User Manual

CVEdge160

Date: March 2026

Doc Version: 1.0

English

Thank you for choosing our product. Please read the instructions carefully before operation. Follow these instructions to ensure that the product is functioning properly. The images shown in this manual are for illustrative purposes only.

For further details, please visit our Company's website www.zkteco.com.

Trademark

ZKTeco is a registered trademark of ZKTeco. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the ZKTeco equipment. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied equipment vests in and is the property of ZKTeco. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ZKTeco.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ZKTeco before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel has read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

ZKTeco offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ZKTeco does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

ZKTeco does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or

relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ZKTeco shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/ unit/ equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on http://www.zkteco.com.

If there is any issue related to the product, please contact us.

ZKTeco Headquarters

Address ZKTeco Industrial Park, No. 32, Industrial Road,
Tangxia Town, Dongguan, China.

Phone +86 769 - 82109991

Fax +86 755 - 89602394

For business related queries, please write to us at: sales@zkteco.com.

To know more about our global branches, visit www.zkteco.com.

About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face template-reader Door Locks. Our security solutions are multi-lingual and localized in over 18 different languages. At the ZKTeco state-of-the-art 700,000 square foot ISO9001-certified manufacturing facility, we control manufacturing, product design, component assembly, and logistics/shipping, all under one roof.

The founders of ZKTeco have been determined for independent research and development of biometric verification procedures and the productization of biometric verification SDK, which was initially widely applied in PC security and identity authentication fields. With the continuous enhancement of the development and plenty of market applications, the team has gradually constructed an identity authentication ecosystem and smart security ecosystem, which are based on biometric verification techniques. With years of experience in the industrialization of biometric verifications, ZKTeco was officially established in 2007 and now has been one of the globally leading enterprises in the biometric verification industry owning various patents and being selected as the National High-tech Enterprise for 6 consecutive years. Its products are protected by intellectual property rights.

About the Manual

This manual introduces the operations of the **CVEdge160**.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Features and parameters with ★ are not available in all devices.

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Software	
Convention	**Description**
Bold font	Used to identify software interface names e.g. **OK**, **Confirm**, **Cancel**.
>	Multi-level menus are separated by these brackets. For example, File > Create > Folder.
For Device	
Convention	**Description**
< >	Button or key names for devices. For example, press <OK>.
[ ]	Window names, menu items, data table, and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forwarding slashes. For example, [File/Create/ Folder].

Symbols

Convention	Description
	This implies about the notice or pays attention to, in the manual.
	The general information which helps in performing the operations faster.
	The information which is significant.
	Care taken to avoid danger or mistakes.
	The statement or event that warns of something or that serves as a cautionary example.

Table of Contents

1 Safety Instructions

1.1 Important Security Instructions

1. Read and follow the instructions carefully before operation. Please keep the instructions for future reference.
2. Accessories: Please use the accessories recommended by the manufacturer or delivered with the product. Other accessories are not recommended, including major alarming systems and monitoring systems. The primary alarming and monitoring system should comply with the local applicable fire-prevention and security standards.
3. Installation cautions: Do not place this equipment on an unstable table, tripod mount, support, or base, lest the equipment falls and get damaged or any other undesirable outcome resulting in severe personal injuries. Therefore, it is essential to install the equipment as instructed by the manufacturer.
4. All peripheral devices must be grounded.
5. No external connection wires can be exposed. All the connections and idle wire ends must be wrapped with insulating tapes to prevent any damage to the equipment by accidental contact of the exposed wires.
6. Repair: Do not attempt to have an unauthorized repair of the equipment. Disassembly or detachment is risky and likely to cause shock. All repairs should be done by a qualified technician.
7. If any of the following cases arise, disconnect the power supply from the equipment first and intimate the technician immediately.
   - The power cord or connector is damaged.
   - Any liquid or material spilled into the equipment.
   - The equipment is wet or exposed to bad weather (rain, snow, etc.).
   - If the equipment cannot work properly, even if it is operated as instructed, please be sure to adjust only the control components specified in the operating instructions. Incorrect adjustments on other control components may cause damage to the equipment; even the equipment may fail to operate permanently.
   - The equipment falls, or its performance changes dramatically.
8. Replacing components: If it is necessary to replace a component, only the authorized technician can replace the accessories specified by the manufacturer.
9. Security inspection: After the equipment is repaired, the technician must conduct security inspection to ensure proper working of the equipment.
10. Power supply: Operate the equipment with only the type of power supply indicated on the label. Contact the technician for any uncertainty about the type of power supply.

Violation of any of the following cautions is likely to result in personal injury or equipment failure. We will not be responsible for the damages or injuries caused thereby.

- Before installation, switch off the external circuit (that supplies power to the system), including locks.
- Before connecting the equipment to the power supply, ensure the output voltage is within the specified range.
- Never connect the power before completion of installation.

1.2 Installation Precautions

1. Network cable selection must be higher specifications (Category 5e or higher network cable with oxygen-free copper material, core nominal diameter 0.5 mm, core nominal diameter 0.5 mm). 100 meters of single wire resistance is less than 10 ohms. Try to choose a higher specification network cable (such as Category 6 oxygen- free copper material), reserve enough margin to meet the maximum load requirements.
2. All wiring must be sleeved, optional PVC pipe and galvanized pipe, to avoid mice bite off the line caused by failure. Although the controller has a good anti-static, lightning, leakage-proof design, please make sure that the controller chassis and AC ground connection is perfect, and the AC ground is truly grounded.
3. It is recommended not to plug and unplug connection terminals frequently when the system is energized. Be sure to unplug the connection terminals before starting any relevant welding job.
4. Do not detach or replace any control panel chip without permission because unprofessional operation may cause damage to the control panel.
5. It is recommended not to connect any other auxiliary devices without permission. All non-routine operations must be confirmed with our engineers in advance.
6. A control panel should not share one power socket with any other large-current devices.
7. It is preferable to install card readers and buttons at a height of 55 inches to 59 inches (1.4m to 1.5m) above the ground, subject to proper adjustment according to customers' usual practice.
8. The device is recommended to be installed in an easy-to-maintain location such as a server room or weak current room..
9. The exposed part of any connection terminal is strongly recommended not be longer than 0.16 inches (4mm). Professional clamping tools may be used to avoid short-circuit or communication failure resulting from accidental contact with excessive exposed wires.
10. If you need to keep a record of access control events, periodically export the data from the controller.

