User Manual

Timber Sentry

RECOMMENDED FOR
INDOOR INSTALLATION



Sebury

Introduction
Page 1

Features
Page 2 to 3

Specifications
Page 4 to 5

Package, Installation, Wiring
Page 6 to 9

User Operations
Page 9 to 12

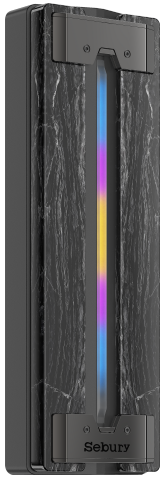
Administrator Operations
Page 13

Mobile Credentials
Page 13 to 14

User Encryption Card
Page 14

Firmware Update
Page 15 to 16

1 Introduction



Timber Sentry is the most secure product series of physical access control card readers.

It is the latest generation of access control card readers that supports OSDP, the latest SIA OSDP 2.2 version, and can use AES128 encrypted data transmission, making it safe and reliable.

Timber Sentry supports reading UID from various contactless cards, including EM, HID, and Mifare cards. It supports sector encryption for Mifare Classic and Mifare Plus EV2 cards, ensuring card security against duplication.

Additionally, it supports virtual card numbers via Bluetooth on mobile phones, allowing easily access even without a physical card.

Timber Sentry can adjust machine parameters through a mobile app according to users' personalized needs, to accommodate different equipments and locations.

2 Features

Powerfully Secure

OSDP supports the latest SIA OSDP 2.2 version, using AES128 encrypted data transmission for greater security and reliability.

It can read Mifare Classic and Mifare Plus EV2 encrypted sector data and output it as a card number, which can be customized by the customers.

The card UID can be output through MIFARE Classic and Mifare Plus EV2 sector key verification, making the access control system more secure.

The metal induction sensor triggers an anti-tamper alarm, which outputs an alarm signal through the OSDP and solid-state relay interface, and the buzzer emits a dedicated alarm sound.

Meet More Need

Built-in 125 kHz card reading antenna can read EM and HID cards.

Built-in 13.56 MHz card reading antenna can read Mifare cards (ISO14443A) and NFC-enabled mobile phones.

Built-in 2.4G Bluetooth module can read the virtual card number of the mobile phone.

When the OSDP controller is not detected, it automatically switches to Wiegand mode.

RGB three-color LED indicator light strip, capable of displaying various working states, with multiple lighting effects to choose.

External input RED, GREEN, BLUE indicator light control wires can control LED display RGB colors.

External input BEEP control wire, which can control the buzzer to sound.

Manage , Upgrade and Configure

The LED lighting effects and all other parameters can be adjusted through the mobile app management software.

LED indicator light color and brightness: Off or 7 colors, 21 levels of brightness.

Provide a variety of lighting effects options for LED indicator lights.

Buzzer mode: off or 15 levels of volume.

Tamper alarm: Buzzer off or 1 to 10 minutes alarm, OSDP alarm command.

Wiegand output format: 24 to 66 bits, byte order can be reversed.

OSDP output format: 24 to 66 bits, byte order can be reversed.

EM and Mifare can be set to Wiegand and OSDP output formats respectively.

Card reading type: EM, HID, Mifare Classic, Mifare Plus, Mifare Desfire.

Read Mifare card mode: UID, UID with key or Block Data.

Read Mifare card key setting: 6 bytes for Mifare Classic, 16 bytes for Mifare Plus Ev3.

Firmware upgrade: users can upgrade the firmware of the device using an RS485-USB converter and the manufacturer's upgrade files, without the need to return the device to the factory or disassemble it.

Mobile Credential Technology

Support local Bluetooth virtual card unlocking, require the download of the OSDP Reader App for Apple or Android devices.

Support mobile phone NFC bus card voucher, no need to open the phone screen to approach the card reader to open the door, making access more convenient.

3 Specifications

2.4 GHz (Bluetooth)

Users download the OSDP Reader application and use a virtual card number to unlock the door.

The administrator downloads the OSDP Reader Manager application to manage the parameters of the reader.

13.56 Mhz

UID: Mifare and its compatible cards that comply with ISO14443A, including Mifare Classic, Mifare Plus, Mifare Desfire cards, NFC.

Sector encryption: Mifare Classic and Mifare Plus EV2.

