

CP-R26 and AS-B01

**MIFARE Card Programmer/Full
Fingerprint Enrollment Station**
Hardware and Software Manual



ROSSLARE
SECURITY PRODUCTS

Copyright © 2013 by Rosslare. All rights reserved.

This manual and the information contained herein are proprietary to ROSSLARE ENTERPRISES LIMITED and/or its related companies and/or subsidiaries' (hereafter: "ROSSLARE"). Only ROSSLARE and its customers have the right to use the information.

No part of this manual may be re-produced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of ROSSLARE.

ROSSLARE owns patents and patent applications, trademarks, copyrights, or other intellectual property rights covering the subject matter in this manual.

TEXTS, IMAGES, AND ILLUSTRATIONS INCLUDING THEIR ARRANGEMENT IN THIS DOCUMENT ARE SUBJECT TO THE PROTECTION OF COPYRIGHT LAWS AND OTHER LEGAL RIGHTS WORLDWIDE. THEIR USE, REPRODUCTION, AND TRANSMITTAL TO THIRD PARTIES WITHOUT EXPRESS WRITTEN PERMISSION MAY RESULT IN LEGAL PROCEEDINGS.

The furnishing of this manual to any party does not give that party or any third party any license to these patents, trademarks, copyrights or other intellectual property rights, except as expressly provided in any written agreement of ROSSLARE.

ROSSLARE reserves the right to revise and change this document at any time, without being obliged to announce such revisions or changes beforehand or after the fact.

Table of Contents

- 1. Introduction..... 8**
 - 1.1 The CP-R26 System..... 8
 - 1.2 Desktop Convenience 8
 - 1.3 Intuitive Software System..... 8
 - 1.4 Compatibility..... 9
 - 1.5 CP-R26 Desktop Programmer..... 9
 - 1.6 AS-B01 Software 9
- 2. Specifications and Requirements..... 10**
 - 2.1 CP-R26 Hardware Specifications 10
 - 2.2 AS-B01 Software Requirements 10
- 3. Installation 11**
 - 3.1 Unpacking the Equipment..... 11
 - 3.2 CP-R26 Description..... 11
 - 3.3 AS-B01 Software Installation..... 12
 - 3.4 CP-R26 Hardware Installation..... 15
- 4. AS-B01 Software Overview and LEDs 17**
 - 4.1 Software Overview 17
 - 4.2 Indication LEDs 18
- 5. Programming Cards and Tags..... 20**
 - 5.1 Programming a Master Card 22
 - 5.2 Programming Configuration Cards..... 22
 - 5.2.1 Sector Reader Configuration Cards 23
 - 5.2.2 Full Finger Capacitive Reader Configuration Cards 24
 - 5.3 Programming User Cards or Tags..... 26
 - 5.3.1 Programming a Sector Reader User Card..... 26
 - 5.3.2 Programming and Enrolling Fingerprint User Card for MOC Reader Type 27
 - 5.3.3 Programming and Enrolling User Card for 1:1 and 1:N Reader Types 30

Table of Contents

5.3.4	Programming Auxiliary Card for 1:1 and 1:N Readers.....	31
6.	Additional Programmer Utilities.....	32
6.1	Card Utilities.....	32
6.1.1	Reading a Configuration Card.....	32
6.1.2	Reading an ID from a User Card.....	33
6.1.3	Programming a User Card ID.....	33
6.1.4	Changing the User Card KeyA in a Specific Sector	34
6.1.5	Changing the User Card KeyA in All Sectors.....	35
6.1.6	Erasing Specific User Card Data.....	36
6.1.7	Read Serial Number and Card Type	37
6.1.8	Changing KeyA and Erasing All Data.....	37
6.2	Fingerprint Utilities.....	39
6.2.1	Enrolling Fingerprints on a Pre-configured User Card	39
6.2.2	Verifying Fingerprint Enrollment on a User Card.....	40
7.	Global Options	41
7.1	Change Password.....	41
7.2	Card Overwrite	42
7.3	Updating Firmware	42
A.	Maintenance	44
B.	Field Descriptions	45
C.	Additional MIFARE Card Memory Map Information... ..	47
C.1	Manufacture Block	47
C.2	Data Blocks.....	47
D.	Sample Worksheets	49
E.	Limited Warranty	50

List of Figures

Figure 1: CP-R26 Description	11
Figure 2: Configuration Tab Area	20
Figure 3: CP-R26 Antenna Areas	21
Figure 4: MIFARE 1K Memory Diagram	48

List of Tables

Table 1: Indication LEDs.....	18
Table 2: Field Descriptions	45

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

Rosslare's CP-R26 is a desktop MIFARE® and full finger capacitive fingerprint card programmer for MIFARE 1K and 4K RFID proximity cards and tags.

The CP-R26 makes managing fingerprint and MIFARE cards easier and can help facilitate the effective deployment and control of any facility code application, including access control, intrusion, and time and attendance applications.

1.1 The CP-R26 System

The CP-R26 is built for high-security, portability and ease of use, enabling high quality MIFARE and fingerprint enrollment at a low cost.

The CP-R26 programmer is controlled by computer using Rosslare's powerful AS-B01 Programmer software package.

1.2 Desktop Convenience

The CP-R26 is small and lightweight, with a slim and attractive design. It is built for convenience and portability, with a USB 2.0 computer interface that makes it quick to install and allows it to run without any additional power source.

Designed to sit safely on any desktop, the CP-R26 is sturdily built, with large card and fingerprint trays and surface-gripping rubber feet.

1.3 Intuitive Software System

AS-B01 is a software application intended for programming MIFARE cards, tags, and fingerprints using Rosslare's CP-R26 Desktop Programmer.

The system includes a security authentication system and a real-time operations log.

Using this tool requires basic understanding of MIFARE cards memory architecture and access condition mechanisms.

The software does not support all MIFARE card features required by the systems using the CP-R26 programmed MIFARE cards.

1.4 Compatibility

The CP-R26 Desktop Programmer and AS-B01 software is compatible with other products, including but not limited to:

- AY-W6260 and AY-W6360 MIFARE Contactless Smart Card Sector Readers Family
- AY-Q6260 and AY-Q6360 Anti-Vandal MIFARE Contactless Smart Card Sector Readers Family
- AY-Bx660 (x=1,2) MIFARE Smart Card Full Finger Capacitive Sensor Reader Family
- AY-B7661– MIFARE Smart Card Full Finger Capacitive Sensor Reader

1.5 CP-R26 Desktop Programmer

- Enables the user to read, verify and program MIFARE proximity cards
- Uses a capacitive type fingerprint sensor
- Supports USB 2.0 computer connections
- Utilizes LED and buzzer sub-systems to indicate programming, card and power supply status
- Runs a thorough internal diagnostic self-test every time it is powered up

1.6 AS-B01 Software

- Programs fingerprints on Users cards
- Programs ID data on Users cards
- Produces configuration cards for Rosslare MIFARE readers
- Performs firmware updates on supported desktop programmers
- Maintains a user log to provide feedback to the software user
- Provides password protection
- Indicates valid connections with Desktop Programmer

2. Specifications and Requirements

2.1 CP-R26 Hardware Specifications

Data Specifications	
Cards	MIFARE Classic 1K and 4K
RF Frequency	13.56 MHz
Bit Rate	106 KHz
Fingerprint Reader Specifications	
Sensor Type	capacitive type TCS2
Sensor ESD Rating	Sensor technology – Capacitive sensor
Electrostatic Discharge	Up to +/- 15 kV air discharge on the sensor surface
Electrical Specifications	
Operating Voltage	5 VDC Via USB
Input Current	Standby – 155 mA Maximum – 230 mA
CP-R26 Physical Specifications	
Dimensions (L x W x H)	17.3 x 5.8 x 3.3 cm (6.18 x 2.28 x 1.30 in.)
Weight	309 g (10.89 oz.)
Environmental Data	
Operating Temperature Range	10°C to 50°C (50°F to 122°F)
Operating Humidity Range	5% to 93% (non-condensing)

2.2 AS-B01 Software Requirements

Minimum Software Requirements	
Operating System	Windows XP SP2
Framework	Microsoft .NET 2
Processor	400 MHz Pentium or equivalent
RAM Memory	512 Mbytes
Free HD Space	1 Gigabyte
Connection Port	USB

3. Installation

3.1 Unpacking the Equipment

The CP-R26 programmer is ready to use immediately "out of the box" and includes a USB cable and documentation.