11. Prepared countermeasures against unexpected power failure, like selecting power supply with UPS.
12. In order to prevent the self-induced electromotive force generated by the electric lock at the moment of switching on and off from affecting the access control system, it is necessary to connect a diode in parallel with the electric lock (please use the FR107 diode supplied with the system) to release the self-induced electromotive force generated at the moment of switching on and off of the electric lock during the wiring of the access control system on-site application.
13. It is recommended to use the power supply delivered with the system as the control panel power supply.
14. In a place with strong magnetic interference, galvanized steel pipes or shielded cables are recommended, and proper grounding is required.

2 Overview

The CVEdge 160 by ZKTeco is an AI-powered access control controller with video analytics. It provides enhanced access control management and delivers greater security and convenience.

The CVEdge 160 supports multiple authentication methods, including fingerprint authentication, RFID, QR code (static) and password verification. These authentication methods can be configured in various combinations to meet diverse risk profiles.

When CVEdge 160 is paired with ZKTeco's DE10 door expansion units, it can manage a maximum of 16 doors, allowing for scalable door control. Alternatively, the CVEdge 160 provides primary-secondary mode, connecting as many as 15 secondary CVEdge 160 units, making it ideal for campuses, banks, hospitals, and retail warehouses.

More importantly, CVEdge 160 stands out due to its video analytics functionality, including object detection, line-crossing detection and intrusion alarm. The CVEdge 160 can connect up to four IP cameras to monitor entrances from different angles and coordinate video analytics with access control for unified monitoring and event review. For instance, the areaintrusion alarm can be linked to access event to prevent tailgating, ensuring that only one person passes per valid credential. The CVEdge 160 also supports a 3.5-inch surveillance-grade HDD for local recording. Each alert event can trigger video capture for forensic review. Builtin video search helps operators quickly locate relevant event footage.

CVEdge 160 provides flexible connectivity for easy setup and unified management. Its onboard web console enables direct login from PC or mobile web browsers, even via device's Wi-Fi AP mode, so that you can manage devices, configure personnel management, access control and video analytics management, plus perform online firmware upgrade with no external server required.

2.1 Core Capabilities

- **Scalable Door Management**

Manage up to 16 doors by expanding with DE10 door expansion units (up to 15). Or by switching to primary–secondary mode and connecting up to 15 CVEdge 160 secondary controllers.

- **On-board Web Console for Local & Remote Access**

Features an on-board web console supporting PCs, mobile phones and tablets browser for device administration, personnel management, access control, video analytics configuration, and firmware updates via Ethernet or Wi-Fi AP mode-no external server required.

- **Multiple Authentication Methods and Expanded Capacities**

- Fingerprint authentication up to Supports 10,000 fingerprint templates (optional upgrade to 20,000).
- RFID authentication: up to 5,000 card users (optional upgrade to 100,000).
- QR code (static): up to 5,000 (Optional: 100,000)
- Transactions capacity: 300,000 records.

- **Connectivity for Unified Management**

- Provides RS485 for long-distance, multi-drop reader networks. TCP/IP uplink for connection to host PCs / platforms, enabling unified management and remote maintenance
- Support RS485 readers for RFID card and password authentications. Wiegand input via WR485 (RS485 to Wiegand) adapter, compatible with W26 / W34 / W66 formats (Coming soon).

- **Video Analytics for Greater Access Control Capabilities**

Each CVEdge 160 supports up to four IP cameras locally. When CVEdge 160 is switched to primary-secondary mode, scalable to 64 camera channels across 15 secondary CVEdge 160 units to monitor its local doors. Its video analytics include absence detection, line-crossing counting, object detection, area detection, and tripwire detection. Area-intrusion alarms integrated with access control: enforces single-person entry per valid credential. Alarm events trigger local recording with structured search for rapid footage retrieval.

- **Elevated Capacity and Data Security**

Supports 10,000 fingerprint templates (optional upgrade to 20,000), 5,000 card users (optional upgrade to 100,000) and 5,000 static QR codes (optional upgrade to 100,000). Each user can enroll up to two fingerprints: one for normal access and one for duress. Deploys the AES 256-bit algorithm encryption to protect data storage. And also secures communication between web clients through HTTPS / TLS1.2 encryption.

- **Versatile Connectivity**

Supports wired TCP/IP for PC access. It also supports Wi-Fi AP mode that turns CVEdge 160 into a local hotspot, connect your mobile devices to auto-launch the login page for instant on-site access.

- **Comprehensive Alarm System Integration**

The controller features one onboard auxiliary alarm input and supports seamless expansion through its RS485 interface. Add EX0808 I/O expansion boards-each provides 8 additional

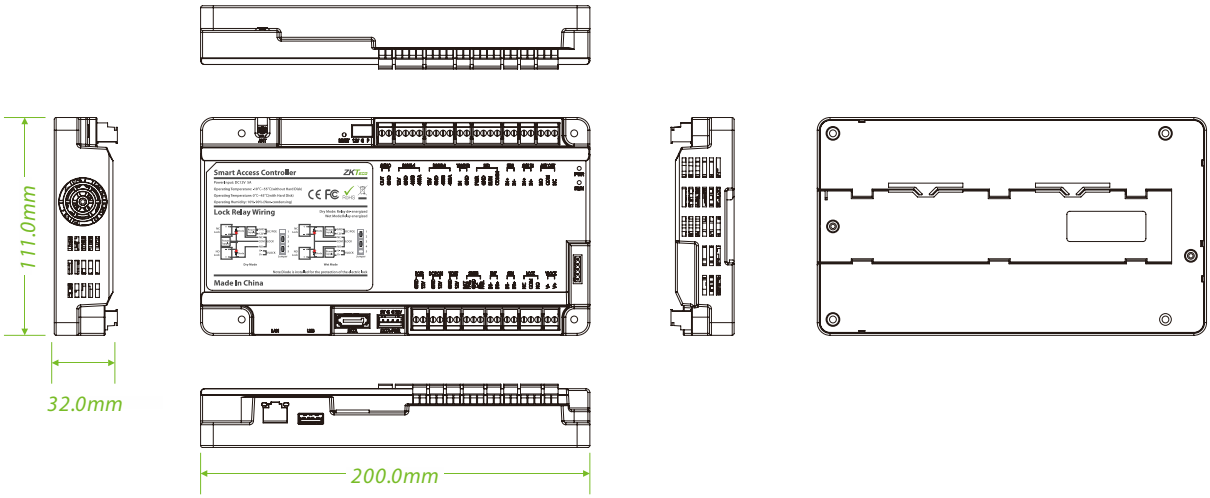
inputs-with support for up to 8 boards, scaling to 64 auxiliary inputs total. This scalable design lets you integrate a wide range of alarm sensors to handle diverse alarm types and evolving site requirements. The integrated AI video algorithms use computer vision for multi-type intelligent detection and alerting.