125 kHz

EM Proximity, HID Proximity

Max Read Range

EM or HID: 1.97 inches (5 cm)

Mifare or NFC: 0.79 inch (2 cm)

Dimensions (width x length x depth)

1.77 in × 5.59 in × 0.79 in (45 mm × 142 mm × 20 mm)

Operating Voltage

12 V DC

Current Draw

Normal standby: 80 mA

Peak: 250 mA

Max. Avg: 100 mA

Device Input

Tri-color LED: Hold @ Active Low

Buzzer: Hold @ Active Low

Device Output

Tamper: Solid-state relay 0 to 12 V DC @ 100 mA Max. (Dry Contact)

Operating Temperature
-31° F to 150° F (-35° C to +66° C)

Operating Humidity
0% to 95% non-condensing

Storage Temperature
-40° F to 185° F (-40° C to +85° C)

Waterproof Rating
IP65

Communication Interface
Wiegand and RS-485 Half Duplex (OSDP)

OSDP Baud Rate
9600, 19200, 38400, 57600, 115200 bps automatic adaptation

Panel Connection
Pigtail 19.69 inches (50 cm)

Device Management
Mobile phone (Bluetooth communication)

Wiegand Format
EM: 26-bit, 34-bit, 42-bit with check bit, 32-bit, 40-bit without check bit

HID: Automatically output 26-37 bits according to card data

Mifare or NFC: 32-bit MSB, 32-bit LSB, 56-bit MSB, 56-bit LSB, 40-bit MSB, 40-bit LSB, 64-bit MSB, 64-bit LSB without check bit, 26-bit MSB, 26-bit w/Facility Code, 34-bit MSB, 37-bit LSB, HID 35-bit, HID 48-bit, 58-bit MSB, 37-bit MSB, 66-bit MSB with check bit

OSDP Format
EM: 24-bit, 32-bit, 40-bit Raw Bit Array format, 26-bit, 34-bit, 42-bit P/data/P format

HID: Automatically output 26-37 bits P/data/P format according to the card data

Mifare or NFC: 24-bit, 32-bit, 56-bit, 64-bit Raw Bit Array format, 26-bit, 34-bit, 58-bit, 66-bit P/data/P format

4 Installation and Wiring

4.1 Package Contents



Timber Sentry



User Manual



Hex Key



Drilling Template

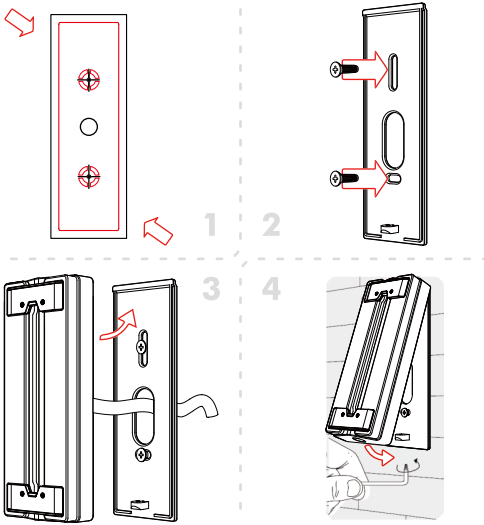


KA 4 × 25 mm Self-tapping Screw (2)



Φ6 × 30 mm PVC Anchor (2)

4.2 Installation



Step 1, mounting holes for back plate:

Stick the Drilling Template on the wall at a suitable position.

Drill a hole with diameter bigger than 10 mm for the pigtail wire to pass though.

Drill 2 holes with 6 mm diameter for the PVC anchors, and then insert the 2 PVC anchors.

Step 2, install the back plate:

Unscrew one tamper screw which are under the reader with a screwdriver, take away the back plate of the reader, fix it on the wall with the 2 pcs KA 4 × 25 mm self-tapping screws, use the drilled holes as a guide.

Step 3, wire the cables to the access panel system:

Cut the wires to a suitable length.

Connect them to the access panel system wires through the wall or the pre-embedded box.

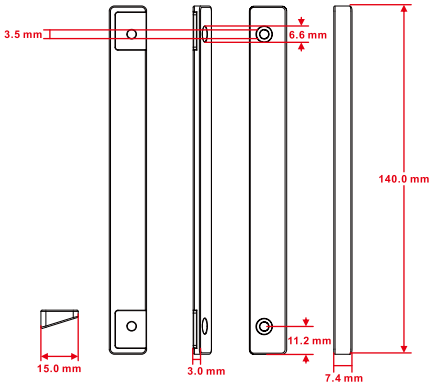
PAY ATTENTION NOT TO CONNECT WRONGLY OR SHORT CIRCUIT, OTHERWISE THE READER MAYBE BURN DOWN!

