 and 3000 for super users. When programming user codes, use the following general formula after entering base programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

1 **A A A A** **#** **B B B B B B** **#** – After a short beep, you may continue to add users by repeating these steps, but without repeating the function code **1**.

1 – Add Users function code (LED will change to steady orange)

A – **1 0 0 1** to **3 0 0 0** – 1998 unique user IDs for user codes to trigger the device (and 2 super user IDs for super user codes to toggle between disable and enable user access)

B – User code – 4~6 digits long

NOTES:

- Each User ID must be unique and cannot be repeated for multiple user fingerprints or codes.
- Additional users may be entered in succession without repeating the function code **1**.
- To return to base programming mode to program other functions, press the **#** key (the LED will flash red) followed by the function code for that function (LED becomes steady orange).
- Exit programming mode by pressing the ***** key after all programming is completed. One beep will sound and the LED will return to steady red. After 25 seconds of inactivity, the keypad will automatically exit programming mode and return to standby.

Examples:

1. Program user code **2 2 7 5** for User ID #1001:

1 **1 0 0 1** **#** **2 2 7 5** **#**

2. Program user code **1 2 3 4 5** for User ID #2750:

1 **2 7 5 0** **#** **1 2 3 4 5** **#**

3. Program two user codes – 67890 for User ID #2015, and 654321 for User ID #2017

1 **2 0 1 5** **#** **6 7 8 9 0** **#** wait for beep, then

2 0 1 7 **#** **6 5 4 3 2 1** **#**

NOTE: The add user function code **1** places you into this programming mode. Press the add user function code only before adding the first user. To continue to add other users in the same session, do not repeat the add user function code **1**.

Deleting User Fingerprints or User Codes:**Deleting User Fingerprints Using the Master Delete Fingerprint When User is Present:**

If you have programmed a master add/delete fingerprint, to delete a user fingerprint with the master delete fingerprint without entering programming mode, and when the user is present (see "Programming the Master Add/Delete Fingerprints," pg. 9-10):

[D] **[U]** (One beep will sound if fingerprint is successfully deleted. Repeat to delete additional user fingerprints) **[D]**

[D] – Master Delete fingerprint.

[U] – User's fingerprint.

Examples Using the Master Delete Fingerprint:

1. Delete a user fingerprint for single user using the master add fingerprint:

[D] **[U]** **[D]**

2. Delete user fingerprints for two users using the master add fingerprint:

[D] **[U]** (1st user) wait for beep, then **[U]** (2nd user) **[D]**

NOTE: The master delete fingerprint can only be used to delete fingerprint users, not user codes.

Deleting User Fingerprints When User Is Present:

To delete user fingerprints when the user is present, use the following general formula from within base programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

[2] **[U]** – After a short beep, you may continue to delete users by presenting additional user fingerprints, but without repeating the function code **[2]**.

[2] – Delete Users function code (LED will change to steady orange)

[U] – User fingerprint

Deleting User Fingerprints/Codes When User Is Not Present:

To delete user fingerprints when the user is not present, or to delete user codes, use the following general formula from within base programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

[2] **[A]** **[A]** **[A]** **[A]** **#**

[2] – Delete Users function code (LED will change to steady orange, must be repeated before each user code)

[A] – **[1]** to **[30000]** – User ID

ENFORCER Fingerprint Reader and Keypad

Deleting User Fingerprints or User Codes (Continued):

Deleting All User (Fingerprints and Codes):

To delete all users (fingerprints and codes), use the following formula from within base programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

2 **X** **X** **X** **X** **X** **X** **X** **#**

2 – Delete Users function code (LED will change to steady orange, must be repeated before each user code)

X – Master programming code

NOTES:

- To return to base programming mode to program other functions, press the **#** key (the LED will flash red) followed by the function code for that function (LED becomes steady orange).
- Exit programming mode by pressing the ***** key after all programming is completed. One beep will sound and the LED will return to steady red. After 25 seconds of inactivity, the keypad will automatically exit programming mode and return to standby.