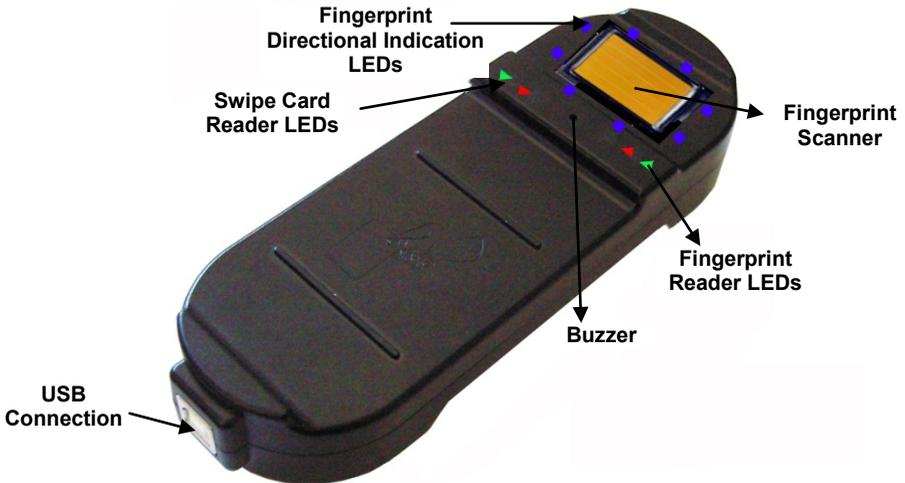
Please confirm all the items listed below are received before beginning. If any items are missing, contact your dealer immediately.

- One CP-R26 Programmer
- One Male A to Male B USB Cable
- One software CD
- Instruction Manual

3.2 CP-R26 Description

The following figure illustrates the CP-R26 components:

Figure 1: CP-R26 Description



Installation

3.3 AS-B01 Software Installation

The AS-B01 software is included on the installation CD-ROM, which is packaged with the CP-R26 hardware.

To install the AS-B01 software for the first time:

1. Insert the CD into the computer's CD drive.
2. If the Autoloader does not initiate the installation, open My Computer, double-click on the CD drive icon and then double-click the AS-B01 setup file.

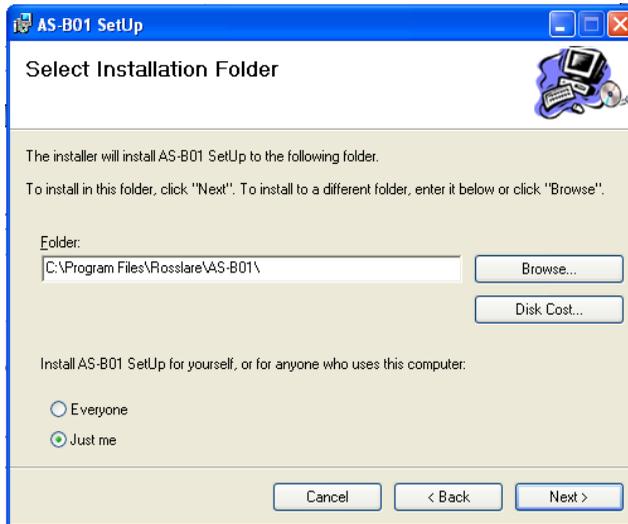


If Microsoft .NET 2 Framework is not installed on the computer, it is installed automatically before beginning the AS-B01 installation.

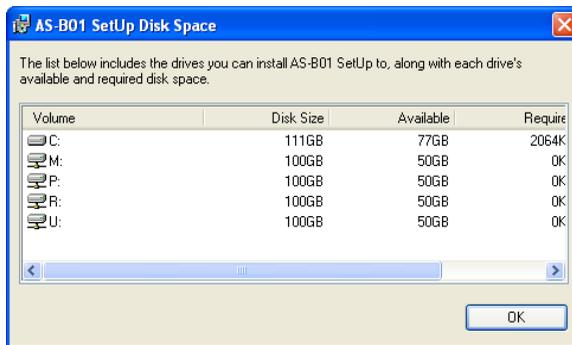
The installation package extracts the installation files. After the files are extracted the *Welcome to the AS-B01 Setup Wizard* window opens.



3. Click **Next**.
The *Select Installation Folder* window opens.



4. [Optional]Click **Disk Cost....** to ensure the computer has sufficient space.
The *AS-B01 Setup Disk Space* window opens.



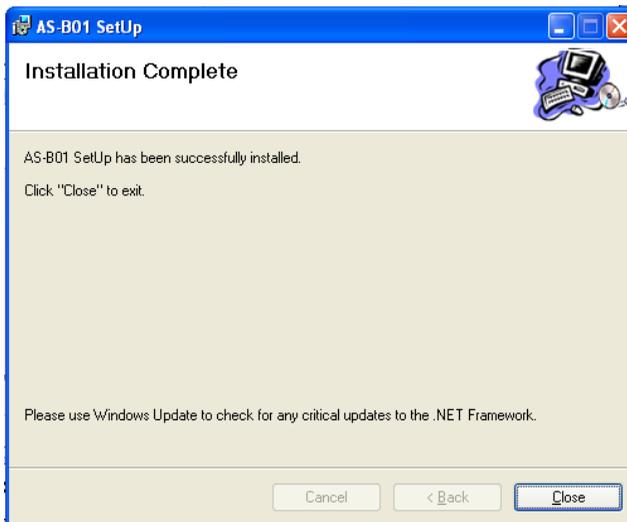
5. Select the users allowed to use the program, **Everyone** or **Just me**.
For security purposes it is suggested that **Just me** is selected.
6. [Optional] You can change the destination folder of the installation:
 - a. Click **Browse**.
The standard Windows Explorer window opens.
 - b. Navigate to and select the required folder.

Installation

- Click **Next** to continue the installation process.
The *Confirm Installation* window opens.



- Click **Next**.
The installation process is initiated. When the process finishes, the *Installation Complete* window opens.



- Click **Close** to complete the installation process.

3.4 CP-R26 Hardware Installation

Before connecting the CP-R26 hardware, check that the ASB01 software is installed and running.

To connect the CP-R26:

1. Click the AS-B01 icon on the desktop or select the program from the Rosslare folder in the **Start** menu. The login dialog opens.

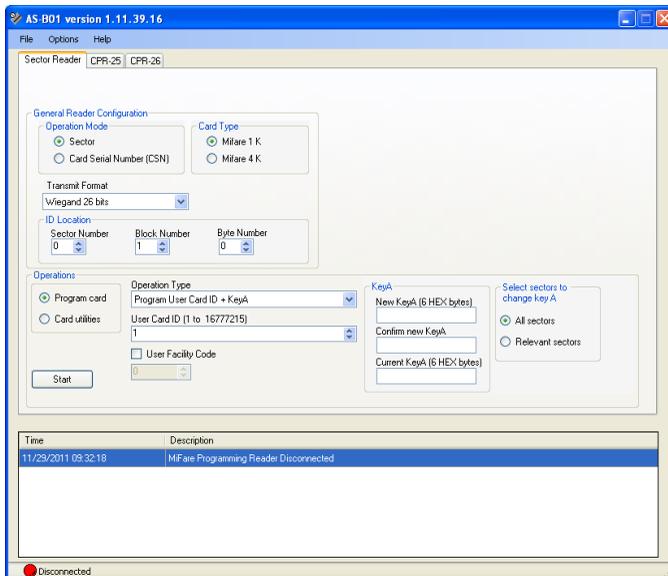


2. Enter a password.
When using the application for the first time, use the default password of "admin".



Note After initial use, make sure to change the default password to your company's approved password (see Section 7.1).

The AS-B01 software Main window opens.



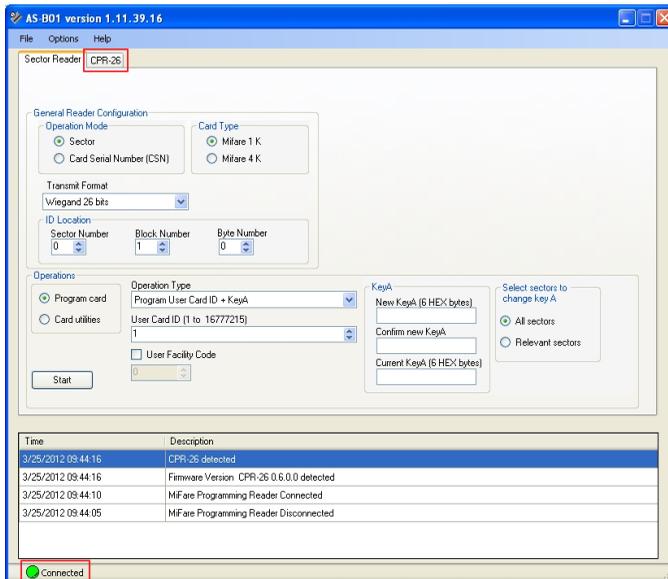
At the bottom left of the Main window the connection indication is red with the description "**Disconnected**".

Installation

3. Connect the Desktop Programmer to a PC using the USB cable – one cable end connects to the PC USB host port output and the other end connects to the USB connector on the Desktop Programmer.

