AY-Q6x60 Series

Anti-Vandal MIFARE® Contactless Smart Card / Sector Readers

Installation and User Manual

Models:

AY-Q6260
AY-Q6360

AY-Q6260

AY-Q6360

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 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 AY-Q6260 and AY-Q6360 are metallic, anti-vandal, MIFARE® contactless smart card sector readers used in access control system solutions.

The readers scan information from a MIFARE smart card, which is stored in a specific and protected sector, and send the data on to a connected access control system.

The system reads MIFARE 1K and MIFARE 4K card sector data, as well as the unique ID number of the following cards: MIFARE 1K, MIFARE 4K, MIFARE Ultralight, and MIFARE DESFire. The readers transmit the identification numbers they receive to an access control system.

The readers can also check the validity of cards before scanning them. When checking, readers only send card information to the access control system from cards with the correct security pass-code. The readers are suitable for both indoor and outdoor installations.

Reader setup and operation is controlled using a configuration card to adjust settings directly, without having to connect a remote computer or remove the unit. The configuration card is a regular MIFARE 1K card, which can be pre-programmed using Rosslare’s CP-R25 (or CP-R26) desktop MIFARE programmer, together with its associated software the AS-B01.

The AY-Q6260 and AY-Q6360 readers are compatible with almost all access controllers, including Rosslare's AC-115, AC-215, and AC-225 controllers.

1.1 Supported RFID Transponders

The AY-Q6260 and AY-Q6360 read the following transponders:

- MIFARE Ultralight (card serial number only)
- MIFARE Classic 1K
- MIFARE 4K
- MIFARE DESFire (card serial number only)

1.2 Box Content

Before beginning, verify that all of the following is in the box. If anything is missing, please report the discrepancy to your nearest Rosslare office.

- 1 reader
- 1 manual
- Installation kit including:
  - 1 self-adhesive drilling template
  - 1 security spline key
  - 1 security hex key
  - 2 mounting screws
  - 2 wall plugs

2. Installation

> Note: Installation of an RFID reader adjacent to metallic surfaces might alter the reader's specifications. To diminish this interference, use a plastic spacer when mounting the reader.

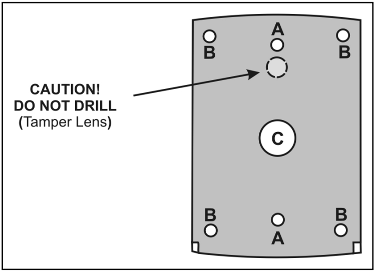
2.1 Mounting

Before starting, select the location to mount the unit. This location should be at shoulder height.

To mount the unit:

1. Peel off the back of the self-adhesive installation template and attach the template to the required location.
2. At the bottom of the unit's case, remove the screw.
3. Remove the cover by gently sliding it up and then pulling it apart. Once you remove the cover, you will see the screw holes for mounting.
4. Depending on the type of installation, gang box or panel mount, drill the respective holes in the rear cover: for gang box mounting, drill two holes marked "A"; for flat panel mount, drill four holes marked "B" (Figure 1).

Figure 1: Drilling Mounting Holes



5. Drill a 10-mm (7/16”) hole for the cable. If the surface is metal, place a grommet or electrical tape around the edge of the hole.
6. Insert the unit’s cable wire into the cable hole and wire the unit as described in Section 2.2.
7. Screw the back cover to its mounting location.
8. Carefully re-attach the front cover of the unit.
9. Secure the front cover by using the supplied security Torx screw. A Torx security screw tool is provided to tighten the security Torx screw.

2.2 Wiring

The units are supplied with a 10-conductor 46-cm (18-in.) pigtail with exposed wires coated with solder.

> Note
> The reader's power supply must either share the access controller's power supply or a common ground with the access control system.

To connect the reader to the controller:

1. Select the appropriate connections according to Table 1.

Table 1: Wiring the Reader to the Controller

Color	Function
Red	DC+ Input
Black	Ground
White	Data 1 /Clock
Green	Data 0 / Data
Brown	LED/Buzzer Control
Purple	Tamper
Orange	Factory Use
Yellow	N/A
Blue	Factory Use
Gray	Factory Use

2. Prepare the controller cable by cutting the cable jacket back 3.2 cm (1¼”) and stripping the wire 1.3 cm (½”).
3. Splice the reader’s pigtail wires to the corresponding controller wires and cover each joint with insulating tape.
4. Trim and cover all unused conductors.

