AYC-x6355 Series

CSN SELECT Smart Card Readers/Controllers

Installation and User Manual

Models:

AYC-H6355
AYC-M6355
AYC-Q6355

AYC-H6355

AYC-M6355

AYC-Q6355

ROSSLARE
SECURITY PRODUCTS

Table of Contents

List of Figures

List of Tables

Notice and Disclaimer

This manual's sole purpose is to assist installers and/or users in the safe and efficient installation and usage of the system and/or product, and/or software described herein.

BEFORE ATTEMPTING TO INSTALL AND/OR USE THE SYSTEM, THE INSTALLER AND THE USER MUST READ THIS MANUAL AND BECOME FAMILIAR WITH ALL SAFETY REQUIREMENTS AND OPERATING PROCEDURES.

- The system must not be used for purposes other than those for which it was designed.
- The use of the software associated with the system and/or product, if applicable, is subject to the terms of the license provided as part of the purchase documents.
- ROSSLARE exclusive warranty and liability is limited to the warranty and liability statement provided in an appendix at the end of this document.
- This manual describes the maximum configuration of the system with the maximum number of functions, including future options. Therefore, not all functions described in this manual may be available in the specific system and/or product configuration you purchased.
- Incorrect operation or installation, or failure of the user to effectively maintain the system, relieves the manufacturer (and seller) from all or any responsibility for consequent noncompliance, damage, or injury.
- The text, images and graphics contained in the manual are for the purpose of illustration and reference only.
- All data contained herein subject to change without prior notice.
- In no event shall manufacturer be liable for any special, direct, indirect, incidental, consequential, exemplary or punitive damages (including, without limitation, any and all damages from business interruption, loss of profits or revenue, cost of capital or loss of use of any property or capital or injury).
- All graphics in this manual are for reference only, some deviation between the image(s) and the actual product may occur.
- All wiring diagrams are intended for reference only, the photograph or graphic of the PCB(s) are intended for clearer illustration and understanding of the product and may differ from the actual PCB(s).

1. Introduction

The CSN SELECT AYC-x6355 is a series of multi-credential technology contactless smart card readers with keypad for use in access control system solutions and includes Rosslare's convertible technology.

CSN SELECT readers have the capability to read the Card Serial Number (CSN) from many smart card RFID Standards implementations. The following list shows the credential technologies for which we have confirmed compatibility:

- ISO14443A – MIFARE® Ultralight® Nano / EV1/ C, MIFARE Classic® / Classic EV1, MIFARE Plus® S / SE / X / EV1, MIFARE DESFire® EV1 / EV2, NFC N-TAG / Card Emulation
- ISO14443B - China National ID
- ISO15693 – HID® iClass®, PicoPass, iCode, LEGIC
- ISO18092 – SONY® FeliCa® (Hong Kong Octopus)

This list is continuously updated, for the latest compatibility list contact your sales representative.

The standard readers output the Wiegand CSN data in Wiegand 26-Bit format. Other Wiegand formats are available upon request.

With Rosslare's convertible technology, the unit automatically determines whether to function as a reader or as a controller. If the unit is connected to a standard access control unit, then it functions as a reader. If the unit is connected to Rosslare's secured intelligent power supply such as the PS-A25T, PS-C25T or PS-C25TU, it functions as a secured controller.

As controllers, the units accept up to 500 users, and allow entry via a personal identification number (PIN) and/or by presenting a proximity card. The PIN code length for the controller has several options. The PIN code length can be a set number of 4, 5, or 6 digits or it can be a 4-8 digits option.

For information on how the unit functions as a reader, see Chapter 6. For information on how the unit functions as a controller, see

Chapter 7.

1.1 Installation Kit

The installation kit consists of the following items to be used during the installation procedure:

- 1 self-adhesive mounting label template
- 2 mounting screws and 2 screw anchors
- 1 pin Torx key tool
- 1 pin Torx security screw

1.2 Ancillary Equipment

The following equipment is required to complete your installation:

1.2.1 Function as a Reader

- Compatible host controller (not supplied)

1.2.2 Function as a Controller

- Secured intelligent power supply (such as the PS-A25T, PS-C25T or PS-C25TU)

  The controller connects to the following:

  - Electric lock strike mechanism or a magnetic lock device, which implements fail safe (power to lock) or fail secure (power to open) functions.
  - REX button – Normally open type, switch is closed when pressed.
  - Door monitor switch

Rosslare accessories can be found on www.rosslaresecurity.com.

2. Technical Specifications

Electrical Characteristics	
Power Supply Type	Regulated
Operating Voltage Range	8 to 16 VDC
Current @ 12 V	AYC-H/M6355: Standby: 120 mA, max: 160 mA
	AYC-Q6355: Standby: 145 mA, max: 200 mA
Read Range*	AYC-H/M6355: 9 cm (3.5 in.)
	AYC-Q6355: 5 cm (2.5 in.)
Green LED Control**	Dry Contact, N.O.
Red LED Control**	Dry Contact, N.O.
Buzzer Control**	Dry Contact, N.O.
Tamper Output**	Open collector, active low, max. sink current 16 mA
Maximum Cable Distance to Controller	Wiegand: 150 m (500 ft) with 18-AWG cable OSDP (RS-485): 1,200 m (4,000 ft) with 2x2 18-AWG twisted shielded cable
Environmental Characteristics	
Operating Temp. Range	-35°C to 66°C (-31°F to 150°F)
Operating Humidity Range	0 to 95% (non-condensing)
Outdoor Usage	Weather-resistant, UV-resistant, epoxy-potted, suitable for indoor and outdoor use

* Measured using a Rosslare MIFARE Classic EV1 (ISO Card). Read range with other credential technologies may vary. Range also depends on electrical environment and proximity to metal.

** Control Lines are factory programmable and can be custom configured upon request.

Physical Characteristics	
Dimensions (H x W x D)	AYC-H6355: 110.7 × 75.0 × 18.2 mm (4.4 x 3.0 x 0.7 in.)
	AYC-M6355: 89.5 × 88.9 × 18.3 mm (3.5 x 3.5 x 0.7 in.)
	AYC-Q6355: 120.0 × 76.0 × 21.5 mm (4.7 x 3.0 x 0.9 in.)
Weight	AYC-H6355: 185 g (6.5 oz)
	AYC-M6355: 169 g (5.9 oz)
	AYC-Q6355: 430 g (15.2 oz)

3. Mounting

Before mounting, you should determine the best location for the reader.

To mount the units:

1. Peel off the back of the self-adhesive mounting label template and place it at the required mounting location.
2. Using the template as a guide, drill two holes (sizes indicated on the template) used for mounting the back plate onto the surface.
3. Insert a suitable wall plug into each screw hole.
4. Drill a 10-mm (7/16") hole for the cable. If mounting on metal, place a grommet or electrical tape around the edge of the hole.
5. Wire the reader as described in Chapter 4. A linear type power supply is recommended.
6. Remove the reader's snap-off front cover to reveal the two screw holes (see Figure 1).

Figure 1: Removing the Top Cover

Note: The location of the screws varies depending on the model number of the reader.

7. Align the two holes of the reader with those drilled in the wall and firmly attach the reader to the wall with two screws, whose size is indicated on the template.
8. Relocate the front cover onto the reader.

The reader can also be mounted using strong epoxy glue. After application, the reader should be firmly held in place until the glue dries

4. Wiring Instructions

An AYC-x6355 unit is supplied with a 10-conductor 22" (56-cm) pigtail.

4.1 Wiring the Unit as a Reader

If you connect the unit to a standard access control unit, it automatically functions as a reader.

To connect the unit as a reader to an access control unit:

1. Prepare the reader cable by cutting its jacket back about 3 cm (1¼") and strip the insulation from the wires about 1.3 cm (½").
2. Prepare the controller cable by cutting its jacket back about 3 cm (1¼") and strip the insulation from the wires about 1.3 cm (½").
3. Splice the reader's pigtail wires to the corresponding controller wires (as indicated in Table 1) and cover each joint with insulating tape.

