TLR401 FINGERPRINT KEY

Manual **Version 1.4**

TIMELINK **International GmbH**

TIMELINK **International GmbH**
Mollenbachstrasse 19
D-71229 Leonberg
Phone (0 71 52) 93979-0
Fax (0 71 52) 93979-50
info@de.timelink.com

TLR401 Manual
Version 1.4
Firmware 1.150 or higher

Content

1 General Comments

1.1 Symbols

The following symbols have been used in this manual:

Notice	Helpful tips and special characteristics of the TLR401.
Careful	Possible danger, which – if the warning is not observed – can result in damage to property, or slight to moderate bodily injury.
Caution	Possible danger, which - if the warning is not observed - can result in death or serious bodily injury.

1.2 Device name

This manual outlines the TLR401 and the supported functions.

1.3 Intended Usage

The device may only be used under conditions and for purposes for which it has been designed.
(See Chapter Environment Conditions)

1.4 Protection Class

The device conforms to the conditions of protection class IP65. Protection class III EN60950-1.

Protection class IP65 DIN EN 60529

1.5 Safety Measures

The device has been built according to the current and recognized technical safety rules EN60950-1 and left our manufacturing facility in perfect condition. Improper handling and operation outside the specified conditions can result in dangers due to electrical current. This can endanger the lives of persons and damage the device.

1.6 Before Commissioning

Inspect the device for visible damage resulting from shipment or improper storage. Do not commission a damaged device.

Careful

The device may only be operated with DC voltage 10 to 28V DC.

The device is protected against polarity reversal.

1.7 Operation

Do not subject the device to any mechanical stresses such as impacts, violent shaking or heavy loads. Impacts and shaking can damage the electronics.

1.8 Installation and Service

The device may only be opened by trained specialists. Disconnect the device from the power source before opening.

- You may only perform repairs in collaboration with **Time**Link International.

1.9 CE Conformance

This device is manufactured according to the safety requirements of EN 60950.

Safety of electrical equipment

- European Norm EN 60950

This device complies with interference resistance criteria according to EN 55022; EN 61000-3-2/-3; EN 55024

2 Technical Data

2.1 Mechanical Structure

- Plastic body + metal wall mount panel
- Resin sealed electronics
- 12 inch cable molded into body

2.2 Hardware Features

- Fingerprint biometric sensor
- iCLASS- reader
- 12-key Keypad
- Beeper
- 4 red LEDs and 4 green LEDs
- Keyboard illumination
- 3 Opto-Inputs
- Wiegand output
- RS485 host interface

2.3 Biometric Sensor

- Thin optical sensor
- 500 dpi @ 8 bit per pixel
- Active area: 0,5 x 0,9 in
- Template size: 130...250 bytes
- Memory: 1000 templates (optionally 6000)

2.4 Visual and Audible Indicators

- 4 red LED and 4 green LED user interface
- Beeper (3khz)

2.5 Connection

- Cable with 11 circuits

2.6 Interface

- RS485 interface, 19200 Baud (8/N/1)
- Wiegand Output
- 3 Opto-inputs, active

2.7 Power Supply

- DC Voltage, 10...28V
  Minimum 1A and complying with Limited Power Source according to IEC/EN 60950-1
- Power consumption max 5W

2.8 Environment Conditions

- Temperature range 14° to 122º F
- Indoor and Outdoor
- Protection class IP65

2.9 Dimensions and Weight

- 4,5 in x 2,5 in x 2 in (H x W x D)
- Approx. 0.4 lb

2.10 Cable Specifications

- **RS485**
  Shielded twisted pair cable (4000 feet max)

  Examples:

  1. 2x2 strands litz wire AWG24 (0.4 kcmil)
  2. J-Y(ST)Y 2x2x0,6
  3. CAT 5 ... 7 STP (Shielded Twisted Pair)

- **Wiegand**
  Non-twisted shielded cable (500 feet max)

  Examples:

  1. 10 pair shielded wire AWG22 (0.64 kcmil)

  For shorter distances or using higher supply voltage:

  2. 8 pair AWG24 (0.4 kcmil)

3 Installation

3.1 Installation Requirements

☞ **Notice**

For outdoor use, determine an appropriate place for mounting the TLR401. Avoid mounting in direct sunlight as this may affect the function of the biometric sensor.

Direct sunlight may overheat the TLR401.

3.2 Condition

Check the following for mounting the TLR401

√ Device needs proper clearance.

√ All cabling must be provided, electrical cable, data cable and door opener cabling.

√ Power supply is provided.

3.3 Wiring

Do not install data cables parallel to cables conducting high voltage. If unavoidable, install the data cables in conduit and keep them at a distance of 1 yd to protect them against electromagnetic interference.