- **Advance Access Control Functions**

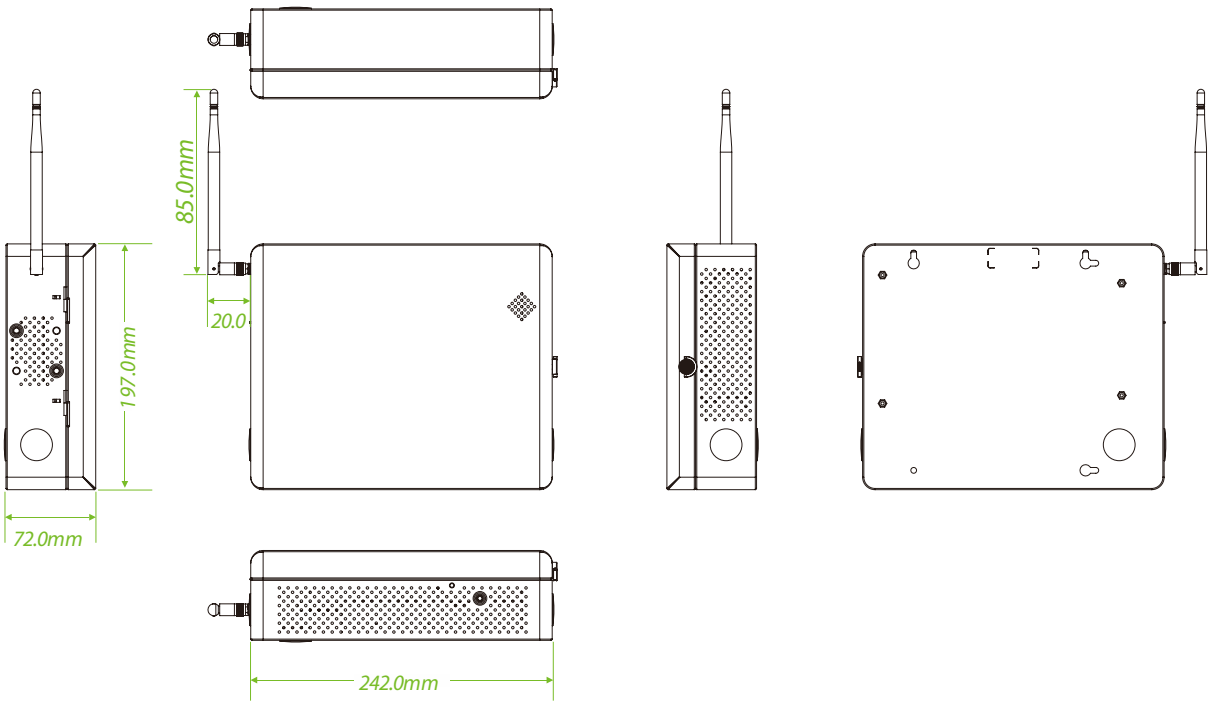
Equipped with a suite of standard access control functions including a built-in web server, support for up to 14-digit User IDs, customizable access levels and groups, holiday scheduling, anti-passback, anti-tailgating, and multiple verification methods.

2.2 Appearance

- **CVEdge160**



CVEdge160 Enclosure



2.3 Technical Specifications

Model	CVEdge160
Operation System	Linux
Hardware	CPU: Quad Core with max. clock rate 1.5GHz RAM: 2GB eMMC: 16GB Compute Power: 4 Tops
Authentication method	Fingerprint / RFID / QR code (static) / Password
Access Point Capacity	Onboard Access Point: 1 Scalabe Door Control Points: up to 16 via ZKTeco's DE10 door unit OR via Primary-Secondary mode
Type of Reader Supported	RS-485: ZKTeco RS-485 Protocol / OSDP (Version 2.1.7) Wiegand: 26 / 34 / 66-bit (via WR485) (Coming Soon)
IO Expansion Board Capacity	8pcs EX0808 (RS-485 connection)
User Capacity	5,000(Optional:100,000)
Card Capacity	5,000 (1:N) (Standard) Optional:100,000(1:N)
Fingerprint Template Capacity	10,000 (1:N) (Standard) Optional:20,000(1:N)
Facial Template Capacity	N/A
QR Code Capacity	5,000 (Static QR Code); Optional: 100,000
Transaction Capacity	300,000
Fingerprint Authentication Speed	less than 0.5sec (Fingerprint)
Fingerprint Authentication Algorithms	ZKFingerprint Algorithm V13.0(Default)/V10.0
False Acceptance Rate (FAR) %	FAR 0.0001% (Fingerprint)
False Rejection Rate (FRR) %	FRR 0.01% (Fingerprint)
Number of Inputs	1*Exit Button, 1*Door Status, 1 *AUX Inputs,1*Tamper,1*Fire Alarm; or 64 (with 8pcs of EX0808 IO expansion board)
Number of Outputs	1*Form C Relay for Lock, 1* Form C Relay for Aux Output, 1*Audio output; or 64 (with 8pcs of EX0808 IO expansion board)