Table 1: Wiring the Unit as a Reader to a Control Panel

Wire Color	Output
Red	Power
Black	Ground
Green	Data 0 / Data / C2
White	Data 1 / Clock / C1
Orange	Green LED control
Brown	Red LED control
Purple	Tamper Output
Yellow	Buzzer control
Blue	RS-485 - A / OSDP*
Gray	RS-485 - B / OSDP*
* RS-485 is used for firmware update.	

4. Trim and cover all unused conductors.

Note

- The individual wires from the reader are color coded according the Wiegand standard.
- When using a separate power supply for the reader, this supply and that of the controller must have a common ground.
- The reader's cable shield wire should be preferably attached to an earth ground, or a signal ground connection at the panel, or the power supply end of the cable. This configuration is best for shielding the reader cable from external interference.

4.2 Wiring the Unit as a Controller

If you connect the unit to a Rosslare PS-x25 secured power supply, it automatically functions as a controller.

To connect the unit as a controller:

1. Prepare the reader cable by cutting its jacket back about 3 cm (1¼") and strip the insulation from the wires about 1.3 cm (½").
2. Prepare the PS-x25 secured power supply's cable by cutting its jacket back about 3 cm (1¼") and strip the insulation from the wires about 1.3 cm (½").
3. Splice the controller pigtail wires to the corresponding PS-x25 secured power supply's wires (as indicated in Table 2) and cover each joint with insulating tape.

Table 2: Wiring the Unit as a Controller

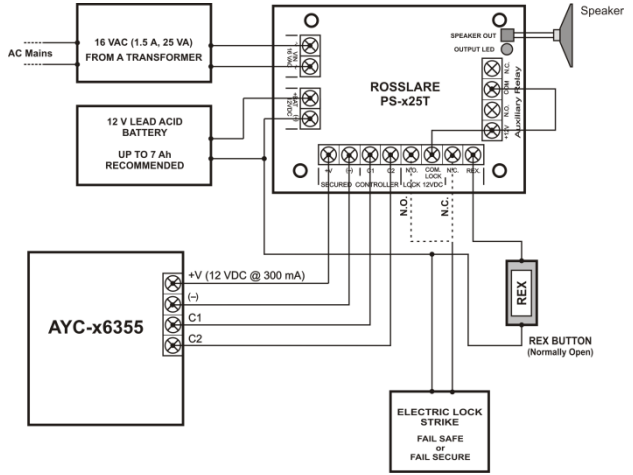
Controller	Color	Functionality	Note
12 VDC	Red	+DC Input	Wired to the PS-x25
Shield/ Ground	Black	Ground	Wired to the PS-x25
C 1	White	Communication	Wired to the PS-x25
C 2	Green	Communication	Wired to the PS-x25
AUX. IN	Yellow	Auxiliary Input	Wired to input

4. Trim and cover all unused conductors.

To connect the unit to the desired power supply option, refer to the following wiring diagrams.

Figure 2 shows the wiring for the Controller Application using a dual relay secured intelligent power supply.

Figure 2: Controller Application Wiring Diagram



Note

This wiring diagram is for reference only. Please wire according to actual PS-x25 samples.

Figure 3 shows the auxiliary output connection using the internal power.

Figure 3: Auxiliary Output Connection with Internal Power

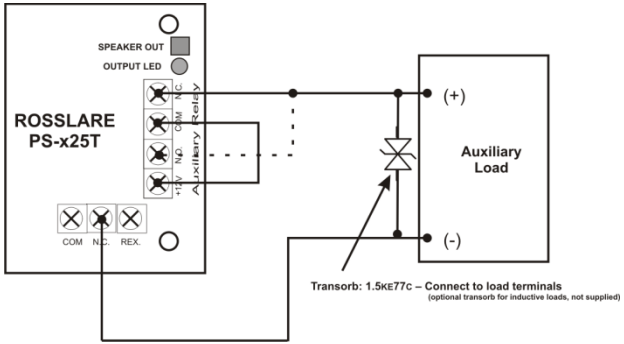
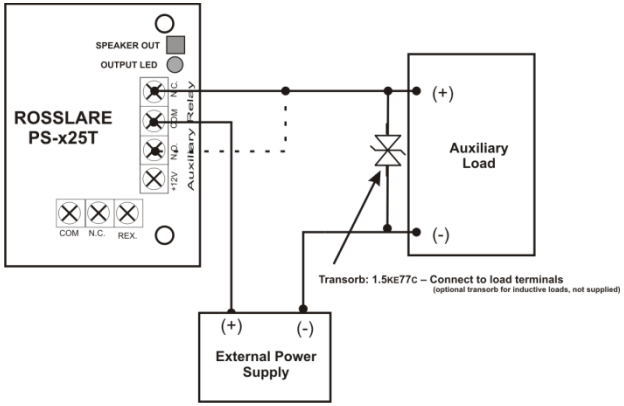


Figure 4 shows the auxiliary output connection using external power.

Figure 4: Auxiliary Output Connection with External Power



5. OSDP Operation

Note

- In OSDP mode, all control lines (Inputs/Outputs) are disabled.
- In OSDP mode, if a connection is not established or lost with the controller, the LED flashes orange continuously.

CSN SELECT readers that support OSDP operation are compatible with all reader-related OSDP commands. The reader address is set using DIP switches on the back of the reader.

Release the screw on the back of the reader to remove the door to access the DIP switches (Figure 5).

Figure 5: DIP Switch Compartment

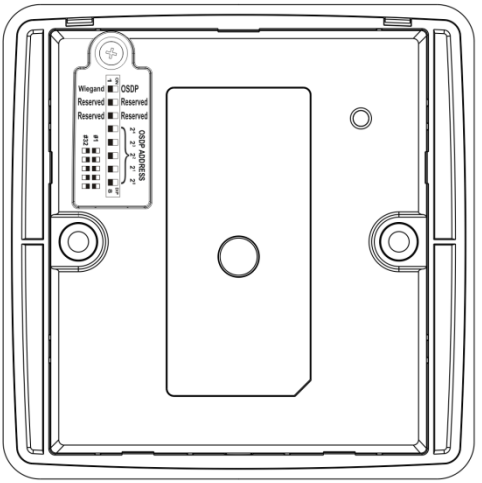
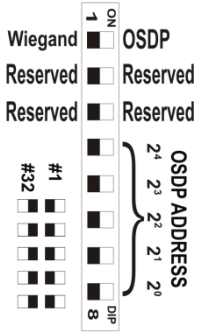


Figure 6 shows the DIP switch settings, which are also described below.

Figure 6: DIP Switch Settings



DIP Switch 1

This switch is used to select the reader output (Wiegand or OSDP):

- Off = Wiegand
- On = OSDP

DIP Switch 2

This switch is reserved for future use.

DIP Switch 3

This switch is reserved for future use.

DIP Switches 4 to 8

These switches set the address of the reader for OSDP protocol.

DIP Switch 4 is MSB and DIP Switch 8 is LSB. The address is the DIP switch state +1.

Examples:

- All the DIP switches in Off position, address = 1
- All the DIP switches in On position, address = 32

6. Reader Functionality

Upon power on, the unit flashes red, then green, and then orange, each for 1 second and a beep is heard for each color. The unit searches for the presence of Rosslare's secured intelligent power supply. If a secured intelligent power supply is not detected, the unit is automatically configured as a reader.

6.1 Transmit Mode

The default mode of the reader is Transmit mode. In Transmit mode, the unit is ready to receive data from a presented proximity card or an entered PIN code.

When the reader is in Transmit mode, the left LED is red and the right LED is off.

When a proximity card is presented or a keypad entry is being transmitted, the left LED flashes green.

Keypad data can be sent via one of eight different Keypad Transmission Formats (see Section 6.2.3).

Proximity cards presented to the reader are sent in either various Wiegand formats or Clock & Data format (see Section 6.2.4).

6.2 Programming as a Reader

Programming is done solely via the unit's keypad driven Programming Menu System. During the manufacturing process, certain codes and settings are pre-programmed. These settings are called the default factory settings.

Table 3 shows the names of all the reader menus.

Default factory settings are marked by a "*" sign.

