BEYOND SECURITY

KABA®

Fingerprint Key AR402

Technical Manual (Version 1.0)

First Edition (for V01): January 2014

Fingerprint Key AR402
Technical Manual
Version 1.0

Technical Support
Please call Kaba ADS America's Technical Support phone line at 800.849.8324 or 336.725.1331 between 8:00 a.m. and 5:00 p.m., Monday through Friday (except holidays), Eastern Standard Time.

Trademarks

iCLASS is a registered trademark of HID Global Corporation.

LIT1077 0314

1 About this Document

This document describes the functions, mounting and configuration of the biometric access control reader AR402. The instructions should be followed at all times to ensure flawless and safe application.

The AR402 operates with Kaba embedded access control systems.

1.1 Validity

The information in this document is valid as of firmware release:

- 1.738

Further details can be found in the Release Notes.

1.2 Change Protocol

The most important changes to the last issue of this manual are listed below:

Version Number	Edition	Brief Description
V01	01/2014	First edition

1.3 Used Terminology

Unknown terms and abbreviations may cause uncertainty and operating errors. The most important terms and abbreviations are therefore explained below:

Term	Explanation
Enrollment	The process of capturing live fingers via the biometric sensor, identifying characteristic points of the fingerprint and storing these.
Minutiae	Characteristic points of a fingerprint (ridges, valleys).
Template	The biometric template is the list of minutiae; the encoded fingerprint data.
Template on Card (ToC)	Biometric template written to a card for verification.
Verification	A template stored on a card is matched against a live finger.
Identification	A live finger is matched against all templates stored on the reader's memory.
False Rejection Rate (FRR)	Probability that an authorized person is falsely rejected by the reader.
False Acceptance Rate (FAR)	Probability that an unauthorized person is falsely accepted by the reader.

1.4 Target Groups

This manual is only intended for specialist personnel. The descriptions from the manufacturer require trained personnel. These are not a substitute for product training.

The target groups for which the specific technical manual is valid are listed below:

Project Managers

Project managers responsible for systems, entrusted with project planning and project implementation.

Installation Personnel

Specialists in completing mounting and installation.

Persons with appropriate technical training and experience and authorized by the manufacturer following appropriate product training.

Hardware Service Technicians

Specialists for putting the site into operation and maintaining it.

Persons with appropriate technical training and experience and authorized by the manufacturer following appropriate product training.

Software Systems Technicians

Put devices into operation within the network, thus ensuring availability of devices within the network.

Operators/Customers

Consider the use of Kaba products or services or own and operate a Kaba product, device, or system.

Legally authorized and charged with commercial procurement and the resulting contractual obligations. Have completed the necessary training for operation of the system with an authorized and trained sales partner.

ATTENTION

In the interests of device safety, certain activities must only be performed by Kaba certified technicians and installers. In accordance with DIN EN 60950-1:2006, the Installation Personnel and Service Technicians are the only legitimate groups of persons who may perform maintenance work.

1.5 Occupational and Operational Safety

ATTENTION

Groups of persons commissioned with activities on the site must have read and understood the appropriate documents, particularly chapter 2, Basic Safety Information/page 9 before commencing work.

1.6 Conventions

1.6.1 Document Designation

All documents are designated in English with names comprising a maximum of six fields:

Example: TM_AR402_V01_US

TM	Identifier for the manual (TM = technical manual)
AR402	Name of the product
V01	Version of the manual
US	Country ID for the USA

1.7 Hazard Categories and Symbols

1.7.1 Hazard Categories

Notes with information/commands and prohibitions to prevent damage to persons and property are specially identified.

Please observe this hazard information. This should help to prevent accidents and to avoid damage.

Hazard information is split into the following categories:

DANGER

Designates an immediate risk of danger that will result in severe physical injury or death.

WARNING

Designates a potentially hazardous situation that could result in severe physical injury or death.

CAUTION

Designates a potentially hazardous situation that could result in minor physical injuries.

ATTENTION

Important notes for proper handling of the product.
Failure to observe this information may result in malfunction, and the device or something in its environment may be damaged.

1.7.2 Symbols

Depending on the source of the hazard, symbols are used for the hazard information, and these have the following meanings:

 General danger	 Danger from electrical current
 Danger of explosion	 Danger for electronic components from electrostatic discharge

Notes

Please pay particular attention to the notes marked with symbols.

User tips and useful information that help to make optimal use of the product and its functions.

2 Basic Safety Information

The devices are constructed in accordance with the latest technological standards and recognized safety regulations. However, the use of this product may pose hazards for persons and valuables.

Please read and observe the following safety information before using the product.

2.1 Intended Use

The device/site is only intended for the use outlined in the Device Description chapter of the corresponding technical manual.

Any other kind of use is not considered proper. The manufacturer accepts no liability for any damage resulting from such use. The user/operator bears the sole risk for this.

2.2 Mounting and Installation

Mounting and installation of the device must only be performed by Kaba certified technicians and installers; see chapter 1.4 / page 7.

The device must only be installed in locations that fulfill the climatic and technical conditions specified by the manufacturer.

Kaba AG accepts no liability for damage resulting from improper handling or defective installation.

2.3 Servicing and Maintenance

Maintenance Work/Troubleshooting

Troubleshooting and maintenance work must only be performed by Kaba certified technicians and installers; see chapter 1.4 / page 7.

Conversions and Modifications

Conversions and modifications of the device must only be performed by Kaba certified technicians and installers; see chapter 1.4 / page 7. Any conversions and modifications performed by other persons will result in a complete exclusion of liability.

Testing and Checking the Products' Functionality

- Inform persons before checking alarm devices and allow for possible panic reactions
- Inform any fault and alarm receiving centers connected to the system before a test transmission

Changes to the System Design and the Products

Changes to the system and individual products may result in faults and defective function. It is essential that you obtain written approval for the intended changes and extensions to the system from the sales partner and appropriate safety authorities.

Components and Spare Parts

- Components and spare parts procured locally must conform to the technical requirements specified by the manufacturer. This is guaranteed for original parts supplied by us
- Only use fuses with the required characteristics
- Incorrect battery types and improper replacement of batteries will result in danger of explosion. Only use the same battery type or an equivalent type recommended by the battery manufacturer

2.4 Hazards

2.4.1 Electrical Hazards

Installations on mains voltage must only be performed by authorized specialist contractors or authorized electrical experts.

WARNING

Live Connections in the Access Hub or External Power Supply Units.
Negligence may result in electric shock.

- Work must only be performed by Kaba certified technicians and installers
- Access hubs on which maintenance or repair work is to be performed must, if possible, be disconnected from the power supply
- Connection terminals with external voltage must be fitted with a 'DANGER external voltage' sign
- Mains supply lines to the access hub should be laid separately and must be safeguarded with their own clearly marked fuse
- The grounding must be executed in accordance with local safety requirements

2.4.2 Handling Lithium Batteries

CAUTION

Lithium Batteries Can Explode or Burst Explosively.
Improper handling of lithium batteries can result in fires and explosions.

- Lithium batteries must only be replaced by Kaba certified technicians and installers
- They must only be replaced with batteries of the same type
- Do not open, drill through or crush lithium batteries
- Do not burn lithium batteries or expose them to high temperatures
- Do not short-circuit lithium batteries
- Do not recharge lithium batteries

2.4.3 ESD Protective Measures

ATTENTION

Danger for Electronic Components from Electrostatic Discharge.
Improper handling of electronic circuit boards or components can result in damage, leading to complete failure or sporadic errors.

- The general ESD protective measures must be observed during installation and repair of the device

The Following Rules Must Be Observed:

- Wear an ESD grounding wrist strap when handling electronic components
- Connect the end of the strap to a discharge connector or unlacquered, grounded metal component. This will conduct static loads away from your body safely and effectively
- Only hold circuit boards by the edges. Do not touch circuit boards and connecting plugs
- Place removed components on an anti-static surface or in an anti-static shielding container
- Avoid contact between circuit boards and clothing. The wrist strap only protects circuit boards from electrostatic discharge voltage to the body. However, damage can also occur from electrostatic discharge to clothing
- Removed modules must only be transported and shipped in electrostatic shielding, conductive, protective bags

2.4.4 Environmental Protection

2.4.4.1 Disposal of Packaging

Environmentally-Friendly Disposal of Packaging.
The packaging materials are recyclable. Please ensure that the packaging is recycled and not thrown out with the general waste.

2.4.4.2 Disposing of Devices and Batteries

Do not Dispose of Electrical Devices with General Waste
Electrical devices should be disposed of in accordance with national waste disposal and environmental directives.
Disposal in Germany:
Kaba devices are registered in the used electrical appliances register (EAR) under B2B. Kaba guarantees to accept the return of the product and to dispose of it.

Do not Dispose of Used Batteries with General Waste
Used batteries should be disposed of in accordance with national and local requirements.
Batteries for disposal should be stored carefully to avoid short circuits, crushing, or destruction of the battery housing.

3 Device Description

The AR402 is a biometric reader operating via RS-485 with Kaba embedded access control systems. Additional flexibility is provided by the AR402 Wiegand interface.
Integrated display elements signal both the operating state and access decision visually as well as acoustically.
Conforming to protection class IP65 the reader is prepared for outdoor installations.
In addition to its fingerprint sensor the AR402-iCLASS can read and write to iCLASS media.

Its RS-485 and Wiegand interfaces allow for the following modes of operation:

Modes	Details
RS-485 see chapter 5, page 22	• Kaba embedded access system: AM300, AM524 or TLC200 / AD500 or DU200. • Running the reader using the RS-485 interface means that AR402 administration is done on the access manager. All Admin Functions are disabled on the AR402 (optionally enrollment is accessible). • Fingerprint templates are managed by the access controller and distributed to connected AR402 readers. • No support of the 'Template on Card' mode (AR402-iCLASS only)
Wiegand see chapter 6, page 27	• Access control system: Either AM300, AM524 or TLC200 / AD500 or DU200 or 3rd party Wiegand system. • Running the reader using the Wiegand interface means that AR402 administration is done on the reader's keypad. All Admin Functions are enabled on the AR402. • Fingerprint templates cannot be distributed to connected AR402 readers. • Enrollment needs to be carried out on each AR402 of a Wiegand access control system. • Support of the 'Template on Card' mode (AR402-iCLASS only)
RS-485 and Wiegand please refer to chapter 'Fingerprint Module' in AM300/AM524 manuals	• Access control system: AM300 or AM524 / AD500 or DU200 and 3rd party Wiegand system. • The AR402 supports parallel operation of RS-485 and Wiegand, e.g. to make use of the fingerprint template distribution via RS-485 enhancing a 3rd party Wiegand access control system. • No support of the 'Template on Card' mode (AR402-iCLASS only)
AD102 see chapter 7, page 45	• Single Door Unit AD102 • Running the reader with the AD102 means that AR402 administration is done on the readers' keypad. All Admin Functions are enabled on the AR402. • No fingerprint distribution. System limited to one access point.

Please refer to the section covering the relevant mode of operation. Reading section 'AD102 Mode' is unnecessary if operating AR402 in 'RS-485 Mode' for instance.