Windows[®] automatically installs the required drivers. The Desktop Programmer receives its power through the USB; no external power supply is required.

On the AS-B01 main window, the connection indicator at the bottom of the window changes from red to green with the description “**Connected**” to indicate that the CP-R26 Desktop Programmer is connected. In addition, the CPR-25 tab that was previously visible closes, leaving only the CPR-26 tab visible.



The event log displays a connected message.

If the indicator does not turn green, and the description still indicates **Disconnected** after the USB cable is connected, try disconnecting the USB cable from the Desktop Programmer and reconnecting it.

When the hardware and software are disconnected, the software can only function in demonstration mode.

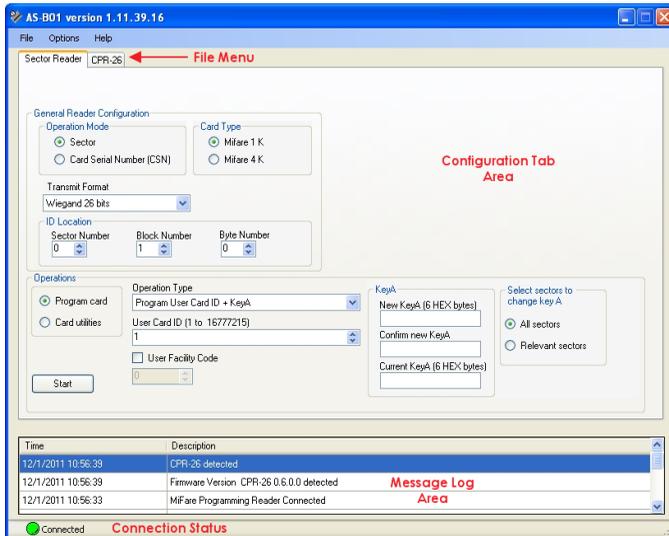
Once the indicator is green and the description is **Connected**, the CP-R26 Desktop Programmer is ready for use.

4. AS-B01 Software Overview and LEDs

This section describes the AS-B01 and CP-R26 LEDs.

4.1 Software Overview

Once the log-in is completed with the correct password, the main software window opens.



The AS-B01 main window consists of the following functional areas:

- File menu area – Used for general operations such as setting global options on the Desktop Programmer, getting version information, and closing the software.
- Configuration Tab area – The main working area, which is used for entering and displaying all card and swipe configuration parameters.



Note Descriptions for fields requiring parameters under all the tabs are described in Appendix B.

AS-B01 Software Overview and LEDs

There are two programming tabs:

- Sector reader – Used to configure and read sector reader cards. This tab allows configuring both User ID/Card Serial number user cards as well as Reader Configuration cards.
- Swipe reader – Used to write and read cards containing fingerprint templates. This tab also allows creating configuration cards for fingerprint readers.
- Message log area – The event log records all activities and provides the user with real time system monitoring. The information messages may either be operation success or failure messages, or instruction messages such as during fingerprint enrollment.
- Status information area – Indicates connection status with the CP-R26 Desktop Programmer hardware.

4.2 Indication LEDs

Table 1 describes LED behavior on the CP-R26 Programmer (see Figure 1).

Table 1: Indication LEDs

Event	Swipe Card Reader LED	Fingerprint Reader LED	Buzzer	Fingerprint Directional Indication LED
General				
Power on	One red LED lights for several seconds followed by all the LEDs flashing and the buzzer beeps 3 times for the duration of 3 seconds.			
Card Programming				
Card not loaded	Green flashing	All off	Off	All on
Card loaded	On card detection green turns on for 1 second, then off	All off	On card detection short beep, then off	All on
Write card success	Green on for 3 sec	Green on for 3 sec	3 High tone beeps	All on
Write card fail	Red on for 3 seconds	All off	Long buzz	All on

Event	Swipe Card Reader LED	Fingerprint Reader LED	Buzzer	Fingerprint Directional Indication LED
Fingerprint Scanning-Match On Card Mode				
Waiting for fingerprint	Off	Green flashing	Off	Rolling LEDs in circular mode to indicate finger swipe
Read fingerprint success	Off	Green on for 3 sec	3 High tone beeps	Rolling LEDs in circular mode to indicate finger swipe
Read fingerprint fail	Off	Red on for 3 sec	Long buzz	Turning all LEDs on, and then according to status, leaving all on or going back to circular mode

Read finger timeout – When no finger is passed over the scanner for 25 seconds, the CP-R26 Desktop Programmer goes back to Standby mode of swipe LEDs.

5. Programming Cards and Tags

To configure the MIFARE cards and tags, the Configuration Tab area of the Main Window is used.

Within the Configuration Tab Area, there are three sub-areas whose display changes depending on what options are selected.

Two of the sub-areas always appear:

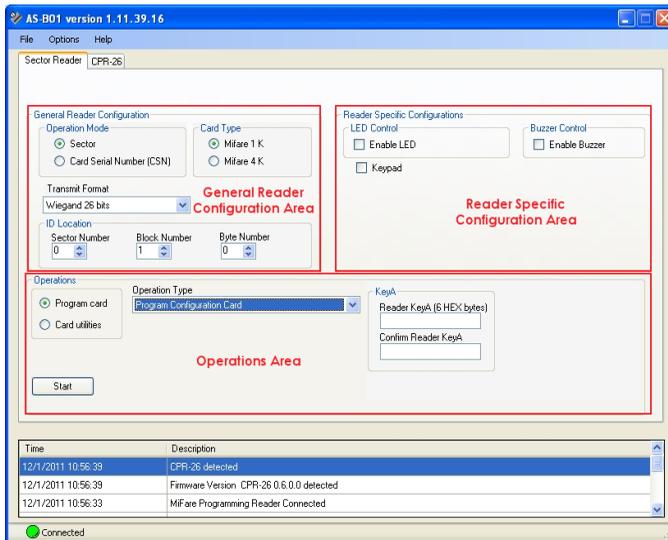
- General Reader Configuration area – This area is the same for all configuration functions
- Operations area – This area varies according to the configuration function being performed. The configuration function is selected in the Operation Type dropdown menu.

The following two sub-areas appear depending on what options are selected in *Operation Mode* and *Operation Type*.

- *Reader Specific Configurations* area – This area is visible when the Sector Reader tab is active and **Program Configuration Card** is selected in *Operation Type*.
- *Finger options* – This area is visible when the CPR-26 tab is active and *Operation Type* is **Program User Card KeyA + template**.

Figure 2 illustrates one of the possible appearances of the Configuration Tab area.

Figure 2: Configuration Tab Area



When programming a MIFARE card or tag, the card or tag is placed on the CP-R26 Desktop Programmer antenna area. Figure 3 illustrates where these areas are located on the CP-R26 Desktop Programmer.

Figure 3: CP-R26 Antenna Areas



The CP-R26 Programmer configures four card or tags types. The four card types are:

- Configuration card – This card is used to configure a reader upon power up during the initial setup. The Configuration card is simply held up against a reader to automatically program the reader with the relevant security information thus allowing the reader to identify the user cards or tags.
- Master card – This card is used to put the reader into Configuration mode so that a Configuration card can then be used to program the reader.
- User card – MOC and 1:1 (One-to-One) modes – This is used to enable access by presenting the card or tag to the reader. With readers requiring fingerprint identification the same card or tag is used in conjunction with swiping of the fingertip.
- Program Auxiliary cards – This is used when using 1:1 and 1:N (One-to-Many) readers to define to which sector record the reader writes the template to or deletes from.

Programming Cards and Tags

5.1 Programming a Master Card

The Master card is used to put the reader into Configuration mode in which a Configuration card is then used to program the reader.

To prepare a Master card:

1. Select either the **Sector Reader** or **CP-R26** tab.
2. In *Operation Type* in the Operations area, select **Create Master Card**.



Note

The Operation Mode field is not relevant for configuring Master card. The default value of Sector can be used.

3. In *Card Type*, select either **MIFARE 1 K** or **MIFARE 4 K**.
4. From the *Transmit Format* dropdown menu, select the applicable transmission format.
5. Place a blank MIFARE card or a card previously configured as a Configuration card on the CP-R26 Desktop Programmer antenna area.
6. Click **Start** to begin programming the MIFARE card.

On completion, a message is displayed in the Message Log area to verify that the programming succeeded.

If the programming is a failure there is a short buzz and the Swipe Card Reader LEDs light red for three seconds.

5.2 Programming Configuration Cards

A Configuration card is used for configuring specific Rosslare MIFARE and Fingerprint reader's operation modes. Holding the Configuration card in front of the reader after presenting the Master card configures that reader. The organization's Configuration card should be kept in a safe place to avoid being copied by unauthorized persons as it stores the organization/site KeyA. It is advisable to create a backup Configuration card and store it in a safe place.