Examples:

1. Delete a user fingerprint for an available fingerprint:

2 **U** (present the user fingerprint to be deleted)

2. Delete a user fingerprint for an unavailable fingerprint assigned to User ID #1:

2 **1** **#**

3. Delete a user code for User ID #2501:

2 **2** **5** **0** **1** **#**

4. Delete user code or fingerprint for Users # 855 and #1505:

2 **8** **5** **5** **#** wait for beep, then **1** **5** **0** **5** **#**

5. Delete all users where the master code is 456789:

2 **4** **5** **6** **7** **8** **9** **#**

Programming the Output Mode and Time:

The relay can be programmed to toggle the relay ON and OFF (toggle mode), or to trigger for a programmed length of time up to 99 seconds before automatically turning OFF. The toggle or timed output can be used for locking or unlocking a door or for a variety of functions that can be controlled with the fingerprint reader/keypad.

When programming the output mode and time, use the following general formula from within base programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

3 **A** **A** **#**

3 – Program Output Mode and Time function code (LED will change to steady orange)

A – Output Mode and Output Time

Programming the Output Mode and Time (Continued):**Output Mode and Output Time:**

- **[0]** – Start/stop (toggle) mode. In this case, the output starts when a user fingerprint/code is entered, and stops when a user fingerprint/code is entered again.
- **[1]** to **[9][9]** – The output triggered by a user fingerprint/code lasts up to 99 seconds before automatically turning off (1=100ms, default: 5 seconds).

NOTES:

- For programming the output timing, 1=100ms. 2~99 represents full seconds.
- To return to base programming mode to program other functions, press the **[#]** key (the LED will flash red) followed by the function code for that function (LED becomes steady orange).
- Exit programming mode by pressing the **[*]** key after all programming is completed. One beep will sound and the LED will return to steady red. After 25 seconds of inactivity, the keypad will automatically exit programming mode and return to standby.

Examples:

1. Set the output to toggle mode:

[3] **[0]** **[#]**

2. Set the output to 60 seconds:

[3] **[6]** **[0]** **[#]**

Programming the Access Mode / Security Level:

The fingerprint reader/keypad can be programmed to one of four access modes / security levels:

- User code only – a user must use a user code for access
- Fingerprint only – a user must use a fingerprint for access
- Either user code or fingerprint – a user may use either a user code or a fingerprint for access
- Multiple user codes or fingerprints – multiple (2~9) user codes/fingerprints are required for access. Any combination of user codes or fingerprints in any order up to the set number must be used with no more than 5 seconds between each code/fingerprint. No particular user code/fingerprint can be repeated. This could be used for extremely secure areas requiring authentication by more than one person or requiring one person to either use both a user code and a fingerprint or multiple fingerprints/user codes (by assigning more than one user ID to that person, see pgs. 11~14).

NOTES:

- If the same fingerprint or user code is repeated, the device will return to standby without triggering the output.
- In multiple user code/fingerprint mode, the time between each user code/fingerprint must not exceed 5 seconds, otherwise, the device will return to standby.

ENFORCER Fingerprint Reader and Keypad

Programming the Access Mode / Security Level (Continued):

When programming the access mode / security level, use the following general formula from within base programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

4 **A** (**A**) **#**

4 – Program Access Mode function code (LED will change to steady orange)

A – Access Mode

Access Mode:

- **0** – User code access only
- **1** – Fingerprint access only
- **2** – Either user code or fingerprint (factory default)
- **3** **2**~**9** – Multiple user codes or fingerprints (the second number 2~9 sets the number of codes/fingerprints required for access).

NOTES:

- To return to base programming mode to program other functions, press the **#** key (the LED will flash red) followed by the function code for that function (LED becomes steady orange).
- Exit programming mode by pressing the ***** key after all programming is completed. One beep will sound and the LED will return to steady red. After 25 seconds of inactivity, the keypad will automatically exit programming mode and return to standby.

Examples:

1. Set the access mode to fingerprint only:

4 **1** **#**

2. Set the access to require four user codes / fingerprints:

4 **3** **4** **#**

Programming the Keypad Sounds/Notifications:

The keypad sounds/notifications can be set to silent (The LED indicator will still function normally). This affects all sounds from the keypad, including keypad presses, door propped-open, door forced-open, wrong-code alarm, and successful fingerprint/code entry notifications. When programming the keypad sounds/notifications, use the following general formula from within base programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

6 **A** **#**

6 – Program Keypad Sounds/Notifications function code (LED will change to steady orange)

A – Keypad Sounds/Notifications Enabled/Disabled

Keypad Sounds/Notifications Enabled/Disabled:

- **4** – Disable
- **5** – Enable (factory default)

Programming the Keypad Sounds/Notifications (Continued):

NOTES:

- Disabling the keypad sounds/notifications only affects the internal notifications. The external alarm is programmed separately.
- Some notifications will trigger both the internal notification beep and the external alarm, but some will trigger only one or the other.
- The **#** key returns you to base programming mode (the LED will flash red). To program other functions, press the function code for that function (LED becomes steady orange).
- Exit programming mode by pressing the ***** key after all programming is completed. One beep will sound and the LED will return to steady red. After 25 seconds of inactivity, the keypad will automatically exit programming mode and return to standby.

