Quick Start Guide

Model: InBioPC Series

Version: 1.0

English

1 Precaution

Please note the following safety precautions. Misuse may result in device failure or even personal injury:

1. Do not energize until installation is complete; operation with electricity is prohibited. Be sure to confirm correct wiring before energizing.
2. All peripheral devices must be grounded.
3. It is recommended that all alignments be sleeved, either with PVC or galvanized pipe.
4. It is strongly recommended that the exposed portion of all terminals should not exceed 4mm. to prevent the bare wire from being too long leading to accidental contact and causing short circuit and other faults.

Other matters:

1. **RESET button:** Long press 1 to 5 seconds for USB disk upgrade; 5 to 10 seconds to reboot the controller; more than 10 seconds to restore factory settings. When restoring the factory settings, it will restore the device's network configuration and Webserver login password, and the device's data will be cleared.
2. The default IP address of the primary NIC is 192.168.1.201.

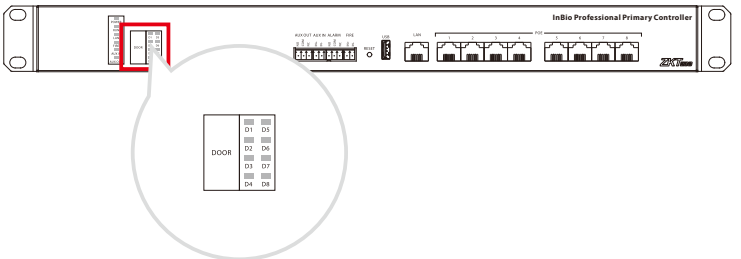
2 Indicator Description

(The illustrations in this document take InBioPC-800 as an example.)

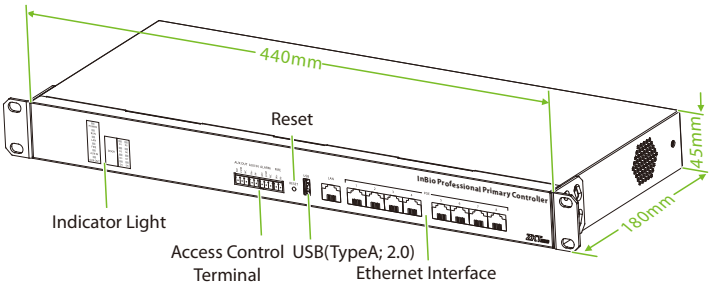
After connecting the controller correctly and turning on the power, the indicator light description under normal state is as follows.

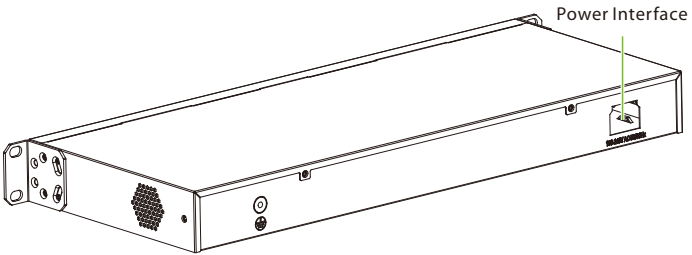
- **POWER (Red):** Normally illuminated indicates normal energization.
- **RUN (Green):** A slow flash indicates that the system is normal, and a fast flash indicates that a firmware upgrade is in progress.
- **LAN (Green):** Normally lit indicates no data interaction, blinking indicates data interaction, and off indicates network abnormality.
- **FIRE (Red):** Fire signal, blinking indicates that a short-circuit signal is received, and off indicates that a short-circuit signal is not received.
- **AUX IN (Red):** Auxiliary input signal, blinking to indicate that the signal is received, off to indicate that the signal is not received.
- **AUX OUT (Red):** Auxiliary output signal, blinking to indicate that an alarm signal is being output.

- **DOOR (Green):** Normally illuminated indicates that the online status door sensor is off/no door sensor, off indicates offline, and blinking indicates that the online status door sensor is on.