After checking, power on for a short moment to test whether the indicator light is on and whether the buzzer beeps once.

IF THE TEST FAILS, POWER OFF AND RECHECK THE WIRING IMMEDIATELY!

Step 4, attach the reader to the back plate:

Once wiring well, attach the reader to the back plate with the tamper screws.

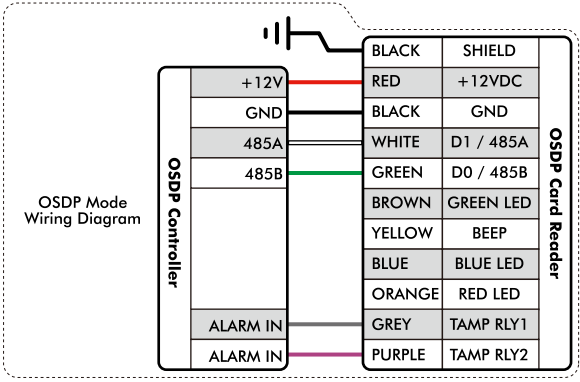


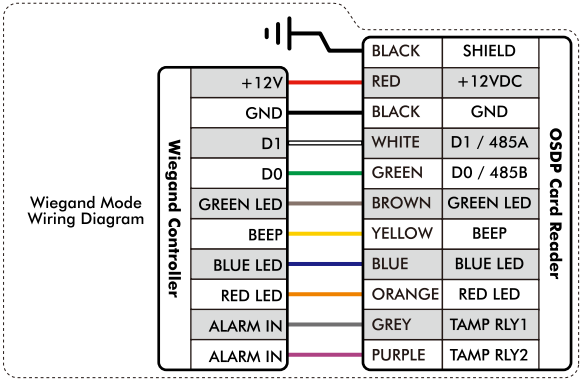
The model of slat have been open-sourced, please contact us to get it.

4.3 Wiring Diagram

The definition of wires is shown in the table below:

Color	Symbol	Function
Black	SHIELD	Shielding Wire
Red	+12VDC	Positive Pole
Black	GND	Negative Pole
White	D1 / 485A	D1 (Wiegand) or 485A (OSDP)
Green	D0 / 485B	D0 (Wiegand) or 485B (OSDP)
Brown	GREEN LED	Green Indicator Light Control Wire
Yellow	BEEP	Buzzer Control Wire
Blue	BLUE LED	Blue Light Control Wire
Orange	RED LED	Red Indicator Light Control Wire
Grey	TAMP RLY1	Solid State Relay NO Terminal
Purple	TAMP RLY2	Solid State Relay COM Terminal





5 User Operations

5.1 OSDP Mode Operation

If the card reader is connected to an access controller with OSDP functionality, the card reader must have the OSDP function enabled. In this case, the card reader and the controller use the OSDP protocol to transmit card numbers.

According to the controller's requirements, the card reader automatically selects AES128 encryption or no encryption.

The OSDP address can be set by the controller, with an address range of 0 to 126.

The OSDP communication baud rate can be automatically adapted by the controller, and can also be modified by the controller, with a range of 9600, 19200, 38400, 57600, and 115200 bps.

The OSDP tamper-proof function is enabled by default and can be disabled.

When the tamper-proof function is enabled, if the back cover is detected to be opened or restored, the corresponding OSDP command will be output to the controller.

When swiping a user card, if it is an **EM card**, the default output format is 26-bit P/data/P.

Customers can **customize the format** to 24-bit, 32-bit, 40-bit Raw Bit Array format, or 26-bit, 34-bit, 42-bit P/data/P format.

When swiping a user card, if it is an **HID card**, the system will automatically output the 26-37bit P/data/P format according to the internal format of the HID card.

When swiping a user card, if it is a **Mifare card** or a mobile phone **NFC**, the default output format is 32-bit Raw Bit Array.

Customers can **customize the format** to 24-bit, 32-bit, 56-bit, 64-bit Raw Bit Array format, or 26-bit, 34-bit, 58-bit, 66-bit P/data/P format.

If it is a mobile App opening the door, the output format is the same as the **Mifare card settings**.