Table 3: Reader Programming Menus

Menu	Description	Default
1	**Selecting Keypad Transmission Format**	
	Single Key, 6-Bit Wiegand (Rosslare Format)	*
	Single Key, 6-Bit Wiegand with Nibble + Parity Bits	
	Single Key, 8-Bit Wiegand, Nibbles Complemented	
	4 Keys Binary + Facility Code, Wiegand 26-Bit	
	1 to 5 Keys + Facility Code, Wiegand 26-Bit	
	6 Keys BCD and Parity Bits, Wiegand 26-Bit	
	1 to 8 Keys BCD, Clock & Data	
	Single Key, Wiegand 4-Bit	
2	**Selecting Card Transmission Format**	
	Wiegand 26-Bit	*
	Clock & Data	
	Wiegand 32-Bit	
	Wiegand 32-Bit Reversed Byte	
	Wiegand 34-Bit	
	Wiegand 40-Bit	
	Wiegand 56-Bit	
	Wiegand 64-Bit	
3	**Changing the Programming Code**	**1234**
4	**Changing the Facility Code**	**0**
6	**Backlight Options**	
	Off	
	On (Default)	*****
	Off until key press when on for 10 seconds	
	Dimmed until key press when on for 10 seconds	
0	**Return to Factory Default Settings**	

6.2.1 Entering Programming Mode

To reach the Programming Menu System, the unit must first be placed into Programming mode.

Note

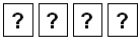
- The factory 4-digit Programming code is 1234.
- If a Programming code is not entered within 20 seconds, the unit returns to Transmit mode.

To enter Programming mode:

1. Press **#** four times.

   The left LED turns off and the right LED turns red.

2. Enter your 4-digit Programming code.



   If the Programming code is valid, the right LED turns green.

   If the Programming code is invalid, you hear a long beep and the reader returns to Transmit mode.

6.2.2 Exiting Programming Mode

To exit Programming mode:

1. Press **#** to exit Programming mode at any time.

   - You hear a beep.
   - The left LED turns red and the right LED turns off.

   This indicates that the unit has returned to Transmit mode.

   Wrong entries may reset the reader back to Transmit mode. If no key is pressed for 20 seconds while in Programming mode, the unit exits Programming mode and returns to Transmit mode.

6.2.3 Selecting Keypad Transmission Format

The AYC-x6355 has nine different keypad transmission formats.

See Table 4 in Section 6.2.3.1 for more information on keypad transmission formats.


Note

- Only one keypad transmission format can be active at any one time.
- When using the keypad transmission format "1 to 8 keys BCD, Clock & Data" (Option 8), an additional input is required to specify the number of keys in the PIN code.

To select the appropriate keypad transmission format:

1. Enter Programming mode.

2. Press **1** to enter Menu 1.

   The left LED turns red.

3. Enter the appropriate option number for the keypad transmission format that you wish to select.

   You hear three beeps.

   The system returns to Transmit mode.

   If an incorrect option number is entered, the reader returns to Transmit mode and the keypad transmission format remains unchanged.

6.2.3.1 Keypad Transmission Format Option Number

Table 4 presents the eight different keypad transmission formats.

Table 4: Keypad Transmission Format Option Number

Keypad Transmission Format	Option Number
Single Key, Wiegand 6-Bit (Rosslare Format)	1*
Single Key, Wiegand 6-Bit with Nibble + Parity Bits	2
Single Key, Wiegand 8-Bit, Nibbles Complemented	3
4 Keys Binary + Facility Code, Wiegand 26-Bit	4
1 to 5 Keys + Facility Code, Wiegand 26-Bit	5
6 Keys BCD and Parity Bits, Wiegand 26-Bit	6
1 to 8 Keys BCD, Clock & Data Single Key	8
Single Key, Wiegand 4-Bit	9

* Option 1 is the default factory setting.

More information on each of the different keypad transmission formats is available below and on the following pages.

Option 1: Single Key, Wiegand 6-Bit (Rosslare Format)

Each key press immediately sends 4 bits with 2 parity bits added – even parity for the first 3 bits and odd parity for the last 3 bits.

0 = 1 1010 0 = "A" in Hexadecimal
1 = 0 0001 0
2 = 0 0010 0
3 = 0 0011 1
4 = 1 0100 1
5 = 1 0101 0
6 = 1 0110 0
7 = 1 0111 1
8 = 1 1000 1
9 = 1 1001 0
* = 1 1011 1 = "B" in Hexadecimal
# = 0 1100 1 = "C" in Hexadecimal

Option 2: Single Key, Wiegand 6-Bit Nibble and Parities

Each key press immediately sends 4 bits with 2 parity bits added – even parity for the first 3 bits and odd parity for the last 3 bits.

0 = 0 0000 1	6 = 1 0110 0
1 = 0 0001 0	7 = 1 0111 1
2 = 0 0010 0	8 = 1 1000 1
3 = 0 0011 1	9 = 1 1001 0
4 = 1 0100 1	* = 1 1010 0 = "A" in Hexadecimal
5 = 1 0101 0	* = 1 1011 1 = "B" in Hexadecimal

Option 3: Single Key, Wiegand 8-Bit Nibbles Complemented

This option inverts the most significant bits in the message leaving the least 4 significant bits as a Binary Coded Decimal (BCD) representation of the key. The host system receives an 8-bit message.

0 = 11110000	6 = 10010110
1 = 11100001	7 = 10000111
2 = 11010010	8 = 01111000
3 = 11000011	9 = 01101001
4 = 10110100	* = 01011010 = "A" in Hexadecimal
5 = 10100101	# = 01001011 = "B" in Hexadecimal

Option 4: 4 Keys Binary + Facility Code, Wiegand 26-Bit

This option buffers 4 keys and outputs keypad data with a 3-digit Facility code like a standard 26-Bit card output.

The Facility code is set in Programming Menu number four and can be in the range 000 to 255. The factory default setting for the Facility code is 000 (see Section 6.2.6).

The keypad PIN code is 4-digit long and can range between 0000 and 9999. On the fourth key press of the 4-digit PIN code, the data is sent across the Wiegand Data lines as binary data in the same format as a 26-Bit Card.

If ***** or **#** are pressed are pressed during PIN code entry, the keypad clears the PIN code entry buffer, generate a beep and is ready to receive a new 4-digit keypad PIN code.

If the entry of the 4-digit keypad PIN code is disrupted and no number key is pressed within 5 seconds, the keypad clears the PIN code entry buffer, generates a beep and is ready to receive a new 4-digit keypad PIN code.

(EP) FFFF FFFF AAAA AAAA AAAA AAAA (OP)

Where:

EP = Even parity for first 12 bits

OP = Odd parity for last 12 bits

F = 8-bit Facility code

A = 16-bit code generated from keypad

Option 5: 1 to 5 Keys + Facility Code, Wiegand 26-Bit

Option 5 buffers up to 5 keys and outputs keypad data with a Facility code like a 26-Bit card output.

The Facility code is set in Programming Menu number four and can be in the range 000 to 255. The factory default setting for the Facility code is 000 (see Section 6.2.6).

The keypad PIN code can be one to five digits in length and can range between 1 and 65,535. When entering a keypad PIN code that is less than 5 digits in length, **#** must be pressed to signify the end of PIN code entry. For keypad PIN codes that are 5 digits in length, on the fifth key press of the 5-digit PIN code, the data is sent across the Wiegand Data lines as binary data in the same format as a 26-Bit Card.

If ***** is pressed during PIN code entry or a PIN code greater than 65,535 is entered, the keypad clears the PIN code entry buffer, generates a beep and is ready to receive a new 5-digit keypad PIN code.

If the entry of the 1- to 5-digit keypad PIN code is disrupted and a number key or **#** is not pressed within 5 seconds, the keypad clears the PIN code entry buffer, generates a medium length beep and is ready to receive a new 1- to 5-digit keypad PIN code.

(EP) FFFF FFFF AAAA AAAA AAAA AAAA (OP)

Where:

EP = Even parity for first 12 bits

OP = Odd parity for last 12 bits

F = 8-bit Facility code

A = 16-bit code generated from keypad

Option 6: 6 Keys BCD and Parity Bits, Wiegand 26-Bit

Option 6 sends buffer of 6 keys, adds parity and sends a 26-Bit Binary BCD message. Each key is a four bit equivalent of the decimal number.