3 Dimensions and Interfaces

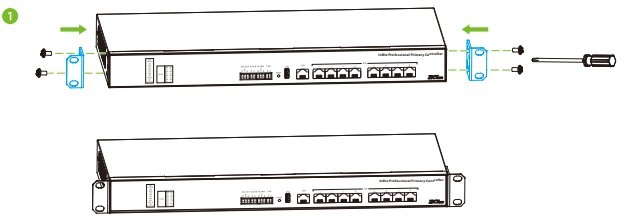


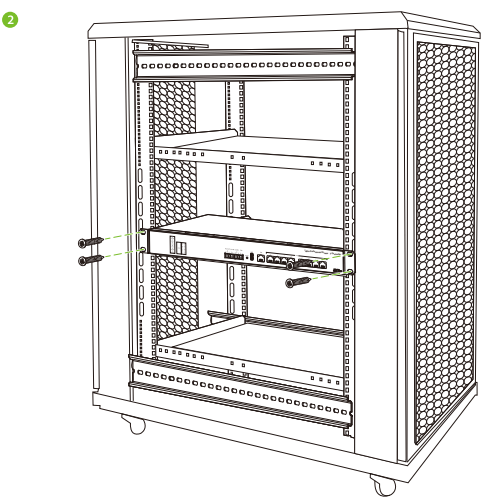


4 Installation Procedures

❖ Cabinet Installation

1. Attach the back plate to the device as shown in the figure below.
2. Place the device in the cabinet and secure it with screws.

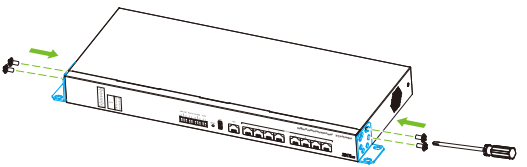




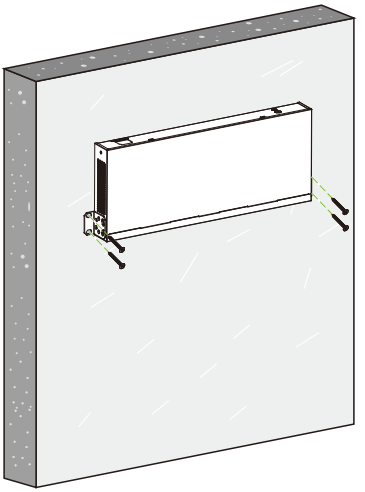
❖ Wall-Mount Installation

1. Attach the Back Plate to the appliance as shown in the figure below.
2. Place the device in the cabinet and secure it with screws.