4 Operation

4.1 View of the Control Elements

4.2 Basics

The TLR401 is manufactured in two versions:

1. TLR401 with built-in biometrical sensor and keypad
2. TLR401-iCLASS with built-in biometrical sensor and keypad + embedded iCLASS reader

The TLR401 identifies authorized users by scanning their fingerprints (and optionally their PINs and iCLASS cards). Successful identification sends a trigger signal to an access controller within a protected area and is followed by a door lock or release.
The TLR401-iCLASS reads fingerprints and iCLASS cards alternatively.

Fingerprint authentication requires that the authorized user's fingerprints have been enrolled in advance and that they have been linked to a unique User ID.
Enrollment can be performed on the TLR401, which stores the collected data (Templates).

The 'Template on Card' mode allows you to write Templates onto iCLASS cards (currently 16k2 cards only).

The TLR401 can either be run using the RS485 interface or the Wiegand output:

RS485 Configuration Running the reader using the RS485 interface means that administration of the TLR401 is done on the NEXTOR Series access controller.
All administrator functions, except for enrollment, are disabled on the TLR401.
Fingerprint Templates are managed by the access controller and can be distributed to the connected TLR401 readers.

Wiegand Configuration All administrator functions described in this manual, except for enrollment, only apply to the Wiegand configuration. All settings are entered on the keypad of the TLR401.
Fingerprint templates are stored on the TLR401 and cannot be distributed to connected TLR401 readers.

4.3 Basic Operating Principles

General Pressing any key triggers a beep.

Release Beep tone and all LEDs flashing green

Green and Red / Green LEDs Guides an administrator through the setup menus

Red LEDs and Beeps Generally indicates an error

Error Message 3 short beeps and all LEDs flashing red 3 times indicate an error. The desired function was not performed.

3x Key "#" Press "#" three times to reset the reader to keypad default state after typing errors or wait for timeout (10-30 seconds, depending on status) to return to the default position.

4.4 User Operation

4.4.1 Authentication, TLR401:

Authorized users who's fingers have been enrolled and who's PIN have been registered are granted access when entering:

Finger without PIN:	Press ✱	=> Bio-Sensor is illuminated	
	Apply Finger	=> Green LEDs	(Access granted)
Finger plus PIN:	Press ✱	=> Bio-Sensor is illuminated	
(Wiegand)	Apply Finger	=> LEDs flash	(Waiting for PIN entry)
	Enter PIN	=> Green LEDs	(Access granted)
Finger plus PIN:	Press ✱	=> Green and Red LEDs 1 and 4 flash	(Waiting for PIN entry)
(RS485)	Enter PIN	=> Bio-Sensor is illuminated	
	Apply Finger	=> Green LEDs	(Access granted)

4.4.2 Authentication, TLR401-iCLASS:

Authorized users who's fingers have been enrolled and who's iClass cards and PIN have been registered on the access controller are granted access when entering:

Finger:	as above		
Card without PIN:	iCLASS card	=> Beep and short green signal	(Indication card was read)
		=> Green LEDs	(Access granted)
Card plus PIN:	iCLASS card	=> Beep and short green signal	(Indication card was read)
(Wiegand)		=> LEDs flash	(Waiting for PIN entry)
	Enter PIN	=> Green LEDs	(Access granted)
Card plus PIN:	iCLASS card	=> Beep and short green signal (LEDs 2/3)	(Indication card was read)
(RS485)		=> Green and Red LEDs 1 and 4 flash	(Waiting for PIN entry)
	Enter PIN	=> Green LEDs	(Access granted)

4.4.3 Authentication, 'Template on Card' (TLR401-iCLASS only)

Authorized users who's fingers have been stored onto their card and who's iCLASS cards and PIN have been registered on the access controller are granted access when entering:

Card without PIN:	iCLASS card	=> LEDs flash green.	
		Beep when finished reading the card	(Indication card was read)
		=> Green LEDs	(Access granted)
Card plus PIN:	iCLASS card	=> LEDs flash green.	
		Beep when finished reading the card	(Indication card was read)
		=> LEDs flash	(Waiting for PIN entry)
	Enter PIN	=> Green LEDs	(Access granted)

The TLR401-iCLASS reads fingers and iCLASS cards alternatively without having to switch between operating modes.
If a mistype occurs on the keypad simply press the “#” three times to reset and start over.
The various operating modes are configured in the administrator’s menu as described in section 5.

5 Wiegand Configuration - Administrator Functions

With the exception of enrollment all administrator functions described in this section only apply to the Wiegand configuration, i.e. connecting the TLR401 to the access controller via Wiegand.

Administration of the TLR401 with Wiegand is done on the reader. The Fingerprint Key user interface is comprised of the keypad, fingerprint reader and iCLASS reader as input devices and the LEDs and beeper as output devices.

The administrator functions allow administrators to configure the operating modes and the Admin code.

TIMELINK delivers the device with the default Admin Code '1234'.

☞ **Notice** **For security reasons the default Admin Code should be changed. (see below)**

In addition to the Admin Code each device has a fixed access code. This code corresponds with the device's serial number, a 12-digit hexadecimal code, which is printed on the back of the reader. The 12-digit code serves as a basis for calculating the access code if your Admin Code is lost. In this case please contact **TIME**LINK.