Preparing a sector reader Configuration card requires a KeyA value. Do not expose the KeyA value to any unauthorized personnel while preparing the Configuration card.



Note

Refer to the specific readers' installation manual for a detailed explanation of the various options.

5.2.1 Sector Reader Configuration Cards

A Sector Reader Configuration card allows you to create a configuration card, which is used to configure the various sector readers such as the AY-W6260, AY-W6360, AY-Q6260, and AY-Q6360 units.

To prepare a Sector Reader Configuration card:

1. Select the **Sector Reader** tab.
2. Select the applicable *Operation Mode*, either **Sector** or **Card Serial Number (CSN)**.
3. From the *Operation Type* dropdown menu, select **Program Configuration Card**.
4. In *Card Type*, select either **MIFARE 1 K** or **MIFARE 4 K**.
5. From the *Transmit Format* dropdown menu, select the applicable transmission format.
6. For **Sector** operation mode, select values for the **Sector Number**, **Block Number**, and **Byte Number** fields in *ID Location*.
7. Ensure that *Operations* is set to **Program Card**.
8. Define the *Led and Buzzer Control* behavior by selecting or clearing the **Enable Led** and **Enable Buzzer** checkboxes.
9. For readers with a keypad:
 - a. Select the **Keypad** checkbox.
Additional keypad options appear.
 - b. In the **Backlight options** dropdown menu, select the backlight behavior.
 - c. From the **Transmit Format** dropdown menu, set the keypads' transmission format.
10. For **Sector** mode, enter the KeyA to be used by the reader as the unique KeyA for the organization or site in both the **Reader KeyA** and the **Confirm Reader KeyA** fields.



Note

The KeyA number is hidden by "*" characters, so write down the new key and keep it in a safe place to avoid exposing this secret key to unauthorized personnel. The KeyA value is entered as a 6 hexadecimal digit. The default KeyA is FFFFFFFF.

11. Place a blank MIFARE card or a card previously configured as a Configuration card on the CP-R26 Desktop Programmer antenna area.
12. Click **Start** to begin programming the MIFARE card.
On completion, a message appears in the Message Log area to verify that the programming succeeded.
If the programming fails, there is a short buzz and the Swipe Card Reader LEDs light red for three seconds.

Programming Cards and Tags

5.2.2 Full Finger Capacitive Reader Configuration Cards

The Full Finger Capacitive Reader Configuration card allows you to create a configuration card, which is used to configure the various full finger capacitive readers.

5.2.2.1 MOC Reader Modes

To prepare a Biometric Capacitive Configuration card in MOC Mode:

1. Select the **CPR-26** tab.
2. In *Reader Mode*, select **Match on card**.
3. In *Operation Mode*, select either **Sector** or **Card Serial Number (CSN)**.
4. In *Card Type*, select either **MIFARE 1 K** or **MIFARE 4 K**.
5. From the *Transmit Format* dropdown menu, select the applicable transmission format.
6. For **Sector** operation mode, define the *ID Location* using the **Sector Number**, **Block Number**, and **Byte Number** fields.
7. From the *Operation Type* dropdown menu, select **Program Configuration Card**.
8. Ensure that *Operations* is set to **Program Card**.
9. Define the *Led and Buzzer Control* behavior by selecting or clearing the **Enable Led** and **Enable Buzzer** checkboxes.
10. For reports on operational failures, select the **Failed operation reporting** checkbox.
11. To enable the *Lockout* feature:
 - a. Select the **Enable** checkbox.
 - b. Define the lockout behavior using the **Attempts** and **Duration** fields.
12. In *KeyA*, enter the KeyA to be used by the reader as the unique KeyA for the organization or site in both the **Reader KeyA** and the **Confirm Reader KeyA** fields.



The KeyA number is hidden by "*" characters, so write down the new key and keep it in a safe place to avoid exposing this secret key to unauthorized personnel. The KeyA value is entered as a 6 hexadecimal digit. The default KeyA is FFFFFFFF.

13. Place a blank MIFARE card or a card previously configured as a Configuration card on the CP-R26 Desktop Programmer antenna area.
14. Click **Start** to begin programming the MIFARE card.

On completion, a message appears in the Message Log area to verify that the programming succeeded.

If the programming fails, there is a short buzz and the swipe Card Reader LEDs light red for three seconds.

5.2.2.2 1:1 and 1:N Reader Modes

To prepare a Biometric Capacitive Configuration Card in 1:1 and 1:N Modes:

1. Select the **CPR-26** tab.
2. In *Reader Mode*, select **One to one (1:1)** or **One to many (1:N)**.
3. In *Operation Mode*, select either **Sector** or **Card Serial Number (CSN)**.
4. In *Card Type*, select either **MIFARE 1 K** or **MIFARE 4 K**.
5. From the *Transmit Format* dropdown menu, select the applicable transmission format.
6. For **Sector** operation mode, define the *ID Location* using the **Sector Number**, **Block Number**, and **Byte Number** fields.
7. From the *Operation Type* dropdown menu, select **Program Configuration Card**.
8. Ensure that *Operations* is set to **Program Card**.
9. In *Type*, choose either **Reader** or **Controller**.

If you choose **Reader**, the following parameters are available for configuration:

The screenshot shows a configuration window for a Reader. At the top, the 'Type' dropdown menu is set to 'Reader'. Below this, there are four checkboxes arranged in two rows: 'Enable LED', 'Enable Buzzer', 'Failed operation reporting', and 'Restore to factory default'. All checkboxes are currently unchecked.

If you choose **Controller**, the following parameters are available for configuration:

The screenshot shows a configuration window for a Controller. The 'Type' dropdown is set to 'Controller'. The 'Lock open time' is set to 4 seconds. The 'Enable Aux Input' checkbox is checked. The 'Restore to factory default' checkbox is unchecked. Under the 'Aux Output' section, the 'Time' radio button is selected and set to 1 second, while the 'Toggle' radio button is unselected. The 'Bell' checkbox is checked.

10. Configure the relevant parameters as necessary.
11. To enable the *Lockout* feature:
 - a. Select the **Enable** checkbox.
 - b. Define the lockout behavior using the **Attempts** and **Duration** fields.
12. In *KeyA*, enter the KeyA to be used by the reader as the unique KeyA for the organization or site in both the **Reader KeyA** and the **Confirm Reader KeyA** fields.

Programming Cards and Tags



The KeyA number is hidden by "*" characters, so write down the new key and keep it in a safe place to avoid exposing this secret key to unauthorized personnel. The KeyA value is entered as a 6 hexadecimal digit. The default KeyA is FFFFFFFF.

13. Place a blank MIFARE card or a card previously configured as a Configuration card on the CP-R26 Desktop Programmer antenna area.
14. Click **Start** to begin programming the MIFARE card.
On completion, a message appears in the Message Log area to verify that the programming succeeded.
If the programming fails, there is a short buzz and the swipe Card Reader LEDs light red for three seconds.

5.3 Programming User Cards or Tags

In this section both cards and tags are referred to as cards. The card configuration type depends on what level of system security is implemented. The cards configuration depends on the reader type used. There are two reader types that determine what tab to use when configuring the cards.

- Sector reader – Used to configure and read sector reader cards. This tab allows configuration of both User ID/Card Serial number user cards as well as Reader configuration cards.
- Capacitive reader – Used to write and read cards containing fingerprint templates. The *CP-R26* tab also allows the creation of configuration cards for fingerprint readers.

The AS-B01 application offers various configuration options including the following:

- For a new MIFARE User card, configuring the Card ID, card key and fingerprint enrollment separately.
- For a previously configured MIFARE User card, configuring the Card ID and card key at the same time.
- For a previously configured MIFARE User card, configuring the Card ID, card key, and fingerprint enrollment at the same time.
- Configuring auxiliary cards that define the enrollment or deletion order of the template record, which is stored in the AYC-B7661 standalone reader.

Once a card is configured, the Card ID and the KeyA value can be modified, or if required, completely wiped from the card.

5.3.1 Programming a Sector Reader User Card

The first stage of preparing a MIFARE sector read User card is configuring a card ID and card KeyA value. These two configuration values are done simultaneously.

To program a MIFARE Sector Read User card:

1. Select the **Sector Reader** tab.
2. In *Operation Mode*, select the **Sector**.

Programming Cards and Tags

3. In *Card Type*, select either **MIFARE 1 K** or **MIFARE 4 K**.
4. From the *Transmit Format* dropdown menu, select the applicable transmission format.
5. In *ID Location*, select values for the **Sector Number**, **Block Number**, and **Byte Number** fields.



Note

If the Card Serial Number operation mode is being used by the organization, no programming is available for the user card.

6. Ensure that the *Operations* is set to **Program Card**.
7. From the *Operation Type* dropdown menu, select **Program User Card ID + KeyA**.
8. Enter the **User Card ID** number or scroll to a value using the Up and Down arrows.