❶

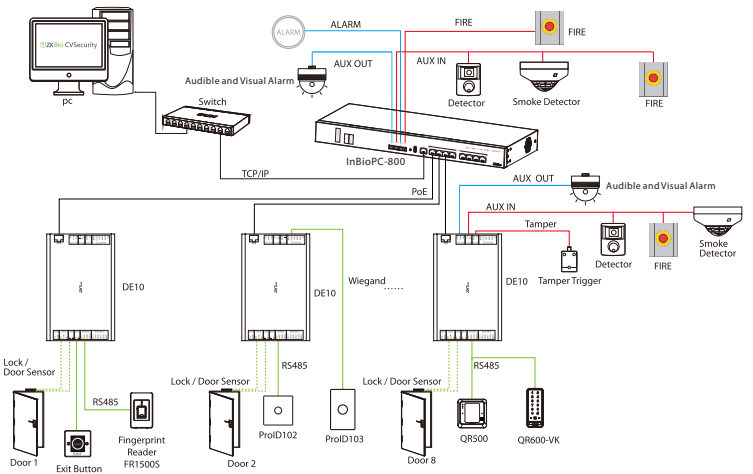


❷



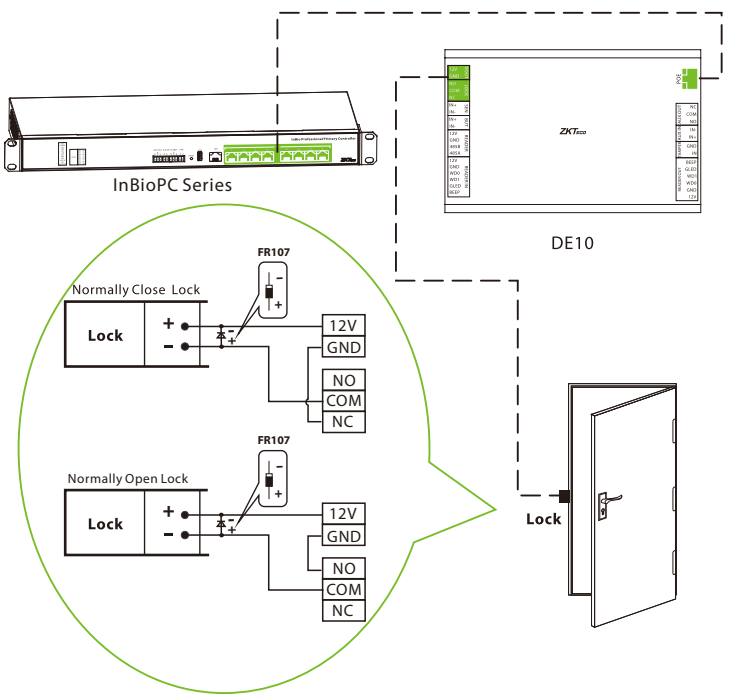
5 Configuration

Please use the power supply configured for the InBioPC series controller which is rated 100-240V, AC50/60Hz.



6 Lock Connections

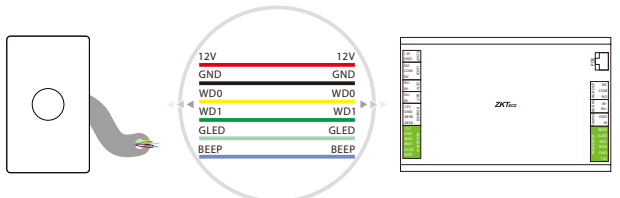
1. Each DE10 Door Unit supports the control of exactly one door lock. The InBioPC controller manages multiple DE10 units, allowing control of up to 4 locks (InBioPC-400) or 8 locks (InBioPC-800) depending on your model.
2. The system supports both Normally Open Lock and Normally Close Lock. The NO Lock (normally open when powered) is connected with 'NO1' and 'COM' terminals, and the NC Lock (normally close when powered) is connected with 'NC1' and 'COM' terminals.
3. In order to prevent the electric lock from generating self-induced electromotive force on the access control system at the moment of switching, it is necessary to connect a diode in parallel with the electric lock (please use the FR107 supplied with the system) to release the self-induced electromotive force during the wiring of the field application of the access control system.
4. The VOUT terminal of the DE10 can supply power to the electric lock, but the lock's current draw must be less than 800mA.



7 Reader Connections

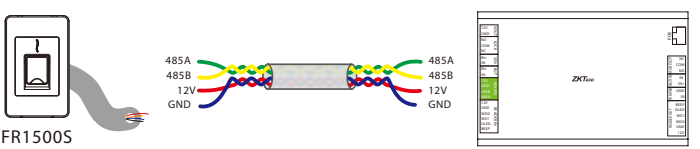
❖ Wiegand Reader

Each DE10 Door Unit features two Wiegand reader interfaces (labeled 'READER IN' and 'READER OUT'), allowing for bidirectional access control on a single door. This configuration enables entry and exit verification using separate card readers for the same door.



❖ RS485 Reader

1. Shielded twisted-pair cables, which are internationally recognized, must be used. The recommended type of shielded twisted-pair cable is RVVSP4*0.5. The use of shielded twisted-pair cable helps to reduce and eliminate the distributed capacitance between the two 485 communication lines as well as the common-mode interference generated around the communication lines.
2. 485A and 485B data lines must be twisted, DE10 GND, 485A, 485B were connected to the RS485 reader GND, 485A, 485B. wiring must be cloth multi-stranded shielded twisted-pair cable, multi-stranded for backup, shielding is for debugging when a special situation arises, twisted because of the 485 communication using the principle of differential mode communication, twisted anti-jamming of the best.

