2012
March

AY-Q6x60 Family

Mifare® Anti-Vandal Smartcard Contactless Read-Sector Readers

Installation and Programming Manual

Models:

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 ENTERPRISES LIMITED and/or its related companies and/or subsidiaries' (hereafter: "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.
- 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 AY-Q6260 and AY-Q6360 are metallic, anti-vandal, contactless smartcard readers, used in access control system solutions.

The readers scan information from a Mifare® smartcard, stored in a specific and protected sector, and send the data on to a connected access control system.

1.1 Usability

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 state-of-the-art AC-115, AC-215, AC-225 and AC-525 controllers.

1.2 Main Features

The AY-Q6260 and AY-Q6360 are fully-featured metallic, anti-vandal smartcard proximity readers, ideal for all facility code applications in access control, intrusion, and time and attendance applications.

- Reads Mifare® ISO14443 Type A Standard cards with two operation modes: Secure mode or Card Serial Number (CSN) mode

- Pre-validation of smartcards by secure pass-code
- Configure readers directly and easily using Configuration and Master smartcards
- Suitable for indoor and outdoor use (fully-potted and IP65 compliant)
- Built-in anti-tampering security system
- Multiple, programmable card transmission formats
- Dedicated LED and buzzer control input
- 3x4 keypad for programming and PIN codes (AY-Q6360)
- Multiple keypad transmit formats (AY-Q6360)
- Programmable keypad backlight (AY-Q6360)

1.3 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)

2. Technical Specifications

Electrical Characteristics	AY-Q6260	AY-Q6360
Operating Voltage Range	5–16 VDC	
Absolute Maximum	18 VDC (non-operating)	
Input Current @ 12V	150 mA Maximum: 190 mA	200 mA Maximum: 240 mA
LED/Buzzer Control Input	Dry Contact, N.O.	
Tamper Output	Open collector, active low, 30 mA maximum sink current	

Environmental Characteristics	AY-Q6260	AY-Q6360
Operating Temp. Range	-25°F to145°F (-31°C to 63°C)	
Operating Humidity	0–95% (non-condensing)	
Operating Environment	Suitable for outdoor use (IP65 compliant) Water resistant	

Dimensions	AY-Q6260	AY-Q6360
Height x Width x Depth	4.92 x 3.27 x 1.16 inch (125 x 83 x 29.5 mm)	
Weight	1.08 lbs (480 g)	

Operational Characteristics	AY-Q6260	AY-Q6360
Maximum Cable Distance to Controller	500 feet (150 m) with 18 AWG cable	
Proximity Read Range	0.787 in. (20 mm)	
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	None	User programmable

3. Installation

The AY-Q6260 and AY-Q6360 packs include everything needed to install and operate the smartcard sector readers. Mount the reader on the required surface and connect it to the access control system.

3.1 Unpacking the Reader

Confirm receipt of all items listed below before installing. If any items are missing, contact your dealer immediately.

- One reader
- This manual
- Installation kit including:
  - One self-adhesive drilling template
  - One security spline key
  - One security hex key
  - Two mounting screws
  - Two wall plugs

3.2 Mounting the Reader

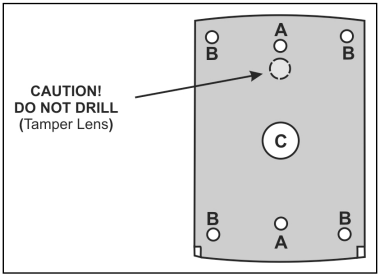
Attach the reader to a surface before connecting it to its power and the access control computer.

To mount the reader on a surface:

1. Remove the reader's front cover using the security spline key.

   The screw holes on the back plate are now visible.
2. Select an approximate location for the reader.
3. Peel off the back of the self-adhesive installation template and attach the template to the required location.
4. Using the template as a guide, drill four holes into the surface. The required hole size is marked on the template (Figure 1).

Figure 1: Back Plate



5. Drill an additional 7/16" (10 mm) hole for the cable.

   When installing the reader on a metallic surface, cover the inside of the hole with a grommet or electrical tape.
6. Route the reader's cable to the power and access control system.

   A regulated linear power supply is recommended.
7. Screw the back plate into the surface. Ensure the screws are the size specified on the installation template.
8. Alternatively, the reader can be mounted with any strong epoxy glue:
   a. Apply the glue.
   b. Hold the reader's back plate firmly in place until the glue dries.
9. Re-attach the reader's front cover.

3.3 Wiring Instructions

The AY-Q6260 and AY-Q6360 use an 18" pigtail controller cable, consisting of 10 wires, to connect to the access control system and for power.

Individual wires are color coded according to the Wiegand standard.