The range of possible values is shown just above the *User Card ID* field.

9. In *KeyA*:
 - a. Enter the KeyA to be used by the reader as the unique KeyA for the organization or site in both the **Reader KeyA** and the **Confirm Reader KeyA** fields.
 - b. Enter the current KeyA of the card being programmed.



Note

- The KeyA number is hidden by "*" characters, so write down the new key and keep it in a safe place to avoid exposing this secret key to unauthorized personnel. The KeyA value is entered as a 6 hexadecimal digit. The default KeyA is FFFFFFFF.
- The current KeyA during a new installation is the default KeyA FFFFFFFF. For existing sites, the current KeyA is the KeyA entered the original site installation. The current KeyA remains active until it is changed after configuring the reader.

10. Place a MIFARE card on the CP-R26 Desktop Programmer antenna area.
11. Click **Start** to begin programming the MIFARE card.
On completion, a message appears in the Message Log area to verify that the programming succeeded.
If the programming fails, there is a short buzz and the swipe Card Reader LEDs lights red for three seconds.
12. To program additional MIFARE User cards, repeat Step 8 and then Steps 10 and 11.

5.3.2 Programming and Enrolling Fingerprint User Card for MOC Reader Type

Before enrolling a card user's fingerprint, the card must have a configured card ID and KeyA value.

Programming Cards and Tags

There are two options for enrolling fingerprints on a MIFARE User card. Either one or two fingerprints can be programmed on the card. The number of fingerprints is defined by the company security specifications and the card type used.



Mifare 1K cards can only hold one fingerprint, while Mifare 4K cards can hold up to two fingerprints.

Note

To enroll MOC fingerprints on a MIFARE User card:

1. Select the **CP-R26** tab.
2. From the *Reader Mode* section, select **Match on card**.
3. Select the applicable *Operation Mode*, either **Sector** or **Card Serial Number (CSN)**.
4. In *Card Type*, select either **MIFARE 1 K** or **MIFARE 4 K**.
5. From the *Transmit Format* dropdown menu, select the applicable transmission format.
6. For **Sector** operation mode, select values for the **Sector Number**, **Block Number**, and **Byte Number** fields in *ID Location*.
7. Ensure that the *Operations* is set to **Program Card**.
8. From the *Operation Type* dropdown menu:
 - a. If *Operation type* is Sector, select **Program User Card ID + KeyA + template**.
 - b. If *Operation type* is **Card Serial Number (CSN)**, select **Program User Card KeyA + template**.
9. For **Sector** *Operation Mode*, enter the **User Card ID** number or scroll to a value using the Up and Down arrows.

The range of possible values is shown just above the *User Card ID* field.
10. In *KeyA*:
 - a. Enter the KeyA to be used by the reader as the unique KeyA for the organization or site in both the **Reader KeyA** and the **Confirm Reader KeyA** fields.
 - b. Enter the current KeyA of the card being programmed.



Note

- The KeyA number is hidden by "*" characters, so write down the new key and keep it in a safe place to avoid exposing this secret key to unauthorized personnel. The KeyA value is entered as a 6 hexadecimal digit. The default KeyA is FFFFFFFF.
- The current KeyA during a new installation is the default KeyA FFFFFFFF. For existing sites, the current KeyA is the KeyA entered the original site installation. The current KeyA remains active until it is changed after configuring the reader.

11. In *Fingers options*, select the number of fingers per card to enroll onto the MIFARE User card.



Note

Dual fingerprint is only available with 4K MIFARE cards; the system does not allow enrollment of dual fingerprint when using 1K cards.

12. [Optional] Select the **Verify after enrollment** checkbox to verify the enrolled fingerprints if required. This is usually not required as the CP-R26 Desktop Programmer has an automatic internal verification during enrollment.
13. If needed, select the **Ignore Template** checkbox for a cardholder who is unable to present a finger for verification.

Note that when this option is selected, the parameters in *Finger options* in Step 11 are grayed out.

14. Select the **User Facility Code** checkbox to set a single facility code to all enrolled cards and then change only number of the **User Card ID**.
15. Place a MIFARE card on the CP-R26 Desktop Programmer antenna area.
16. Click **Start** to begin programming the MIFARE card.
17. Instruct the person whose fingerprints are being enrolled to place his/her finger on the finger sensor, located on the CP-R26 Desktop Programmer.
18. Follow the instructions messages in the Message Log area to repeat the fingerprint placement twice.

If enabled in the system settings (see Section 7.2), the system alerts if the card being programmed is not empty. The "The Card is not empty. Do you want to overwrite it?" prompt message is displayed. "Choose **Continue** or **Cancel**."

On successful completion of all three reads and card programming, 3 short beeps are generated and a success message "Writing template to card succeeded" is displayed in the Message Log area.

If the programming fails, there is a short buzz and the Capacitive Card Reader LEDs light red for three seconds.

The software initiates the enrollment process up to three times automatically and performs a verification process as well.

19. To program and enroll additional user cards, repeat Steps 15 to 18.



Note

To write the finger template onto a specific card sector, define the sector number by typing or selecting the number in the **Sector Number** field located in the finger options section of the screen

Programming Cards and Tags

5.3.3 Programming and Enrolling User Card for 1:1 and 1:N Reader Types

With this option, the reader is used to add a user card that points to the specific fingerprint record where the template is stored for the benefit of responsiveness.

To enroll fingerprints on a MIFARE User card:

1. Select the **CP-R26** tab.
2. From the *Reader Mode* section, select **One to one(1:1) or One to many(1:N)**.
3. In *Operation Mode*, select **Sector**.
4. In *Card Type*, select either **MIFARE 1 K** or **MIFARE 4 K**.
5. From the *Transmit Format* dropdown menu, select the applicable transmission format.
6. For **Sector** operation mode, select values for the **Sector Number**, **Block Number**, and **Byte Number** fields in *ID Location*.
7. Ensure that the *Operations* is set to **Program Card**.
8. From the *Operation Type* dropdown menu, select **Program User Card ID + KeyA**.
9. Enter the **User Card ID** or scroll using the Up and Down arrows.
10. In *KeyA*:
 - a. Enter the KeyA to be used by the reader as the unique KeyA for the organization or site in both the **Reader KeyA** and the **Confirm Reader KeyA** fields.
 - b. Enter the current KeyA of the card being programmed.



Note

- The KeyA number is hidden by "*" characters, so write down the new key and keep it in a safe place to avoid exposing this secret key to unauthorized personnel. The KeyA value is entered as a 6 hexadecimal digit. The default KeyA is FFFFFFFF.
- The current KeyA during a new installation is the default KeyA FFFFFFFF. For existing sites, the current KeyA is the KeyA entered the original site installation. The current KeyA remains active until it is changed after configuring the reader.

11. Select the **User Facility Code** checkbox to set a single facility code to all enrolled cards and then change only number of the **User Card ID**.
12. Place a MIFARE card on the CP-R26 Desktop Programmer antenna area.
13. Click **Start** to begin programming the MIFARE card.

5.3.4 Programming Auxiliary Card for 1:1 and 1:N Readers

The auxiliary card is used to define the memory placement for enrolling or deleting fingerprint within the readers' memory slots.

To define an auxiliary card:

1. Select the **CP-R26** tab.
2. From the *Reader Mode* section, select **One to one(1:1)** or **One to many(1:N)**.
3. Ensure that the *Operations* is set to **Program Card**.
4. From the *Operation Type* dropdown menu, select **Program Auxiliary Cards**.
5. From the *Card type* dropdown menu, select the desired card between: **+1**, **+10**, **ENROLL**, **DELETE** and **ADD CARD**.
6. In *KeyA*:
 - a. Enter the KeyA to be used by the reader as the unique KeyA for the organization or site in both the **Reader KeyA** and the **Confirm Reader KeyA** fields.
 - b. Enter the current KeyA of the card being programmed.



- The KeyA number is hidden by "*" characters, so write down the new key and keep it in a safe place to avoid exposing this secret key to unauthorized personnel. The KeyA value is entered as a 6 hexadecimal digit. The default KeyA is FFFFFFFF.
- The current KeyA during a new installation is the default KeyA FFFFFFFF. For existing sites, the current KeyA is the KeyA entered the original site installation. The current KeyA remains active until it is changed after configuring the reader.

7. Place a MIFARE card on the CP-R26 Desktop Programmer antenna area.
8. Click **Start** to begin programming the MIFARE card.

On successful completion of the programming, 3 short beeps are generated.

If the programming fails, there is a short buzz and the Capacitive Card Reader LEDs light red for three seconds.
9. To program and enroll additional auxiliary cards, repeat Steps 4 to 8.

6. Additional Programmer Utilities

The AS-B01 software includes additional utilities that allow you to use the programmer in the best and easiest possible way.