The keypad PIN code must be 6 key presses long. On the sixth key press of the 6-digit PIN code, the data is sent across the Wiegand Data lines as a BCD message.

If the entry of the 6-digit keypad PIN code is disrupted and no number key is pressed within 5 seconds, the keypad clears the PIN code entry buffer, generates a medium length beep and is ready to receive a new 6-digit keypad PIN code.

(EP) AAAA BBBB CCCC DDDD EEEE FFFF (OP)

Where:

EP = Even parity for first 12 bits

OP = Odd parity for last 12 bits

A = The first key entered	D = Fourth key entered
B = Second key entered	E = Fifth key entered
C = Third key entered	F = Sixth key entered

Option 8: 1 to 8 Keys BCD, Clock & Data

Buffers up to 8 keys and outputs keypad data without a Facility code like standard Clock and Data card output.

The keypad PIN code can be one to eight digits in length. The PIN code length is selected while programming the reader for Option 8. The reader transmits the data when it receives the last key press of

the PIN code. The data is sent across the two data output lines as binary data in Clock & Data format.

If ***** or **#** key is pressed during PIN code entry, the keypad clears the PIN code entry buffer, generates a beep, and is ready to receive a new keypad PIN code.

If the entry of the digit keypad PIN code is disrupted and a number key or **#** is not pressed within 5 seconds, the keypad clears the PIN code entry buffer, generates a medium length beep, and is ready to receive a new keypad PIN code.

When using the keypad transmission format "1 to 8 keys BCD, Clock & Data" (Option 8) an additional input is required to specify the number of keys in the PIN code.

Option 9: Single Key, Wiegand 4-Bit

Each key press immediately sends 4 bits of data, with no parity bits added.

0 = 0000	6 = 0110
1 = 0001	7 = 0111
2 = 0010	8 = 1000
3 = 0011	9 = 1001
4 = 0100	* = 1010 ="A" in Hexadecimal
5 = 0101	# =1011 ="B" in Hexadecimal

6.2.4 Selecting Proximity Card Transmission Format

There are eight different proximity card transmission formats.

See Table 4 in Section 6.2.3.1 for more information on keypad transmission formats.

To select the Proximity Card Transmission format:

1. Enter Programming mode.

2. Press **2** to enter Menu 2.

The left LED turns red.

3. Enter the appropriate option number for the proxy card transmission format that you wish to select:
   - Option 1: Wiegand 26-Bit
   - Option 2: Clock & Data
   - Option 3: Wiegand 32-Bit
   - Option 4: Wiegand 32-Bit Reversed Byte
   - Option 5: Wiegand 34-Bit
   - Option 6: Wiegand 40-Bit
   - Option 7: Wiegand 56-Bit
   - Option 8: Wiegand 64-Bit

   You hear three beeps.

   The system returns to Transmit mode.

6.2.4.1 Proximity Card Transmission Format Option Number

Table 5 presents the nine different keypad transmission formats.

Table 5: Proximity Card Transmission Format Option Number

Proximity Card Transmission Format	Option Number
Wiegand 26-Bit	1*
Clock & Data	2
Wiegand 32-Bit	3
Wiegand 32-Bit Reversed Byte	4
Wiegand 34-Bit	5
Wiegand 40-Bit	6
Wiegand 56-Bit	7
Wiegand 64-Bit	8

* Option 1 is the default factory setting.

More information on each of the different keypad transmission formats is available below and on the following pages.

Option 1: Wiegand 26-Bit

In this mode, 3 LSB bytes from the card serial number (UID) are transmitted in Wiegand 26-Bit format. Two parity bits are added. An even parity bit is sent first, followed by three bytes of card data, and by an odd parity bit.

(EP) AAAA AAAA AAAA AAAA AAAA AAAA (OP)

Where: EP = Even parity for first 12 bits
OP = Odd parity for last 12 bits
A = 3 bytes code generated from card data

Option 2: Clock and Data

In this mode, up to 6 bytes of the card serial number are transmitted in Clock & Data format.

Option 3: Wiegand 32-Bit

In this mode, 4 LSB bytes from the card serial number are transmitted in Wiegand 32-Bit format. No parity bits are added.

AAAA AAAA BBBB BBBB CCCC CCCC DDDD DDDD

Where: A = 4^{th} (MSB) byte of card serial number
B = 3^{rd} byte of card serial number
C = 2^{nd} byte of card serial number
D = 1^{st} (LSB) byte of card serial number

Option 4: Wiegand 32-Bit Reversed Byte

In this mode, 4 LSB bytes from card serial number are transmitted in Wiegand 32-bit format. Bytes are sent in reversed order. The LSB part of the card serial number is sent first and the MSB byte is sent last. No parity bits are added.

DDDD DDDD BBBB BBBB CCCC CCCC AAAA AAAA

Where: D = 1st (LSB) byte of card serial number
C = 2nd byte of card serial number
B = 3rd byte of card serial number
A = 4th (MSB) byte of card serial number

Option 5: Wiegand 34-Bit

In this mode, 4 LSB bytes of card serial number are transmitted in Wiegand 34-Bit format. Bytes are sent in reversed order. The LSB part of the card serial number is sent first and the MSB byte is sent last. An even parity is sent first, followed by 32-Bit data and an odd parity bit.

(EP) AAAA AAAA BBBB BBBB CCCC CCCC DDDD DDDD (OP)

Where: EP = Even parity for first 16 data bits
OP = Odd parity for last 16 data bits
A = 4th (MSB) byte of card serial number
B = 3rd byte of card serial number
C = 2nd byte of card serial number
D = 1st (LSB) byte of card serial number

Option 6: Wiegand 40-Bit

In this mode, 4 LSB bytes of card serial number are transmitted in Wiegand 40-Bit format. Bytes are sent in reversed order. The LSB part of card serial number is sent first. The last byte sent is a Checksum byte generated by adding 4 data bytes and discarding the remainder beyond 8 bytes.

AAAA AAAA BBBB BBBB CCCC CCCC DDDD DDDD (CSUM)

Where: A = 4th (MSB) byte of card serial number
B = 3rd byte of card serial number
C = 2nd byte of card serial number
D = 1st (LSB) byte of card serial number
CSUM = Checksum value, 1 byte (A+B+C+D)

Option 7: Wiegand 56-Bit

In this mode, 7 bytes of card serial number are transmitted in Wiegand 56-Bit format. No parity bits are added.

AAAA AAAA BBBBBBBB CCCCCCCC DDDDDDDD EEEEEEEE FFFFFFFF GGGGGGGG

Option 8: Wiegand 64-Bit

In this mode, 8 bytes of card serial number are transmitted in Wiegand 64-Bit format. No parity bits are added.

AAAA AAAA BBBBBBBB CCCCCCCC DDDDDDDD EEEEEEEE FFFFFFFF GGGGGGGG HHHHHHHH

6.2.5 Changing the Programming Code

Note

- The Programming code cannot be erased, meaning the code 0000 is invalid and does not erase the Programming code.
- The factory default 4-digit Programming code is 1234.

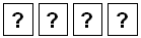
To change the Programming code:

1. Enter Programming mode.

2. Press **3** to enter Menu 3.

The left LED turns red.

3. Enter the new 4-digit code you wish to set as the Programming code.



You hear three beeps.

The system returns to Transmit mode.

6.2.6 Changing the Facility Code

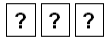
Note
- The Facility code can be in the range of 000 to 255.
- The default Facility code is 0.

1. Enter Programming mode.

2. Press **4** to enter Menu 4.

The left LED turns red.

3. Enter the new 3-digit code you wish to set as the Facility code.



You hear three beeps.

The system returns to Transmit mode.

6.3 Setting the Backlight

To set the backlight behavior:

1. Enter Programming mode.

2. Press **6** to enter Menu 6.

The Transmit LED turns red.

3. Enter the appropriate option number for the backlight option that you wish to select:
   - **0** for always off
   - **1** for always on
   - **2** for 10 sec. backlight after a key is pressed otherwise off
   - **3** for 10 sec. backlight after a key is pressed otherwise dimmed

You hear three beeps.

The system returns to Transmit mode.

6.4 Return to Factory Default Settings

> Warning
> You must be very careful before using this command! This erases the entire memory and return all codes to their factory default setting.