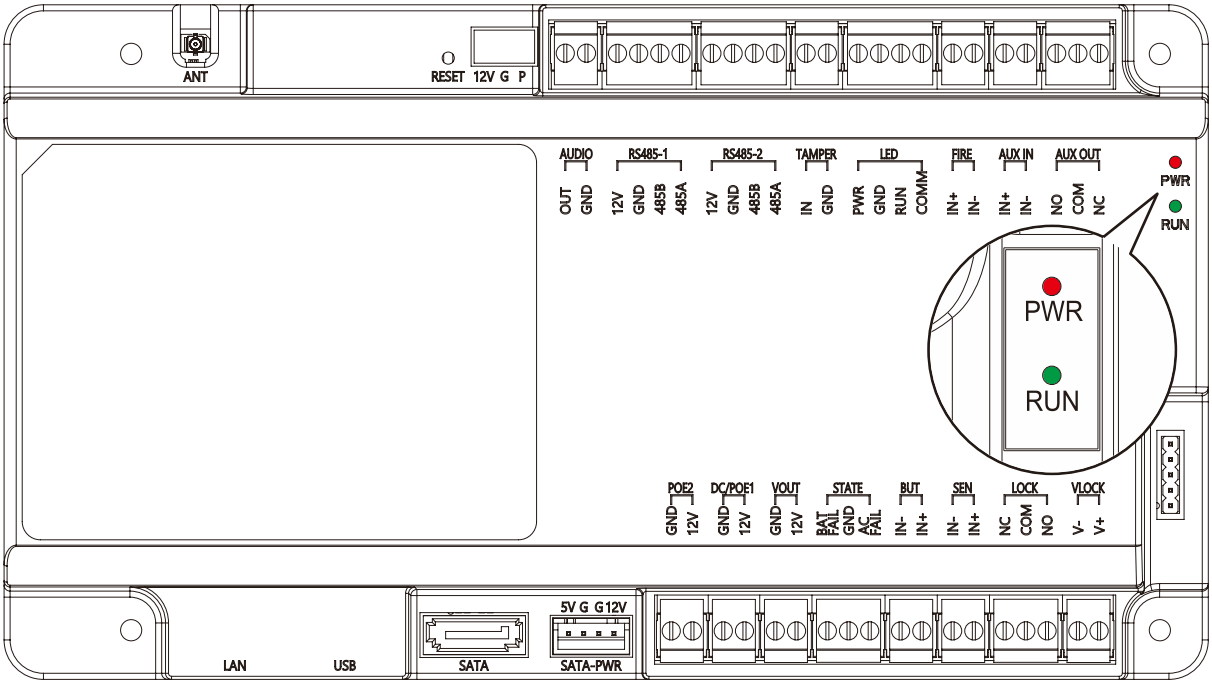
Max. Card Number Length	16 digits
QR Code	Standard QR code (Static)
Communication	TCP/IP *1 RS-485: ZKTeco RS-485 / OSDP (Optional)*2 USB 3.0: Type A (USB Drive Only)*1 SATA: (3.5" SATA HDD, up to 20TB)*1 Wi-Fi: IEEE 802.11 b/n/g @ 2.4 GHz; AP mode Aux Inputs *1, Aux Outputs *1, Electric Lock*1, Door Sensor*1, Exit Button*1, Alarm*1, Tamper*1, Audio out*1;
Standard Functions	Webserver, Up to 14-digit User ID, Access Levels, Access Groups, Holidays, Anti-passback, Anti-tailgating, Linkage, Global Linkage, Multiple Authentication Methods, Power Detection, LED Status Output, Primary-Secondary Mode.
Access Control Interface	RS-485 (RS-485 Card Reader / Fingerprint Reader / QR code Reader); Wiegand (Card Reader) (Coming soon)
Intelligent Video Analytics (IVA)	
Audio and video	Video Channel: 4 Decoding Format: H.264/H.265; Split Screen: 4; Decoding Capacity: 4; Synchronized Playback Channels: 4; Maximum video resolution: 8MP/5MP/3MP/1080P/960P/720P/D1VGAV4CIF/DCIF/2CIF/CIF/OCIF
Absence Detection (Standard)	Absence detection, Detects employee absence from designated stations. Configurable: zone occupancy count, motion sensing, time threshold. Alarm triggered when absence duration exceeded.
Cross-line Count (Standard)	Cross line statistics(target counting). Configurable detection lines within zones count targets crossing in / out. Supports flow statistics alarm (triggers when count reaches threshold within statistical interval) and cumulative statistics alarm (triggers when total count reaches threshold over defined period). Countable targets: person, motor vehicle, non-motor vehicle.
Object Detection (Standard)	Supports missing object detection, abandoned object detection, and object removal / abandonment detection.
Area Detection (Standard)	Monitors zone entry, exit, entry / exit, loitering, and intrusion (persistent alarm on zone breach).

Tripwire Detection (Standard)	Triggers when persons, motor vehicles, or non-motor vehicles cross designated lines.
Anti-Tailgating (Standard)	Validates single-person entry during access authentication. Video intrusion detection counts individuals in the verification zone-door unlocks only when exactly one person is detected. Door remains locked if count exceeds one or no person is detected.
Video Structured Search (Coming Soon)	Fast recorded video search based on on customizable criteria by person attributes (gender, age, clothing color, eyewear, mask, headwear) or vehicle attributes (licence plate number,licence color, vehicle type/color).
Optional Detection	Spark & Smoke Detection, Safety Hat Detection, Bear Detection, Pose Detection (Hands-up Duress mode), Pose Detection 3D(Fall Detection).
General	
Power Supply	DC 12V 5A
Operating Temperature	-10℃ to 55℃ (Without Hard Disk) 0℃ to 45℃ (With Hard Disk)
Operating Humidity	10% to 90% RH (Non-condensing)
Dimensions	200mm*111mm* 32mm (L*W*H)
Gross Weight	0.55 Kg
Net Weight	0.35 Kg
Ingress Protection	N/A
Supported Software	On-board web console
Installation	Supported DIN35 Rail / Wall mount / Metal Enclosure (Optional)
Enclosure (Optional)	Size: 242mm*197mm*72mm (L*W*H) Material: SPCC steel Net Weight: 2.12 kg (without hard disk)
Certifications	ISO14001, ISO9001, CE, FCC, Equivalent to RoHs
Factory ID	AC02-CB41H-42

3 Controller Terminal Description

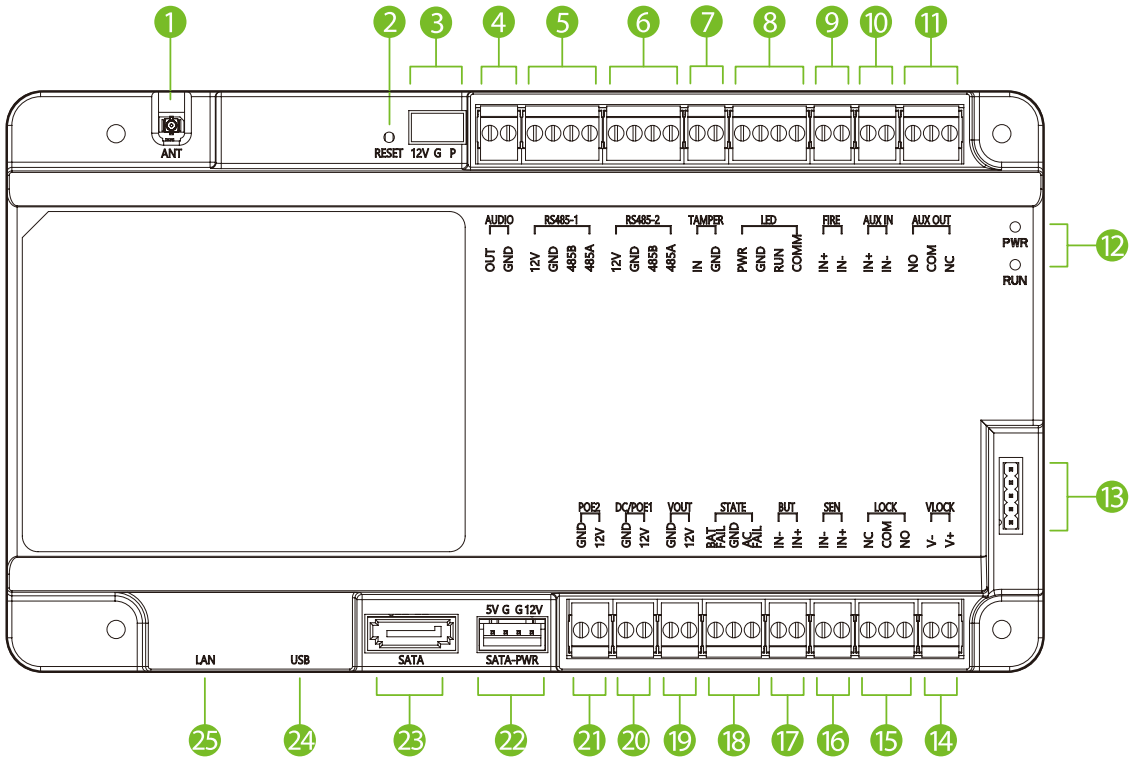
3.1 Description of the LEDs on the Controller Panel