3.1 Composition

1	Execute Key #	Press 1x to execute entries / Press 3x to escape
2	Position of Antenna	Present iCLASS card here (AR402-iCLASS only)
3	Fingerprint Sensor	Apply finger when lit
4	Asterisk Key ✱	Press to trigger a biometric access request
5	Numerical Keys	Optionally enter PIN & finger/badge or code for Admin Functions
6	LEDs Green/Red	Status indication
7	12-digit Reader ID	Unique ID for identification of reader on RS-485 bus (here printed without the closing 4 zeros)
8	Buzzer	Remove tape seal for louder buzzer
9	Programming interface	For firmware updates (also updatable via RS-485)
10	Variable Capacitor	Adjust iCLASS reading distance

3.2 Cable Allocation

Black	DC-IN (–)	Power input
Red	DC-IN (+)	12…24 V DC
Pink	RS-485A	RS-485 data bus
Gray	RS-485B	
Green	D0 (data)	Wiegand output
White	D1 (clock)	
Purple	Common	
Orange	Opto-IN-1	Green LEDs
Yellow	Opto-IN-2	Buzzer
Brown	Opto-IN-3	Red LEDs
Blue	Tamper-1	Tamper contact 1
Light brown	Tamper-2	Tamper contact 2

3.2.1 Opto-Inputs

The Opto-Inputs are activated, when connected to Wiegand Common. When used as a Wiegand reader Opto-IN-1 enables the green LEDs, Opto-IN-2 the buzzer. Optionally the red LEDs can be activated via Opto-IN-3.

3.2.2 Tamper switch

Optionally the external tamper monitoring function of the AR402 can be connected. As soon as the AR402 is removed from its mounting plate, the open tamper switch can be evaluated as sabotage (e.g. at the input of an alarm system). When closed, the isolated tamper switch is closed (0 Ohm between the wires Tamper contact 1 and Tamper contact 2).

3.3 Technical Data

Mechanics

Mounting	Indoors or in protected outdoor areas Flush cable mounting
Housing	Reader: • Material: MABS • Available color: black • Resin sealed electronics Mounting plate: • Material: DX51D+Z, thin sheet galvanized
Combustion category	HB (UL94)
Dimensions	AR402 incl. mounting plate: 4.5x2.6x2 inches (HxWxD)
Cable	Cable molded into body. Length 20 inches, Ø 0.3 inches

Power Supply

Input voltage	Limited Power Source (output current ≤ 8 A, output power ≤ 100 W) 12 … 24 V DC, current consumption max. 420 mA Power consumption: AR402 typically 2.5 W; max. 5 W AR402-iCLASS typically 3 W; max. 5 W

Interfaces

Fingerprint biometric sensor	500 dpi @ 8 bit per pixel Sensor area: 0.5x0.9 inch Template size: 130...250 bytes Memory: 1000 fingerprints (optionally 6000)
Optional: iCLASS reader	Integrated 13.56 MHz iCLASS reader and antenna
Keypad	• Capacitive, backlit keypad • 10 numerical keys, 2 function keys
RS-485 interface	For connecting AR402 to Door Unit or Single Door Unit • proprietary protocol; galvanic isolated, 2-wire • Baud rate 19.200, 8 data bits, no parity, 1 stop bit • Terminating resistor for bus wiring
Wiegand output	Alternative connection to Door Unit • Data 0 (Data), Data 1 (Clock), Common • Wiegand out D0/D1 is open collector to Wiegand Common
Programming interface	For firmware updates. AM300, AM524 can update AR402 firmware if connected via a RS-485 Door Unit.

Inputs and Outputs

3 binary inputs	Activated in AR402 Wiegand Mode when connected to Common • Opto-IN-1 - Green LEDs • Opto-IN-2 - Buzzer • Opto-IN-3 - Red LEDs
1 tamper switch	Isolated switch (NO): Max. 24 V DC/0.1 A

Ambient Conditions

Ambient Conditions	Operating temperature:	+5°…+131 ºF
	Storage temperature:	−4°…+158 ºF
	Relative humidity:	10…95 %, non-condensing
	Protection type:	IP 65

3.4 Dimension Drawing

3.5 Conformity of Fingerprint Key AR402

3.5.1 Intended Use

The AR402 is a biometric reader operating via RS-485 with Kaba embedded access control systems. Additional flexibility is provided by the AR402 Wiegand interface. Optionally it is equipped with an iCLASS reader. Access decisions and operating states are signaled visually as well as acoustically on the AR402. Its IP65 conformity allows for outdoor installations.

ATTENTION

The AR402 technical manual describes the mounting, installation, functions, operating modes, configuration, putting into operation, and servicing of the AR402. The instructions should be followed at all times to ensure flawless and safe application.
This will also ensure conformity with standards and directives in accordance with the conformity declaration.

3.5.2 Standards and Directives

The AR402 conforms to the following standards:

ETSI EN 301489-1 V1.8.1	Electromagnetic compatibility
ETSI EN 300330-1 V1.7.1	Electromagnetic compatibility – efficient use of the radio frequency spectrum Part 1: Technical characteristics and test methods
ETSI EN 300330-2 V1.5.1	Part 2: Harmonized EN under article 3.2 of the R&TTE Directive
EN 60950-1:2011 UL 60950-1:2007 CSA-C22.2 No. 60950-1:2007	Information technology equipment - Safety - Part 1: General requirements

Electrical Safety certified by TÜV-SÜD America, a Nationally Recognized Testing Laboratory NRTL.

To the best of our knowledge, this device does not contain any materials (in terms of the concentrations or applications involved) whose circulation within products is prohibited according to the relevant requirements under Directive 2011/65/EU ('RoHS').

3.5.3 Declaration of Conformity

Kaba GmbH, Access & Workforce Management, Mollenbachstrasse 19, D-71229 Leonberg hereby declares that the AR402 Fingerprint Key conforms to the basic requirements and other relevant provisions of Directive 2004/108/EC (EMC).

The AR402 conforms to the following standard:

FCC Rules 47 CFR Part 15 Subpart C Section 15.207; 15.209; 15.225	Class B Digital Device Radio Frequency Devices

3.5.4 Device Labeling

A label is affixed on the bottom side of the device as well as on the packaging. The following information can be found on the label:

- Device designation
- Serial number
- Manufacturer
- CE / FCC mark / TÜV US

3.5.5 Manufacturer

KABA
Kaba Ilco Inc.
7301 Decarie Boulevard
Montreal, Quebec H4P 2G7
CANADA
Phone +1 514 735 5410
Email: info@kaba-ilco.com
http://www.kaba-ilco.com

4 Mounting with Installation Instructions

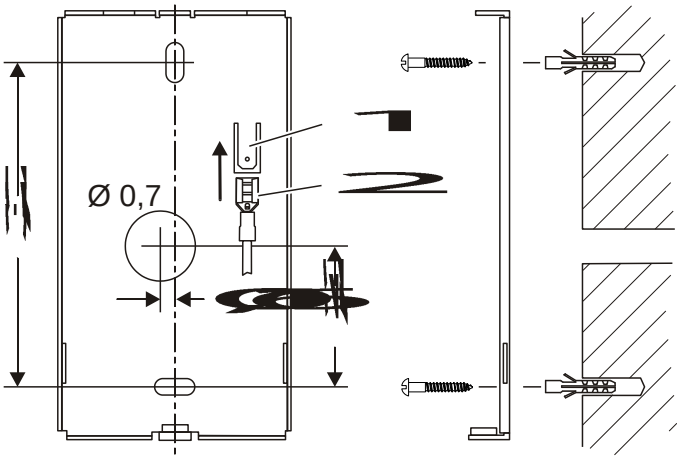
ATTENTION

- The AR402 controllers must be installed in a tamper-proof place (indoors or in protected outdoor area)
- Lines must be concealed in the wall or laid in a tamper-proof area
- Do not install data cables parallel to power cords. If unavoidable, install the data cables in grounded steel conduit and keep a distance of 3 feet to protect them against electromagnetic interference

The mounting plate

The mounting plate is mounted directly to the wall using screws. There are two slot holes available. The holes measure 0.16x0.4 inch.

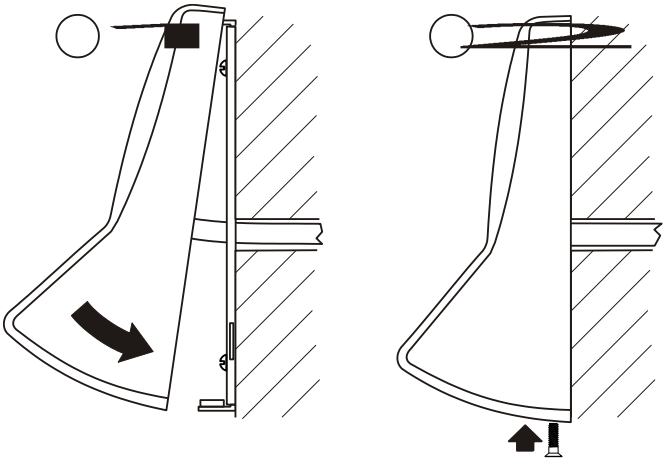
Connect the AR402 wires to the installation cable according to your requirements placing the cable through the Ø 0.7 inch hole. For AR402 cable allocation see chapter 3.2, page 14.



The mounting plate must be grounded separately, if the installation location favors electrostatic discharge, e. g. is covered with carpet.

Connect the ground cable using a 0.25 inch female blade connector (2) and push it onto the blade (1) of the AR402 mounting plate.

Fasten the AR402 to the mounting plate



1. Insert the access reader into the mounting plate brackets and press the bottom against the plate.
2. Attach the AR402 with the M3 screw (supplied) to the mounting plate.

4.1 Cable lengths and recommended cable types

4.1.1 RS-485 connection and power supply

Central power supply (1 cable)

Cable type CAT.5 S-UTP	4 x 2 x AWG 24	4 x 2 x AWG 22	4 x 2 x AWG 20
Max. cable length	< 160 ft.	< 330 ft.	< 1150 ft.

Local power supply (2 cables)

	RS-485	**Power supply**
Cable type CAT.5 S-UTP	2 x 2 x AWG 24	1 x 2 x AWG 24
Max. cable length	< 3.900 ft.	< 33 ft.

4.1.2 Wiegand connection and power supply

Central power supply (1 cable)

Cable type CAT.5 S-UTP	4 x 2 x AWG 24	4 x 2 x AWG 20
Max. cable length	< 160 ft.	< 490 ft.

Local power supply (2 cables)

	Wiegand	**Power supply**
Cable type CAT.5 S-UTP	3 x 2 x AWG 24	1 x 2 x AWG 24
Max. cable length	< 490 ft.	< 33 ft.

4.2 Grounding concept

4.2.1 Mounting plate

The metal mounting plate is to be grounded in electrostatic discharge sensitive environments; see chapter 4, page 18.

4.2.2 Power supply

The AR402 is contained within a plastic housing and a metal mounting plate and is per default not grounded

- If an AR402 is operated with an ungrounded power supply, then neither the power supply nor the peripheral device is grounded
- If an AR402 is operated with a grounded power supply, only the power supply is grounded

4.2.3 Communication connections

4.2.3.1 RS-485 connection

The shielding of the RS-485 cables is not grounded, but is instead attached to the C (common) connection on the Door Unit; see chapter 4.4.1, page 21.

With bus cabling for the communication connections, please also ensure that there is a continuous connection between the shielding of the RS-485 line and the stubs.

4.2.3.2 Wiegand connection

The shielding of the Wiegand cables is not grounded; see chapter 4.4.2, page 21.

4.3 Installation instructions for the power supply

A distinction is made between the central and the local power supply.

4.3.1 Central power supply

Power is provided by one central supply.

- For information on max. cable lengths see chapter 4.1, page 19

4.3.2 Local power supply

The local power supply is used where it is more cost effective than a long distance central power cable and where increased requirements are placed on the AR402 in terms of operational reliability.
A separate power supply unit is used for this purpose.