Note

To shield the cable from external interference, attach it to one of the following:

- The same earth ground as the access control system
- The signal ground connection at the panel
- The power supply end of the cable

3. Configuring the Reader

To provide the highest level of security, the reader is programmed to validate only MIFARE cards whose settings correspond to the master card that is used to prepare the reader for configuration. A configuration card is then used to configure the settings.

Configuration and master cards make it possible to set up and adjust a reader's settings directly without connecting a remote computer and without removing the unit from its place.

Rosslare’s CP-R25 (or CP-R26) desktop MIFARE card programmer together with its associated software AS-B01 must be used to create configuration cards.

3.1 Operation Modes

The reader operates in two modes:

- Card Serial Number mode

  The reader scans every card and sends each card's serial number to the access control system. This CSN is unique for each card. In this mode, keypad programming is enabled and can be used to program some reader settings.

> Note
>
> In some circumstances, not all serial number digits are transmitted. This depends on selected reader transmit format and on card type being read.

- Secure mode

  The reader only scans cards with a valid pass code (predefined key of the MIFARE card). When a user card has the correct pass code, the reader then scans a specified location on the card for an identification number and sends this information to the access control system. A card with the wrong pass code is not transmitted.

The reader's operation mode is controlled by a configuration setting stored on the configuration card. All access information and locations for Secure mode operations are also controlled by configuration settings. In this mode, programming the reader via the keypad is not possible.

By default, the reader operates in Card Serial Number mode.

Note

In this mode, only MIFARE 1K and MIFARE 4K cards are supported. MIFARE Ultralight and DESFire cards are non functional.

3.2 Configuration Card Structure

MIFARE smart cards are split into multiple sectors (on a MIFARE 1K card, for example). Each sector contains 4 blocks of 16 bytes each. The information on how to program and configure readers is stored in sector zero of the configuration smart card.

Refer to the CP-R25 (or CP-R26) and AS-B01 manual for further configuration options and descriptions.

3.3 Configuring Settings

The configuration card stores a variety of preference settings to apply to readers. Settings are stored in sector zero of the card.

3.4 Configuration Procedure

It is recommended to configure the reader one time only, following installation and on its initial use. However, if needed, configuring the reader can be done anytime using the same procedure described below.

To configure the reader:

1. Present the master card.

   A short beep is generated and the reader LED is orange as the reader goes into Configuration mode.

2. Within 30 seconds (while the reader is still in Configuration mode), present a valid configuration card to the reader.

   If the configuration is valid, three short beeps are emitted and the reader LED turns red.

   If configuration fails (due to a bad configuration card), three long beeps are generated and the reader exits Configuration mode.

   If the reader has been previously been configured, then following a failed configuration, the reader returns to Standby mode and continues to work with its previous configuration settings.

4. How to Use the Reader

After the reader has been mounted, connected to an access control system, and configured, it is ready for use.

4.1 Normal Operation

Turn on the reader. The LED turns red. If the reader has not yet been configured, the reader can only read the CSN. However, you must still configure the card for additional configurations (see Section 3.4).

4.1.1 Card Serial Number Mode

In this mode, presentation of an access card results in the transmission of the card's factory programmed serial number. A short beep is emitted and the LED momentarily turns green, and then returns to red.

> Note
>
> If the card serial number is not fully transmitted, only the LSB portion of the serial number is transmitted. This depends on the reader transmit format of the selected reader and the length of the card serial number. For example, when the Wiegand 26-bit transmit format is selected; the MSB byte of the MIFARE 1K card's serial number is not transmitted.

4.1.2 Secure Mode

In this mode, the reader attempts to read data programmed in the user card sector memory. If the reader's Pass Code A is identical to the card's Key A and access conditions are valid, the reader transmits the data, emits a short beep, and momentarily turns the LED to green and then back to red.

If the reader fails to read the programmed data, it emits a long beep to indicate that an error has occurred. This error may either be the result of the wrong Pass Code A or the wrong access conditions. This mode is intended to support MIFARE 1K and MIFARE 4K cards only.

4.2 Manual LED and Buzzer Control

LED and buzzer behavior depend upon the reader firmware. For example, three beeps on reset and successful configuration, or one short beep and a flashing LED upon card transmission. However, it is possible that the host control panel, to which the reader is connected, may control the LED, the buzzer, or both. This depends upon manipulation of the LED/buzzer control input, and only if these options are enabled by the reader configurations.