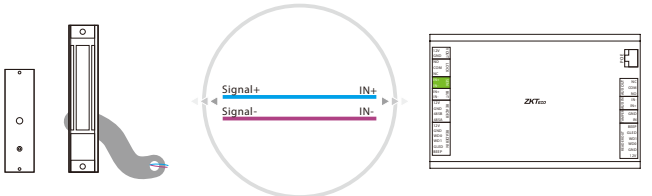


Note: When the DE10 is operating under either of these conditions: (1) not connected to the controller's POE port configured in Main-Sub mode, or (2) in factory default state without prior controller connection, the system will automatically grant access to any presented credential. Any card, password, fingerprint, or QR code presented to the connected readers will trigger a 5-second door unlock without saving access records. For secure operation, ensure proper controller configuration.

8 Sensor, Exit Button and Tamper Switch Connections

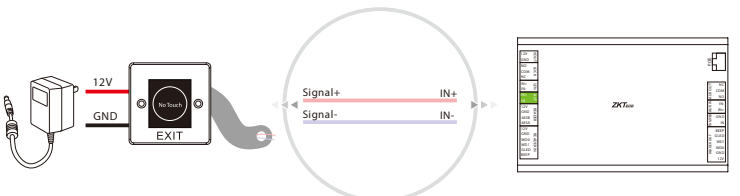
❖ Sensor

Door sensor is used to sense the switching state of the door, the access controller can detect the door being opened illegally through the door sensor switch, and then it will output an alarm.



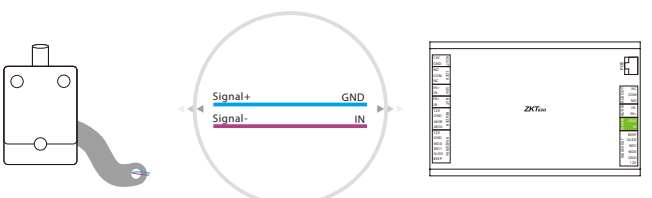
❖ Exit Button

The exit button is a switching device for opening the door installed inside the room, and the door can be opened when the exit button is closed.



❖ Tamper Switch

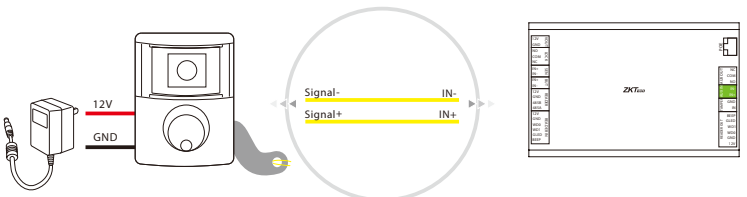
The tamper signal of the DE10 is connected to the tamper switch of the cabinet.



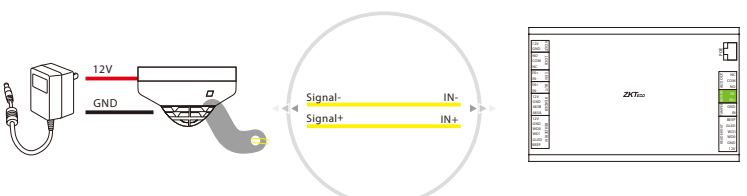
9 Auxiliary Input Connections

The DE10 provides 1 auxiliary input port for connecting infrared body sensing detectors or smoke detectors etc.

❖ Infrared Human Body Sensor Detector

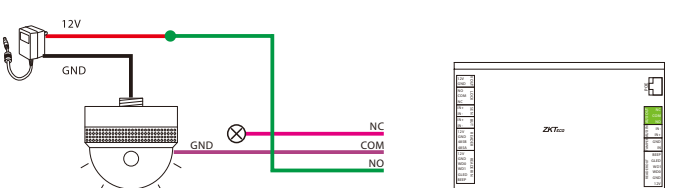


❖ Smoke Detector



10 Auxiliary Output Connections

The DE10 provides 1 auxiliary output connector for connecting an audible and visual alarm.