When the CVEdge160 is powered on, normally the POWER indicator (red) is lit constantly, the RUN indicator (green) shall flash slowly (indicating the system is normal).



Menu	Color	Description
PWR	Red	Red light always on (power supply normal power supply) Red light off (abnormal power supply)
RUN	Green	Green light flashes slowly (system normal) Green light flashes fast (firmware upgrade in progress) Green light off (dead)

3.2 Terminal Description



No.	Name	Interface	Description
1	ANT	Wi-Fi / Bluetooth	Wi-Fi is used to provide hotspot services, enabling mobile devices to access the web via the hotspot for viewing or configuration purposes. The maximum number of simultaneous connections is 20.
2	Reset	Reset Switch	**Press 0 to 5 s:** Firmware upgrade (insert U disk beforehand). **Press 6 to 10 s:** Restart the device. **Hold ≥10 s:** Restore factory defaults. This reset includes: All device data is restored to factory defaults. Web-server default-account password reset to the factory default. The HTTPS port for web-server login is reset to the default 443. The device Wi-Fi hotspot password is reset to its factory default. Network parameters are reset to factory defaults. The LAN port IP address is initialized to 192.168.1.201. Server IP is initialized to 0.0.0.0 and server port to 8088. NTP is reset to the default disabled state. All device parameters are reset to factory defaults.

3		12V, G, P	
4	AUDIO	OUT, GND	Connect an external amplifier for voice output
5	RS485-1	12V, GND, 485B, 485A	Connects 2 readers (single door)
6	RS485-2	12V, GND, 485B, 485A	Connects up to 8 EX0808 expansion boards
7	TAMPER	IN, GND	Timely notification to stop illegal dismantling of device. Maximum input voltage 12VDC.
8	LED	PWR, GND, RUN, COMM	Extended Status Indicator (enclosure): PWR (Red LED) : Normal power on, light red. RUN (Green LED) : Flashes when normal, off if abnormal. COMM (Yellow LED) : Normal send/receive data, yellow light flashes.
9	FIRE	IN+, IN-	Fire input, external fire button, trigger the fire button, all doors forced normally open Maximum input voltage 12VDC.
10	AUX IN	IN+, IN-	Auxiliary input, can be connected to infrared human body sensing detector, fire alarm or smoke detector, etc. Maximum input voltage 12VDC.
11	AUX OUT	NO, COM, NC	Auxiliary output, can be connected to alarm or doorbell, etc. Maximum switching voltage of the contact is 24VDC, maximum switching current is 1A.
12	LED	PWR, RUN	PWR (Red LED): Normal power on, light red. RUN (Green LED): Flashes when normal, off if abnormal.
13	Jumpers	1, 2, 3, 4, 5	By setting the jumper terminal, you can select the device power supply or lock power supply for the lock (that is, the wet mode or dry mode). Wet mode jumper: short 1-2 and 3-4 Dry mode jumper: short 2-3 and 4-5
14	VLOCK	V-, V+	Provides power to the lock and supports wet mode.
15	LOCK	NC, COM, NO	Connecting door lock Maximum switching voltage of contacts 30VDC, maximum switching current 5A.

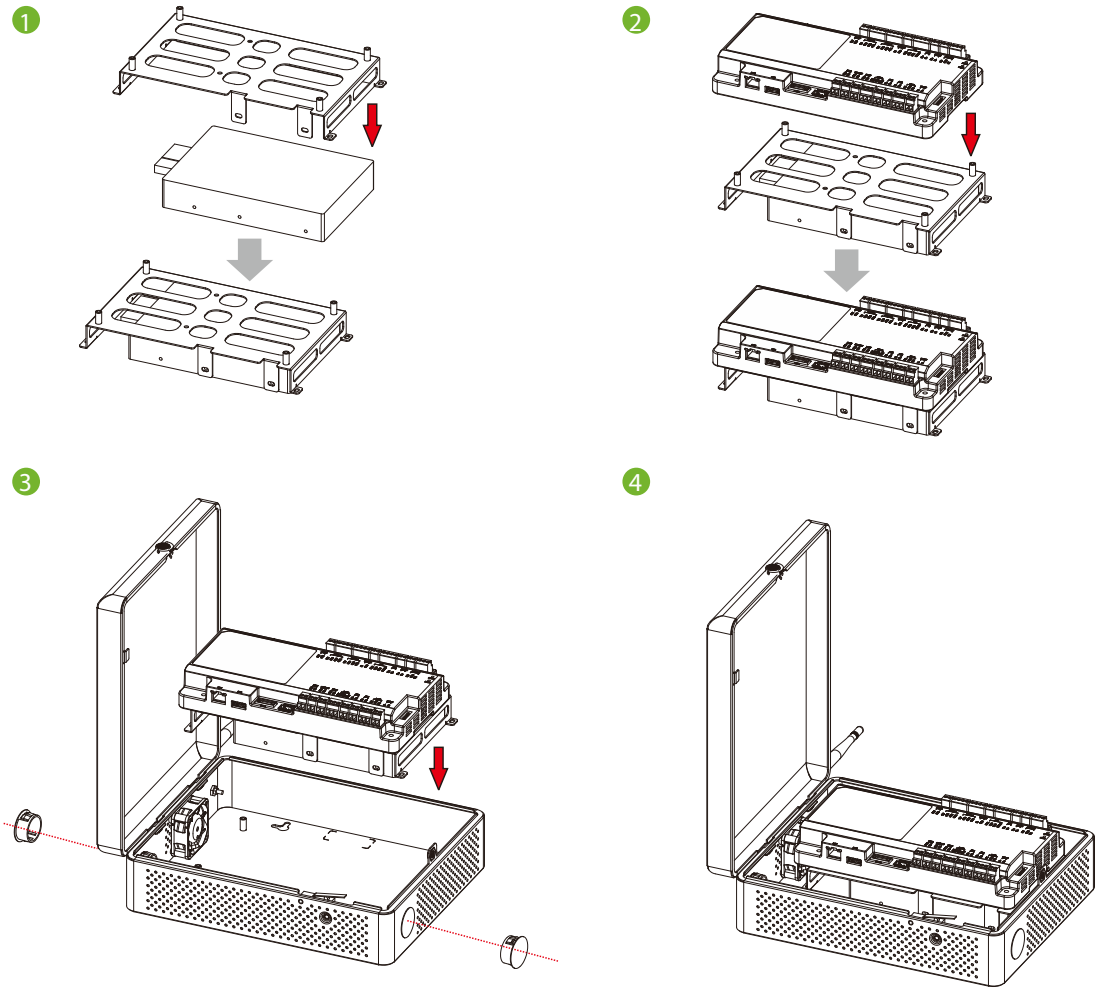
16	SEN	IN-, IN+	Connecting door sensor Maximum input voltage 12VDC
17	BUT	IN-, IN+	Connection of door exit button Maximum input voltage 12VDC
18	STATE	BAT FAIL, GND, AC FAIL	
19	VOUT	GND, 12V	Power Output
20	DC/POE1	GND, 12V	Power Input, AC power supply, 12V, 5A
21	POE2	GND, 12V	coming Soon
22	SATA-PWR	5V, G, G, 12V	SATA power interface
23	SATA		SATA data interface supports connecting external 3.5-inch hard drives .
24	USB		USB 3.0 port for saving background logs and image burning (excluding firmware upgrades).
25	LAN		Connect a switch for network communication.