These settings can be overridden using the brown LED/buzzer control wire:

- LED/buzzer control wire is left open:
    - LED and buzzer behave naturally, on the basis of firmware preferences.
- LED/buzzer control wire is connected to ground:
    - If the LED control is enabled, the LED turns green.
    - If the buzzer control is enabled, the buzzer continuously buzzes.
    - If both LED and buzzer control are enabled, the led turns green and buzzer contentiously operated.

Use the LED/buzzer control wire to drive the behavior of the LED and buzzer directly from the access control software.

> Note
>
> LED and buzzer control function can be only programmed by configuration card. They cannot be programmed using the reader keypad.

4.3 Optical Back Tamper

The AY-Q6260 and AY-Q6360 includes an optical back tampering mechanism which detects all attempts to dismantle the unit or remove it from the wall.

The status of the tamper mechanism is indicated by the purple Tamper control wire.

When the back tamper optical sensor is in “darkness” status, the internal tamper output transistor is pulled to low.

When the back tamper optical sensor is in its "lit" status, the internal tamper output transistor's collector is open. A tamper signal is detected by the host control panel.

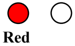
5. Programming

> Note
>
> Programming applies to the AY-Q6360 model only.

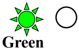
5.1 Standby Mode

When the AY-Q6360 is in Standby mode, it is ready to read MIFARE CSN or entered PIN code data.

When the reader is in Standby 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.



Keyboard data can be sent via one of eight keypad transmission formats. Refer to Section 5.5 for more information on selecting keypad transmission formats.

MIFARE cards presented to the reader are always sent in Wiegand or Clock & Data format. Refer to Section 5.6 for more information on selecting card transmission formats.

5.2 Programming Menu

Various reader options can be programmed using the reader keypad, but not all of them.

Keypad programming is only enabled when the reader is in CSN mode.

Once in Secure mode, keypad programming is disabled.

Programming is done via the unit's keypad driven Programming Menu System. Table 2 shows the names of all the programming menus. Default factory settings are marked by an asterisk (*).

Table 2: Programming Menu

	Menu Description	Default
1	**Selecting Keypad Transmission Format** 1 – Single Key, Wiegand 6-Bit (Rosslare Format, Default) 2 – Single Key, Wiegand 6-Bit with Nibble + Parity Bits 3 – Single Key, Wiegand 8-Bit, Nibbles Complemented 4 – 4 Keys Binary + Facility Code, Wiegand 26-Bit 5 – 1 to 5 Keys + Facility Code, Wiegand 26-Bit 6 – 6 Keys BCD and Parity Bits, Wiegand 26-Bit 8 – 1 to 8 Keys BCD, Clock & Data Single Key	*
2	**Selecting MIFARE Card Transmission Format** 1 – Wiegand 26-Bit (default) 2 – Clock & Data 4 – Wiegand 26-Bit with Facility code output 5 – Wiegand 32-Bit 6 – Wiegand 32-Bit reverse output 7 – Wiegand 34-Bit 8 –.Wiegand 40-Bit	*
3	**Changing the Programming Code**	1234
4	**Changing the Facility Code**	001
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**	

Note

Reader settings are affected by both keypad programming and configuration card settings. Note that settings are preset by the last operation, either configuration card or keypad programming.

5.3 Entering Programming Mode

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

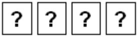
> - The factory default Programming code is 1234.
> - If a Programming code is not entered within 30 seconds, the unit returns to Standby mode.

To enter Programming mode:

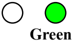
1. Press # four times.

   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.



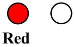
   If the Programming code is invalid, you hear a long beep and the reader returns to Standby mode.

5.4 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 Standby mode.

   Wrong entries may reset the reader back to Standby mode. If no key is pressed for 30 seconds while in Programming mode, the unit returns to Standby mode.

5.5 Selecting Keypad Transmission Format

There are eight keypad transmission formats.

More information on each of the keypad transmission formats is presented in Section 5.5.1.

> Note
>
> Only one keypad transmission format can be active at any one time.

To select the keypad transmission format:

1. Enter Programming mode.

   ○ ● Green

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

   [1]

   The left LED turns red.