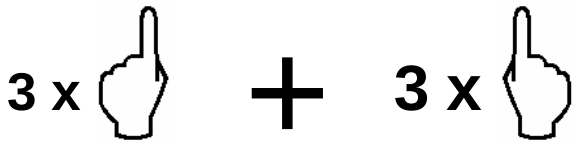
5.1 Change the Admin Code

The default Admin Code is '1234'.
For security reasons it is advisable to change the Admin Code!
The Admin Code can be a 4-digit to 8-digit code.

Admin Mode	**# 99 #**	**Green 1+2**	
Default Admin Code **1234**			
or enter your Admin Code	**xxxx #**	**Green 1+2+3**	
Function Menu	**14 #**	**Green 1+2 flashing**	**Beep**
Change Admin Code	**15 #**	**Green 2+3 flashing**	**Beep**
(Default = 1234)	**4 - 8 digits #**	**Green 1+2 flashing**	**Beep**
Finalize by 3 x #	**###**		
or wait for Timeout			

5.2 Enrollment

The TLR401 assigns 2 different fingers (e.g. left index finger, right index finger) to the unique User ID of a person. Each of the 2 fingers must be scanned 3 times by the Fingerprint Key reader. The biometric sensor reads fingers best when placing your finger on the sensor with some pressure.



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

5.2.1 Enroll user

The fingers of a new user are enrolled by entering the following on the reader's keypad:

Admin Mode Default Admin Code **1234** or enter your Admin Code	**# 99 #** **xxxx #**	**Green 1+2** **Green 1+2+3**
Enter Enrollment Code	**12 #**	**Green 1+2+3+4 flashing**
Enter User ID *	**xxxxx #**	**Green 1 flashing** **Sensor Red**
Apply 2 Fingers 3x		if successful: **Green 1+2+3+4 flashing**
Finalize by 1 x # **or wait for Timeout**	#	

Entering a User ID with an incorrect number of digits, an already existing User ID, or variant IDs with Validation enabled and also if your fingers already have been scanned will prompt an error message (all red LEDs flashing three times) and cause the reader to return to it's default position.

* With Validation enabled enter your User ID a second time. After the first entry of your User ID and the '#' key, the four green quickly flashing LEDs indicate the reader to expect your User ID for a second time.

5.2.2 Write Template onto iCLASS Card (TLR401-iCLASS only)

Setting the reader to 'Template on Card' is required for this operation (see "Choose iCLASS Mode", page 19) and the reader must 'know' the encryption of your iCLASS cards. The 'Template on Card' mode does not store fingerprint templates to the TLR401 but writes them onto iCLASS cards instead. The reader identifies authorized users by comparing the fingerprint templates stored on the card with the scanned finger of the card holder. If the two match the reader will send the facility code and card number to the controller.
'Template on Card' may be expedient where storing biometric data is prohibited. In addition this mode offers a good alternative using biometric readers in a Wiegand configuration as users will not have to enroll on multiple readers.
At this point 'Template on Card' only works with 16K2 iCLASS cards and in a Wiegand configuration.

The TLR401-iCLASS will store the fingers of a new user onto iCLASS cards when entering the following on the keypad:

Admin Mode	**# 99 #**	**Green 1+2**
Default Admin Code **1234** or enter your Admin Code	**xxxx #**	**Green 1+2+3**
Enter Enrollment Code	**16 #**	**Green 1 flashing** **Sensor Red**
Apply 2 Fingers 3x		if successful: **Green 1+2+3+4 flashing**
Apply Card until the writing process is completed		**Green 1 flashing** **Sensor Red**
Enroll next finger or		
Finalize by 3 x # **or wait for Timeout**	**###**	

5.3 Define the Number of Digits for the User ID (optional)

Here the length of the User IDs (Default = 5 digits) can be set to a value between 2 and 9 digits.
In the process of enrollment User IDs need to be entered as a personal and unique ID.

Admin Mode	**# 99 #**	**Green 1+2**	
Default Admin Code **1234**			
or enter your Admin Code	**xxxx #**	**Green 1+2+3**	
Function Menu	**14 #**	**Green 1+2 flashing**	**Beep**
Number of Digits for User ID	**16 #**	**Green 3+4 flashing**	**Beep**
(Default = 5)	**2 - 9 digits #**	if successful:	
		Green 1+2 flashing	**Beep**
Finalize by 3 x #	**###**		
or wait for Timeout			

5.4 Enable Validation of the User ID (optional)

This menu allows you to enable the validation of the User ID for enrollment to eliminate incorrect entries.