If the **Reverse option** is checked, the output format will be reversed byte-for-byte, such as the original hexadecimal card number A1B2C3, after checking the Reverse option, the output card number will be C3B2A1.

In **OSDP mode**, the functions of the indicator lights and buzzer are controlled by OSDP commands, and the control wires for BEEP, GREEN LED, BLUE LED, and RED LED are invalid.

5.2 Wiegand Mode Operation

If the card reader is chosen to connect to an access controller with Wiegand function, the card reader must have the Wiegand function enabled.

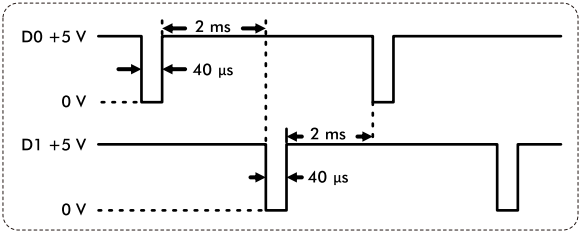
At this time, the card reader and the controller use the Wiegand protocol to transmit card numbers.

Wiegand format output uses low levels on D0 and D1 wires to represent output data, defined as follows:

D0, a low voltage level represents 0, and the lead wire is green.

D1, a low voltage level represents 1, and the lead wire is white.

The pulse width of the low-level pulse is 40 μs, and the pulse interval is 2 ms.



The Wiegand output address defaults to 0 and can be set within the range of 0 to 255.

When swiping a user card, if it is an EM card, the default output format is 26-bit. Customers can customize the format to 26-bit, 34-bit, 42-bit with check bit, or 32-bit, 40-bit without check bit.

When swiping a user card, if it is an HID card, the system will automatically output the 26-37bit format according to the internal format of the HID card.

When swiping a user card, if it is a Mifare card or a mobile phone NFC, the default output format is 32-bit Raw Bit Array. Customers can customize the format to 32-bit MSB, 32-bit LSB, 56-bit MSB, 56-bit LSB, 40-bit MSB, 40-bit LSB, 64-bit MSB, 64-bit LSB without check bit, 26-bit MSB, 26-bit w/Facility Code, 34-bit MSB, 37-bit LSB, HID 35-bit, HID 48-bit, 58-bit MSB, 37-bit MSB, 66-bit MSB with check bit.

If it is a mobile App for door opening, the output format is the same as that set for Mifare cards.

If the Reverse option is checked, the output format will be reversed byte-for-byte, for example, if the original hexadecimal card number is A1B2C3, after checking the Reverse option, the output card number will be C3B2A1.

When a user swipes their card or uses their phone's NFC, the card reader will beep once, the indicator light bar will display a green door-opening effect, and a designated Wiegand signal will be output.

When the mobile App is used to open the door, the card reader emits a sound, the indicator light bar displays a blue door-opening effect, and the designated Wiegand signal is output.

When the BEEP wire becomes low, the buzzer keeps sounding.

The GREEN LED, BLUE LED, and RED LED wires independently control the color of the indicator lights. When each of them lower, the indicator lights can be controlled to display RGB mixed colors, as shown in the table below.

Inpuut Wire	Default	Red	Green	Amber	Blue	Magenta	Cyan	White
Red LED	High	Low	High	Low	High	Low	High	Low
Green LED	High	High	Low	Low	High	High	Low	Low
Blue LED	High	High	High	High	Low	Low	Low	Low

5.3 External Output Control

TAMP RLY1 and TAMP RLY2 are internal solid-state relay normally open contact output wires, without positive and negative distinction.

The external voltage is 0 to 12 V DC, with a maximum current of 100 mA (dry contact).

When the machine's back cover is opened, the switch is activated, outputting an alarm switch signal externally.

When the back cover is restored, the switch is deactivated, ceasing the external output of the alarm switch signal.

6 Administrator Operations

If users need to change the parameters of the card reader, such as Wiegand output format, OSDP output format, LED indicator light color, brightness, and lighting effects, buzzer mode, volume, etc., they can operate and adjust these parameters through the mobile management App "**OSDP Reader Manager**" to fulfill their personalized needs.

*The App needs to be downloaded before use.

6.1 Pairing A Mobile Phone With A Device

Open the mobile App "**OSDP Reader Manager**", power on the card reader again, and within 1 minute, add the card reader on your mobile phone.