- For information on max. cable lengths see chapter 4.1, page 19

4.4 Installation instructions for the communication connections

4.4.1 RS-485 cabling

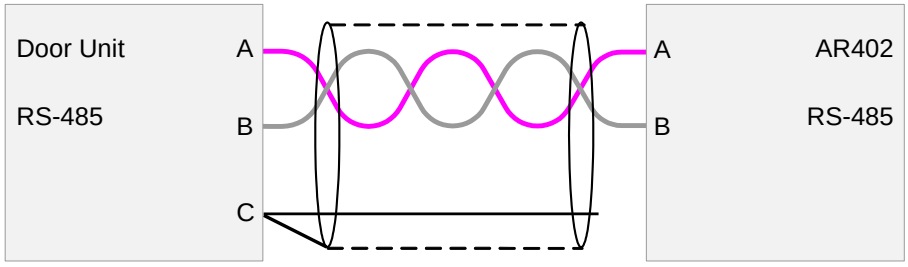
ATTENTION

The AR402 is connected to a Door Unit via a 2-wire party line connection (RS-485).
Please observe the local legal regulations (e.g., VDE) when installing components. Information on structured cabling can be found in standard EN 50173.

Recommended cable: Category 5 cable with 2 conductor pairs, AWG 24 (0.6 wire Ø), and S-UTP design (Screened Unshielded Twisted Pair). This cable is fitted with a foil screen (screened). The individual conductor pairs are not shielded from each other (unshielded). Two color-coded conductors are twisted together in each case (twisted pairs).

Please note that the foil screen is connected by means of a sheath wire. To avoid short circuits, the sheath wire should be insulated with a heat-shrinkable tube, for example.

Lines A and B are routed as a twisted pair of conductors and are not transposed.



4.4.1.1 Bus cabling

The RS-485 terminating resistor on the AR402 is set to 120 Ω. There is no provision to set it to open.
Each AR402 needs to be directly connected to a Door Unit.

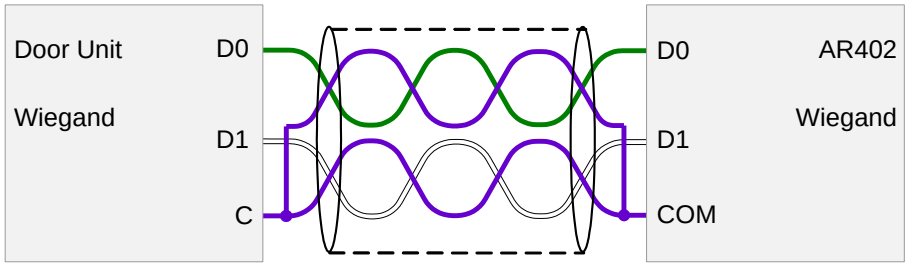
4.4.2 Wiegand cabling

ATTENTION

The AR402 is connected to a Door Unit via Wiegand.
Please observe the local legal regulations (e.g., VDE) when installing components. Information on structured cabling can be found in standard EN 50173.

Recommended cable: Category 5 cable with 2 conductor pairs, AWG 24 (0.6 wire Ø), and S-UTP design (Screened Unshielded Twisted Pair). This cable is fitted with a foil screen (screened). The individual conductor pairs are not shielded from each other (unshielded). Two color-coded conductors are twisted together in each case (twisted pairs).

Lines D0 and COM, and D1 and COM are routed as a twisted pair of conductors and are not transposed.



5 RS-485 Mode

Running the reader using the RS-485 interface implies that administration of the AR402 is done on the access controller. All Admin Functions are disabled on the AR402 (optionally Enrollment and Reset are accessible).
Fingerprint templates are managed by the access controller and can be distributed to connected AR402 and readers of the 401 series.

AR402 are delivered in Wiegand mode, indicated by the 4 red lit LEDs when first put into operation. The reader will automatically switch to RS-485 mode once it is connected to a RS-485 Kaba embedded access control system, indicated by all LEDs off; see chapter 5.2, page 23.

5.1 Logical Device Addresses on Door Unit 200

On RS-485 data buses devices are distinguished by their device addresses.
Connected to a Door Unit 200 this logical device address is assigned automatically to AR402 readers. Based on the AR402 ID, a 12-digit hexadecimal code (e.g. B463AA130000), the controller allocates the readers according to the following rationale:

- The DU200 recognizes two unassigned readers:
  The lower value of the two IDs is assigned to Reader 0 (e.g. 672692150000)
  The higher value of the two IDs is assigned to Reader 1 (e.g. B463AA130000)
- The DU200 recognizes one already assigned and one unassigned AR402 ID:
  The already assigned reader will keep its assignment
  The unassigned reader will be assigned the available ID as Reader 0 or Reader 1
- Both AR402 are assigned by the DU200:
  The readers keep their address assignment

For installations with RS-485 AR402 on Door Unit 200 it is good practice to note the AR402 IDs for each reader location. The ID is printed on the inside of each AR402, e.g. 672692150000. The zeros may be omitted in print; see chapter 3.1, page 13.
On the Access Manager's web interface the automatic AR402 address allocation can be exchanged.

The automatic assignment of logical device addresses to AR402 does not apply to the Door Unit 500 (AD500). On the AD500 logical device addresses of AR402 are linked to the connector the readers are plugged into connector: Reader 1 – Logical address = 0 / Reader 2 – Logical address = 1

5.2 Status Indication

The table below gives an overview of AR402 status indication via the four green/red LEDs and the buzzer in RS-485 mode. Generally the AR402 confirms each key entry acoustically by a short beep and visibly by deactivating the keypad backlight briefly.

Status	**Reader Indication**		
	LEDs		Buzzer
RS-485 mode - online and idle	LEDs	○○○○ off	
RS-485 mode - offline	Red LED	○○○● flashing	
Access granted	Green LEDs	●●●● on	1x Beep
Access denied	Red LEDs	●●●● on	2x Beep
Access point locked down	Red LEDs	●●●● on	
Access point permanently open	Green LEDs	●●●● on	
Fingerprints sync	Red LEDs	○●●○ flashing	
Firmware update in progress	Green LED	○○○● flashing quickly	
Error / Incorrect entry	Red LEDs	●●●● flashing 3x	3x Beep

For more details on the reader's signaling in its various states please refer to the following chapters.

5.3 Access Procedure and Indication

5.3.1 Finger only

Steps	**Enter**	**Reader Indication**	
		LEDs/Sensor	Buzzer
1. Press	*	 Sensor on	
2. Apply Finger		if granted: Green LEDs ●●●● on	Beep
		if denied: Red LEDs ●●●● on	2x Beep

5.3.2 Finger & PIN

Steps	**Enter**	**Reader Indication**	
		LEDs/Sensor	Buzzer
1. Press	*	Green LEDs ●○○● flashing	
2. Enter PIN	[PIN]	 Sensor on	
3. Apply Finger		if granted: Green LEDs ●●●● on	Beep
		if denied: Red LEDs ●●●● on	2x Beep

5.3.3 Card only

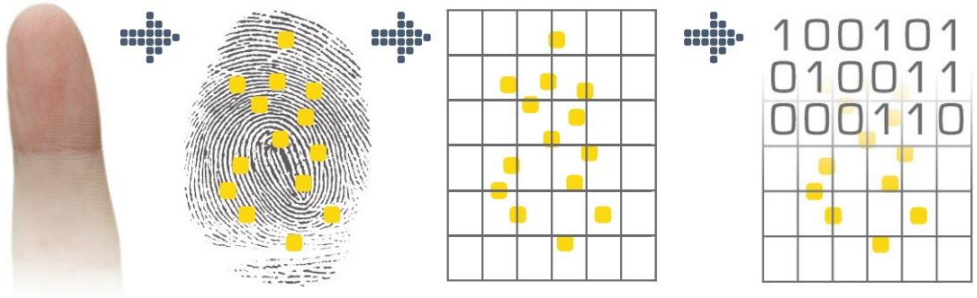
Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Present Card		Green LEDs ○●●○ on	Beep
		if granted: Green LEDs ●●●● on	
		if denied: Red LEDs ●●●● on	Beep

5.3.4 Card & PIN

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Present Card		Green LEDs ○●●○ on	Beep
		Green LEDs ●○○● flashing	
2. Enter PIN	[PIN]	if granted: Green LEDs ●●●● on	Beep
		if denied: Red LEDs ●●●● on	2x Beep

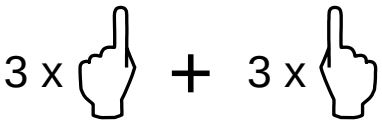
5.4 Enrollment

The AR402 identifies authorized users by reading their fingerprints or iCLASS cards and optionally their PINs. Successful identification sends a trigger signal to an access controller which grants or refuses the access request.
Fingerprint authentication requires authorized users to have enrolled their fingerprints in advance with a unique Fingerprint Number.
Enrollment means to capture a live finger, to identify minutia points that form a unique pattern, and to then encode it. This code (template) is saved to the reader's memory; it cannot be reconverted into an image. The AR402 does not store fingerprint images.



Enrollment may be performed on the AR402. Alternatively enrollment is carried out on an enrollment station in RS-485 configurations where templates can be distributed to connected AR402 readers.

The AR402 assigns 2 fingers (e.g. the left index finger and the right index finger) to a unique ID, or Fingerprint Number. Each of the two fingers is scanned three times.



The biometric sensor reads fingerprints best when placing your finger on the sensor with some pressure.

Bright daylight may affect the function of the biometric sensor.
Shadowing the sensor with your hand will help.

For more guidance on how to best place the finger on the biometric sensor please refer to the appendix; see chapter 8.1, page 65)

5.4.1 Enroll User

To safeguard the AR402 Admin Functions, the reader's Admin Mode may not be accessible, depending on the reader settings of the Access Manager.

Steps to enroll fingerprints to the AR402 memory.

Steps	Enter	Reader Indication LEDs/Sensor	Buzzer
1. Enter Admin Mode	# 99 #	Green LEDs ●●○○ on	
2. Default Admin Code 1234 or enter your Admin Code	_____ #	Green LEDs ●●●○ on	
3. Enrollment	12 #	Green LEDs ●●●● flashing	
4. Enter Fingerprint Number (Default no. of digits = 5)	_____ #	Green LED ●○○○ flashing  Sensor on	
5. Apply 2 Fingers 3x each[1]	3 x + 3 x	If successful: Green LEDs ●●●● flashing	Beep
6. Enroll additional Fingers?	Yes / No		
7. Escape Enrollment or wait for Timeout	#		

[1] The table below shows the AR402 indication guiding the user through each step of the enrollment process. Repeat these steps for the second finger. The LED indication is identical for finger 2.

LED Indication	Detailed Enrollment Steps
Green LED ●○○○ flashing	Scan finger 1 a first time
Green LED ●○○○ on	Remove finger 1 from the sensor
Green LED ○●○○ flashing	Scan finger 1 a second time
Green LED ●●○○ on	Remove finger 1 from the sensor
Green LED ○○●○ flashing	Scan finger 1 a third time
Green LED ●●●○ on	Remove finger 1 from the sensor

Entering a Fingerprint Number with an incorrect number of digits, an already existing Fingerprint Number, or attempts to enroll already enrolled fingers will prompt an error indication (all red LEDs flashing three times) and cause the reader to return to its idle state.