Admin Mode	**# 99 #**	**Green 1+2**	
Default Admin Code **1234**			
or enter your Admin Code	**xxxx #**	**Green 1+2+3**	
Function Menu	**14 #**	**Green 1+2 flashing**	**Beep**
Validation of User ID	**22 #**	**Green 3+4 flashing**	**Beep**
Enable	**1 #**	**Green 1+2 flashing**	**Beep**
or Disable (Default)	**0 #**	**Green 1+2 flashing**	**Beep**
Finalize by 3 x #	**###**		
or wait for Timeout			

5.5 Delete Specific User(s)

This function allows you to remove a single user (User ID with its fingerprints) or several users of your choice from memory.

Admin Mode	**# 99 #**	**Green 1+2**
Default Admin Code **1234**		
or enter your Admin Code	**xxxx #**	**Green 1+2+3**
Delete Specific User(s)	**13 #**	**Green 1+2+3+4 flashing**
User ID	**xxxxx #**	if successful: **Green 1+2+3+4 flashing** **Beep**
Optional: More User IDs	**xxxxx #**	**Green 1+2+3+4 flashing** **Beep**
Finalize by 3 x # **or wait for Timeout**	**###**	

5.6 Delete Entire Database

Caution This function deletes all users of the reader's database!

Admin Mode	**# 99 #**	**Green 1+2**
Default Admin Code **1234**		
or enter your Admin Code	**xxxx #**	**Green 1+2+3**
Enter Delete Database	**1357 #**	**Red 1+2+3+4 flashing** **Beep**
Press ✱ key to confirm	**✱**	if successful: **Green 1+2+3** **Beep**
Finalize by 3 x # **or wait for Timeout**	**###**	

If you see red LEDs after pressing ✱ this indicates the database was not deleted and the procedure needs to be repeated.

5.7 Select iCLASS Mode (TLR401-iCLASS only)

In its default setting the iCLASS mode is activated on TLR401-iCLASS readers. This mode reads fingerprints and iCLASS cards alternatively.
This menu allows you to disable the iCLASS module or to enable the 'Template on Card' mode instead (cp. "Enrollment with 'Template on Card' enabled, page 16).

Admin Mode	**# 99 #**	**Green 1+2**	
Default Admin Code **1234**			
or enter your Admin Code	**xxxx #**	**Green 1+2+3**	
Function Menu	**14 #**	**Green 1+2 flashing**	**Beep**
iCLASS Menu	**24 #**	**Green 3+4 flashing**	**Beep**
Enable iCLASS (Default)	**1 #**	**Green 1+2 flashing**	**Beep**
or Enable 'Template on Card'	**2 #**	**Green 1+2 flashing**	**Beep**
or Disable iCLASS	**0 #**	**Green 1+2 flashing**	**Beep**
Finalize by 3 x # **or wait for Timeout**	**###**		

5.8 Define Facility Code

These settings only apply to the trigger signal of the reader's biometric sensor sent to the access controller. The Facility Code of iCLASS cards is sent to the access controller untouched and independent of these settings.
In a Wiegand configuration you can set the Facility Code of the biometric sensor according to your requirements. The Default Facility Code for 37-bit is '830'.

Admin Mode	**# 99 #**	**Green 1+2**	
Default Admin Code **1234**			
or enter your Admin Code	**xxxx #**	**Green 1+2+3**	
Function Menu	**14 #**	**Green 1+2 flashing**	**Beep**
Define Facility Code	**20 #**	**Green 3+4 flashing**	**Beep**
	1 – 5 digits #	**Green 1+2 flashing**	**Beep**
37-bit (Default = 830) 26-bit (Default = 1)	0 … 65535 # 0 … 255 #		
Finalize by 3 x # **or wait for Timeout**	###		

Caution

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

5.9 Choose 37-bit or 26-bit Format

These settings only apply to the trigger signal of the reader's biometric sensor sent to the access controller. The Facility Code of iCLASS cards is sent to the access controller untouched and independent of these settings.
In a Wiegand configuration the format of the biometric sensor's trigger signal to the access controller can be defined (e.g. Set the biometric sensor's format to the 26-bit format if HID cards with 26-bit standard format are used).

Admin Mode	**# 99 #**	**Green 1+2**	
Default Admin Code **1234**			
or enter your Admin Code	**xxxx #**	**Green 1+2+3**	
Function Menu	**14 #**	**Green 1+2 flashing**	**Beep**
Choose Format	**19 #**	**Green 3+4 flashing**	**Beep**
37-bit with Facility Code (Default)	**0 #**	**Green 1+2 flashing**	**Beep**
26-bit with Facility Code	**1 #**	**Green 1+2 flashing**	**Beep**
Finalize by 3 x # **or wait for Timeout**	###		

5.10 Reset - Manually switch to Wiegand mode

This function allows you to reset the TLR401 to its factory defaults. All settings like the changed Admin Code, the enabled Validation of the User ID will be affected. Users however will remain untouched.

The reader will be set to Wiegand mode.