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

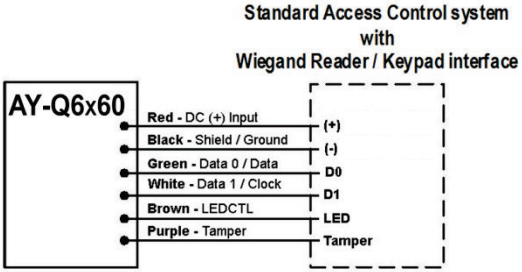
To connect the reader to the controller:

1. Remove 1¼" (32 mm) of the reader cable's insulation jacket.
2. Strip ½" (13 mm) of the insulation from the wires.
3. Splice the reader's pigtail wires to the corresponding input wires for the access control system, as listed in Table 1 and Figure 2.

Table 1: Wiring Colors

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

Figure 2: Connecting the Reader to an Access Control System



4. Cover the spliced joints with insulating tape and then trim and cover all unused connectors.

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

4. 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. Then, a Configuration card is 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 set up configuration cards.

4.1 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.

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.

4.2 Configuration Card Structure

Mifare® smartcards 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 smartcard.

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

4.3 Configuring Settings

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

4.4 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.

5. How to Use the Reader

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

5.1 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 4.4).

5.1.1 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.

5.1.2 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.

5.2 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.

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

5.3 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.

6. Keypad Operation Instructions (AY-Q6360)

6.1 Transmit Mode

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

When the reader is in Transmit Mode, the Transmit LED is red.

When a card or PIN entry is being transmitted, the Transmit LED flashes green.

Keyboard data can be sent via one of several different Keypad Transmission Formats. Refer to Section 6.5 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 6.7 for more information on selecting card transmission formats.

6.2 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.

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.

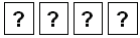
6.3 Entering Programming Mode

To enter Programming mode:

1. Press the # key 4 times.

   The Transmit LED turns off and the Program LED turns red.

2. Enter your Programming code.



3. If the Programming Code is valid, the program LED turns green and the AY-Q6360 enters Programming mode.

Note

- The factory default Programming Code is 1234.
- If a Programming code is not entered within 30 seconds, the AY-Q6360 returns to Transmit mode.

6.4 Exiting Programming Mode

To exit Programming mode:

1. Press the **#** key.

   You hear a long beep and the Transmit LED turns red.

   This indicates that the AY-Q6360 has returned to Transmit mode.

   While in Programming mode, if no key is pressed for 30 seconds, the AY-Q6360 exits Programming mode and returns to Transmit mode.

6.5 Selecting Keypad Transmission Format

The AY-Q6360 has eight different keypad transmission selectable formats (see Section 6.6 for more information).

To select the keypad transmission format:

1. Enter Programming mode.

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

   The Transmit LED turns red.

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

   Three 3 beeps are emitted on success.

   When selecting Option 8, the Program LED turns orange and awaits additional key input selecting the number of keys.

   The system returns to Transmit mode.

   You hear three beeps and the Transmit LED turns red.

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

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

6.6 Keypad Transmission Format Option Number

See Table 3 to determine the option number for the keypad transmission format you wish to select.

Table 3: Keypad Transmission Formats

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 in the following subsections.

6.6.1 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 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

6.6.2 Single Key, Wiegand 6-Bit, Nibble & 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

6.6.3 Single Key, Wiegand 8-Bit, Nibbles Complemented

This options inverts the most significant bits in the message leaving the least 4 significant bits as 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

6.6.4 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 6.10 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 the "*****" or the "**#**" 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 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

6.6.5 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 6.10 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, the "**#**" key 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 the "*****" key 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

6.6.6 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, (Pound **#**, and Asterisks ***** keys 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 D = Fourth key entered

B = Second key entered E = Fifth key entered

C = Third key entered F = Sixth key entered

6.6.7 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 the "*****" or the "**#**" 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 no number key or "**#**" 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 keypad PIN code.

6.6.8 Single Key, Wiegand 4-Bit

Each key press immediately sends 4 bits data, 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

6.7 Selecting Proximity Card Transmission Format

The AY-Q6360 has different selectable card transmission formats (see Section 6.8).

To select the proximity card transmission format:

1. Enter Programming mode.

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

   The Transmit LED turns red.

3. Enter the appropriate option number for the card transmission format you want.

   Three beeps are emitted on success.

   The system returns to Transmit mode. You hear three beeps and the Transmit LED turns red.

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

6.8 Card Transmission Format Option Number

Keypad Transmission Format	Option Number
Wiegand 26-Bit (default)	1
Clock & Data	2
Wiegand 26-Bit with facility code output	4
Wiegand 32-Bit	5
Wiegand 32-Bit reverse output	6
Wiegand 34-Bit	7
Wiegand 40-Bit	8

6.8.1 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.

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

6.8.2 Clock and Data

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

6.8.3 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.


Note

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

6.8.4 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 = 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

6.8.5 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

6.8.6 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

6.8.7 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)

6.9 Changing the Programming Code

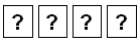
To change the Programming code:

1. Enter Programming mode.

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

The Transmit LED turns red.