The card utilities are identical for both the Sector Read and CP-R26 tabs. The CP-R26 tab has additional utilities designed specifically for the full finger capacitive application.

6.1 Card Utilities

The card utilities vary depending on the selection of either **Sector** or **Card Serial Number (CSN)** in *Operation Mode*.

When **Card Serial Number (CSN)** is selected, there are two card utility options available.

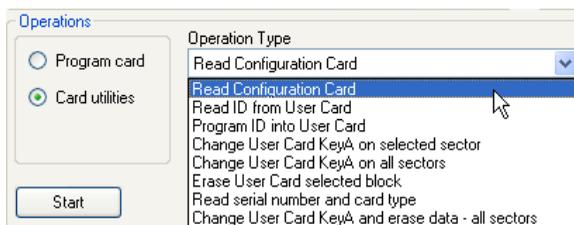
When **Sector** is selected, the same two card utilities are available, plus six additional utilities specific to the Sector type card.

6.1.1 Reading a Configuration Card

This function is used to confirm the card configuration when performing other functions in order to save time and enhance accuracy.

To read the Configuration cards:

1. Select either the **Sector Reader** or **CP-R26** tab.
2. In the *Operations* area, select **Card utilities**.
3. In the *Operation Type* field, select **Read Configuration Card** from the dropdown menu.



4. Place the MIFARE Configuration card on the CP-R26 Desktop Programmer antenna area.
5. Click **Start** to begin reading the Configuration card.
The configuration options are displayed on the screen.



The KeyA shown depends on whether or not the configuration card was used to previously configure the reader or not.

If the configuration card was used, the KeyA shown is the actual KeyA configured by the user; otherwise, the previous KeyA is shown.

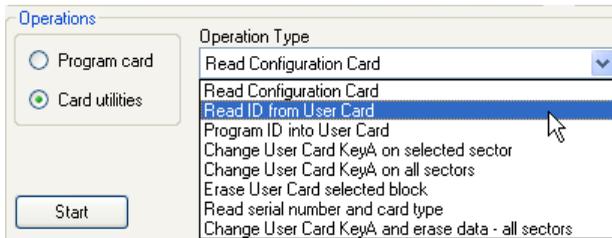
6.1.2 Reading an ID from a User Card

This utility is used to ensure that the MIFARE User card is configured properly.

This option is only available for the **Sector** *Operation Mode*.

To read an ID from a MIFARE User card:

1. Select either the **Sector Reader** or **CP-R26** tab.
2. *In Operation Mode*, select **Sector**.
3. Select the *Card Type*, either **MIFARE 1 K** or **MIFARE 4 K**.
4. From the *Transmit Format* dropdown menu, select the applicable transmission format.
5. In *Operations*, select **Card utilities**.
6. From the *Operation Type* field dropdown menu, select **Read ID from User Card**.



7. The **KeyA** and **MIFARE User Card ID** fields appear.
8. Enter the **KeyA** of the card being read.
9. Place the MIFARE User card on the CP-R26 Desktop Programmer antenna area.
10. Click **Start** to display the card ID in the **MIFARE User Card ID** field.

6.1.3 Programming a User Card ID

This utility is used to program the User Card ID into a specific location on the User card without configuring the card template or KeyA.

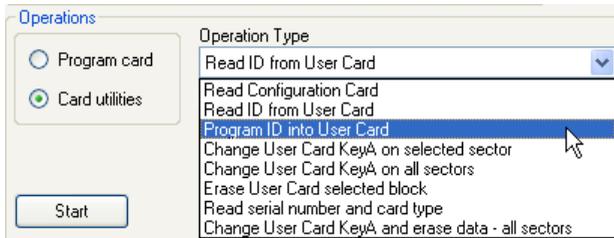
This option is only available for the **Sector** *Operation Mode*.

To program an ID into a MIFARE User card:

1. Select either the **Sector Reader** or **CP-R26** tab.
2. *In Operation Mode*, select **Sector**.
3. Select the *Card Type*, either **MIFARE 1 K** or **MIFARE 4 K**.
4. From the *Transmit Format* dropdown menu, select the applicable transmission format.
5. In *Operations*, select **Card utilities**.

Additional Programmer Utilities

- From the *Operation Type* field dropdown menu, select **Program ID into User Card**.



- The **KeyA** and **MIFARE User Card ID** fields appear.
- Enter the **KeyA** of the card being programmed.
 - Enter the **User Card ID** or scroll to the value using the Up and Down arrows. The value can be between 0 and 1677215.
 - Select values for the **Sector Number**, **Block Number**, and **Byte Number** fields in *ID Location*.
 - Place the MIFARE User card on the CP-R26 Desktop Programmer antenna area.
 - Click **Start** to begin programming procedure.

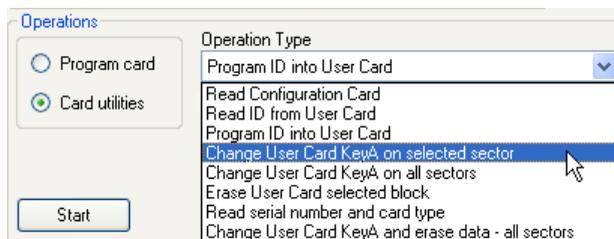
6.1.4 Changing the User Card KeyA in a Specific Sector

Use this utility to change the KeyA value in a specific sector of the User card without changing the card template or User Card ID.

This option is only available for the **Sector Operation Mode**.

To change the KeyA in a specific sector:

- Select either the **Sector Reader** or **CP-R26** tab.
- Select the **Sector Operation Mode**.
- Select the *Card Type*, either **MIFARE 1 K** or **MIFARE 4 K**.
- Define the *ID Location* using the **Sector Number** field.
- In *Operations*, select **Card utilities**.
- From the *Operation Type* field dropdown menu, select **Change User Card KeyA on selected sector**.



The **KeyA** fields are displayed.

7. In *KeyA*:
 - a. Enter the KeyA to be used by the reader as the unique KeyA for the organization or site in both the **Reader KeyA** and the **Confirm Reader KeyA** fields.
 - b. Enter the current KeyA of the card being programmed.



Note

- The KeyA number is hidden by "*" characters, so write down the new key and keep it in a safe place to avoid exposing this secret key to unauthorized personnel. The KeyA value is entered as a 6 hexadecimal digit. The default KeyA is FFFFFFFF.
- The current KeyA during a new installation is the default KeyA FFFFFFFF. For existing sites, the current KeyA is the KeyA entered the original site installation. The current KeyA remains active until it is changed after configuring the reader.

8. Place the MIFARE User card on the CP-R26 Desktop Programmer antenna area.
9. Click **Start** to program the card with the new KeyA.

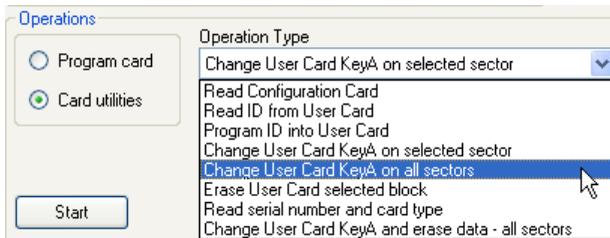
6.1.5 Changing the User Card KeyA in All Sectors

Use this utility to change the KeyA value in all sectors of the User card without changing the card template or User Card ID.

This option is only available for the **Sector Operation Mode**.

To change the KeyA in a specific sector:

1. Select either the **Sector Reader** or **CP-R26** tab.
2. Select the **Sector Operation Mode**.
3. Select the *Card Type*, either **MIFARE 1 K** or **MIFARE 4 K**.
4. In *Operations*, select **Card utilities**.
5. From the *Operation Type* field dropdown menu, select **Change User Card KeyA on all sectors**.



The **KeyA** fields are displayed.

6. In *KeyA*:
 - a. Enter the KeyA to be used by the reader as the unique KeyA for the organization or site in both the **Reader KeyA** and the **Confirm Reader KeyA** fields.
 - b. Enter the current KeyA of the card being programmed.

Additional Programmer Utilities



Note

- The KeyA number is hidden by "*" characters, so write down the new key and keep it in a safe place to avoid exposing this secret key to unauthorized personnel. The KeyA value is entered as a 6 hexadecimal digit. The default KeyA is FFFFFFFF.
- The current KeyA during a new installation is the default KeyA FFFFFFFF. For existing sites, the current KeyA is the KeyA entered the original site installation. The current KeyA remains active until it is changed after configuring the reader.

7. Place the MIFARE User card on the CP-R26 Desktop Programmer antenna area.
8. Click **Start** to program the card with the new KeyA.