Admin Mode	**# 99 #**	**Green 1+2**
Default Admin Code **1234**		
or enter your Admin Code	**xxxx #**	**Green 1+2+3**
Enable Wiegand Mode	**1 #**	Device resets to all defaults and reboots

5.11 Reset - Manually switch to RS485 mode

This function allows you to manually set the TLR401 to RS485 mode. All settings will be reset. The reader indicates its' offline status by the red flashing LED 4. The TLR401 will automatically go online once it is connected via RS485 to a controller of the NEXTOR series.

Admin Mode	**# 99 #**	**Green 1+2**
Default Admin Code **1234**		
or enter your Admin Code	**xxxx #**	**Green 1+2+3**
Enable RS485 Mode	**2 #**	Device resets and signals its' RS485 offline status

6 RS485 Configuration with NEXTOR Series Access Controller

For detailed information on the administration in the RS485 configuration please turn to the manuals of the NEXTOR Series access controllers.

The TLR401 is controlled by the NEXTOR Series access controller. Administrator functions are carried out on the access controller.

For security reasons the identification of the templates is processed by the TLR401. Templates are managed by the NEXTOR Series access control system and can be distributed to the connected TLR401 readers.

6.1 Status Indication

"Always Open"
All 4 green LEDs are permanently on, further input is accepted.

"Always Closed"
All 4 red LEDs are permanently on, no further input is accepted.

Offline Display
Offline = LED 4 flashing red, no further input is accepted.

User Input is also temporarily disabled when the reader is synchronizing data from the NEXTOR Series access controller. This is indicated by LEDs 2 and 3 flashing red.

6.2 Allocation of IDs on the NEXTOR Series Access Controller

On a RS485 data bus the devices are distinguished by a device ID (address). The NEXTOR Series access controller recognizes serial numbers of TLR401 readers on the bus line. These serial numbers are 12-digit hexadecimal codes (e.g. C03859110000) printed on the back of the readers. The access controller assigns the two reader IDs, ID-0 and ID-1, based upon the serial numbers according to the following rationale:

1. The NEXTOR Controller recognizes two unassigned serial numbers:

   The lower value of the two is assigned to ID-0
   The higher value of the two is assigned to ID-1

2. The NEXTOR Controller recognizes an already assigned serial number and one unassigned serial number:

   The assigned serial number will keep its ID assignment
   The unassigned serial number will be assigned the available ID (0 or 1)

3. Both serial numbers are assigned by the NEXTOR Controller:

   The devices keep their ID assignment

The NEXTOR Series access controller allows you to change the automatic allocation.

☞ **Notice** It is good practice to make note of the serial numbers for each reader location during installation.

7 Maintenance

Caution

Danger of electric shock! Disconnect the device from the power supply before opening and before connecting cables.

7.1 Customer Service

First Response identify defects and causes

Contact the **Time**Link hotline in the event of any device error.

Have the following ready before placing your call:

- Serial number of the TLR401
- Customer details
- What troubleshooting steps have you already taken to correct the error?
- LED status
- Device and controller errors
- What occurred before the error?

7.2 Repairs

Careful

You may only undertake repair work after coordination with Time Link **International.**

7.3 Warranty, Limitation on Liability to Third Parties

In accordance with national statutory regulations at the place where the device is installed

Caution:
Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the this equipment.

8 Datasheet

Credentials
iCLASS card reading
Template on card
Biometric (fingerprint)
PIN Code

Host Interface
RS485
Wiegand

Biometric Features:

Search Modes
1 to 1 identification
1 to many verification

Response/Reads
Enrollment <= 1 sec
Identification <= 1 sec
Verification <= 0.8 sec
FAR & FRR adjustable

Sensor
Thin optical sensor
500 dpi @ 8-bit per pixel
Active area: .55 x .87 in (14mm x 22mm)

Templates

Template Size: ~130 to 250 bytes
Storage Capacity: 1000 or 6000 templates by model (not valid for template on card)

Power

10 bis 28V DC / 67mA -160mA

Operating Temperature
0 to 122 F (-18 to 50 °C)

Relative Humidity
0 to 95%,

Mechanical
NEMA IP65 rated
Metal Mounting Plate
Resin-sealed hard plastic enclosure

Color Options
Black, Silver and White

Dimensions
4.7 x 2.4 x 1.8 in (120 x 60 x 45 mm)

Appendix

8.1 Quick Guide to Admin Functions

Enter	Functions	Page
# 99 #	**Open Admin Mode**	
1234 #	**Enter Default Admin Code (or your Admin Code)**	
1 #	Reset - Manually switch to Wiegand Mode	21
2 #	Reset - Manually switch to RS485 Mode	21
12 #	Enroll user	15
16 #	Write Template onto iCLASS Card (TLR401-iCLASS only)	16
13 #	Delete Specific User(s)	18
1357 #✱	Delete Entire Database	18
14 #	**Open Function Menu**	
Optional 15 #	Change the Admin Code (4-8 digits) Default = 1234	14
Optional 24 #	Select iCLASS Mode (TLR401-iCLASS only) Default = 1 0 = disabled 1 = enabled 2 = enable 'Template on Card'	19
Optional 16 #	Define the Number of Digits for the User ID (2-9 digits) Default = 5	17
Optional 22 #	Enable Validation of the User ID Default = 0 0 = disabled 1 = enabled	17
Optional 19 #	Choose 37-bit or 26-bit Format Default = 0 0 = 37-bit 1 = 26-bit	20
Optional 20 #	Define Facility Code Default = 830 0 - 65535 (37-bit) Default = 1 0 - 255 (26-bit)	20