5.5 Reset - Manually switch to RS-485 Mode

To safeguard the AR402 Admin Functions, the reader's Admin Mode may not be accessible, depending on the reader settings of the Access Manager.

This function allows you to manually set the AR402 to RS-485 mode.
All settings including the changed Admin Code will be reset. The reader indicates its offline status by the red flashing LED 4. The AR402 will automatically go online once it is connected to an access control system via RS-485. The controller will configure the reader according to its settings, including the Admin Code if it was altered.

Steps	**Enter**	**Reader Indication**	
		LEDs/Sensor	Buzzer
1. Enter Admin Mode	# 99 #	Green LEDs ●●○○ on	
2. Default Admin Code 1234 or enter your Admin Code	_____ #	Green LEDs ●●●○ on	
3. Enable RS-485 Mode	2 #	Red LED ○○○● flashing	
Device resets and signals its RS-485 offline status			

5.6 Quick Guide to RS-485 Mode Admin Functions

To safeguard the AR402 Admin Functions, the reader's Admin Mode may not be accessible, depending on the reader settings of the Access Manager.

Enter	**Function**	**Page**
# 99 #	Enable Admin Mode	
1234 #	Enter Default Admin Code (or your Admin Code)	
2 #	Reset - Manually Switch to RS-485 Mode	26
12 #	Enroll User	25

6 Wiegand Mode

In an RS-485 configuration, the AR402 is controlled by a separate Access Manager. However, in a Wiegand environment, the settings must be managed locally at the AR402 keypad.
AR402 settings are referred to as Admin Functions which include features like enrolling fingerprints, deleting fingerprints, setting the number of digits for fingerprint numbers, AR402 reset, etc.
These Admin Functions are protected by the Admin Code which by default is set to: '1234'.

We recommend to disable the default Admin Code by employing the Admin Finger feature (see chapter 6.3.1, page 30) or alternatively by replacing it with your own individual Admin Code; see chapter 6.4, page 35.

There is an additional emergency access code to the Admin Mode for AR402 with unknown Admin Fingers and Admin Codes. The access code is based on the reader's ID, a 12-digit hexadecimal code, printed on the inside of the AR402, e.g. 672692150000. The zeros may be omitted in print; see chapter 3.1, page 13.
Please contact the relevant Kaba support personnel for your access code.

Wiegand configuration users need to be enrolled to each Wiegand AR402 since automatic distribution of fingerprint data to all connected fingerprint readers requires RS-485 communication.
AR402 are delivered in Wiegand mode, indicated by the four LEDs lit red when put into operation (see table below).

6.1 Status Indication

The table below gives an overview of AR402 status indication via the four green/red LEDs and the buzzer in Wiegand mode. Generally the AR402 confirms each key entry acoustically by a short beep and visibly by deactivating the keypad backlight briefly.

Status	**Reader Indication**		
	LEDs		Buzzer
Wiegand mode - idle	Red LEDs	on	
Access granted	Green LEDs	on	1x Beep
Access denied	Red LEDs	on	2x Beep
Access point blocked	Red LEDs	on	
Access point permanently open	Green LEDs	on	
Error / Incorrect entry	Red LEDs	flashing 3x	3x Beep

For more details on the reader's signaling in its various states please refer to the following chapters.

6.2 Access Procedure and Indication

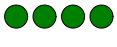
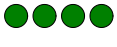
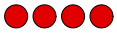
6.2.1 Finger only

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Press	*	 Sensor on	
2. Apply Finger		if granted: Green LEDs  on	Beep
		if not enrolled: Red LEDs  flashing	3x Beep
		if denied: Red LEDs  on	2x Beep

6.2.2 Finger & PIN

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Press	*	 Sensor on	
2. Apply Finger		if enrolled: Green LEDs  flashing	Beep
		if not enrolled: Red LEDs  flashing	3x Beep
3. Enter PIN	[PIN]	if granted: Green LEDs  on	Beep
		if denied: Red LEDs  on	2x Beep

6.2.3 Card only

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Present Card		Green LEDs  on	Beep
		if granted: Green LEDs  on	
		if denied: Red LEDs  on	2x Beep

6.2.4 Card & PIN

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Present Card		Green LEDs flashing	Beep
2. Enter PIN	[PIN]	if granted: Green LEDs on	Beep
		if denied: Red LEDs on	2x Beep

6.2.5 Template on Card w/o PIN

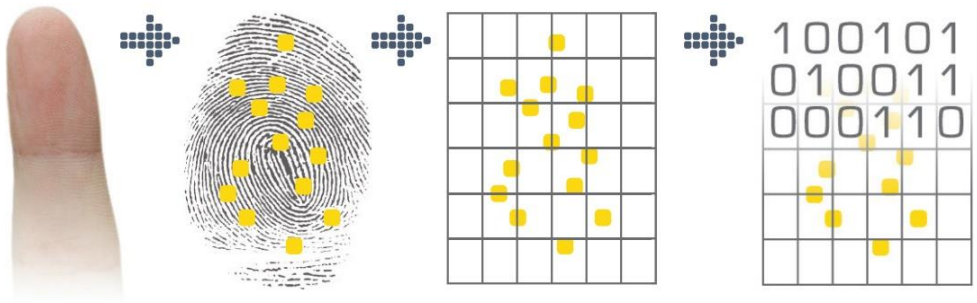
Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Present Card		Green LEDs flashing	Beep
		Sensor on	
2. Apply Finger		if granted: Green LEDs on	Beep
		if not verified: Red LEDs flashing	3x Beep
		if denied: Red LEDs on	2x Beep

6.2.6 Template on Card & PIN

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Present Card		Green LEDs flashing	Beep
		Sensor on	
2. Apply Finger		if verified: Green LEDs flashing	
		if not verified: Red LEDs flashing	3x Beep
3. Enter PIN	[PIN]	if granted: Green LEDs on	Beep
		if denied: Red LEDs on	2x Beep

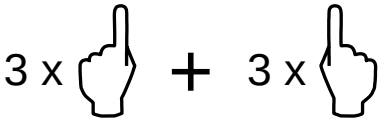
6.3 Enrollment

The AR402 identifies authorized users by reading their fingerprints and/or iCLASS cards and optionally their PINs. Successful identification sends a trigger signal to an access controller which grants or refuses the access request.
Fingerprint authentication requires authorized users to have enrolled their fingerprints in advance with a unique Fingerprint Number.
Enrollment means to capture a live finger, to identify minutia points that form a unique pattern, and to then encode it. This code (template) is saved to the readers memory; it cannot be reconverted into an image. The AR402 does not store fingerprint images.



In Wiegand configurations enrollment must be performed on each AR402. Distribution of fingerprint templates to connected readers is not possible. Each reader stores the templates to its memory.
The AR402-iCLASS 'Template on Card' feature allows writing templates to iCLASS cards.

The AR402 assigns 2 fingers (e.g. the left index finger and the right index finger) to a unique ID, or Fingerprint Number. Each of the two fingers is scanned three times.



The biometric sensor reads fingerprints best when placing your finger on the sensor with some pressure.

Bright daylight may affect the function of the biometric sensor.
Shadowing the sensor with your hand will help.

For more guidance on how to best place the finger on the biometric sensor please refer to the appendix; see chapter 8.1, page 65.

6.3.1 Admin Finger

The Admin Finger is a feature to safeguard the AR402 Admin Functions by biometrics. The Admin Finger replaces and disables the default Admin Code '1234' (or your individual Admin Code).
A maximum of two users may enroll an Admin Finger in addition to their regular enrollment for access.
As a fallback there is a 6-digit Admin Code for each of the two Admin Fingers which is set during the Admin Finger enrollment process.
We recommend the Admin Finger feature as it offers the most effective protection for the AR402 Admin Functions. It also allows quicker access to the Admin Mode than entering # 99 # 1234 #.
Admin Fingers do not trigger access requests. Enroll a different finger as Admin Finger than for access.
Attempts to enroll a finger twice will be denied.

6.3.1.1 Enroll Admin Finger

Steps to enroll Admin Finger-1 or Admin Finger-2

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	# 99 #	Green LEDs ●●○○ on	
2. Default Admin Code 1234 or enter your Admin Code	_____ #	Green LEDs ●●●○ on	
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Enroll Admin Finger-1	30 #	Green LEDs ○●●○ flashing	Beep
or Admin Finger-2	31 #	Green LEDs ○●●○ flashing	Beep
5. Admin Code Finger-1 (or 2)	[6 digits] #	Green LED ●○○○ flashing  Sensor on	
6. Apply 2 Fingers 3x each[1]	3 x  + 3 x 	If successful:	Beep

[1] The table below shows the AR402 indication guiding the user through each step of the enrollment process. Repeat these steps for the second finger. The LED indication is identical for finger 2.

LED Indication	Detailed Enrollment Steps
Green LED ●○○○ flashing	Scan finger 1 a first time
Green LED ●○○○ on	Remove finger 1 from the sensor
Green LED ○●○○ flashing	Scan finger 1 a second time
Green LED ●●○○ on	Remove finger 1 from the sensor
Green LED ○○●○ flashing	Scan finger 1 a third time
Green LED ●●●○ on	Remove finger 1 from the sensor

6.3.1.2 Unlocking Admin Mode with Admin Finger

Steps to access the AR402 Admin Mode with the Admin Finger

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	✱	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
3. move on to desired option e.g. Enrollment	12 #		

Alternatively enter the Admin Finger's Admin Code.
The default Admin Code '1234' is disabled once an Admin Finger is enrolled.

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	# 99 #	Green LEDs ●●○○ on	
2. Admin Code Finger-1 (or 2)	[6 digits] #	Green LEDs ●●●○ on	
3. move on to desired option e.g. Enrollment	12 #		

6.3.1.3 Delete Admin Finger(s)

Steps to delete the Admin Finger(s)

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	✱	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Delete Admin Finger-1	301 #		Beep
or Admin Finger-2	311 #		Beep

Once the Admin Finger(s) is/are deleted the AR402 Admin Code is reset to its default '1234'.

6.3.1.4 Effects of AR402 Reset or Delete All Templates on Admin Finger(s)

Operation	Enter	Effects
Reset to Wiegand	✱ [Admin Finger] 1 # or # 99 # [Admin Code] # 1 #	Admin Finger(s) will remain untouched and Admin Code will be reset to '1234'
Delete Memory	✱ [Admin Finger] 1357 # ✱ or # 99 # [Admin Code] # 1357 # ✱	Admin Finger(s) will be deleted and Admin Code will be reset to '1234'

6.3.2 Enroll User

Steps to enroll fingers to the AR402 memory.

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Enrollment	12 #	Green LEDs ●●●● flashing	
4. Enter Fingerprint Number (Default no. of digits = 5)	_____ #	Green LED ●○○○ flashing	
		 Sensor on	
5. Apply 2 Fingers 3x each[1]	3 x  + 3 x 	If successful: Green LEDs ●●●● flashing	Beep
6. Enroll additional Fingers?	Yes No		
7. Escape Enrollment or wait for Timeout	#		

[1] The table below shows the AR402 indication guiding the user through each step of the enrollment process. Repeat these steps for the second finger. The LED indication is identical for finger 2.

LED Indication	Detailed Enrollment Steps
Green LED ●○○○ flashing	Scan finger 1 a first time
Green LED ●○○○ on	Remove finger 1 from the sensor
Green LED ○●○○ flashing	Scan finger 1 a second time
Green LED ●●○○ on	Remove finger 1 from the sensor
Green LED ○○●○ flashing	Scan finger 1 a third time
Green LED ●●●○ on	Remove finger 1 from the sensor

Entering a Fingerprint Number with an incorrect number of digits, an already existing Fingerprint Number, or attempts to enroll already enrolled fingers will prompt an error indication (all red LEDs flashing three times) and cause the reader to return to its idle state.