After successful pairing, the indicator light will flash green once and the buzzer will sound once, indicating that the administrator's mobile phone has successfully paired with the card reader.

6.2 Set Card Reader Parameters

The administrator's phone, which has been configured, can operate the card reader at any time for various settings.

For specific operations, refer to the mobile App.

NOTE: IF A NEW MANAGEMENT PHONE IS PAIRED, THE PREVIOUS MANAGEMENT PHONE WILL BE AUTOMATICALLY DELETED.

7 Mobile Credentials

7.1 Mobile Phone Bluetooth

Support local Bluetooth virtual card unlocking, requiring the download of the App "**OSDP Reader**" before use.

If adjustments to device parameters are required, the administrator needs to download the App "**OSDP Reader Manager**".



7.2 Mobile NFC

Support for smartphone NFC virtual card credentials allows for door opening via proximity to the card reader without needing to open the phone screen, making it more efficient and convenient.

8 User Encryption Card

If users need to use an encrypted card to open the door, when purchasing a card reader, they need to choose to enable the encrypted card function.

The manufacturer will configure the card reader key and use the accompanying user encrypted card.

The card number read by the card reader is the data of the sector, not the UID.

The encrypted card must be Mifare Classic or Mifare Plus EV2.

The encrypted card reader can only read encrypted cards and will no longer read the UID of non-encrypted Mifare cards.

To ensure greater security, other card types must be blocked, and only encrypted card types should be read.

Otherwise, the encryption becomes meaningless.

9 Firmware Upgrade

Due to the addition of new features or the discovery of product defects, the manufacturer will improve the product software and release an upgrade package file, such as **OSDP Reader ISP V1.7**.

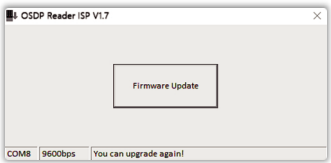
Users can use the upgrade package file to upgrade the firmware of the product.

Before upgrading the firmware, it is necessary to connect the product to a **Windows system computer** via a **USB to RS485** converter (corresponding drivers may need to be installed), and power up the card reader with a **12 V power supply**.



Double-click the upgrade file on the computer, as shown below, to open a software interface.





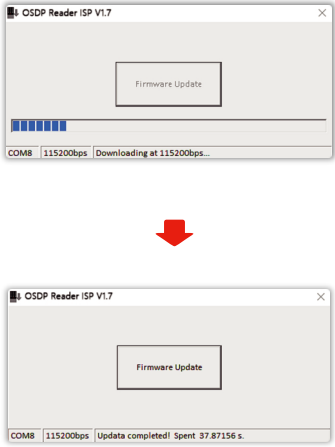
OSDP Reader ISP V1.7

If the device connection is normal, it will automatically connect.

After successful connection, a prompt "**You can upgrade again!**" will appear in the status bar.

Click "**Firmware Update**", and a blue progress bar will appear, indicating that the firmware upgrade is starting.

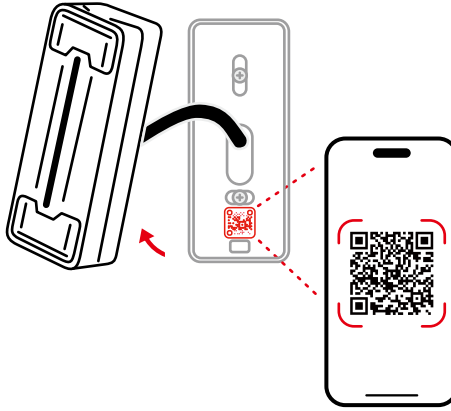
Wait for more than 30 seconds, and "**Update completed!**" will appear, indicating that the upgrade is complete.



If the upgrade process is interrupted by **a power outage** or **wire failure**, resulting in a failed upgrade, it may not be possible to perform the upgrade again.

In this case, manual upgrade is required. Short-circuit the **brown wire 9 / 9** of the card reader to **GND**, power it back on, then disconnect the brown wire from GND.

Open the upgrade file again and repeat the above steps to perform the **upgrade again**.



If you lost this manual, please unpack the shell and scan the QR code on the back shell to get the E-instruction.

Sebury Technology Co., Ltd
Shenzhen, China

Website: www.sebury.com
E-mail: sales@sebury.com.cn

©2026 Sebury Technology Co.,Ltd all rights reserved.