8.2 Allocation of the Cable

		Connectors on the Door Unit	
Color	**Purpose**	**RS485**	**Wiegand**
Shield	Shield		
Yellow	RS485A	X38/X39 (3)	
Black of Yellow	RS485B	X38/X39 (2)	
Red	DC in + 12...24V	X36/X37 (+)	X36/X37 (+)
Black of Red	DC in (–)	X36/X37 (–)	X36/X37 (–)
White	Wiegand out D1		X38/X39 (2)
Brown	Wiegand out D0		X38/X39 (3)
Black of Brown	Wiegand ground		X38/X39 (1)
Blue	Green LEDs (Opto-In 1)		X15/X17 (1)
Black of Blue	Beeper (Opto-In 2)		X16/X18 (1)
Black of Green	Red LEDs (Opto-In 3)		
Green	Tamper Switch-NO		

Remarks:

The wires are arranged in twisted pairs, one colored wire with a black wire respectively.

The Opto-Inputs are activated, when connected to "Wiegand Ground" (e.g. when used as a Wiegand reader "Opto-In-1" enables the green LEDs, "Opto-In-2" the beeper and "Opto-In-3" the red LEDs).

"Wiegand out D0/D1" is open collector to "Wiegand ground".

The "tamper switch" switches to "Wiegand ground" (Normally open).

8.3 Wiring Requirements

Notice:
Do not install data cabling parallel to high voltage cables. If unavoidable install data cabling in conduit and keep a distance of 3 ft. to protect from electromagnetic interference.

RS485
Shielded twisted pair cable (4000 feet max) e.g.:

1. 2x2 strands litz wire AWG24 (0.4 kcmil)
2. J-Y(ST)Y 2x2x0,6
3. CAT 5 ... 7 STP (Shielded Twisted Pair)

Wiegand
Non-twisted shielded cable (500 feet max) e.g.:

1. 10 pair shielded wire AWG22 (0.64 kcmil)

For shorter distances or using higher supply voltage:

2. 8 pair AWG24 (0.4 kcmil)

Consider whether or not to supply power with the data cable. Long distances require an increased gauge of cable. Supplying power locally or having an extra power cable pull may be preferable. Because of voltage drop over longer distances use of a 24V power source is the recommended choice.

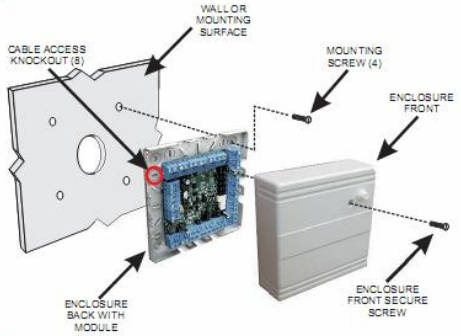
Example for calculating the power supply wiring:

1. AWG22 cable (0,34 mm^2):
   Loop resistance ca 115 ohm / km
   TLR401 current with 12V = 0,2A
   Cable length 150m
   Voltage drop: 115 ohm / km * 0.15km * 0,2A = 3.45V
   The supply voltage should be ≥ 15V in this case

2. AWG24 cable (0,25 mm^2):
   Loop resistance ca 180 ohm / km
   TLR401 current with 12V = 0,2A
   Cable length 150m
   Voltage drop: 180 ohm / km * 0.15km * 0,2A = 5,4V
   The supply voltage should be ≥ 18V in this case

TIMELINK. Quick Set-Up Guide for the NEXTOR Series MU200

Step 1 Mount



Step 2 Wire

A Connect MU200 (Master Unit) and DU (Door Unit)
- RS485 between MU200 and DU modules
- 10 to 28VDC Transformer

B Proximity reader connection to DU (Door Unit)
- 10 to 28VDC (red)
- GND (black-red)
- Data A (yellow)
- Data B (black-yellow)

C Connect door locking hardware
- Locking device (*magnetic lock shown)
- Door contact (Integrated in magnetic lock)
- Request to exit / PIR (*exit button shown)
- Locking hardware power (*12/24VDC Transformer)