6.3.3 Enroll User to iCLASS Card (AR402-iCLASS only)

Setting the reader to 'Template on Card' (ToC) is required for this operation; see chapter 6.8, page 37. The 'Template on Card' mode does not store fingerprint templates to the AR402 memory but will write them onto iCLASS cards instead. The reader verifies authorized users by comparing the fingerprint template stored on the card with the scanned finger of the card holder. If the two match, the reader will send the card number and facility code to the controller.
'Template on Card' offers a good alternative using biometric readers in a Wiegand configuration as users will not have to enroll on multiple readers.

Requirements for the 'Template on Card' mode:
- Wiegand configuration
- 16K2 or 16K16 iCLASS cards
- Read/write key to the protected application area of your iCLASS cards

Steps to write templates to iCLASS cards.

Steps	Enter	Reader Indication LEDs/Sensor	Buzzer
1. Admin Mode	*	Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Enrollment ToC	16 #	Green LED ●○○○ flashing	
		Sensor on	
4. Apply 2 Fingers 3x each[1]	3 x + 3 x	If successful: Green LEDs ●●●● flashing	
5. Present Card until the writing process is completed		Green LED ●○○○ flashing	Beep
6. Enroll additional Fingers?	Yes / No	Sensor on	
7. Escape Enrollment ToC or wait for Timeout	###		

[1] The table below shows the AR402 indication guiding the user through each step of the enrollment process. Repeat these steps for the second finger. The LED indication is identical for finger 2.

LED Indication	Detailed Enrollment Steps
Green LED ●○○○ flashing	Scan finger 1 a first time
Green LED ●○○○ on	Remove finger 1 from the sensor
Green LED ○●○○ flashing	Scan finger 1 a second time
Green LED ●●○○ on	Remove finger 1 from the sensor
Green LED ○○●○ flashing	Scan finger 1 a third time
Green LED ●●●○ on	Remove finger 1 from the sensor

6.4 Change Admin Code

Default Admin Code: '1234'
For security reasons it is advisable to change the Admin Code!
The Admin Code may be 4 to 8 digits long.
We recommend the Admin Finger feature as it offers the most effective protection for the AR402 Admin Mode; see chapter 6.3.1, page 30.

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	# 99 #	Green LEDs ●●○○ on	
2. Default Admin Code 1234 or enter your Admin Code	_____ #	Green LEDs ●●●○ on	
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Change Admin Code	15 #	Green LEDs ○●●○ flashing	Beep
5. New Admin Code (Default = 1234)	[4 - 8 digits]	Green LEDs ●●○○ flashing	Beep
6. Escape Function Menu or wait for Timeout	###		

6.5 Define the Number of Digits for Fingerprint Numbers

In the enrollment process a Fingerprint Number needs to be entered as a unique ID.
Set the length of Fingerprint Numbers to a value between 2 and 9 digits (Default = 5).

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Number of digits for Finger ID (Default = 5)	16 #	Green LEDs ○○●● flashing	Beep
5. E.g. enter '3' for 3-digit Fingerprint Numbers (2 - 9 digits)	[no. of digits] #	Green LEDs ●●○○ flashing	Beep
6. Escape Function Menu or wait for Timeout	###		

6.6 Delete a specific Template

Remove a single Fingerprint Number (Finger ID) with its template from the AR402 memory.

Steps	Enter	Reader Indication LEDs/Sensor	Buzzer
1. Admin Mode	✱	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Delete a specific Finger ID	13 #	Green LEDs ●●●● flashing	Beep
4. Finger ID	_____ #	if successful: Green LEDs ●●●● flashing	Beep
5. Delete additional Finger IDs?	Yes / No		
6. Escape Function Menu or wait for Timeout	###		

6.7 Delete all Templates

ATTENTION

Notice.
This entry deletes all enrolled fingerprints including the Admin Finger of the reader's memory!

Steps	Enter	Reader Indication LEDs/Sensor	Buzzer
1. Admin Mode	✱	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Delete Memory	1357 #	Red LEDs ●●●● flashing	3x Beep
4. Confirm 'Delete Memory'	✱	if successful: Green LEDs ●●○○ on	Beep
5. Escape Function Menu or wait for Timeout	###		

Red LEDs after pressing ✱ indicate that the memory was not deleted.
The procedure needs to be repeated.

6.8 Enable/Disable iCLASS (AR402-iCLASS only)

In its default setting the iCLASS mode is enabled on AR402-iCLASS readers.
This mode reads fingerprints and iCLASS card numbers alternatively.

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. iCLASS Menu	24 #	Green LEDs ○○●● flashing	Beep
Enable iCLASS (Default)	1 #	Green LEDs ●●○○ flashing	Beep
or Disable iCLASS	0 #	Green LEDs ●●○○ flashing	Beep
5. Escape Function Menu or wait for Timeout	###		

6.9 Enable ‘Template on Card’ (AR402-iCLASS only)

In its default setting the iCLASS mode is enabled on AR402-iCLASS readers.
This mode reads fingerprints (identification) and iCLASS card numbers alternatively.
Enable the ‘Template on Card’ (ToC) mode which compares the template stored on the iCLASS card against the finger applied to the biometric sensor (verification) and then sends the card number to the controller. Available options are:

- 16K16 or 16K2 iCLASS cards
- disable or enable identification and enrollment to the AR402 memory in addition to ToC.

The AR402 needs to load the key to the protected application area of your iCLASS cards.

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Card Type	05 #	Green LEDs ○○●● flashing	Beep
iCLASS 16K16	1 #	Green LEDs ●●○○ flashing	Beep
or iCLASS 16K2	4 #	Green LEDs ●●○○ flashing	Beep
5. iCLASS Menu	24 #	Green LEDs ○○●● flashing	Beep
‘ToC only’	2 #	Green LEDs ●●○○ flashing	Beep
or ‘ToC + AR402 memory’	3 #	Green LEDs ●●○○ flashing	Beep
6. Load standard iCLASS key	0409 #	if successful: Green LEDs ●●●● flashing	Beep

How to write templates onto iCLASS cards is described above; see chapter 6.3.3, page 34.

6.10 Select 37-bit or 26-bit Format

These settings only apply to the trigger signal of the reader's biometric sensor to the access controller. The facility code of iCLASS cards is sent to the access controller untouched and independent of these settings. In Wiegand configurations the format of the biometric sensors trigger signal to the access controller can be defined (e.g. set the biometric sensor's format to 26-bit format if 26-bit iCLASS cards are used).

Steps	**Enter**	**Reader Indication**	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Format	19 #	Green LEDs ○○●● flashing	Beep
5. Set 37-bit with Facility Code (Default)	0 #	Green LEDs ●●○○ flashing	Beep
or 26-bit with Facility Code	1 #	Green LEDs ●●○○ flashing	Beep
6. Escape Function Menu or wait for Timeout	###		

6.11 Set Facility Code

These settings only apply to the trigger signal of the reader's biometric sensor to the access controller. The Facility Code of iCLASS cards is sent to the access controller untouched and independent of these settings. In Wiegand configurations you can set the Facility Code of the biometric sensor according to your requirements; see also chapter 6.10, page 39.
Set the Facility Code for 37-bit to a value between 0 and 65535 (Default = 830)
Set the Facility Code for 26-bit to a value between 0 and 255 (Default =1)

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Facility Code	20 #	Green LEDs ○○●● flashing	Beep
5. Set 37-bit (0 … 65535)	[1 - 5 digits] #	Green LEDs ●●○○ flashing	Beep
or 26-bit (0 … 255)	[1 - 3 digits] #	Green LEDs ●●○○ flashing	Beep
6. Escape Function Menu or wait for Timeout	###		

If both fingers and iCLASS cards are employed in a Wiegand configuration your range of fingerprint numbers must not overlap with your range of card numbers!

6.12 Select Keypad Entry Transmission Mode

In its default setting the AR402 sends each keypad entry via Wiegand output to the access controller. Alternatively, select transmission modes sending

- no keypad entries at all or
- all keypad entries except the asterisk key

Steps	Enter	Reader Indication LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Keypad Signal Mode	26 #	Green LEDs ○○●● flashing	Beep
5. Enable signal for all keys (Default)	0 #	Green LEDs ●●○○ flashing	Beep
or Disable signal for all keys	1 #	Green LEDs ●●○○ flashing	Beep
or Disable signal for * key	2 #	Green LEDs ●●○○ flashing	Beep
6. Escape Function Menu or wait for Timeout	###		

6.13 Set Keypad Backlight Color

Steps to change the AR402 keypad backlight color.

Steps	Enter	Reader Indication			
		LEDs/Sensor			Buzzer
1. Admin Mode	*		Sensor on		
2. Apply Admin Finger		Green LEDs		on	
or enter Admin Mode with Admin Code	# 99 # [Code] #				
3. Change Backlight Color	88 #	Red LEDs		flashing	3x Beep
4. White (Default)	0	Red LEDs		flashing	
or Red	1	Red LEDs		flashing	
or Green	2	Red LEDs		flashing	
or Blue	3	Red LEDs		flashing	
or Yellow	4	Red LEDs		flashing	
or Purple	5	Red LEDs		flashing	
or Light Blue	6	Red LEDs		flashing	
or Light Red	7	Red LEDs		flashing	
5. Escape or wait for Timeout	###				Beep

6.14 Reset - Switch to Wiegand Mode

This function allows you to reset the AR402 to Wiegand mode and its factory defaults.
All individual settings like a changed Admin Code will be affected. Enrolled fingers however will remain untouched.

Steps	Enter	Reader Indication			
		LEDs/Sensor			Buzzer
1. Admin Mode	*		Sensor on		
2. Apply Admin Finger		Green LEDs		on	
or enter Admin Mode with Admin Code	# 99 # [Code] #				
3. Enable Wiegand Mode	1 #	Red LEDs		on	
Device resets to all defaults and reboots					

6.15 Quick Guide to Wiegand Mode Admin Functions

Enter	Function		Page
# 99 #	Enable Admin Mode	or enter instead: ✱ [Admin Finger]	
1234 #	Enter Default Admin Code (or your Admin Code)		
1 #	Reset - Switch to Wiegand Mode		42
12 #	Enroll User		33
16 #	Enroll User to iCLASS Card (AR402-iCLASS only)		34
13 #	Delete a specific Template		36
1357 # ✱	Delete all Templates		36
88 #	Set Keypad Backlight Color		42
14 #	Switch to Function Menu		
30 #	Enroll Admin Finger 1		31
31 #	Enroll Admin Finger 2		
301 #	Delete Admin Finger 1		32
311 #	Delete Admin Finger 2		
15 #	Change Admin Code Default = 1234 (4-8 digits)		35
24 #	Select iCLASS Mode (AR402-iCLASS only) Default = 1 0 = Disabled 1 = Read card number 2 = 'Template on Card' (ToC) 3 = ToC & AR402 memory		37, 38
16 #	Define the Number of Digits for Fingerprint Numbers Default = 5 (2-9 digits)		35
19 #	Select 37-bit or 26-bit Format Default = 0 0 = 37-bit 1 = 26-bit		39
20 #	Set Facility Code Default = 830 0-65535 (37-bit) Default = 1 0-255 (26-bit)		40
26 #	Select Keypad Entry Transmission Mode Default = 0 0 = Transmit all key entries 1 = Transmit no key entries 2 = Transmit key entries except ✱		41