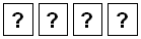
To return to factory default settings:

1. Enter Programming mode.

2. Press **0** to enter Menu 0.

   Both LEDs flash red.

3. Enter your 4-digit Programming code.



   If the Programming code is valid, all memory is erased. You hear three beeps and the reader returns to Transmit mode.

   If the Programming code is invalid, you hear a long beep and the reader returns to Transmit mode without erasing the memory of the reader.

6.5 Replacing a Lost Programming Code

In the event that the Programming code is forgotten, the AYC-x6355 can be reprogrammed in the field using the following instructions:

1. Remove power from the reader.
2. Activate tamper by removing the reader from the wall or removing the reader's case.
3. Apply power to the reader.
4. You now have 10 seconds to enter Programming mode using the factory default Programming code 1234.

7. Controller Functionality

Upon power on or reset, the unit flashes red, then green, and then orange, each for 1 second and a beep is heard for each color. The unit searches for the presence of Rosslare's secured intelligent power supply. If a secured intelligent power supply is detected, the buzzer emits 2 short beeps and the unit is automatically configured as a secure access control unit. The LED returns to its idle state – either green (Normal mode), red (Secure mode), or orange (Bypass mode).

The Lock Strike and Auxiliary outputs, as well as the REX input, are not located on the unit, eliminating the possibility of unauthorized entry to the restricted area.

7.1 Normal, Secure, and Master Users

The unit accepts up to 500 users and provides entry via the use of PIN codes and/or proximity cards. Each user is provided with two code memory slots, Memory Slot 1 (Primary code) and Memory Slot 2 (Secondary code).

The PIN code length has several options. The PIN code length can be a set number of 4, 5 or 6 digits or it can be a 4–8 digits option. When choosing the 4- to 8-digit option, please note that you should either enter zeros before the code, or press pound at the end (for example, if your code is 12345, enter either **00012345** or **12345#)**.

Entering a code refers to either PIN or proximity card.

The way in which the two memory slots are programmed determines a user's access level and also determines the way in which the unit grants access in its three modes of operation. There are three user levels:

- Normal

  A Normal user only has a Primary code and is only granted access when the unit is in Normal or Bypass mode.

- Secure

  A Secure user must have a Primary and Secondary code programmed; the two codes cannot be the same. The Secure user can gain access when the unit is in any of its three modes of operation. In Normal mode, the Secure user must use the Primary code to gain entry. In Secure mode, the Secure user must present both the Primary and Secondary codes to gain entry.

- Master

  A Master user must have both Primary and Secondary codes programmed with the same PIN code. The Master User can gain access during any mode of operation by presenting the PIN code and/or proximity card one time to the controller. (The Master user is convenient but is less secure than a Secure user.)

7.2 Modes of Operation

There are three modes of operation:

7.2.1 Normal Mode

The left LED is green.

Normal mode is the default mode. In Normal mode, the door is locked until a Primary code is presented to the controller. Special codes such as Lock Strike code and Auxiliary code are active in Normal mode. See Sections 7.9.3 and 7.9.4 for more information on the Lock Strike and Auxiliary codes.

7.2.2 Bypass Mode

The left LED is orange.

In Bypass mode, access to the premises is dependent on whether the controller's Lock Strike Relay is programmed for Fail Safe Operation or Fail Secure Operation. When the Lock Strike is programmed for Fail Secure Operation, the door is locked until * is pressed. When the Lock Strike is programmed for Fail Safe Operation, the door is constantly unlocked. In Bypass mode, programmed user codes still function.

7.2.3 Secure Mode

The left LED is red.

Only Secure and Master users can access the premises during the Secured mode.

A Secure user must enter the Primary and Secondary codes to gain entry. After entering their Primary code, the Door LED flashes green for 10 seconds, during which the Secondary code must be entered. A Master user only needs to present the code once to gain entry.

7.2.4 Changing the Modes of Operation

7.2.4.1 Changing from Normal Mode to Secure Mode

The default factory setting for the Normal/Secure code is 3838.

To change from Normal to Secure mode:

1. Enter the Normal/Secure code.

   The left LED flashes red.

2. Press **#** to confirm the mode change.

   The left LED stops flashing.

7.2.4.2 Changing from Secure Mode to Normal Mode

The default factory setting for the Normal/Secure code is 3838.

To change from Secure to Normal mode:

1. Enter the Normal/Secure code.

   The left LED flashes green.

2. Press **#** to confirm the mode change.

   The left LED stops flashing.

7.2.4.3 Changing from Normal Mode to Bypass Mode

See Section 7.9.7 to create/modify the Normal/Bypass code.

To change from Normal to Bypass mode:

1. Enter the Normal/Secure code.

   The left LED flashes orange.

2. Press **#** to confirm the mode change.

   The left LED stops flashing.

7.2.4.4 Changing from Bypass Mode to Normal Mode

See Section 7.9.7 to create/modify the Normal/Bypass code.

To change from Bypass to Normal mode:

1. Enter the Normal/Secure code.

   The left LED flashes green.

2. Press **#** to confirm the mode change.

   The left LED stops flashing.

7.3 Auxiliary Input and Output

For optimum usability in different applications, the controller's auxiliary input and output can be configured in ten different modes of operation.

7.4 Door Alarms

Door alarms can be generated by connecting the Auxiliary Input to a Door Position Switch. Either Door-Forced or Door-Ajar conditions are supported, as well as, a configurable delay timer for each alarm type. Only one door alarm is enabled at any one time. Door alarms may activate auxiliary output and siren depending on the auxiliary settings.

7.5 Internal Case and Back Tamper

If the unit is forcibly opened or it is removed from the wall, a tamper event is triggered. A tamper output opens sending a to the connected Alarm system (purple wire) the event closes when the tamper is closed (case is re-closed or re-attached to the wall).

The tamper event can also activate the auxiliary output if the controller is in Auxiliary Mode 3 (see Table 7).

7.6 Lockout Feature (Keypad/Card Tamper)

If the controller is presented with wrong codes (PIN or card) consecutively several times, the unit goes into Lockout mode.

When a lockout occurs, the controller's reader and keypad are de-activated so no codes can be entered until the set lockout period expires.

During Lockout mode, the left LED is Off, the right LED flashes red, and the controller beeps every two seconds.

7.7 REX Function

The REX button is connected to Rosslare's secured intelligent power supply. The REX button must be located inside the premises to be secured and is used to open the door without the use of a code. It is usually located in a convenient location, such as inside the door or at a receptionist's desk. The function of the REX button depends on whether the Lock Strike Relay is programmed for Fail Safe Operation or Fail Secure Operation.

- Fail Secure Operation – From the moment the REX button is pressed, the door is unlocked until the Lock Strike Release Time passes. After this time, the door is locked even if the REX button is not released.
- Fail Safe Operation – From the moment the REX button is pressed, the door is unlocked until the REX button is released, plus the Lock Strike Release Time. In this case, the Lock Strike Relay only begins its count down once the REX button is released.

7.8 Secured Intelligent Power Supply

Rosslare's secured intelligent power supplies are designed for use with Rosslare's secured standalone access control units, including the AYC-x6355 series. The AYC-x6355 units are designed to operate indoors and are installed within the secured premises. The units must be used with one of Rosslare's secured intelligent power supplies, which provides Lock Strike output and REX input. The AYC-x6355 and the power supply communicate through a proprietary Rosslare protocol, which provides a secure link between them. This in turn activates the door lock.

Each power supply unit contains a speaker connection for all sounder abilities. The sounder provides audible indications for the bell button (*****), door chime, and siren. The functionality of these audible indications is programmable.

For more information, see the *PS-x25T Installation Manual*.

7.9 Programming as a Controller

Programming is done solely via the unit's keypad driven Programming Menu System. To reach the Programming Menu System, the unit must first be put into Programming mode (see Section 7.9.1).

During the manufacturing process, certain codes and settings are pre-programmed. These settings are the called the default factory settings.

Table 6 shows the names of all Controller menus. It also shows of all the default factory codes and settings for the units.