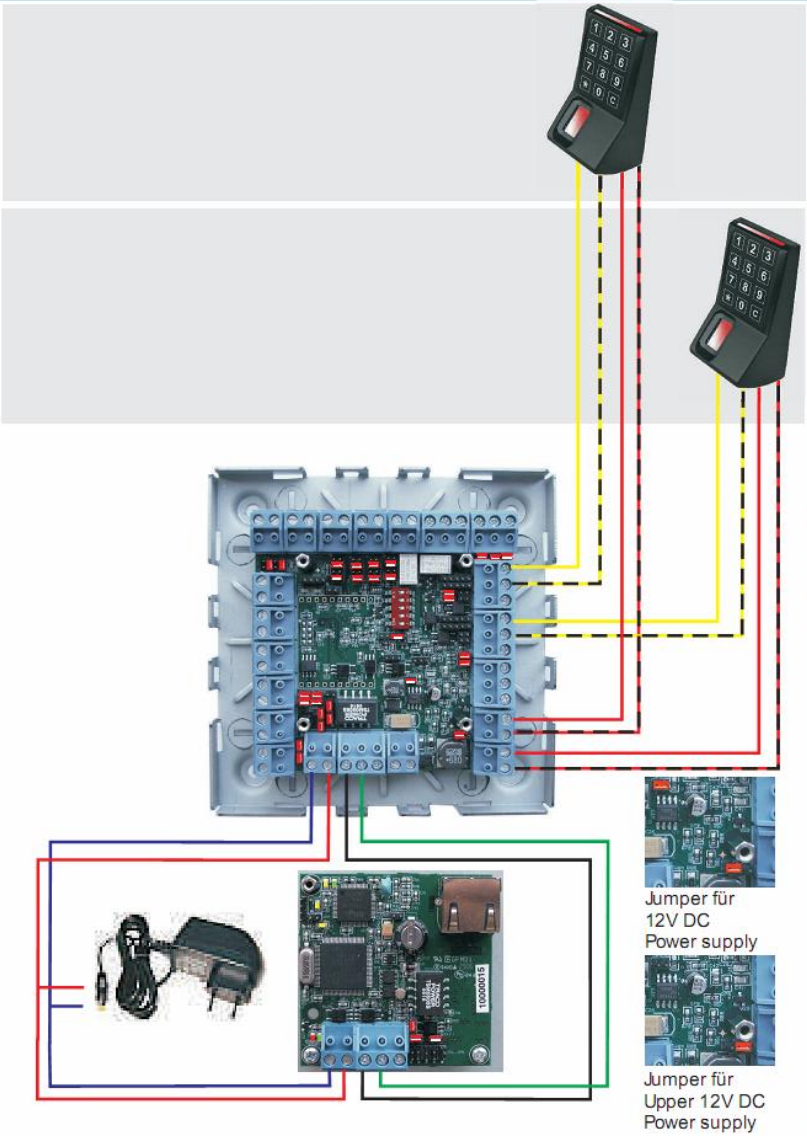
*Configuration example only, not included with packaged solution

Step 3 Network

A Ethernet connection
- Using CAT5 patch cable connect the MU200 (Master Unit) to an Ethernet router or directly to a PC using a CAT5 crossed cable

B Setting the IP address
- Set the IP address of the connected PC to allow connection to the MU200 (Master Unit) default IP address 192.168.50.120

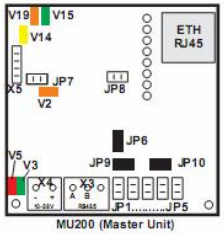
(see Software Configuration Manual for details)



Step 4 Power On

A Plug in transformer to a 120V AC source

B Verify the MU200 (Master Unit) LED indicators
- V2 (On = RS485 data transmission)
- V3 (Blinking = Application software running)
- V5 (On = Power On)
- V14 (On = 100MHz Ethernet connection)
- V15 (On = Ethernet connected)
- V19 (On = Ethernet data transmission)



MU200 (Master Unit)

Step 5 Login and Configure

A Connecting to the MU200 (Master Unit)
- Open the web browser of the connected PC.
- Enter the default IP address of 192.168.50.120 at the address line
- The "Welcome" screen is displayed

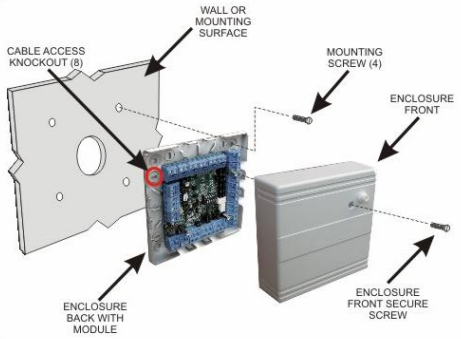
B Login to the system
- Enter the name "user1"
- Enter the password "pw"
- Click Login

C Modify the system for your unique application
- Modify the pre-loaded configuration to your needs
- Enroll Cards and add Card Holders as required

(see Software Configuration Manual for details)

TIMELINK. Quick Set-Up Guide for the NEXTOR Series MU200

Step 1 Mount



Step 2 Wire

A Connect MU200 (Master Unit) and DU (Door Unit)
- RS485 between MU200 and DU modules
- 10 to 28VDC Transformer