6.15.1 Quick Guide to Template on Card (ToC)

Meaning	Enter
Enable mode iCLASS16k16 / ToC only	✱ [Admin Finger] 14 # 05 # 1 # 24 # 2 # ### or # 99 # [Admin Code] # 14 # 05 # 1 # 24 # 2 # ###
Enable mode iCLASS16k2 / ToC only	✱ [Admin Finger] 14 # 05 # 4 # 24 # 2 # ### or # 99 # [Admin Code] # 14 # 05 # 4 # 24 # 2 # ###
Enable mode iCLASS16k16 / ToC + AR402 memory	✱ [Admin Finger] 14 # 05 # 1 # 24 # 3 # ### or # 99 # [Admin Code] # 14 # 05 # 1 # 24 # 3 # ###
Enable mode iCLASS16k2 / ToC + AR402 memory	✱ [Admin Finger] 14 # 05 # 4 # 24 # 3 # ### or # 99 # [Admin Code] # 14 # 05 # 4 # 24 # 3 # ###
Enroll one finger to iClass card	✱ [Admin Finger] 16 # 3x ☝ 3x ☝ present card ### or # 99 # [Admin Code] # 16 # 3x ☝ 3x ☝ present card ###
Enroll fingers to multiple iClass cards	✱ [Admin Finger] 16 # • 3x ☝ 3x ☝ present card • 3x ☝ 3x ☝ present card • 3x ☝ 3x ☝ present card … ###
Delete entire AR402 memory	✱ [Admin Finger] 1357 # ✱ or # 99 # [Admin Code] # 1357 # ✱
Load standard iCLASS keys[1]	✱ [Admin Finger] 14 # 0409 # or # 99 # [Admin Code] # 14 # 0409 #

[1] The iCLASS keys need to be loaded once only. Even after an AR402 reset or firmware update reloading the iCLASS keys is not required.

7 AD102 Mode

The access control solution of AD102 with the AR402 biometric access reader was designed to control one access point. System settings are to be entered on the AR402 keypad and via the AD102 DIP switch. Also refer to the AD102 manual for further information.
AR402 settings are referred to as Admin Functions which include features like enrolling fingerprints, deleting fingerprints, AR402 reset, etc.
These Admin Functions are protected by the Admin Code which by default is set to: '1234'.

We recommend to disable the default Admin Code by employing the Admin Finger feature (see chapter 7.5.1, page 48) or alternatively by replacing it with your own individual Admin Code; see chapter 7.6, page 52.

There is an additional emergency access code to the Admin Mode for AR402 with unknown Admin Fingers and Admin Codes. The access code is based on the reader's ID, a 12-digit hexadecimal code, printed on the inside of the AR402, e.g. 672692150000. The zeros may be omitted in print; see chapter 3.1, page 13.
Please contact the relevant Kaba support personnel for your access code.

7.1 Reset – Switch to AD102 Mode

As a first step in enabling the AR402 to work with an AD102 set the reader to AD102 mode.
By doing so the reader also is being reset to its defaults. All individual settings like a changed Admin Code or the PIN Mode will be affected. Enrolled fingers however will remain untouched.
Disconnect the RS-485 data wires from the AD102 prior to resetting to AD102 mode.
Reconnect the RS-485 data wires once done.

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Enter Admin Mode	# 99 #	Green LEDs ●●○○ On	
2. Default Admin Code 1234 or enter your Admin Code	_____ #	Green LEDs ●●●○ On	
3. Enable AD102 Mode	3 #	Red LED ○○○● Flashing	
Device resets and signals its RS-485 offline status			

7.2 Automatic Pairing

AR402 and AD102 exchange data in encrypted form. In order for the encrypted data exchange to work, reader and AD102 need to be paired as a second step. These initial two steps are required for proper operation.

Steps for pairing AR402 and AD102

1. Remove power from the AD102
2. Set DIP switch 2 to position ON
3. Power up the AD102 and wait until its green status LED is lit permanently
4. Switch off the AD102 again
5. Set DIP switch 2 to position OFF
6. Power up the AD102 and wait until its green status LED will flash quickly.
   The system is now operational.

Unless set to AD102 mode, the reader cannot go online.
Unless AR402 and AD102 are paired, the reader cannot cause the AD102 to open the door.

7.3 Status Indication

The table below gives an overview of AR402 status indication via the four green/red LEDs and the buzzer in AD102 mode. Generally the AR402 confirms each key entry acoustically by a short beep and visibly by deactivating the keypad backlight briefly.
AR402 are delivered in Wiegand mode, indicated by the four LEDs lit red when put into operation. Set the reader to AD102 Mode; see chapter 7.1, page 45.

Status	**Reader Indication**		
	LEDs		Buzzer
AD102 mode - online and idle	LEDs	○○○○ off	
AD102 mode - offline	Red LED	○○○● flashing	
Access granted	Green LEDs	●●●● on	1x Beep
Access denied	Red LEDs	●●●● on	2x Beep
Access point blocked	Red LEDs	●●●● on	
Access point permanently open	Green LEDs	●●●● on	
Error / Incorrect entry	Red LEDs	●●●● flashing 3x	3x Beep
Pre-alarm	Red LEDs	●●●● flashing	Beeping

For more details on the reader's signaling in its various states please refer to the following chapters.

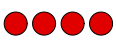
7.4 Access Procedure and Indication

7.4.1 Finger only

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Press	*	 Sensor on	
2. Apply Finger		if granted: Green LEDs  on	Beep
		if denied: Red LEDs  flashing 3x	3x Beep

7.4.2 PIN only

Optionally the Direct Access PIN allows for PIN only access; see chapter 7.11, page 56.

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Enter Direct Access PIN-1 (or 2)	[4 - 8 digits]	if granted: Green LEDs  on	Beep
		if denied: Red LEDs  flashing 3x	3x Beep

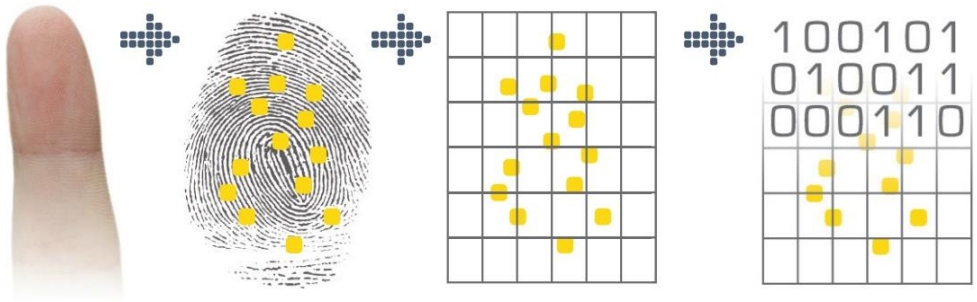
7.4.3 Finger & PIN

In its AD102 default state the AR402 does not require PINs for authentication.
Optionally the PIN Mode may be enabled; see chapter 7.7, page 53.

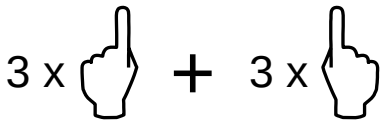
Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Press	*	Green LEDs  flashing	
2. Enter PIN	[PIN]	Sensor on	
3. Apply Finger		if granted: Green LEDs on	Beep
		if denied: Red LEDs  flashing 3x	3x Beep

7.5 Enrollment

The AR402 identifies authorized users by reading their fingerprints and optionally their PINs. Successful identification sends a trigger signal to the AD102 Single Door Unit.
Fingerprint authentication requires authorized users to have enrolled their fingerprints in advance with a unique Fingerprint Number.
Enrollment means to capture a live finger, to identify minutia points that form a unique pattern, and to then encode it. This code (template) is saved to the reader's memory; it cannot be reconverted into an image. The AR402 does not store fingerprint images.



Enrollment is performed on the AR402.
The AR402 assigns 2 fingers (e.g. the left index finger and the right index finger) to a unique ID, or Fingerprint Number. Each of the two fingers is scanned three times.



The biometric sensor reads fingerprints best when placing your finger on the sensor with some pressure.

Bright daylight may affect the function of the biometric sensor.
Shadowing the sensor with your hand will help.

For more guidance on how to best place the finger on the biometric sensor please refer to the appendix; see chapter 8.1, page 65.

7.5.1 Admin Finger

The Admin Finger is a feature to safeguard the AR402 Admin Functions by biometrics. The Admin Finger replaces and disables the default Admin Code '1234' (or your individual Admin Code).
A maximum of two users may enroll an Admin Finger in addition to their regular enrollment for access.
As a fallback there is a 6-digit Admin Code for each of the two Admin Fingers which is set during the Admin Finger enrollment process.
We recommend the Admin Finger feature as it offers the most effective protection for the AR402 Admin Functions. It also allows quicker access to the Admin Mode than entering # 99 # 1234 #.
Admin Fingers do not trigger access requests. Enroll a different finger as Admin Finger than for access.
Attempts to enroll a finger twice will be denied.

7.5.1.1 Enroll Admin Finger

Steps to enroll Admin Finger-1 or Admin Finger-2

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	# 99 #	Green LEDs ●●○○ on	
2. Default Admin Code 1234 or enter your Admin Code	_____ #	Green LEDs ●●●○ on	
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Enroll Admin Finger-1	30 #	Green LEDs ○●●○ flashing	Beep
or Admin Finger-2	31 #	Green LEDs ○●●○ flashing	Beep
5. Admin Code Finger-1 (or 2)	[6 digits] #	Green LED[1] ●○○○ flashing	
		 Sensor on	
6. Apply 2 Fingers each 3x[1]	3 x + 3 x	If successful:	Beep

[1] The table below shows the AR402 indication guiding the user through each step of the enrollment process. Repeat these steps for the second finger. The LED indication is identical for finger 2.

LED Indication	Detailed Enrollment Steps
Green LED ●○○○ flashing	Scan finger 1 a first time
Green LED ●○○○ on	Remove finger 1 from the sensor
Green LED ○●○○ flashing	Scan finger 1 a second time
Green LED ●●○○ on	Remove finger 1 from the sensor
Green LED ○○●○ flashing	Scan finger 1 a third time
Green LED ●●●○ on	Remove finger 1 from the sensor

7.5.1.2 Unlocking Admin Mode with Admin Finger

Steps to access the AR402 Admin Mode with the Admin Finger

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	✱	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
3. move on to desired option e.g. Enrollment	12 #		

Alternatively enter the Admin Finger's Admin Code.
The default Admin Code '1234' is disabled once an Admin Finger is enrolled.

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	# 99 #	Green LEDs ●●○○ on	
2. Admin Code Finger-1 (or 2)	[6 digits] #	Green LEDs ●●●○ on	
3. move on to desired option e.g. Enrollment	12 #		

7.5.1.3 Delete Admin Finger(s)

Steps to delete the Admin Finger(s)

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	✱	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Delete Admin Finger-1	301 #		Beep
or Admin Finger-2	311 #		Beep

Once the Admin Finger(s) is/are deleted the AR402 Admin Code is reset to its default '1234'.

7.5.1.4 Effects of AR402 Reset or Delete All Templates on Admin Finger(s)

Operation	Enter	Effects
Reset to AD102	✱ [Admin Finger] 3 # or # 99 # [Admin Code] # 3 #	Admin Finger(s) will remain untouched and Admin Code will be reset to '1234'
Delete Memory	✱ [Admin Finger] 1357 # ✱ or # 99 # [Admin Code] # 1357 # ✱	Admin Finger(s) will be deleted and Admin Code will be reset to '1234'

7.5.2 Enroll User

Steps to enroll fingers to the AR402 memory.