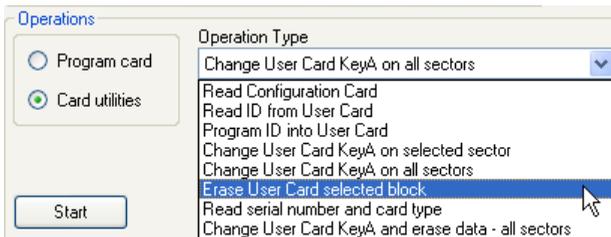
6.1.6 Erasing Specific User Card Data

This utility is used to erase specific information from a defined sector within the card.

This option is only available for the **Sector Operation Mode**.

To erase specific User card data:

1. Select either the **Sector Reader** or **CP-R26** tab.
2. Select the **Sector Operation Mode**.
3. Select the *Card Type*, either **MIFARE 1 K** or **MIFARE 4 K**.
4. In the *Operations* area, select **Card utilities**.
5. From the *Operation Type* field dropdown menu select **Erase User Card selected block**.



The **KeyA** field is displayed.

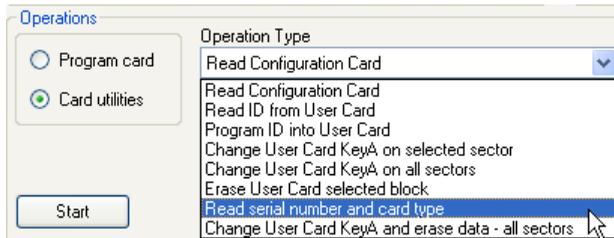
6. Enter the **KeyA** for the card being read.
7. Place the MIFARE User card on the CP-R26 Desktop Programmer antenna area.
8. Click **Start** to erase the data from the specific sector within the card.

6.1.7 Read Serial Number and Card Type

Each MIFARE card has a Unique Serial Number (UID). Use this utility to see a card's UID and card type.

To read a MIFARE User Card Serial Number and Type:

1. Select either the **Sector Reader** or the **CP-R26** tab.
2. From the *Transmit Format* dropdown menu, select the applicable transmission format.
3. In the *Operations* area, select **Card utilities**.
4. From the *Operation Type* field dropdown menu, select **Read serial number and card type**.



The **Serial Number** field appears.

5. Place the MIFARE User card on the CP-R26 Desktop Programmer antenna area.
6. Click **Start** to display the serial number and card type.

6.1.8 Changing KeyA and Erasing All Data

Use this utility to format a card in order to define a new KeyA, which will be written on all sectors.

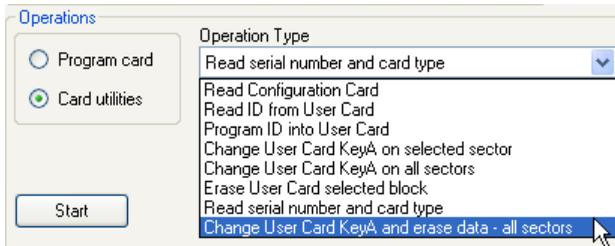
This option is only available for the **Sector Operation Mode**.

To format the User card:

1. Select either the **Sector Reader** or **CP-R26** tab.
2. Select the **Sector Operation Mode**.
3. Select the *Card Type*, either **MIFARE 1 K** or **MIFARE 4 K**.
4. In the *Operations* area select **Card utilities**.

Additional Programmer Utilities

- From the *Operation Type* field dropdown menu, select **Change User Card KeyA and erase data – all sectors**.



The **KeyA** fields are displayed.

- In *KeyA*:
 - Enter the KeyA to be used by the reader as the unique KeyA for the organization or site in both the **Reader KeyA** and the **Confirm Reader KeyA** fields.
 - Enter the current KeyA of the card being programmed.



Note

- The KeyA number is hidden by "*" characters, so write down the new key and keep it in a safe place to avoid exposing this secret key to unauthorized personnel. The KeyA value is entered as a 6 hexadecimal digit. The default KeyA is FFFFFFFF.
- The current KeyA during a new installation is the default KeyA FFFFFFFF. For existing sites, the current KeyA is the KeyA entered the original site installation. The current KeyA remains active until it is changed after configuring the reader.

- Place the MIFARE User card on the CP-R26 Desktop Programmer antenna area.
- Click **Start** to start the formatting procedure.



Note

This operation may take up to 30 seconds for a 1K card and several minutes for a 4K card. Do not close the application or remove the card until you receive a confirmation message.

6.2 Fingerprint Utilities



Applicable for MOC type reader only.

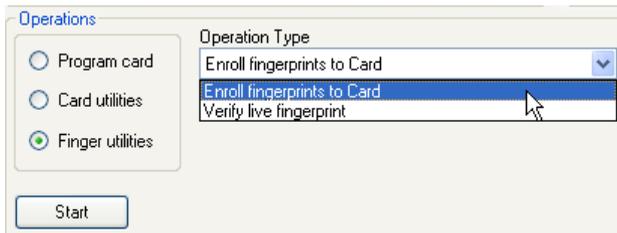
The fingerprint utility allows you to enroll fingerprints to a pre-configured User card without changing the information written on the card, or to verify the fingerprint written on to a card.

6.2.1 Enrolling Fingerprints on a Pre-configured User Card

The AS-B01 software allows you to enroll fingerprints onto a card already configured with the User card ID.

To enroll fingerprints to a pre-configured user card:

1. Select the **CP-R26** tab.
2. In the *Operations* area, select **Finger utilities**.
3. From the *Operation Type* dropdown menu, select **Enroll fingerprints to card**.



4. Select the number of fingerprints to enroll.
5. [Optional] In *Finger options*, select the **Verify after enrollment** checkbox to verify the enrolled fingerprints if required. This usually not required as the CP-R26 Desktop Programmer has an automatic internal verification on enrollment.
6. For security reasons, enter the **KeyA** value.
7. Define the *ID Location* using the **Start Sector** field.
8. Place the card on the CP-R26 Desktop Programmer antenna area.
9. Click **Start** to begin programming the MIFARE card.
10. Instruct the person whose fingerprints are being enrolled to swipe his/her finger on the finger sensor, located on the CP-R26 Desktop Programmer, in the direction indicated by the Fingerprint Directional Indication LEDs.
11. Follow the instructions messages in the Message Log area to repeat the fingerprint enrollment process three (3) times.

Additional Programmer Utilities



To write the finger template onto a specific card sector, define the sector number by typing or selecting the number in the **Sector Number** field located in the *Finger options* section of the screen.

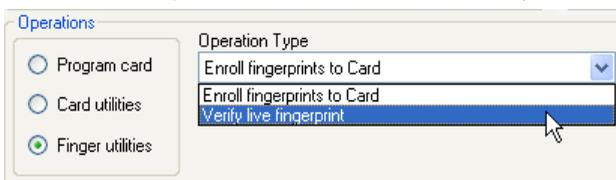
6.2.2 Verifying Fingerprint Enrollment on a User Card

Verifying fingerprint enrollment on a MIFARE User card can be done as a separate function or at the same time an enrollment is preformed.

As an added security measure the CP-R26 Desktop Programmer automatically does an internal verification to ensure accuracy. That is why during the enrollment process, more than one swipe is required.

To verify fingerprint enrollment on a MIFARE User card:

1. Select the **CP-R26** tab.
2. In the *Operations* area, select **Finger utilities**.
3. From the *Operation Type* dropdown menu, select **Verify live fingerprint**.



4. Select the number of fingers that were enrolled for verification.
5. For security reasons, enter the **KeyA** value.
6. Select the sector number that starts the fingerprint template location.
7. Place the card on the CP-R26 Desktop Programmer antenna area.
8. Click **Start** to begin programming the MIFARE card.
9. Instruct the person whose fingerprints are being verified to place their finger on the finger sensor, located on the CP-R26 Desktop Programmer, in the direction indicated by the Fingerprint Directional Indication LEDs.
10. Follow the instructions messages in the Message Log area to repeat the fingerprint swipe process once for each template.

7. Global Options

This section provides instruction on how to define the software behavior and change the password used to enter the application.

7.1 Change Password

For security reasons, it is highly advisable to change the login password to the AS-B01 software from the default password.

To change the AS-B01 application entry password:

1. In the File menu, click **Options > Change Password**.
The *Change Password* window is displayed.



2. Complete the fields as required.
Passwords are case sensitive.
For higher security, make sure that the password you choose is more than 4 letters long. Mixing letters and numbers also substantially strengthens the password.
All passwords are hidden by '*' characters to avoid exposing it to an unauthorized user.
3. Click **OK**.
The password is changed.

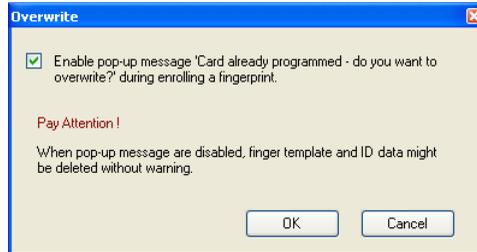
Global Options

7.2 Card Overwrite

Enabling the Card Overwrite option causes the system to issue a warning when attempting to write information onto a card with data already stored on it. If disabled, the system overwrites information automatically without warning the user.