Table 6: Controller Programming Menu

Menu No.	Menu Description	Default			
		4 digits	5 digits	6 digits	4–8 digits
1	Changing Lock Strike Code	2580	25802	258025	25802580
2	Change Auxiliary Code	0852	08520	085208	08520852
3	Changing Program Code	1234	12341	123412	12341234
4	Changing Normal/Secure Code	3838	38383	383838	38383838
5	Changing Normal/Bypass Code	N/A			
6	Changing Door Release Time	0004			
	Define auxiliary inputs/outputs	2004			
	Set Lockout	4000			
	Backlight Behavior	5100			
	Bell Button Behavior	7100			
7	Enrolling PIN Code				
8	Deleting PIN Code				
9	Code Assignment with Strike/Auxiliary				
0	Return to Factory Defaults or Change PIN Code Length				

You will find a complete description and instructions for each of the above menu items on the following subsections.

7.9.1 Entering Programming Mode

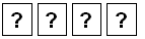
- The unit must be in Normal mode to enter the Programming mode.
- The factory four digit Programming Code is 1234.
- If a Programming Code is not entered within five seconds, the unit returns to Normal mode.

To enter Programming mode:

1. Press **#** twice.

   The left LED turns off and the right LED turns red.

2. Enter your 4-digit Programming code.



   The right LED turns green.

7.9.2 Exiting Programming Mode

To exit Programming mode:

1. Press **#** twice to exit Programming mode at any time.

   You hear 3 beeps.

   The left LED turns green and the right LED turns off.

   Wrong entries reset the controller back to Normal mode.

   While in Programming mode, if no key is pressed for one minute, the unit exits Programming mode and returns to Normal mode.

7.9.3 Changing Lock Strike Code

The Lock Strike code is mainly used as a method to quickly test the Lock Strike Relay during installation.

When the first user is added to the controller, the default Lock Strike code is automatically deleted. Once the code is programmed again, it is not deleted with the entry of additional user codes.

Note

- Lock Strike Code 1 does not work in the Secure mode.
- Wrong entries returns the controller to Normal mode.
- Code 0000 erases the Lock Strike Code 1.
- The factory default 4-digit Lock Strike code is 2580.

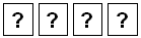
To change the Lock Strike code:

1. Enter Programming mode.

2. Press **1** to enter Menu 1.

The left LED turns red.

3. Enter the new code you wish to set as Lock Strike Code 1.



You hear three beeps.

The system returns to Normal mode.

7.9.4 Changing Auxiliary Code

The Auxiliary code is mainly used as a method to quickly test the Auxiliary Relay during installation.

When the first user is added to the controller, the default Auxiliary code is automatically deleted. Once the code is programmed again, it is not deleted with the entry of additional user codes.

To change the Auxiliary code:

Note

- Auxiliary code does not work in the Secure mode.
- Wrong entries return the controller to Normal mode.
- Code 0000 erases the Auxiliary code.
- The factory default 4-digit Auxiliary code is 0852.

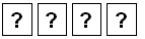
To change the Auxiliary code:

1. Enter Programming mode.

2. Press **2** to enter Menu 2.

   The left LED turns orange.

3. Enter the new code you wish to set as the Auxiliary code.



   You hear three beeps.

   The system returns to Normal mode.

7.9.5 Changing the Programming Code

Note

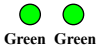
- Programming code cannot be erased, meaning the code 0000 is not valid and does not erase the Programming code.
- The factory four-digit programming code is 1234.

To change the Programming code:

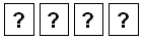
1. Enter Programming mode.

2. Press **3** to enter Menu 3.

The left LED turns green.



3. Enter the new code you wish to set as the Programming code.



You hear three beeps.

The system returns to Normal mode.

7.9.6 Changing the Normal/Secure Code

Note

- Code 0000 erases the Normal/Secure code.
- This code is disabled if the Auxiliary Input is set to toggle between Normal and Secure access modes.
- Default Normal/Secure code is 3838.

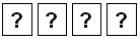
To change the Normal/Secure code:

1. Enter Programming mode.

2. Press **4** to enter Menu 4.

The left LED flashes red.

3. Enter the new code you wish to set as Normal/Secure code.



You hear three beeps.

The system returns to Normal mode.

7.9.7 Changing the Normal/Bypass Code and Door Chime Settings

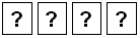
To change the Normal/Bypass code and door chime settings:

1. Enter Programming mode.

2. Press **5** to enter Menu 5.

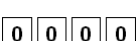
The left LED flashes orange.

3. Enter the new code you wish to set as Normal/Secure code.

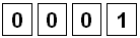


There are four different ways to program the Normal/Bypass code and door chime.

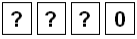
- Enter the code **0000** to disable both Bypass code and the door chime.



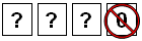
- Enter the code **0001** to disable the Bypass code and enable the door chime.



- Enter any code ending with 0 to enable the Bypass code and disable the door chime.



- Enter a code not ending with 0 to enable the Bypass code and enable the door chime.



You hear three beeps.

The system returns to Normal mode.

7.9.8 Setting Fail Safe/Secure Operation, Tamper Siren and Lock Strike Release Time

Note

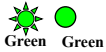
- The default value is 0004, which corresponds to Fail Secure operation, no siren, and 4-seconds Lock Strike release time.
- When the siren is sounding, entering a valid Lock Strike code deactivates the siren until the next siren event.

To set the Fail Safe/Secure Operation, Tamper Siren and Lock Strike Release Time:

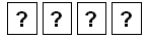
1. Enter Programming mode.

2. Press **6** to enter Menu 6.

   The left LED flashes green.



3. Construct a code using the following instructions:



   - First digit

     For Fail Secure Operation, the first digit should be **0**.

     For Fail Safe Operation the first digit should be **1**.
   - Second digit

     Siren Time in minutes (1–9, 0 – disabled)
   - Third and fourth digits

     Enter the number of seconds (from 1 to 99) that you want the Lock Strike to be released.

   For example, 0312 means a Fail Secure Operation consisting of a 3-minute siren and a 12-second Lock Strike release time.

   You hear three beeps.

   The system returns to Normal mode.

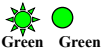
7.9.9 Defining the Auxiliary Input and Output

To define the auxiliary input and output:

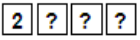
1. Enter Programming mode.

2. Press **6** to enter Menu 6.

   The left LED flashes green.



3. Construct a code using the following instructions:



   - Second digit (Auxiliary Mode)

     In addition to the Lock Strike Relay and Lock Strike REX, the unit features an Auxiliary Input. The Auxiliary mode defines the function of the Auxiliary Input.
   - Third and fourth digits (Auxiliary Setting)

     Each of the Auxiliary modes has a 2-digit setting that affects how the Auxiliary mode functions (Table 7).

   You hear three beeps.

   The system returns to Normal mode.

Table 7: Quick Reference Guide for Auxiliary Mode Setting

Aux. Mode	Aux. Input Function	Aux. Output Activated by	Aux. Relay	Aux. Settings (in seconds)
0	AUX REX	Valid code or AUX REX	N.O.	01 to 99 Aux. relay release time
1	Normal/Secure switch	Valid code	N.O.	01 to 99 Aux. relay release time
2	Normal/Secure switch	Star button (*)	N.O.	01 to 99 Aux. relay release time
3	Normal/Secure switch	Tamper event	N.C.	01 to 99 Aux. relay release time
6	Door Monitor	Forced door	N.C.	01 to 99 Forced delay
7	Door Monitor	Door ajar	N.C.	01 to 99 Ajar delay

7.9.10 Auxiliary Mode Reference Guide

The following are brief descriptions of each auxiliary mode. To implement the features of each mode, refer to Section 7.9.9.

7.9.10.1 Auxiliary Mode 0

Auxiliary input function: Activates the auxiliary output

Auxiliary output activated by: Valid user code, Auxiliary code, and Auxiliary input

For example, in Auxiliary Mode 0, the controller can function as a 2-door controller. The auxiliary relay is to be attached to the lock on the second door. The auxiliary setting defines the door open time for the second door. The auxiliary input is to be attached to the REX pushbutton for the second door. The Door Monitor input feature for the second door is not enabled when using this mode.