4 Installation and Connection

Ensure that the device is installed following the provided installation instructions. Failure to do so may result in voiding of the devices warranty.

4.1 Installing the controller into the enclosure

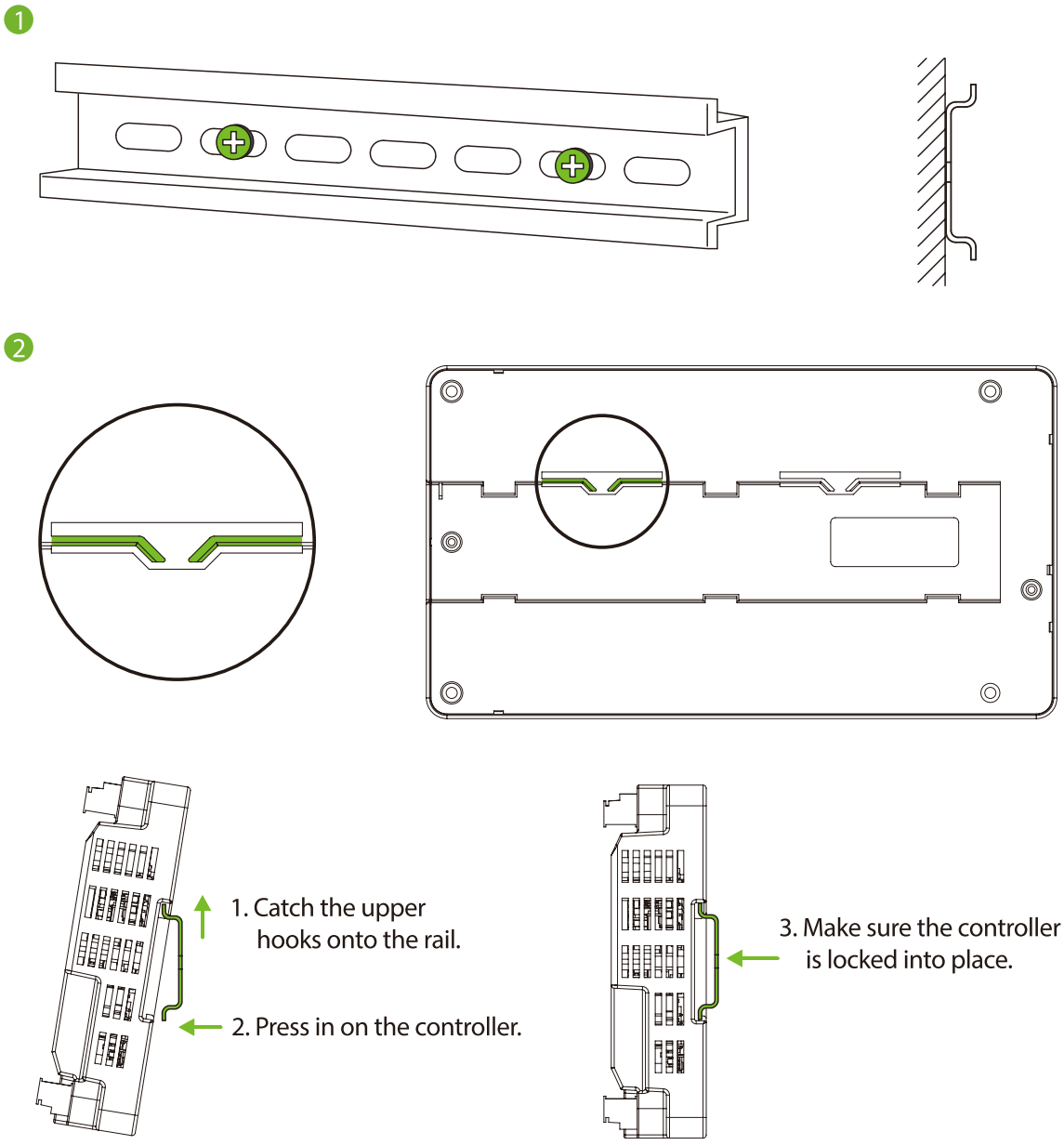
1. Secure the hard drive in the bracket.
2. Then use screws to fix the controller to the bracket.
3. Finally, install the bracket into the enclosure and insert the rubber plugs on both sides.