To enable the Card Overwrite warning:

1. In the File menu click **Options > Card Overwrite**.
The *Overwrite* window opens.



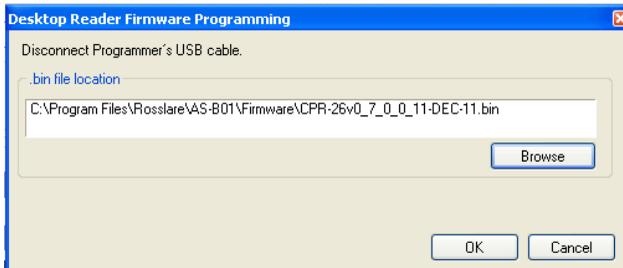
2. Verify that the checkbox is selected.
3. Click **OK**.

7.3 Updating Firmware

You may need to periodically update your firmware.

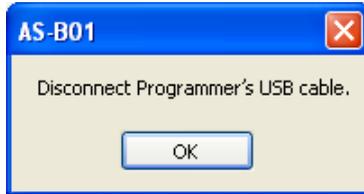
To update the CP-R26 Desktop Programmer firmware:

1. In the File menu click **Options > Firmware Programming**.
The *Desktop Reader Firmware Programming* window opens.



2. [Optional] You can change the default firmware location that is displayed in the *.bin file location* field:
 - a. Click **Browse**.
The standard Windows Explorer window opens.
 - b. Navigate to the folder containing the binary firmware file to download.
 - c. Select the binary firmware file.

3. Make sure the USB cable is disconnected from the CP-R26 Desktop Programmer. If the cable is still connected, a window opens telling you to disconnect the cable.



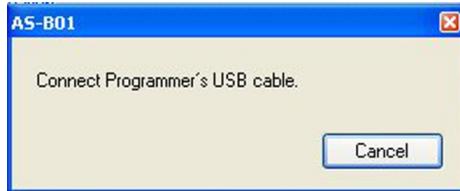
The indicator at the left bottom side of the screen displays **Disconnected**.

4. Click **OK**.

You return to the *Desktop Reader Firmware Programming* window.

5. Click **OK**.

The Connect Cable window opens.



6. Connect the USB Cable.
7. Wait until the indicator at the left bottom side of the screen displays **Connected**.

The installation automatically begins. On completion, a confirmation screen opens.

8. Click **OK**.

The Desktop firmware is now updated.

Two more messages should immediately follow in the Message window: "MIFARE Programming Reader Disconnected" and "MIFARE Programming Reader Connected".

The Desktop Programmer is now ready for use.



Note

Be careful not to select a wrong firmware file, as it may cause permanent Desktop reader hardware failure.

A. Maintenance

To maximize the lifetime of the product, we recommend following these guidelines as closely as possible.

- Do not expose the unit to water or rain or to humidity over the specified safety level.
- Do not expose the unit to direct sunlight for extended periods. This can cause overheating and system failure.
- Avoid dropping the unit onto the ground. This may cause electromechanical failure.

B. Field Descriptions

The AS-B01 software application has fields that need to be completed when configuring the CP-R26 Desktop Programmer, MIFARE cards and/or tags.

The following table describes these fields.

Table 2: Field Descriptions

Field Name	Description
Card Serial Number (CSN)	In the <i>Operation Mode</i> area this option is selected if the reader has to transmit only the card serial number. Each MIFARE card has a Unique Serial Number (UID) to uniquely identify the card.
Card Type	<ul style="list-style-type: none"> • The MIFARE card type determines the size and memory location on the card. There are two options: • MIFARE 1K memory – The 1024 x 8 bit EEPROM memory is organized in 16 sectors with 4 blocks of 16 bytes each. In the erased state the EEPROM cells are read as a logical "0", in the written state as a logical "1". • MIFARE 4K memory – The 4096 x 8 bit EEPROM memory is organized in 32 sectors with 4 blocks and 8 sectors with 16 blocks. Each block contains 16 bytes. In the erased state the EEPROM cells are read as a logical "0", in the written state as a logical "1".
Confirm Password	Used to confirm a new password entered in the <i>New Password</i> field.
Current Password	Password used to enter the AS-B01 software application, and when changing the password.
Enable Aux Input	This enables the auxiliary input that is located in the controller (the primary input is through the PS-25 power supply), which then enables the auxiliary output and bell.
Enable Buzzer	Activates or deactivates the reader's buzzer control.
Enable LED	Activates or deactivates the reader's LED control.
Failed operation	Enables the reader to transmit to the panel any failed operations. These are then displayed in the Message Log Area of the GUI.
ID Location	All sectors in the MIFARE card contain 3 blocks of 16 bytes for storing data. This parameter defines where the data is stored in these data blocks. The location is defined by the company security specifications.
KeyA Password	Unique key used as a security access code. This code used is specified by the company security policies. The key is entered as a 12 digit hexadecimal value with digit values of 0-9, A-F.

Field Descriptions

Field Name	Description
Keypad	Defines the keypad type used to enter codes on an access reader.
Lockout Attempts	Defines the number times a user can present a wrong card or swipe an unverified fingerprint before the reader locks the door for a predefined period of time.
Lockout Duration	Defines how long a card is locked out of the system after too many invalid attempts at swiping the card through the reader or fingerprint scanned due to some inconsistencies with the configured card being used.
New Password	Field used to enter a new password. Passwords are case sensitive. For higher security, make sure that the passwords you choose are more than 4 letters. Mixing letters and numbers also substantially strengthens the password.
Reader KeyA	The MIFARE card storage is divided into sectors with each sector being protected by two different keys, KeyA and KeyB. These keys are programmable according to company security specifications. KeyB is not supported.
Restore to factory default	When the unit is in Controller state, this function allows erasing all enrolled cards and all finger templates stored in memory; when in Reader state, it allows erasing all finger templates from the memory.
Sector	In the <i>Operation Mode</i> area this option is selected if the reader has to transmit encrypted data from the card secured memory. More screen options are added when selecting Sector mode including the <i>Reader KeyA</i> and the <i>ID Location</i> fields.
Transmit Format	Wiegand protocol is a secure transmission format where access control is required. The different bit configuration is used to define different security options specified by the company security officer.
MIFARE User Card ID	Unique ID assigned to the card. This ID number is obtained from the company security officer. The ID number is a numeric with a range of 0 – 1677215.

C. Additional MIFARE Card Memory Map Information

C.1 Manufacture Block

This is the first data block (block 0) of the first sector (sector 0). It contains the IC manufacturer data. Because of security and system requirements, this block is write-protected after having been programmed by the IC manufacturer at production.

When the Rosslare MIFARE reader operation mode is configured to "card serial number", the Unique ID of the card is read from manufacture block.

C.2 Data Blocks

All sectors contain 3 blocks of 16 bytes for storing data (Sector 0 contains only two data blocks and the read-only manufacturer block).

The data blocks can be configured by the access bits as:

- Read/write blocks (for example, contactless access control)
- Value blocks (for example, electronic purse applications – not supported by AS-B01).

An authentication command must be carried out before any memory operation to allow further commands. Authentication commands are based on KeyA, KeyB, and on Access Condition bits. AS-B01 supports programming only KeyA, thus both Access Bits and KeyB modifications are not supported; their location in the following diagram is indicated in black.

Additional MIFARE Card Memory Map Information

Figure 4: MIFARE 1K Memory Diagram

Sector	Block	Byte Number within a Block														Description
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	
15	3	Key A														Sector Trailer 15
	2															Data
	1															Data
	0															Data
14	3	Key A														Sector Trailer 14
	2															Data
	1															Data
	0															Data
:	:															
:	:															
:	:															
1	3	Key A														Sector Trailer 1
	2															Data
	1															Data
	0															Data
0	3	Key A														Sector Trailer 0
	2															Data
	1															Data
	0															Manufacturer Block

For further details about MIFARE cards, refer to the NXP Semiconductor MIFARE datasheet.

D. Sample Worksheets

When entering information, the information must be obtained from the company security officer. To assist in preparing the information to be entered, the following sample form can be used.

Employee Security Card Configuration	
Field	Configuration
Employee Name	
Employee ID #	
Employee Company ID	
Employee Dept.	
Card Serial Number (if applicable)	
Reader KeyA	
Transmit Format	
Card Type (1K or 4K)	
ID Location – Sector Number	
ID Location – Block Number	
ID Location – Byte Number	
MIFARE User Card ID	
Number of Fingerprints (1 or 2)	
LED Control	
Buzzer Control	
Lockout Attempts	
Lockout Duration	
Batch Order Code	

E. 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

ROSSLARE
SECURITY PRODUCTS
www.rosslaresecurity.com