   ● ● Red Green

3. Enter one of the following codes:
   - **1** – Single Key, Wiegand 6-Bit (Rosslare Format) (default)
   - **2** – Single Key, Wiegand 6-Bit with Nibble + Parity Bits
   - **3** – Single Key, Wiegand 8-Bit, Nibbles Complemented
   - **4** – 4 Keys Binary + Facility Code, Wiegand 26-Bit
   - **5** – 1 to 5 Keys + Facility Code, Wiegand 26-Bit
   - **6** – 6 Keys BCD and Parity Bits, Wiegand 26-Bit
   - **8** – 1 to 8 Keys BCD, Clock & Data Single Key
   - **9** – Single Key, Wiegand 4-Bit

> Note
>
> When selecting Option 8, the right LED turns orange and an additional input is required to specify the number of keys in the PIN code.

   You hear three beeps.

   ● ○ Red

   The system returns to Standby mode.

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

5.5.1 Keypad Transmission Formats

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	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 1011 1 = "B" in Hexadecimal
5 = 1 0101 0	# = 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 4 four and can be in the range 000 to 255. The factory default setting for the Facility code is 001 (see Section 5.8 for more information).

The keypad PIN code must be 4 digits in length 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 **#** is pressed during PIN code entry, the keypad clears the PIN code entry buffer, generates 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 = 24-Bit code generated from keyboard

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

This option 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 4 and can be in the range 000 to 255. The factory default setting for the Facility code is 001 (see Section 5.8 for more information).

The keypad PIN code can be one to five digits in length and can range between 0 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 4-digit keypad PIN code.

If the entry of the 1- to 5-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 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 = 24-Bit code generated from keyboard

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

This option sends a buffer of 6 keys, adds parity, and sends a 26-Bit 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, (# and * are valid), 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:

A = The first key entered

B = Second key entered

C = Third key entered

D = Fourth key entered

E = Fifth key entered

F = Sixth key entered

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

This option buffers up to 8 keys and outputs keypad data, much 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 **#** 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.

Option 9: Single Key, Wiegand 4-Bit

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

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

5.6 Selecting Proximity Card Transmission Format

There are eight proximity card transmission formats.

More information on each of the proximity card transmission formats is presented in Section 5.6.1.

To select the proximity card transmission format:

1. Enter Programming mode.

   ○ 🟢 Green

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

   $\boxed{2}$

   The left LED turns red.

   🔴 🟢 Red Green

3. Enter the appropriate option number for the Rosslare proximity card transmission format:
   - **1** – Wiegand 26-Bit
   - **2** – Clock & Data
   - **3** – Wiegand Card + PIN
   - **4** – Wiegand 26-Bit with Facility code output
   - **5** – Wiegand 32-Bit
   - **6** – Wiegand 32-Bit reverse output
   - **7** – Wiegand 34-Bit
   - **8** – Wiegand 40-Bit

   You hear three beeps.

   The system returns to Standby mode.

   🔴 ○ Red

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

5.6.1 Proximity Card Transmission Formats

Option 1: Wiegand 26-Bit

In this mode, 3 bytes of card serial number are transmitted in Wiegand 26-Bit format. Two parity bits are added. An even parity bit is sent first, followed by three bytes card data than followed by odd parity bit.

Note The fourth byte of the cards serial number is not transmitted.

(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 & Data

In this mode, 4 bytes of card serial number are transmitted in Clock & Data format.

Option 3: Wiegand Card + PIN Transmission Format

This unique format is intended to let host controllers get card and keypad data simultaneously. This option overrules the selected keypad transmission format and sends the keypad data as described below.

The AY-Q6360 output data turns into a virtual 52-bit Wiegand – 26-bit card data followed by a 26-bit keypad data.

After a card is presented to the unit, the Transmit LED starts to flash red to indicate that the unit is waiting for the PIN code.

The entered PIN code is buffered up to 5 keys and outputs keypad data with a Facility code much like Option 5 (1 to 5 Keys + Facility Code, 26-Bit Wiegand).

Option 4: Wiegand 26-Bit and Facility Code

In this mode, 1 byte Facility code followed by 2 bytes of the card's serial number are transmitted in Wiegand 26-Bit format. Two parity bits are added. An even parity bit is sent first, followed by one Facility code byte then followed by two bytes card serial number ending with an odd parity bit.

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

Where: EP = Even parity for first 12 bits
OP = Odd parity for last 12 bits
F = 1 byte Facility code
A = 2 bytes code generated from card serial number.

> The third and fourth bytes of the cards serial number is not transmitted.