Note: *The metal enclosure is equipped with an tamper alarm switch. When it is working normally, please keep the enclosure closed.*

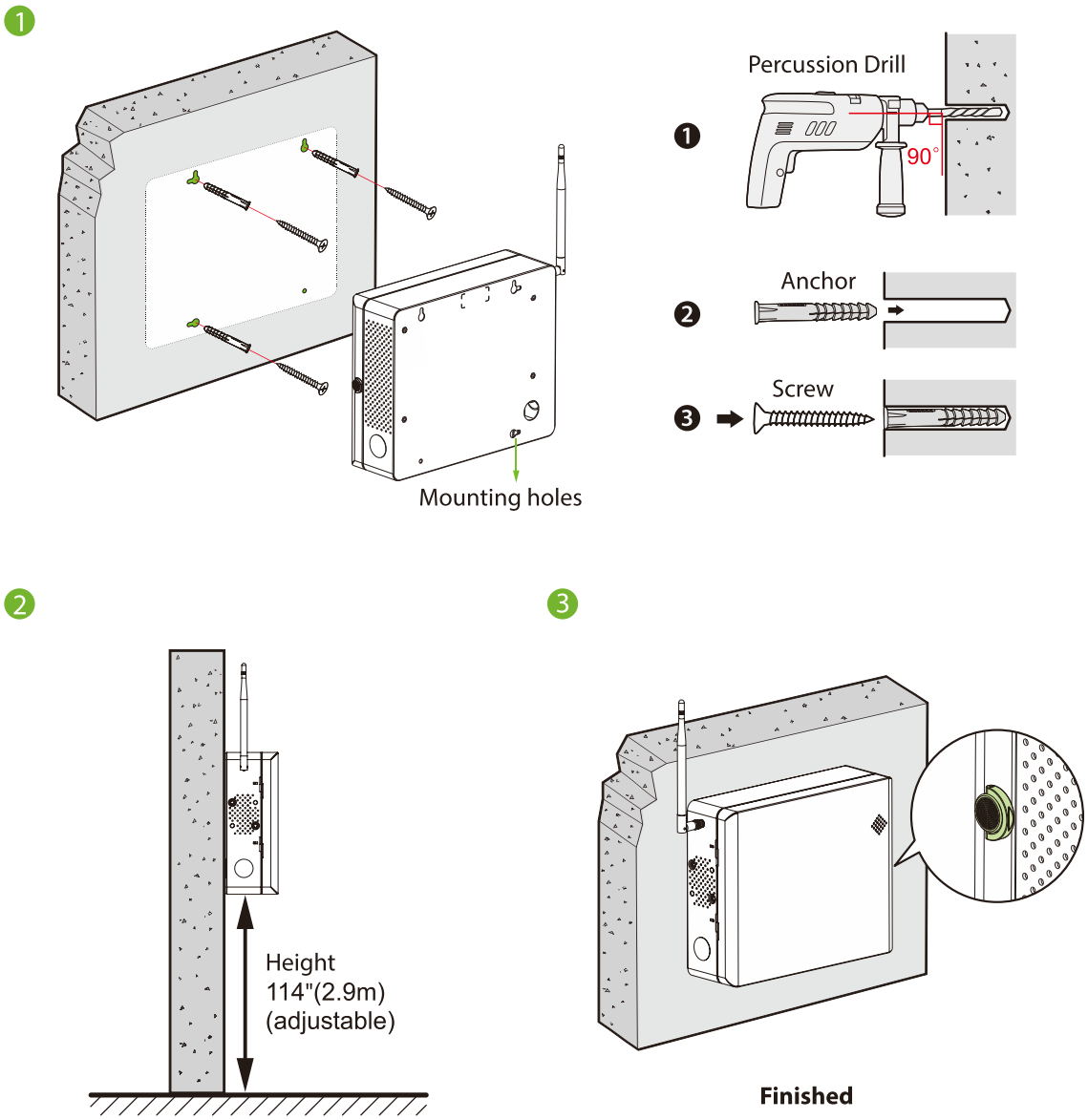
4.2 Installation with 35mm rail

1. Mount the rail directly onto a flat surface, as illustrated in the figure below. Then use screws to fix the controller to the bracket.
2. Engage the hooks on the top of the controller with the rail and firmly press the controller onto the rail until it locks into place.