B Proximity reader connection to DU (Door Unit)
- 10 to 28VDC (red)
- GND (black)
- Data 0 (green)
- Data 1 (white)
- Shield ground
- Beeper (yellow)
- Green LED (orange)

C Connect door locking hardware
- Locking device (*magnetic lock shown)
- Door contact (Integrated in magnetic lock)
- Request to exit / PIR (*exit button shown)
- Locking hardware power (*12/24VDC Transformer)

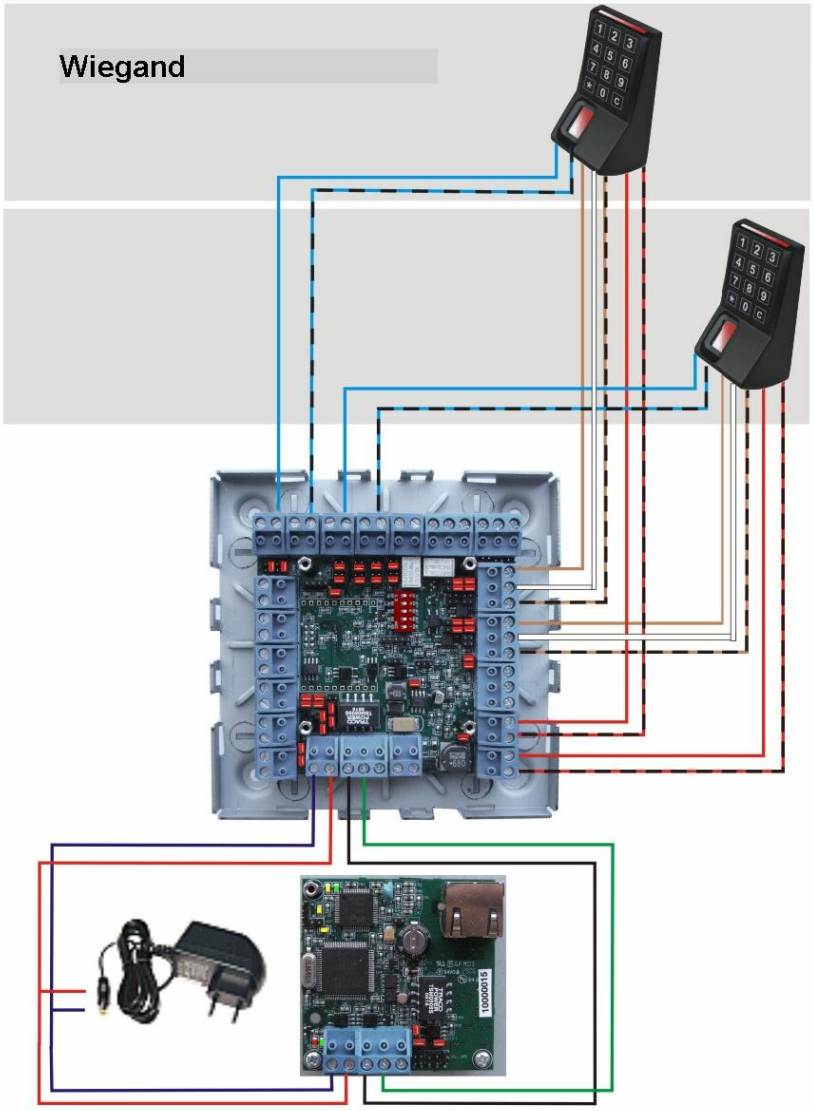
* Configuration example only, not included with packaged solution

Step 3 Network

A Ethernet connection
- Using CAT5 patch cable connect the MU200 (Master Unit) to an Ethernet router or directly to a PC using a CAT5 crossed cable

B Setting the IP address
- Set the IP address of the connected PC to allow connection to the MU200 (Master Unit) default IP address 192.168.50.120

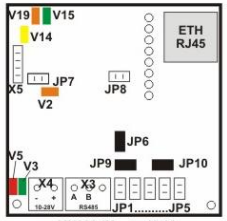
(see Software Configuration Manual for details)



Step 4 Power On

A Plug in transformer to a 120V AC source

B Verify the MU200 (Master Unit) LED indicators
- V2 (On = RS485 data transmission)
- V3 (Blinking = Application software running)
- V5 (On = Power On)
- V14 (On = 100MHz Ethernet connection)
- V15 (On = Ethernet connected)
- V19 (On = Ethernet data transmission)



MU200 (Master Unit)

Step 5 Login and Configure

A Connecting to the MU200 (Master Unit)
- Open the web browser of the connected PC.
- Enter the default IP address of 192.168.50.120 at the address line
- The "Welcome" screen is displayed

B Login to the system
- Enter the name "user1"
- Enter the password "pw"
- Click Login

C Modify the system for your unique application
- Modify the pre-loaded configuration to your needs
- Enroll Cards and add Card Holders as required

(see Software Configuration Manual for details)