Option 5: Wiegand 32-Bit

In this mode, 4 bytes of 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 = 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 32-Bit Reversed

In this mode, 4 bytes of card serial number are transmitted in Wiegand 32-bit format. Bytes are sent in reversed order. LSB part of card serial number is sent first and 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 7: Wiegand 34-Bit

In this mode, 4 bytes of card serial number are transmitted in Wiegand 34-bit format. Bytes are sent in reversed order. LSB part of card serial number is sent first and MSB byte is sent last. An even parity is sent first, followed by 32 bits data followed by 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 8: Wiegand 40-Bit and Checksum

In this mode, 4 bytes of card serial number are transmitted in Wiegand 40-Bit format. Bytes are sent in reversed order. LSB part of card serial number is sent first. Last byte sent is Checksum byte generated by adding 4 data bytes and discarding 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)

5.7 Changing the Programming Code

Note

- The Default Programming code is 1234
- Programming code cannot be erased, meaning the code **0000** is not valid and does not erase the Programming code

To change the Programming code:

1. Enter Programming mode.	○ 🟢 Green
2. Press **3** to enter Menu 3.	3
The left LED turns red.	🔴 🟢 Red Green
3. Enter the new 4-digit code you wish to set as the Programming code.	? ? ? ?
You hear three beeps. The system returns to Standby mode.	🔴 ○ Red

5.8 Changing the Facility Code

Note

- The default Facility code is 001.
- Facility codes can be in the range between 000 and 255.

To change the Facility code:

1. Enter Programming mode.	○ 🟢 Green
2. Press **4** to enter Menu 4.	4
The left LED turns red.	🔴 🟢 Red Green
3. Enter the new 3-digit code you wish to set as the Facility code.	? ? ?
You hear three beeps. The system returns to Standby mode.	🔴 ○ Red

5.9 Setting the Backlight Behavior

To set the backlight behavior:

1. Enter Programming mode.

   ○ 🟢 Green

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

   [6]

   The left LED turns red.

   🔴 🟢 Red Green

3. Enter one of the following codes:
   - **0** – Always off
   - **1** – Always on
   - **2** – Backlight is off, activates for 10 seconds when a key is pressed (left LED also goes on), after which it dims until off (left LED also goes off)
   - **3** – Backlight is dimmed, activates for 10 seconds when a key is pressed (left LED also goes on), after which it returns to a dimmed level

   You hear three beeps.

   The system returns to Standby mode.

   🔴 ○ Red

5.10 Return to Factory Default Settings

> **!** Caution
>
> You must be very careful before using this command! Doing so erases the entire memory that includes all user and special Codes, and returns all codes to their factory default settings.

To return to factory default settings:

1. Enter Programming mode.

   ○ 🟢 Green

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

   [0]

   Both LEDs flash red.

   🔴 🔴 Red 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 Standby mode.

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

5.11 Replacing a lost Programming Code

In the event that the Programming code is forgotten, the unit may 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.

6. Technical Specifications

Electrical Characteristics	
Input Voltage	5 to 16 VDC
Absolute Maximum Voltage (non-operating)	18 VDC
Input Current @ 12V	AY-Q6260: Standby: 110 mA, Maximum: 190 mA
	AY-Q6360: Standby: 160 mA, Maximum: 240 mA
LED/Buzzer Control Input	Dry Contact, N.O.
Tamper Output	Open collector, active low, 30 mA maximum sink current
Operational Characteristics	
Maximum Controller Cable Distance	150 m (500 ft) using 18 AWG cable
Proximity Read Range*	20 mm (0.8 in.)
Operating Frequency	13.56 MHz
Transfer Bit Rate	106 Kbits per second
Output Indicators	One tri-colored LED buzzer
Card Compatibility	MIFARE and all ISO14443A-3 cards
Card Transmit Formats	Programmable
Keypad Transmit Formats	AY-Q6260: None
	AY-Q6360: User programmable
Transmission Formats	Wiegand and Clock & Data

* Measured using a Rosslare proximity card or equivalent. Range also depends on electrical environment and proximity to metal

Environmental Characteristics	
Operating Temp. Range	-31°C to 63°C (-25°F to145°F)
Operating Humidity Range	0 to 95% (non-condensing)
Operating Environment	Suitable for outdoor use (IP65 compliant), water resistant
Physical Characteristics	
Height x Width x Depth	125 x 83 x 29.5 mm (4.9 x 3.3 x 1.2 in.)
Weight	480 g (1.1 lb)

A. 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.

AY-Q6x60 Series

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.
22 Ha'Melacha St., P.O.B. 11407
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
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

ROSSLARE
SECURITY PRODUCTS

TÜVRheinland CERT ISO 9001 ISO 14001 • EN ISO 13485 RoHS COMPLIANT CE