Programming the External Alarm Output:

The external alarm output sends certain notifications to an external alarm. These include the tamper, wrong-code alarm (if enabled, see "Programming the Wrong-Code Lockout/Alarm," pg. 21), and the door-forced-open alarm (if enabled, see "Programming the Door Propped-Open / Forced-Open Detection," pg. 20). When programming the alarm, use the following general formula from within base programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

5 **A** **#**

5 – Program Alarm function code (LED will change to steady orange)

A – Alarm Disable/Enable and Alarm Time

Alarm Disable/Enable and Alarm Time:

- **0** – Disable alarm
- **1** to **3** – Enable and set the alarm time, 1~3 minutes (factory default, 1 minute)

NOTES:

- The **#** key returns you to base programming mode (the LED will flash red). To program other functions, press the function code for that function (LED becomes steady orange).
- Exit programming mode by pressing the ***** key after all programming is completed. One beep will sound and the LED will return to steady red. After 25 seconds of inactivity, the keypad will automatically exit programming mode and return to standby.

Examples:

1. Disable the alarm:

5 **0** **#**

2. Enable the alarm and set it to 2 minutes:

5 **2** **#**

Programming Door Propped-Open / Forced-Open Detection:

The device can be programmed to indicate when the door is left open too long (propped-open) or when there is a forced entry. The door propped-open detection only triggers the internal sounds/notifications, while the door forced-open detection triggers both. If this setting is enabled:

- If the door is open for more than one minute, the keypad will begin beeping to remind a user to close the door. The beeping can be stopped by either closing the door or entering a valid master code, user code, or fingerprint.
- If the door is opened by force, both the internal notification beep and an external alarm will sound and continue to sound until disabled by entering a valid master code, user code, or fingerprint.
- This feature requires the notifications and/or alarm output to be enabled (see "Programming the Keypad Sounds/Notifications," pgs. 18~19 and "Programming the External Alarm Output," pg. 19), an external alarm connection, as well as connection to a door sensor magnetic contact or a lock with a built-in door sensor.

When programming the door propped-open / forced-open detection, use the following general formula from within base programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

6 **A** **#**

6 – Program the Door Propped-Open / Forced-Open Detection function code (LED will change to steady orange)

A –Disable or Enable the Door Propped-Open / Forced-Open Detection

Disable or Enable Door Propped-Open / Forced-Open Detection:

- **0** – Disable the door propped-open / forced-open detection (factory default)
- **1** – Enable the door propped-open / forced-open detection

NOTES:

- The **#** key returns you to base programming mode (the LED will flash red). To program other functions, press the function code for that function (LED becomes steady orange).
- Exit programming mode by pressing the ***** key after all programming is completed. One beep will sound and the LED will return to steady red. After 25 seconds of inactivity, the keypad will automatically exit programming mode and return to standby.

Examples:

1. Disable the door propped-open / forced-open detection:

6 **0** **#**

2. Enable the door propped-open / forced-open detection:

6 **1** **#**

Programming the Wrong-Code Lockout/Alarm:

The device can be programmed to either lockout (deny access) or sound an alarm after 10 successive wrong user codes or fingerprints. The lockout will continue and the LED will flash red for 10 minutes and cannot be reset until the time is expired. The keypad sounds and/or external alarm will sound (depending on your settings for them), but can be stopped with a valid master code, user code, or fingerprint (see "Programming the Keypad Sounds/Notifications," pgs. 18~19 and "Programming the External Alarm Output," pg. 19).