The Fingerprint Number is affected by the AD102 settings. If it was set to Office Mode or Two Door Mode the first digit of the Fingerprint Number will trigger varying access functions.
E.g. the Office Mode allows for opening the door according to the set door opening time or permanently depending on the Fingerprint Number's first digit.
First digit = 1 Set door opening time
First digit = 2 Door open permanently
First digit ≠ 1 or 2 No access permission

Steps	Enter	Reader Indication LEDs/Sensor	Buzzer
1. Admin Mode	*	Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Enrollment	12 #	Green LEDs ●●●● flashing	
4. Enter Fingerprint Number[1] (Default no. of digits = 5)	_____ #	Green LED[2] ●○○○ flashing	
		Sensor on	
5. Apply 2 Fingers 3x each[2]	3 x + 3 x	If successful: Green LEDs ●●●● flashing	Beep
6. Enroll additional Fingers?	Yes No		
7. Escape Enrollment or wait for Timeout	#		

1 With the PIN mode enabled enter your PIN after entering the Fingerprint Number and '#'. The flashing, green LEDs 1 and 4 will indicate the reader to expect your PIN now. Confirm your entry by entering '#'.

2 The table below shows the AR402 indication guiding the user through each step of the enrollment process. Repeat these steps for the second finger. The LED indication is identical for finger 2.

LED Indication	Detailed Enrollment Steps
Green LED ●○○○ flashing	Scan finger 1 a first time
Green LED ●○○○ on	Remove finger 1 from the sensor
Green LED ○●○○ flashing	Scan finger 1 a second time
Green LED ●●○○ on	Remove finger 1 from the sensor
Green LED ○○●○ flashing	Scan finger 1 a third time
Green LED ●●●○ on	Remove finger 1 from the sensor

Entering a Fingerprint Number with an incorrect number of digits, an already existing Fingerprint Number, or attempts to enroll already enrolled fingers will prompt an error indication (all red LEDs flashing three times) and cause the reader to return to its idle state.

7.6 Change Admin Code

Default Admin Code = 1234.
For security reasons it is advisable to change the Admin Code!
The Admin Code may be 4 to 8 digits long.
We recommend the Admin Finger feature as it offers the most effective protection for the AR402 Admin Mode; see chapter 7.5.1, page 48.

Steps	**Enter**	**Reader Indication**	
		LEDs/Sensor	Buzzer
1. Admin Mode	# 99 #	Green LEDs ●●○○ on	
2. Default Admin Code 1234 or enter your Admin Code	_____ #	Green LEDs ●●●○ on	
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Change Admin Code	15 #	Green LEDs ○●●○ flashing	Beep
5. New Admin Code (Default = 1234)	[4 - 8 digits] #	Green LEDs ●●○○ flashing	Beep
6. Escape Function Menu or wait for Timeout	###		

7.7 Enable PIN Mode

The AR402 in its AD102 default state requires biometric identification only. Enable the PIN Mode for additional authentication by PIN. Once the PIN mode is enabled PINs are set in each enrollment process after entering the Fingerprint Number.
Set the length of PINs to a value between 2 and 9 digits (Default = 0).

Consider whether or not to enable the PIN Mode prior to enrolling any users.
Fingerprints enrolled before the PIN Mode was enabled were not given a PIN and cannot gain access. These users need to be enrolled all over again with a valid PIN.

Consider whether or not to change the number of digits for PINs as all fingerprints with invalid PINs (too short/too long) cannot gain access.
These users need to be enrolled all over again with a valid PIN.

Admin Fingers are affected by the PIN Mode insofar as entering a PIN is required for unlocking the Admin Mode. Enter any PIN according to the defined length.
The enrollment process of Admin Fingers is not affected by the PIN Mode.

Steps	**Enter**	**Reader Indication**	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Number of digits for PIN (Default = 0; disabled)	21 #	Green LEDs ○○●● flashing	Beep
5. E.g. enter ‘4’ for 4-digit PINs (2 - 9 digits)	[no. of digits] #	Green LEDs ●●○○ flashing	Beep
6. Escape Function Menu or wait for Timeout	###		

7.8 Define the Number of Digits for Fingerprint Numbers

In the enrollment process a Fingerprint Number needs to be entered as a unique ID.
Set the length of Fingerprint Numbers to a value between 2 and 9 digits (Default = 5).

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Number of digits for Finger ID (Default no. of digits = 5)	16 #	Green LEDs ○○●● flashing	Beep
5. E.g. enter '3' for 3-digit Fingerprint Numbers (2 - 9 digits)	[no. of digits] #	Green LEDs ●●○○ flashing	Beep
6. Escape Function Menu or wait for Timeout	###		

7.9 Delete a specific Template

Remove a single Fingerprint Number (Finger ID) with its template from the AR402 memory.

Steps	Enter	Reader Indication LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Delete a specific Finger ID	13 #	Green LEDs ●●●● flashing	Beep
4. Finger ID	_____ #	if successful: Green LEDs ●●●● flashing	Beep
5. Delete additional Finger IDs?	Yes / No		
6. Escape Function Menu or wait for Timeout	###		

7.10 Delete all Templates

ATTENTION

This entry deletes all enrolled fingerprints including the Admin Finger of the reader's memory!

Steps	Enter	Reader Indication LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Delete Memory	1357 #	Red LEDs ●●●● flashing	3x Beep
4. Confirm 'Delete Memory'	*	if successful: Green LEDs ●●○○ on	Beep
5. Escape Function Menu or wait for Timeout	###		

Red LEDs after pressing * indicate that the memory was not deleted.
The procedure needs to be repeated.

7.11 Set Direct Access PIN

The Direct Access PIN is an AR402 feature in combination with the AD102 allowing for authentication by PIN only. It is helpful when needing to grant access to people who have not been enrolled e.g. while away telling a surprising visitor the Direct Access PIN on the mobile phone or as the solution for people with unreadable fingerprints.
The AR402 supports two Direct Access PINs which both need to be of the same length.
Minimum length: 4 digits / Maximum length: 8 digits.
The Direct Access PIN is not affected by the AR402 PIN Mode settings (on or off, number of digits).

The Direct Access PIN is affected by the AD102 settings. If it was set to Office Mode or Two Door Mode the first digit of the Direct Access PIN will trigger varying access functions.
E.g. the Office Mode allows opening the door for the standard door opening time or permanently depending on the Direct Access PIN's first digit.
First digit = 1 standard door opening time
First digit = 2 door open permanently
First digit ≠ 1 or 2 no access permission

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Enable Direct Access PIN-1	40 #	Green LEDs ○●●○ flashing	Beep
or Direct Access PIN-2	41 #	Green LEDs ○●●○ flashing	Beep
5. Enter Direct Access PIN-1 (or 2)	[4 - 8 digits] #	Green LEDs ●●○○ flashing	Beep
6. Escape Function Menu or wait for Timeout	###		

Anyone who knows the Direct Access PIN can gain access!

As a safeguard the system will disable Direct Access PINs for three minutes after entering five mismatches. With another five mismatches after the three minute period the Direct Access PIN will be disabled for ten minutes. Two more mismatches will delete the Direct Access PINs altogether.

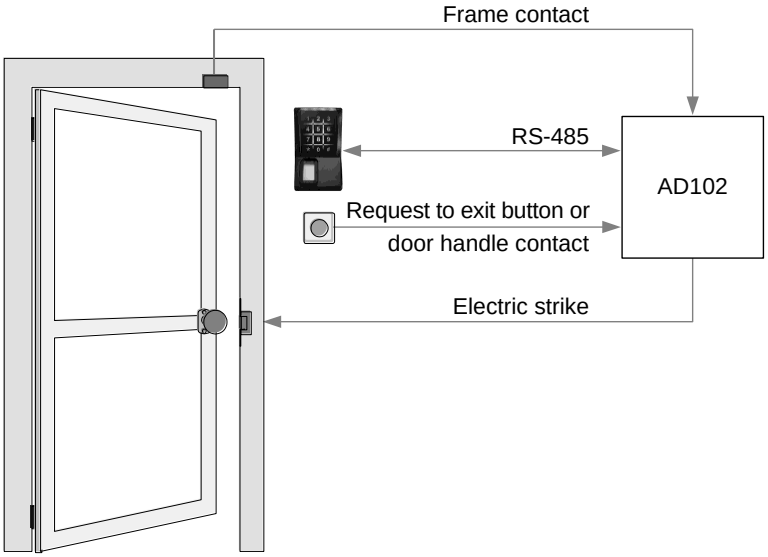
7.12 Delete Direct Access PIN

Remove a Direct Access PIN from the reader's memory.

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Delete Direct Access PIN-1	401 #	LEDs ○○○○ off	
or Direct Access PIN-2	411 #	LEDs ○○○○ off	

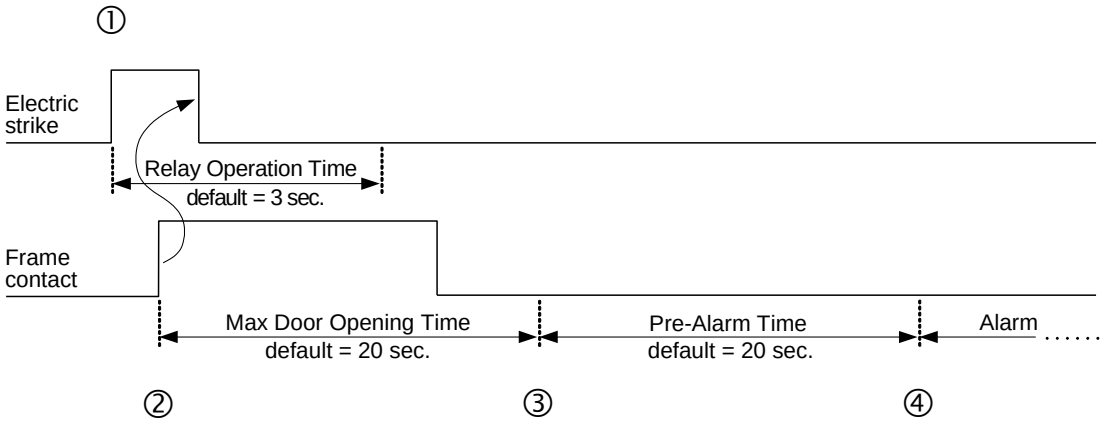
7.13 AD102 Door Control and Monitoring

AR402, AD102 and peripheral equipment



An introduction to the door control and monitoring features:

1. The Relay Operation Time is the period of time for the AD102 relay to be activated from the point on it was triggered by an authorized booking, the request to exit button or the door handle contact.
2. The Max Door Opening Time is the period of time to elapse before the pre-alarm is signaled on the AR402. It begins as soon as the door is opened (the frame contact switched) which also causes the relay to reset to its deactivated state.
3. The Pre-Alarm Time is the period of time to indicate a first alarm on the AR402 reminding the user to close the door (door open too long). The reader signals the pre-alarm by flashing LEDs and beeping. Reset the Pre-Alarm by closing the door.
4. As a last step the AD102 relay-2 is activated (indefinitely) which may serve as a trigger for an external alarm device if the Pre-Alarm Time went by without the door being closed.
   Relay-2 is immediately activated by a forced door, i.e. the frame contact switches and was not preceded by a valid access via AR402, request to exit button or the door handle contact.
   Reset the alarm either by a valid access request on the AR402 or by operating the alarm reset button connected to AD102 Opto-IN-3.