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



The system returns to Transmit mode.
You hear three beeps and the Transmit LED turns red.

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

6.10 Changing the Facility Code

To change the Facility code:

1. Enter Programming mode.

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

The Transmit LED turns red.

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

The system returns to Transmit mode.

You hear three beeps and the Transmit LED turns red.

Note

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

6.11 Setting the Backlight

To set the backlight:

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

The system returns to Transmit mode.

You hear three beeps and the Transmit LED turns red.

6.12 Return to Factory Default Settings

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.

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

The Transmit and Program LEDs flash red.

3. Enter your 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 of the controller

6.13 Replacing a lost Programming Code

In the event that the Programming code is forgotten, the AY-Q6360 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**.

A. Limited Warranty

ROSSLARE'S FIVE-YEAR LIMITED WARRANTY is applicable worldwide. This warranty supersedes any other warranty. ROSSLARE'S FIVE-YEAR LIMITED WARRANTY is subject to the following conditions:

WARRANTY

Warranty of ROSSLARE'S products extends to the original purchaser (Customer) of the ROSSLARE product and is not transferable.

PRODUCTS COVERED BY THIS WARRANTY AND DURATION

ROSSLARE warrants the AY-Q6260 and AY-Q6360, Mifare® Proximity Readers to be free from defects in materials and assembly in the course of normal use and service. The warranty period commences with the date of shipment to the original purchaser and extends for a period of 5 years (60 months).

WARRANTY REMEDY COVERAGE

In the event of a breach of warranty, ROSSLARE will credit Customer with the price of the Product paid by Customer, provided that the warranty claim is delivered to ROSSLARE by the Customer during the warranty period in accordance with the terms of this warranty. Unless otherwise requested by a ROSSLARE representative, return of the failed product(s) is not immediately required.

If ROSSLARE has not contacted the Customer within a sixty (60) day holding period following the delivery of the warranty claim, Customer will not be required to return the failed product(s). All returned Product(s), as may be requested at ROSSLARE'S sole discretion, shall become the property of ROSSLARE.

To exercise the warranty, the user must contact ROSSLARE Enterprises Ltd. to obtain an RMA number after which, the product must be returned to the Manufacturer freight prepaid and insured.

In the event ROSSLARE chooses to perform a product evaluation within the sixty (60) day holding period and no defect is found, a minimum US$ 50.00 or equivalent charge will be applied to each Product for labor required in the evaluation.

ROSSLARE will repair or replace, at its discretion, any product that under normal conditions of use and service proves to be defective in material or workmanship. No charge will be applied for labor or parts with respect to defects covered by this warranty, provided that the work is done by ROSSLARE or a ROSSLARE authorized service center.

EXCLUSIONS AND LIMITATIONS

ROSSLARE shall not be responsible or liable for any damage or loss resulting from the operation or performance of any Product or any systems in which a Product is incorporated. This warranty shall not extend to any ancillary equipment not furnished by ROSSLARE, which is attached to or used in conjunction with a Product, nor to any Product that is used with any ancillary equipment, which is not furnished by ROSSLARE.

This warranty does not cover expenses incurred in the transportation, freight cost to the repair center, removal or reinstallation of the product, whether or not proven defective.

Specifically excluded from this warranty are any failures resulting from Customer's improper testing, operation, installation, or damage resulting from use of the Product in other than its normal and customary manner, or any maintenance, modification, alteration, or adjustment or any type of abuse, neglect, accident, misuse, improper operation, normal wear, defects or damage due to lightning or other electrical discharge. This warranty does not cover repair or replacement where normal use has exhausted the life of a part or instrument, or any modification or abuse of, or tampering with, the Product if Product disassembled or repaired in such a manner as to adversely affect performance or prevent adequate inspection and testing to verify any warranty claim.

ROSSLARE does not warrant the installation, maintenance, or service of the Product. Service life of the product is dependent upon the care it receives and the conditions under which it has to operate.

In no event shall ROSSLARE be liable for incidental or consequential damages.

LIMITED WARRANTY TERMS

This warranty sets forth the full extent of ROSSLARE'S warranty.

The terms of this warranty may not be varied by any person, whether or not purporting to represent or act on behalf of ROSSLARE.

This limited warranty is provided in lieu of all other warranties. All other warranties expressed or implied, including without limitation, implied warranties of merchantability and fitness for a particular purpose, are specifically excluded.

In no event shall ROSSLARE be liable for damages in excess of the purchase price of the product, or for any other incidental, consequential or special damages, including but not limited to loss of use, loss of time, commercial loss, inconvenience, and loss of profits, arising out of the installation, use, or inability to use such product, to the fullest extent that any such loss or damage may be disclaimed by law.

This warranty shall become null and void in the event of a violation of the provisions of this limited warranty.

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
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

ROSSLARE
SECURITY PRODUCTS
www.rosslaresecurity.com

0706-0960335+02