When programming the wrong code lockout, use the following general formula from within base programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

5 **A** **#**

5 – Program Wrong-Code Lockout function code (LED will change to steady orange)

A –Disable or Enable/Configure the Wrong-Code Lockout/Alarm

Disable or Enable/Configure Wrong-Code Lockout:

- **4** – Disable wrong-code lockout (factory default)
- **5** – Enable wrong-code lockout to deny access for 10 minutes
- **6** – Enable wrong-code alarm to sound the keypad notifications / external alarm

NOTES:

- If wrong-code lockout is enabled, the LED will flash red and all access will be denied for 10 minutes after 10 successive wrong codes/fingerprints.
- If wrong-code alarm is enabled, the LED will flash and keypad notifications and/or external alarm will sound and continue for the length of time programmed for the external alarm or until a valid master code, user code, or user fingerprint is entered. This setting requires the keypad notifications and/or external alarm to be enabled.
- The **#** key returns you to base programming mode (the LED will flash red). To program other functions, press the function number for that function (LED becomes steady orange).
- Exit programming mode by pressing the ***** key after all programming is completed. One beep will sound and the LED will return to steady red. After 25 seconds of inactivity, the keypad will automatically exit programming mode and return to standby.

Examples:

1. Disable the wrong-code lockout:

5 **4** **#**

2. Enable the wrong-code lockout to deny access for 10 minutes:

5 **5** **#**

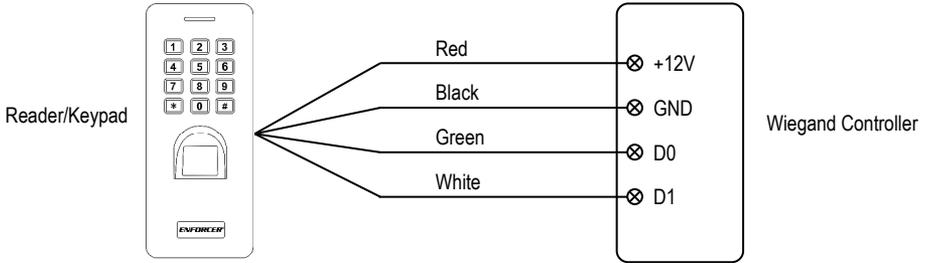
3. Enable the wrong-code lockout to deny access until a valid master code, user code, or user fingerprint is entered:

5 **6** **#**

ENFORCER Fingerprint Reader and Keypad

Wiegand Pass-Through Connection Diagram:

This device can also be connected a Wiegand controller. See the connection diagram below:



Programming Wiegand Pass-Through Operation:

To set up the device to serve as an output reader connected to a Wiegand controller, follow the steps listed below.

Programming Fingerprint Users:

1. Follow the instructions for adding fingerprint users as described in "Programming User Fingerprints" on pgs. 11~13.
2. On the controller, follow the process for adding card users and instruct it to add the fingerprints saved on the fingerprint reader/keypad. The controller will generate a virtual card number from the fingerprint reader/keypad's user ID. When you save this virtual card number on the controller, the fingerprints will be successfully added.

Programming the Wiegand Output Bits/Format:

When programming the Wiegand output format, use the following general formula from within base programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

[8] [A] [#]

[8] – Program Wiegand Output Bits/Format function code (LED will change to steady orange)

[A] – Disable or Set Wiegand Output Bits/Format

Disable or Set Wiegand Output Bits/Format:

- [0] – Disable Wiegand output (factory default)
- [2][6] to [4][4] – Enable Wiegand output and set output bits (26~44, factory default, 26)
- [4], [8], or [1][0] – Program Wiegand PIN output format (4, 8, or 10, factory default, 4)

NOTES:

- The [#] key returns you to base programming mode (the LED will flash red). To program other functions, press the function code for that function (LED becomes steady orange).
- Exit programming mode by pressing the [*] key after all programming is completed. One beep will sound and the LED will return to steady red. After 25 seconds of inactivity, the keypad will automatically exit programming mode and return to standby.

Programming Wiegand Pass-Through Operation (Continued):**Examples:**

1. Disable Wiegand output:

8 **0** **#**

2. Set Wiegand PIN output format to 8 bits:

8 **8** **#**

3. Set Wiegand output bits to 44:

8 **4** **4** **#**

Programming the Device ID:

When using the fingerprint reader/keypad as a Wiegand reader, you can set its device ID for recognition. When a valid user code or fingerprint is entered, the fingerprint reader/keypad will output the virtual card number as a Wiegand 26 bit output.

When setting the device ID, you will need to set the Wiegand output format to 26 bits and the PIN output format to 10 bits (virtual card number) format.