7.13.1 Adjust Operation Time of AD102 Relay-1

Relay-1 is the AD102 output for electrical locking hardware (electric strike, magnet).
Adjust the period of time for relay-1 to be activated after authorized access requests by setting it to a value between 001 and 999 corresponding to a period from 0.1 to 99.9 sec (Default = 3 sec).

Frame contact installed:
Opening the door will discontinue the set Operation Time for Relay-1.
Leaving the door closed will cause AD102 relay-1 to operate and the AR402 to indicate green for the set period of time.

No frame contact installed:
AD102 relay-1 will operate and the AR402 indicate green for the set period of time.

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Set Relay-1 Operation Time (Default = 030)	17 #	Green LEDs ●○○● flashing	Beep
5. E.g. enter '050' for 5 sec.	[3 digits] #	Green LEDs ●●○○ flashing	Beep
6. Escape Function Menu or wait for Timeout	###		

7.13.2 Adjust Operation Time of AD102 Relay-2

The AD102 Two Door Mode assigns relay-2 as the second output for electrical locking hardware (electric strike, magnet). Adjust the period of time for relay-2 to be activated after authorized access requests by setting it to a value between 001 and 999 corresponding to a period from 0.1 to 99.9 sec (Default = 3 sec).

The AD102 Two Door Mode does not support frame contacts:
The AD102 Relay-2 will operate for the set period of time.

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Set Relay-2 Operation Time (Default = 030)	50 #	Green LEDs ●○○● flashing	Beep
5. E.g. enter '050' for 5 sec.	[3 digits] #	Green LEDs ●●○○ flashing	Beep
6. Escape Function Menu or wait for Timeout	###		

7.13.3 Adjust AD102 Max Door Opening Time

This door monitoring feature is the maximum period of time for the door to be opened before the pre-alarm is signaled on the AR402 prompting to close the door. This period begins with the switching of the frame contact indicating the door was opened. By contrast, forced door events actuate the alarm output, relay-2, immediately; see chapter 7.13, page 58.

Adjust the Max Door Opening Time by setting it to a value between 001 and 999 corresponding to a period from 0.1 to 99.9 sec (Default = 20 sec).

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Set Max Door Opening Time[1] (Default = 200)	50 #	Green LEDs ●○○● flashing	Beep
5. E.g. enter ‘600’ for 1 min.	[3 digits] #	Green LEDs ●●○○ flashing	Beep
6. Escape Function Menu or wait for Timeout	###		

[1] Exception: If the AD102 was set to its Two Door Mode the code ‘50’ does not adjust the Max Door Opening Time but the Operation Time of AD102 Relay-2; see chapter 7.13.2, page 60.

Prerequisite for monitoring the door is an installed frame contact.

7.13.4 Adjust AD102 Pre-Alarm Time

The pre-alarm is signaled on the AR402 prompting to close the door. If the door is not closed during the pre-alarm stage the system activates relay-2, the output for an external alarm device; see chapter 7.13, page 58.

Adjust the period of time after AD102 Max Door Opening Time elapsed and before relay-2 is triggered for an external alarm by setting it to a value between 001 and 999 corresponding to a period from 0.1 to 99.9 sec (Default = 20 sec).

Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Function Menu	14 #	Green LEDs ●●○○ flashing	Beep
4. Set Pre-Alarm Time (Default = 200)	51 #	Green LEDs ●○○● flashing	Beep
5. E.g. enter ‘600’ for 1 min.	[3 digits] #	Green LEDs ●●○○ flashing	Beep
6. Escape Function Menu or wait for Timeout	###		

7.14 Set Keypad Backlight Color

Steps to change the AR402 keypad backlight color

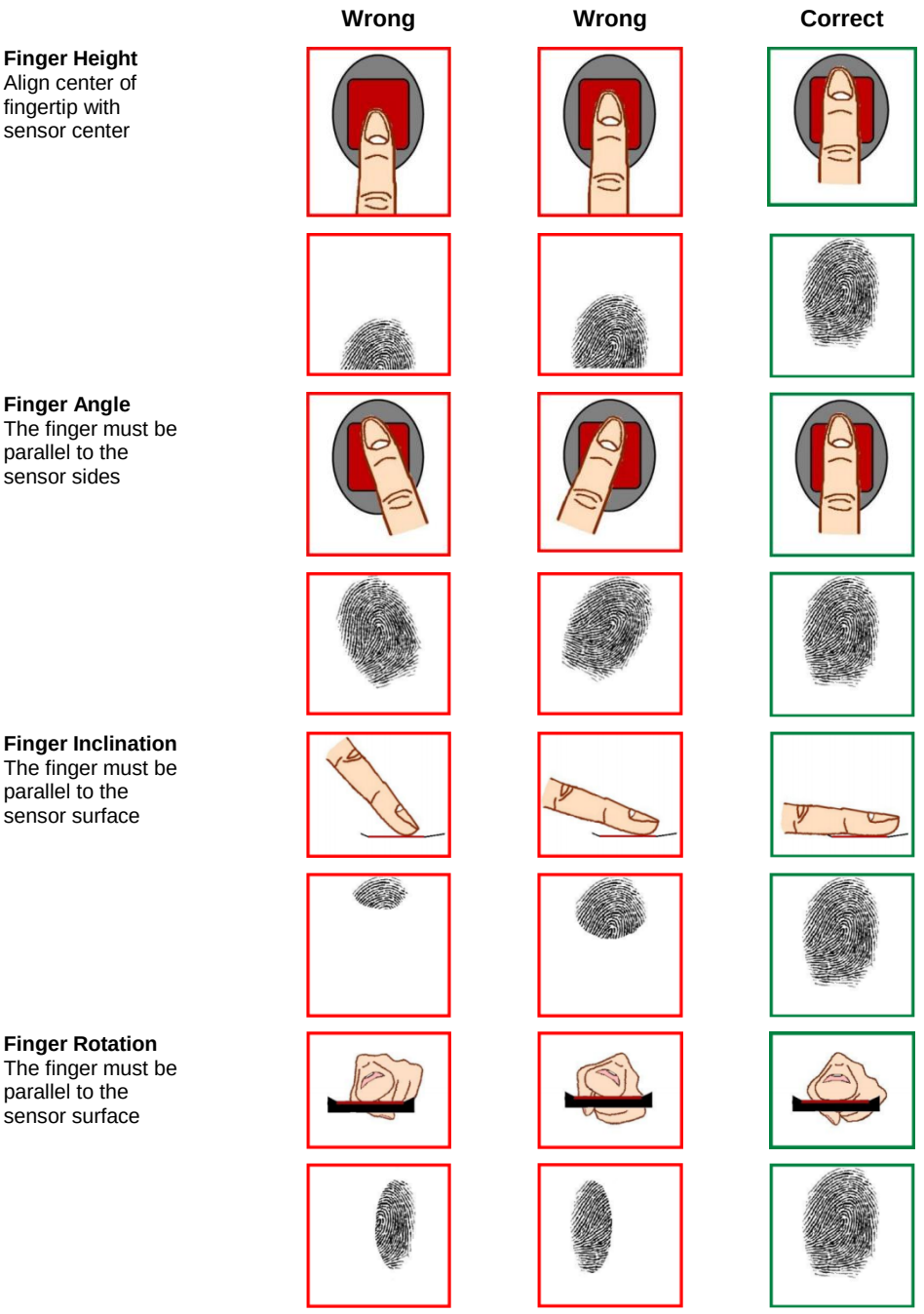
Steps	Enter	Reader Indication	
		LEDs/Sensor	Buzzer
1. Admin Mode	*	 Sensor on	
2. Apply Admin Finger		Green LEDs ●●●○ on	
or enter Admin Mode with Admin Code	# 99 # [Code] #		
3. Change Backlight Color	88 #	Red LEDs ●●●● flashing	3x Beep
4. White (Default)	0	Red LEDs ●●●● flashing	
or Red	1	Red LEDs ●●●● flashing	
or Green	2	Red LEDs ●●●● flashing	
or Blue	3	Red LEDs ●●●● flashing	
or Yellow	4	Red LEDs ●●●● flashing	
or Purple	5	Red LEDs ●●●● flashing	
or Light Blue	6	Red LEDs ●●●● flashing	
or Light Red	7	Red LEDs ●●●● flashing	
5. Escape or wait for Timeout	###		Beep

7.15 Quick Guide to AD102 Mode Admin Functions

Enter	Function		Page
# 99 #	Enable Admin Mode	or enter instead: ✱ [Admin Finger]	
1234 #	Enter Default Admin Code (or your Admin Code)		
3 #	Reset - Manually Switch to AD102 Mode		45
12 #	Enroll User		51
13 #	Delete a specific Template		55
1357 # ✱	Delete all Templates		55
88 #	Set Keypad Backlight Color		63
14 #	Switch to Function Menu		
30 #	Enroll Admin Finger-1		49
31 #	Enroll Admin Finger-2		
301 #	Delete Admin Finger-1		50
311 #	Delete Admin Finger-2		
15 #	Change Admin Code Default = 1234 (4-8 digits)		52
21 #	Enable PIN Mode Default = 0 (2-9 digits)		53
16 #	Define the Number of Digits for Fingerprint Numbers Default = 5 (2-9 digits)		54
40 #	Set Direct Access PIN-1		56
41 #	Set Direct Access PIN-2		
401 #	Delete Direct Access PIN-1		57
411 #	Delete Direct Access PIN-2		
17 #	Adjust Operation Time of AD102 Relay-1		59
50 #	Adjust AD102 Max Door Opening Time		61
51 #	Adjust AD102 Pre-Alarm Time		62
50 #	Adjust Operation Time of AD102 Relay-2 (Two Door Mode)		60

8 Appendix

8.1 Finger Position Recommendations



8.1.1 How to get the best quality

Enrollment needs to be done with extreme care, in order to:

- get the best image quality
- increase recognition performance
- reduce recognition time

It is highly recommended to:

- Maximize the contact between the finger and the sensor
- Exert firm, but not excessive, finger pressure on the surface of the sensor
- Do not press too hard
- Do not slide nor roll the finger across the sensor
- Do not move the finger during acquisition
- Wait for the reader LEDs to light up permanently (stop flashing) before removing the finger
- Shade the sensor with your free hand in case the sensor's function is affected by bright daylight

8.1.2 How to avoid finger recognition issues

When finger biometric data acquisition is difficult, please follow the recommendations below:

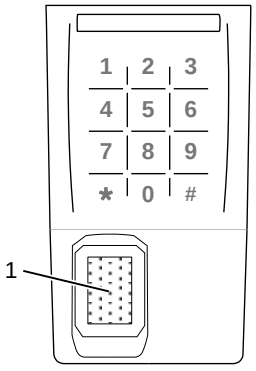
The finger is	Solution
Cold	Warm up the finger
Wet	Wipe the finger
Dry	Warm up the finger and/or add a bit of humidity
Dirty	Wash hands

8.2 Cleaning the Biometric Sensor

The use of a dry cloth is recommended to clean the biometric sensor's surface (1).

Do not use acid liquids, alcohol or abrasive materials.

Make sure to remove all dust or residue with gentle movements, in order not to scratch the biometric sensor's surface.



LIT1077 0314

Kaba Access & Data Systems Americas
2941 Indiana Ave
Winston-Salem, NC 27105
Tel: 1-800-849-8324

www.kaba-adsamericas.com