7.9.10.2 Auxiliary Mode 1

Auxiliary input function: Toggles Normal/Secure modes

Auxiliary output activated by: Valid user code, Auxiliary code

For example, in Auxiliary Mode 1, the controller can function as a 2-door controller. The auxiliary relay is to be attached to the lock on

the second door. The REX feature for the second door is not enabled when using this mode.

The auxiliary setting defines the door open time for the second door. The auxiliary input can switch the mode of operation of the controller between Normal and Secure modes. By connecting a switch timer or alarm system output to the auxiliary input, the controller can be automatically switched from Normal mode (during office hours) to Secure mode (after office hours).

7.9.10.3 Auxiliary Mode 2

Auxiliary input function: Toggles Normal/Secure modes

Auxiliary output activated by: * Button

For example, in Auxiliary Mode 2, the auxiliary relay can function as a general purpose time switch that can be activated when ***** is pressed. The auxiliary setting establishes for how long the auxiliary relay is to be activated. The auxiliary input can switch the mode of operation of the controller between Normal and Secure modes. By connecting a switch timer or alarm system output to the auxiliary input, the controller can be automatically switched from Normal mode (during office hours) to Secure mode (after office hours).

7.9.10.4 Auxiliary Mode 3

Auxiliary input function: Toggles Normal/Secure modes

Auxiliary output activated by: Alarms

For example, in Auxiliary Mode 3, the auxiliary output is activated if the controller is tampered; that is, if the case is forcibly opened or removed from the wall. The auxiliary input can switch the mode of operation of the controller between Normal and Secure modes. By connecting a switch timer or alarm system output to the auxiliary input, the controller can be automatically switched from Normal mode (during office hours) to Secure mode (after office hours).

7.9.10.5 Auxiliary Mode 6

Auxiliary input function: Door Monitor

Auxiliary output activated by: Forced entry

For example, in Auxiliary Mode 6, the controller can trigger the auxiliary relay if the door has been forced. If the siren settings are enabled, the siren is activated.

In this mode, the auxiliary input functions as a door monitor switch and is wired to the magnetic contact switch on the door. The auxiliary relay is to be wired to the alarm system. If the door is forced open, the controller waits for the period of the forced door delay time to elapse and then it activates the auxiliary relay. The auxiliary setting sets the forced door delay period.

7.9.10.6 Auxiliary Mode 7

Auxiliary input function: Door Monitor

Auxiliary output activated by: Door Ajar (door held open)

For example, in Auxiliary Mode 7, the controller can trigger the auxiliary relay if it detects that the door has been held open (ajar) too long. In this mode, the auxiliary input functions as a door monitor switch and is wired to the magnetic contact switch on the door. The auxiliary relay is to be wired to the alarm system. If the door is opened, the controller waits for the Door Ajar Delay time to elapse and if the door does not close prior to the end of this period, the controller activates the auxiliary relay. The auxiliary setting defines the Door Ajar Delay time.

7.9.11 Setting the Lockout Feature

If the controller is presented with wrong codes several times consecutively, the unit goes into Lockout mode.

When a lockout occurs, the controller keypad and reader are locked so no codes can be entered until the set lockout period expires. During Lockout, the left LED is Off, the right LED flashes red, and the controller beeps every two seconds.

The default setting for the Lockout Feature is 4000 (Lockout Disabled).

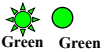
Note: Using the lockout feature is highly recommended, especially when selecting to use short PIN code length (4 or 5 digits).

To set the lockout feature:

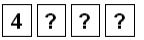
1. Enter Programming mode.

2. Press **6** to enter Menu 6.

   The left LED flashes green.



3. Construct a code using the following instructions:



   - Second digit

     Set the number of wrong code attempts, which causes a Lockout between 0 and 9 attempts.

   - Third and fourth digits

     Sets the Duration of the lockout, between 00 and 99; the value is multiplied by ten, resulting in 0 to 990 seconds.

7.9.12 Setting the Backlight Behavior

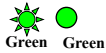
The controller allows you to define the way the unit's backlight works.

To set the backlight behavior:

1. Enter Programming mode.

2. Press **6** to enter Menu 6.

   The left LED flashes green.



3. Enter one of the following codes:
   - **5000** – Backlight off
   - **5100** – Backlight on (default)
   - **5200** – Backlight is off, activates for 10 seconds when a key is pressed, after which it dims until off
   - **5300** – Backlight is dimmed, activates for 10 seconds when a key is pressed, after which it returns to a dimmed level

7.9.13 Setting the Bell Button (*) Behavior

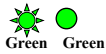
The controller allows you to enable or disable the bell button.

To set the bell button behavior:

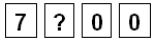
1. Enter Programming mode.

2. Press **6** to enter Menu 6.

   The Mode LED flashes green.



3. Construct a code using the following instructions:



   - **7000** – Bell button Off
   - **7100** – Bell button On (default)

7.9.14 Enrolling Primary and Secondary Codes

7.9.14.1 Primary Codes

- Primary codes can only be enrolled to an empty user slot, meaning a slot where there is no existing Primary code.
- Primary codes must be unique, meaning one user's Primary code may not be the same as other user's Primary code.
- Primary codes cannot be the same as any system codes, such as the Normal/Secure code or Lock Strike code.
- Users who hold a Primary code can gain entry only during Normal mode.
- Primary codes consisting of only zeros (such as '0000') are not allowed.

7.9.14.2 Secondary Codes

- Secondary codes can only be enrolled to a user slot that already has a Primary code enrolled but has no Secondary code.
- Secondary codes do not have to be unique, meaning multiple users can all hold the same Secondary code.
- Secondary codes cannot be the same as any system codes, such as the Normal/Secure or Lock Strike codes.
- Users who hold Secondary codes can gain entry even in Secure mode.
- Secondary codes consisting of only zeros (such as '0000') are not allowed.

7.9.14.3 Methods

There are two methods to enroll Primary and Secondary codes:

- Standard Method

  The Standard Method is mainly used when the user slot number for the user you wish to program is known. You can program both Primary and Secondary codes using the Standard method (see Section 7.9.14.4).

- Code Search Method

  The Code Search Method is mainly used when enrolling a user's Secondary code and the user slot code is unknown.

  The Code Search method only works if a user's Primary code is already enrolled but the Secondary code is not (see Section 7.9.14.5).

7.9.14.4 Enrolling Primary and Secondary Codes using Standard Method

To enroll primary and secondary codes using the Standard method:

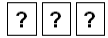
1. Enter Programming mode.

2. Press **7** to enter Menu 7.

   The right LED turns orange.

3. Enter the 3-digit user slot number between 001 and 500 that you wish to enroll a Primary or Secondary code to.

   For example, User Slot 003 represents User #3.



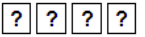
   If the selected slot has no Primary code, the left LED flashes green, indicating that the controller is ready to accept a Primary code.

   If the selected slot already has a Primary code but no Secondary code, the left LED flashes red, indicating that the controller is ready to accept a Secondary code.

   If the selected slot already has a Primary and Secondary code, you hear a long beep and the controller returns to Normal mode.

4. Perform one of the following:

   - Enter the 4- to 8-digit PIN code that you want to assign as the Primary or Secondary code for this slot number.

   - Present your user card that you want to assign as the Primary or Secondary code for this slot number.

   If the PIN or user card presented is valid, the left LED stops flashing and the controller is ready for you to enter the next 3-digit slot number (refer to Step 3) for the slot to which you want to assign a code.

5. Do one of the following:
   - Press **#** to move to the next available user slot number.
   - Enter another 3-digit user slot number.
   - If you do not wish to continue enrolling codes, press **#** twice and the controller returns to Normal mode.

7.9.14.5 Enrolling Secondary Codes using Search Method

The Code Search feature enables you to quickly enroll a Secondary code to a user who already has a Primary code.

To enroll secondary codes using the Code Search method:

1. Enter Programming mode.

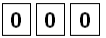
2. Press **7** to enter Menu 7.

   The right LED turns orange.

3. Enter **000** as the 3-digit user slot number.

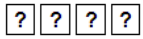
   The right LED flashes orange.

   The controller is now waiting for the Primary code of the user to whom you want to add a Secondary code.

4. Perform one of the following:

   - Enter the 4- to 8-digit PIN code belonging to the user for whom you wish to add a Secondary code.