When setting the device ID, use the following general formula from within base programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

7 **A** **#**

7 – Programming the Device ID function code (LED will change to steady orange)

A – Device ID number (0~255, default, 0)

NOTES:

- The **#** key returns you to base programming mode (the LED will flash red). To program other functions, press the function code for that function (LED becomes steady orange).
- Exit programming mode by pressing the ***** key after all programming is completed. One beep will sound and the LED will return to steady red. After 25 seconds of inactivity, the keypad will automatically exit programming mode and return to standby.

Examples:

1. Set the device ID to 10:

7 **1** **0** **#**

2. Set the device ID to 155:

7 **1** **5** **5** **#**

Fingerprint Transmission Format:

The format for fingerprint transmission is "Device ID,User ID" (5 digits allotted for user ID). For example, if the device ID is 255 and the User ID is 3, the output to the Wiegand controller will be 255,00003. If the fingerprint is not recognized as a valid fingerprint by the fingerprint reader, no output will be sent to the Wiegand controller.

ENFORCER Fingerprint Reader and Keypad

Programming Wiegand Pass-Through Operation (Continued):

User ID Transmission Format:

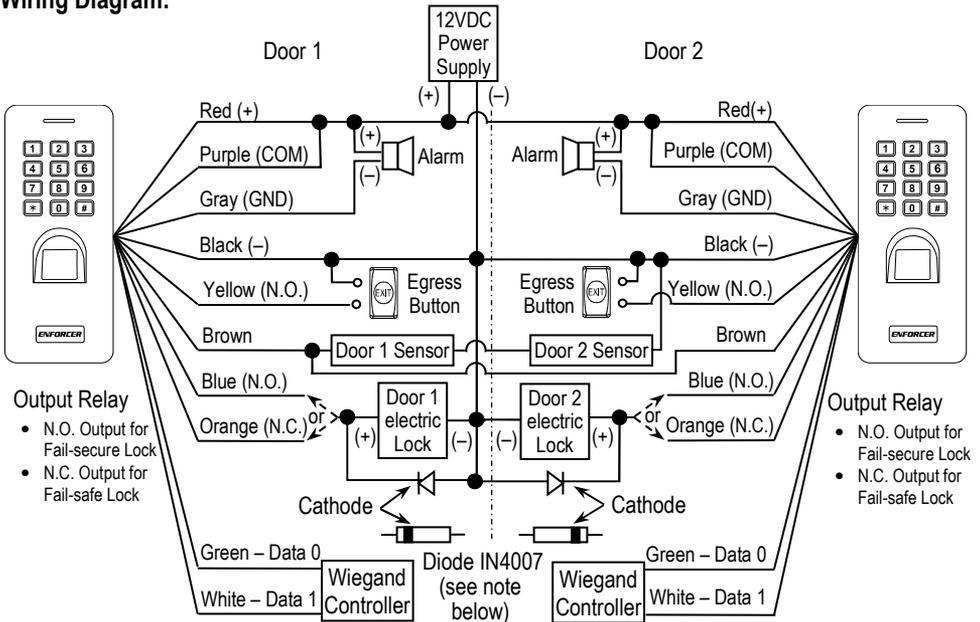
The fingerprint reader/keypad will transmit the user code data when the **#** key is pressed. The transmission format is "Device ID, User Code" (5 digits allotted for user ID). However, if the user code is more than 4 digits, the device ID is not transmitted. Note that the device will transmit any input preceding the **#** key, whether valid or not. See the following examples when the device ID is 255:

- User code 5555 (4 digits), device output is 255,05555
- User code 55555 (5 digits), device output is 000,55555
- User code 555555 (6 digits), device output is 005,55555

Setting Up an Interlock System with Two Keypads:

In this application, two keypads are each connected to separate door locks and egress pushbuttons. While one door is open, the other cannot be opened. The user uses their user code or fingerprint to open the first door, and then must wait till the first door has closed to enter their user code or fingerprint to open the second door.

Wiring Diagram:



NOTE: For DC-powered electric strikes, connect the included diode as close as possible and in parallel with the electric strike. This absorbs possible electromagnetic interference to prevent operation of the strike from damaging the fingerprint reader/keypad. Do not connect a diode when using electromagnetic locks or with AC powered strikes.