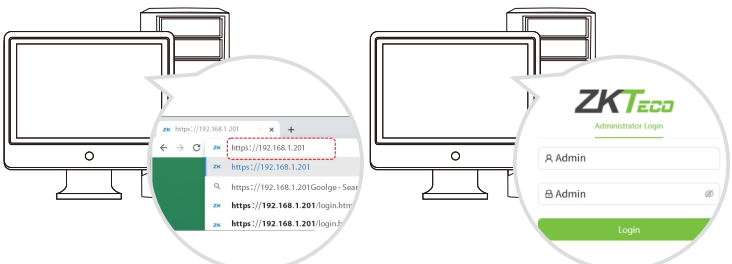


11 WebServer

Built-in WebServer supports setting device parameters and checking device status etc. on PC and mobile phone.

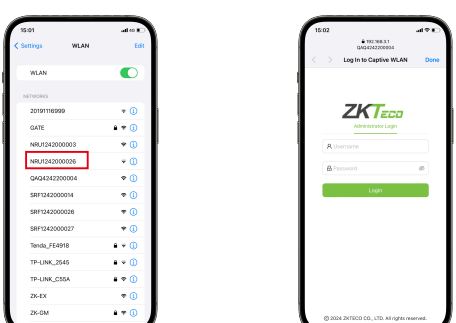
❖ PC

After the device is connected to power and connected to the network, open a browser and log in to the WebServer by entering the address, which is the **https:// IP address**. For example: **https://192.168.1.201**. Enter the WebServer account and password, the default account is: **admin** and the password is: **admin**.



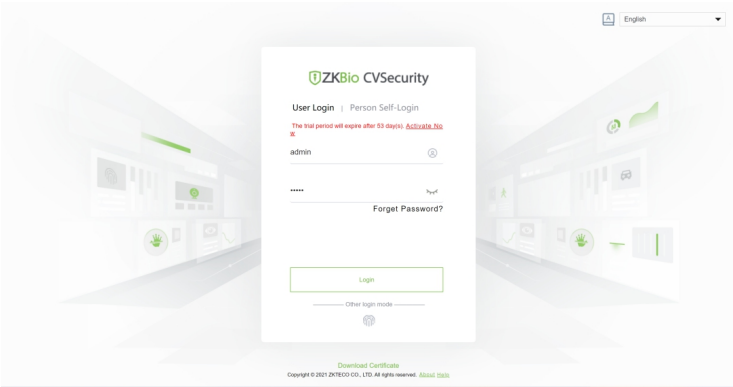
❖ Mobile Phone

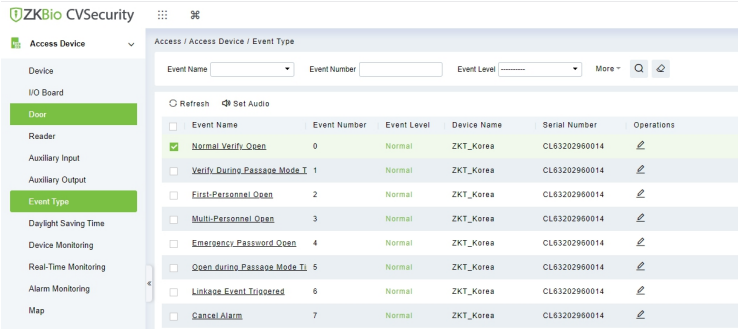
There is no need to enter the IP address of the device on the mobile phone. After the device is connected to the power supply and the network, the mobile phone should be close to the device, find the hotspot of the device (by default, it is the serial number of the device), and then click on it and enter the WebServer account and password in the pop-up login interface.



12 ZKBio CVSecurity Integration

The device connects to ZKBio CVSecurity by setting up ZKBio CVSecurity-related information in **[Web Configuration] > [Server Settings]** of the WebServer (no need to set up if the device and the server are in the same network segment). The device can add devices, set up access control rules, set up global anti-passback, linkage, interlocking, and other access control operations on ZKBio CVSecurity. For more detailed information on the use of the ZKBio CVSecurity, please refer to the *ZKBio CVSecurity User Manual*.





ZKTeco Biometrics India Pvt Ltd.

B-1, Khata No. 31, Devasandra Industrial Estate, Whitefield Main Road,

Beside Phoenix mall, Mahadevapura, Bengaluru-560048, Karnataka, India.

Phone : 080 6828 1342

Mail : sales@zkteco.in

Website : www.zkteco.in