   - Present the user card belonging to the user for whom you wish to add a Secondary code.

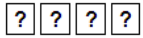
   The left LED flashes red.

   If the Primary code entered is not valid, you hear a long beep and the unit continues to wait for a valid Primary code.

5. Perform one of the following:

   - Enter the 4- to 8-digit code to be used as the Secondary code.

   - Present the user card to be used as the Secondary code.

   If the Secondary code is valid, the controller beeps three times and returns to Normal mode.

   If the Secondary code is invalid, the controller sounds a long beep, and the unit continues to wait for a valid Secondary code to be entered.

7.9.15 Deleting Primary and Secondary Codes

There are two methods to delete Primary and Secondary codes: the Standard Method and the Code Search Method.

When deleting a user slot, both the Primary code and the Secondary code are erased.

7.9.15.1 Deleting Primary and Secondary Codes using Standard Method

Note: It is recommended that a record be kept of added and deleted users so that it is easier to keep track of which user slots are empty and which user slots are not.

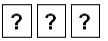
To delete the Primary and Secondary codes using the Standard Method:

1. Enter Programming mode.

2. Press **8** to enter Menu 8.

   The left LED turns red and the right LED turns orange.

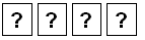
3. Enter the 3-digit User Slot code you wish to delete.



   The left LED flashes red indicating the controller is waiting for the Programming code to confirm the deletion.

   If the user slot is empty, you hear a long beep and the unit returns to Normal mode.

4. Enter your 4-digit Programming code to confirm the deletion.



   If the Programming code is valid, three beeps are heard and the controller returns to Normal mode.

   If the Programming code is invalid, a long beep is heard and the controller returns to Normal mode.

7.9.15.2 Deleting Primary and Secondary Codes using Search Method

> Note: It is recommended that a record be kept of added and deleted users so that it is easier to keep track of which user slots are empty and which user slots are not.

To delete the Primary and Secondary codes using the Code Search Method:

1. Enter Programming mode.

2. Press **8** to enter Menu 8.

   The left LED turns red and the right LED turns orange.

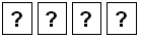
3. Enter **000** as the 3-digit user slot number.

   The right LED flashes orange.

   The controller is now waiting for the Primary code of the user you want to delete.

4. Perform one of the following:

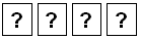
   - Enter the 4- to 8-digit PIN code of the Primary code belonging to the user you want to delete.



   - Present the user card of the Primary code belonging to the user you want to delete.

   The left LED flashes red.

5. Enter your 4-digit Programming code to confirm the deletion.



If the Programming code is valid, you hear three beeps and the unit returns to Normal mode.

If the Programming code is invalid, you hear a long beep and the unit returns to Normal mode.

7.9.16 Relay Codes Assignment

When a primary code is enrolled for any user, the user is authorized to activate the Lock Strike relay. However, different user codes may be set to operate the auxiliary relay instead or operate both the Lock strike and auxiliary relay. Assignment of such codes is achievable for any valid user code entered in the controller.

There are two methods to assign relay codes to users: a standard method and a search method.

7.9.17 Relay Code Assignment using Standard Method

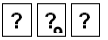
To assign relay code using the Standard method:

1. Enter Programming mode.

2. Press **9** to enter Menu 9.

The left LED turns green and the right LED turns orange.

3. Enter the 3-digit user slot for code assignment.



The left LED flashes green.

4. Enter the assignment digit for the current user slot:
   - **1** activates the Lock Strike relay only default
   - **2** activates the Auxiliary relay only
   - **3** activates the Lock Strike and Auxiliary relays

   If the assignment code is valid, the mode indicator stops flashing.

   The controller is now waiting for another slot number.
5. Do one of the following:
   - Press **#** to move to the next available user slot number.
   - Enter another 3-digit user slot number.
   - If you do not wish to continue enrolling codes, press **#** twice and the controller returns to Normal mode.

7.9.18 Relay Code Assignment using Search Method

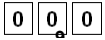
To assign relay code using the Search method:

1. Enter Programming mode.

2. Press **9** to enter Menu 9.

   The left LED turns green and the right LED turns orange.

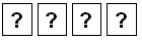
3. Enter **000** for user slot access.



   The right LED flashes orange.

   The controller is now waiting for the primary code of the user.

4. Perform one of the following:
   - Enter the 4- to 8-digit PIN code of the Primary code belonging to the user you want to delete.

   - Present the user card of the Primary code belonging to the user you want to delete.

   The left LED flashes green.

5. Enter the assignment digit for the current user slot:
   - **1** activates the Lock Strike relay only default
   - **2** activates the Auxiliary relay only
   - **3** activates the Lock Strike and Auxiliary relays

   If the assignment digit is valid, three beeps are heard and the controller returns to Normal mode.

   If the assignment digit is invalid, a long beep sounds and the controller waits for another assignment digit to be entered.

7.9.19 PIN Code Length/Factory Default Settings

You must be very careful before using this command! Changing the PIN code length also erases the entire memory contents, including all user and special codes, and return all codes to their factory default settings.

To change the PIN code length:

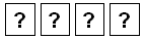
1. Enter Programming mode.

2. Select the desired PIN code length as follows:
   - **00** – Returns to factory defaults and sets a 4-digit code.
   - **05** – Returns to factory defaults and sets a 5-digit code.
   - **06** – Returns to factory defaults and sets a 6-digit code.
   - **08** – Returns to factory defaults and sets a 4- to 8-digit code

Both LEDs flash red.

3. Enter your 4-digit Programming code



If the Programming code is valid, all memory is erased. You hear three beeps and the controller returns to Normal mode.

If the Programming code is invalid, you hear a long beep and the controller returns to Normal mode without erasing the memory contents.

7.9.20 Replacing a Lost Programming Code

The unit must be in Normal mode; otherwise, this does not work. Make sure that the left LED is green before proceeding.

To replace a lost Programming code:

1. Remove power from the power supply unit.
2. Press the REX button on the power supply unit.
3. Apply power to the unit with REX button pressed.
4. Release the REX button.
5. You now have 10 seconds to program a new Programming code into the access control unit using the initial default code 1234, before the controller reverts to the existing code.

7.9.21 Exiting Secure Mode if Normal/Secure Code was Lost

To exit Secure mode if Normal/Secure Code was lost:

1. Remove power from the power supply unit.
2. Press the REX button on the power supply unit.
3. Apply power to the unit with the REX button pressed.
4. Release the REX button.
5. You now have 10 seconds to exit Secure mode using the initial default Normal/Secure code 3838.
6. Program a new normal/secure code as described in Section 7.9.6.

A. Declaration of Conformity

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

B. Limited Warranty

The full ROSSLARE Limited Warranty Statement is available in the Quick Links section on the ROSSLARE website at www.rosslaresecurity.com.

Rosslare considers any use of this product as agreement to the Warranty Terms even if you do not review them.

Asia Pacific, Middle East, Africa

Rosslare Enterprises Ltd.
Kowloon Bay, Hong Kong
Tel: +852-2795-5630
Fax: +852-2795-1508
support.apac@rosslaresecurity.com

United States and Canada

Rosslare Security Products, Inc.
Southlake, TX, USA
Toll Free: +1-866-632-1101
Local: +1-817-305-0006
Fax: +1-817-305-0069
support.na@rosslaresecurity.com

Europe

Rosslare Israel Ltd.
Rosh HaAyin, Israel
Tel: +972-3-938-6838
Fax: +972-3-938-6830
support.eu@rosslaresecurity.com

Latin America

Rosslare Latin America
Buenos Aires, Argentina
Tel: +54-11-4001-3104
support.la@rosslaresecurity.com

China

Rosslare Electronics (Shenzhen) Ltd.
Shenzhen, China
Tel: +86-755-8610 6842
Fax: +86-755-8610 6101
support.cn@rosslaresecurity.com

India

Rosslare Electronics India Pvt Ltd.
Tel/Fax: +91-20-40147830
Mobile: +91-9975768824
sales.in@rosslaresecurity.com

0706-0960600+02

ROSSLARE
SECURITY PRODUCTS
www.rosslaresecurity.com

RoHS COMPLIANT

CE