Setting Up an Interlock System with Two Keypads (Continued):

Programming the Interlock System:

When programming the interlock system, use the following general formula from within base programming mode (see "Enter and Exit Base Programming Mode," pg. 9):

6 **A** **#**

6 – Program the Interlock System function code (LED will change to steady orange)

A – Disable or Enable the Interlock System

Disable or Enable the Interlock:

- **2** – Disable the interlock (factory default)
- **3** – Enable the interlock

NOTES:

- The **#** key returns you to base programming mode (the LED will flash red). To program other functions, press the function code for that function (LED becomes steady orange).
- Exit programming mode by pressing the ***** key after all programming is completed. One beep will sound and the LED will return to steady red. After 25 seconds of inactivity, the keypad will automatically exit programming mode and return to standby.

Resetting the Fingerprint Reader/Keypad to Factory Default:

The fingerprint reader/keypad must be connected to a Request-to-Exit (RTE) button to be reset to factory default settings. When resetting to factory default, user information is retained.

To reset the fingerprint reader/keypad to factory default settings, follow the steps below:

1. Power off the fingerprint reader/keypad
2. Hold down the egress button and power the fingerprint reader/keypad on, continuing to hold down the egress button for at least 30 seconds after you hear 2 beeps and the LED turns orange.
3. After releasing the egress button, the LED will turn red indicating that the reset was successful.

User Operation of the Fingerprint Reader/Keypad:**To Operate with a User Fingerprint:**

- Place the finger on the fingerprint reader for one second to activate the relay.
- You should hear 1 beep (if sounds are enabled) and the status LED should turn green to indicate that the fingerprint is accepted and the door is unlocked.

To operate using a user code:

- Enter the user code followed by the **#** key to activate the relay.
- You should hear 1 beep (if sounds are enabled) and the status LED should turn green to indicate that the user code is accepted and the door is unlocked.

To operate in multiple user code/fingerprint mode:

- Input the required number of user codes each followed by the **#** key and/or fingerprints. They can be input in any order, but with no more than a 5-second interval each code/fingerprint.
- If not complete within 5 seconds, the device will return to standby mode and the users will need to repeat the process.
- You should hear 1 beep (if sounds are enabled) and the status LED should turn green to indicate that the fingerprints/codes have been accepted and the door is unlocked.

Concealing Your User Code When a Bystander Is Present:

For extra security when a bystander is within sight of the keypad, the user may "hide" their true user code within random digits up to a total of 10 digits.

If a user code is less than 6 digits, use preceding zeros as placeholders to make it 6 digits, but with random digits before and/or after the true user code followed by the **#** key.

Examples: (where "x" is any random digit)

- User code is 1234, enter **[x][x][x][x][0][0][1][2][3][4] #**
- User code is 987654, enter **[x][x][x][x][9][8][7][6][5][4] #**
- User code is 2345, enter **[x][x][0][0][2][3][4][5][x][x] #**

ENFORCER Fingerprint Reader and Keypad

Troubleshooting:

Unit fails to accept a new fingerprint	<ul style="list-style-type: none">• Ensure the User ID assigned is between 1 and 1000• Ensure the User ID has not been assigned to another user
Unit fails to accept a new user code	<ul style="list-style-type: none">• Ensure the User ID assigned is between 1001 and 3000• Ensure the user code is between 4-6 digits long and not already assigned to another user
Unit fails to read a programmed fingerprint	<ul style="list-style-type: none">• Ensure the finger being presented is the same finger that was originally programmed• Press the finger evenly on the central area of the reader• Ensure the reader window is clean
Unit fails to respond to a programmed fingerprint or user code	<ul style="list-style-type: none">• Ensure the unit is in standby mode by pressing the  key until the LED becomes steady red

IMPORTANT WARNING: For a weather-resistant installation, ensure that the unit is properly sealed where the housing base meets the wall. Incorrect mounting may lead to exposure to rain or moisture in the enclosure 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 COMPLIANCE STATEMENT

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 UNDESIRE 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.

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 © 2019 SECO-LARM U.S.A., Inc. All rights reserved.

SECO-LARM® U.S.A., Inc.

16842 Millikan Avenue, Irvine, CA 92606
Phone: (949) 261-2999 | (800) 662-0800

Website: www.seco-larm.com
Email: sales@seco-larm.com

 PICSNS

MI_SK-2612-SFSQ_190807.docx