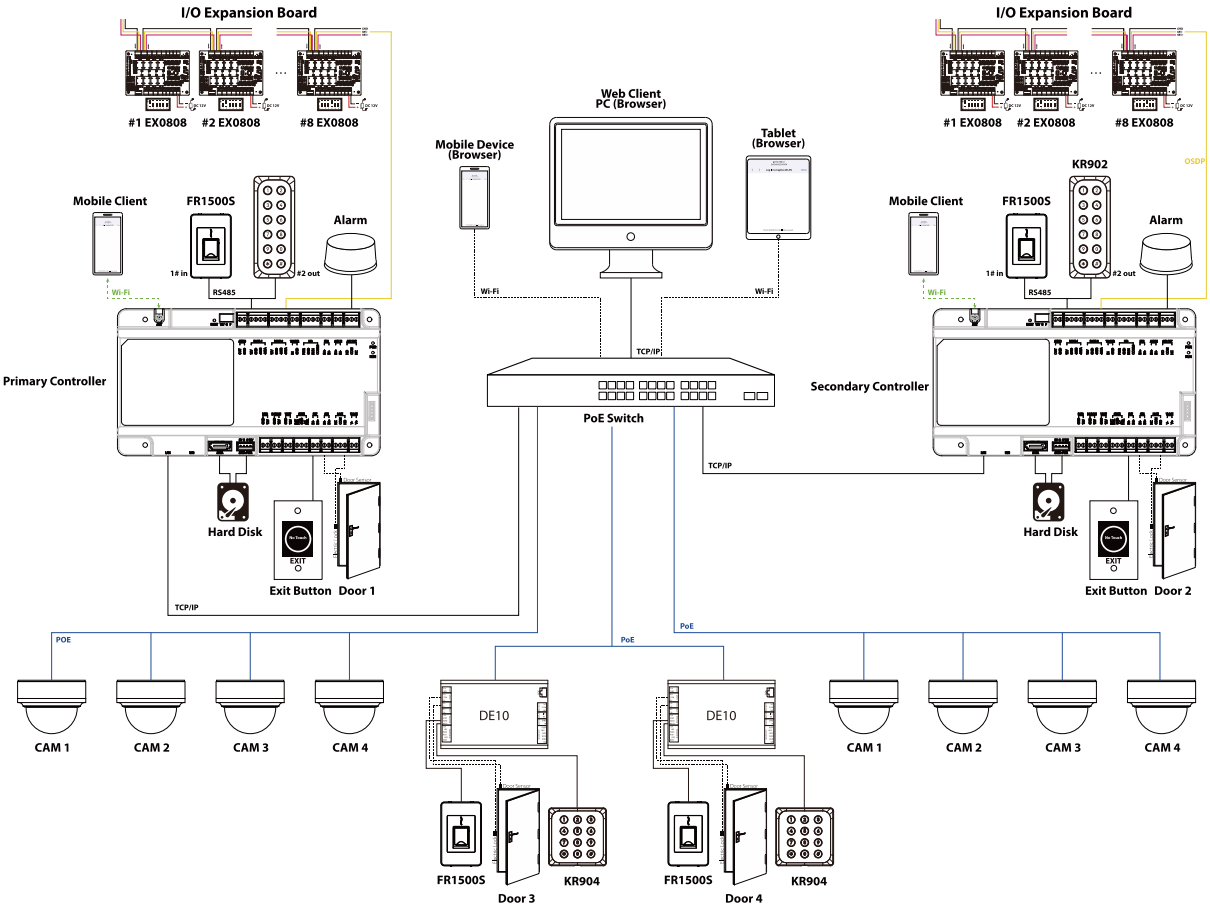


4.3 Installation of the Metal Enclosure on the wall

1. According to the mounting holes position of the metal enclosure. Drill three mounting holes in a suitable spot on the wall and make sure it is about 114 inches (2.9m) above the ground, which can be adjusted according to actual needs. Take care to leave at least 3.937 inches (100 mm) on the left side of the metal enclosure.
2. Insert anchors into the mounting holes and place self-tapping screws into them.
3. Then hook the metal enclosure onto the wall as shown below. Secure the metal enclosure in place.



4.4 Controller System Installation



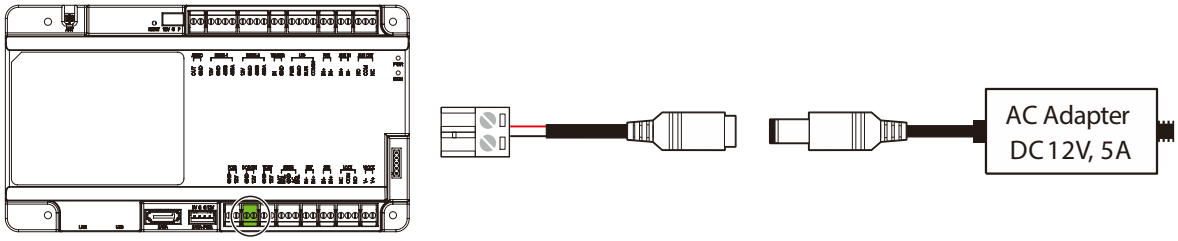
Notes:

- *The auxiliary input can connect to infrared body detectors, fire alarms, or smoke detectors, etc.*
- *The auxiliary output can connect to alarms, cameras or doorbells, etc.*
- *Up to eight EX0808 expansion boards can be connected to one controller to expand a certain number of auxiliary inputs and auxiliary outputs. The RS485/OSDP address of each EX0808 is set via the DIP switch before power is applied. Each EX0808 requires a separate power supply.*
- *Single door 4-way IPC is supported by default.*
- *The CVEdge160 (primary controller) adds DE10 door controls via device management to increase the number of doors. Up to 15 DE10s can be added.*

5 Access Controller Wiring

5.1 Wiring Description

5.1.1 Power Wiring

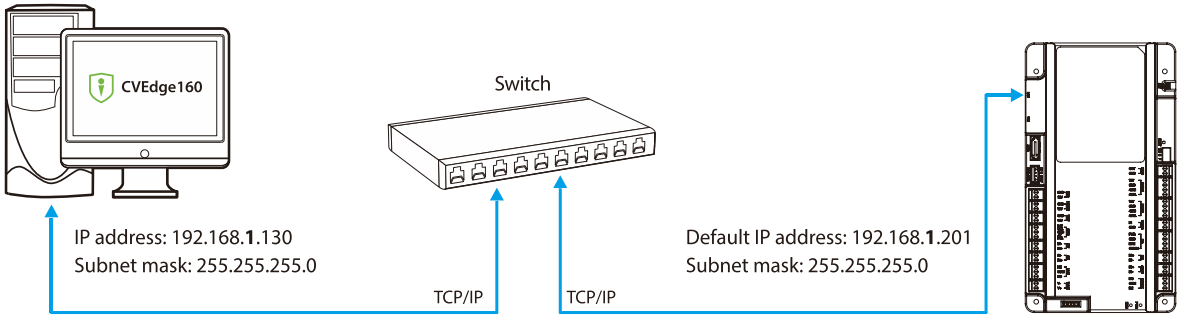


Recommended power supply:

- Recommended AC adapter: **12V, 5A**.
- To share power with other devices, use an AC adapter with higher current ratings.

5.1.2 Network Wiring

Establish the connection between the device and the software using an Ethernet cable. An illustrative example is provided below:

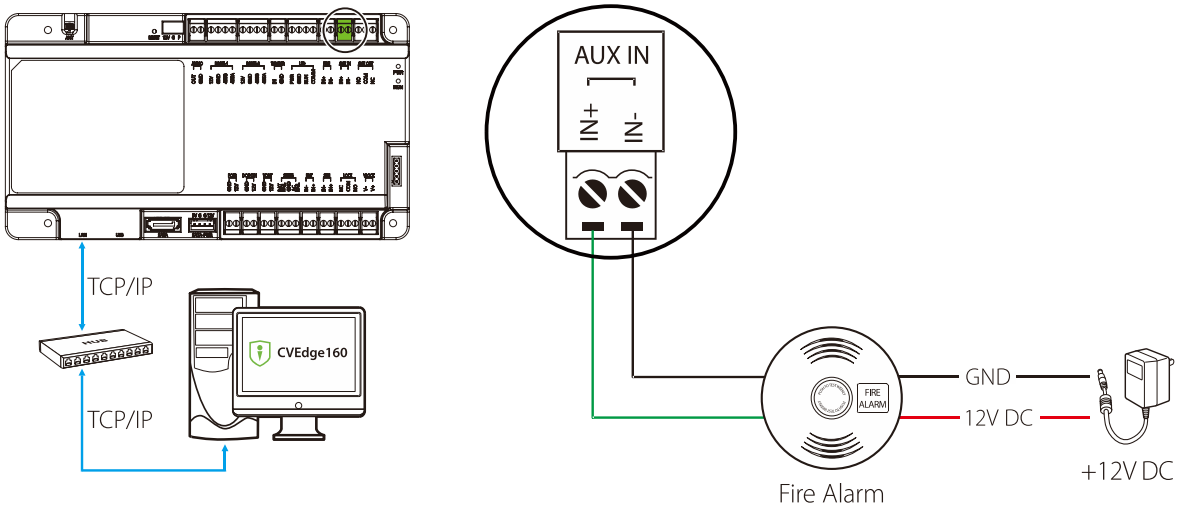


Note:

- *In LAN, IP addresses of the server (PC) and the device must be in the same network segment when connecting to the software.*
- *The default IP address of the controller is 192.168.1.201.*

5.1.3 Auxiliary Input Wiring

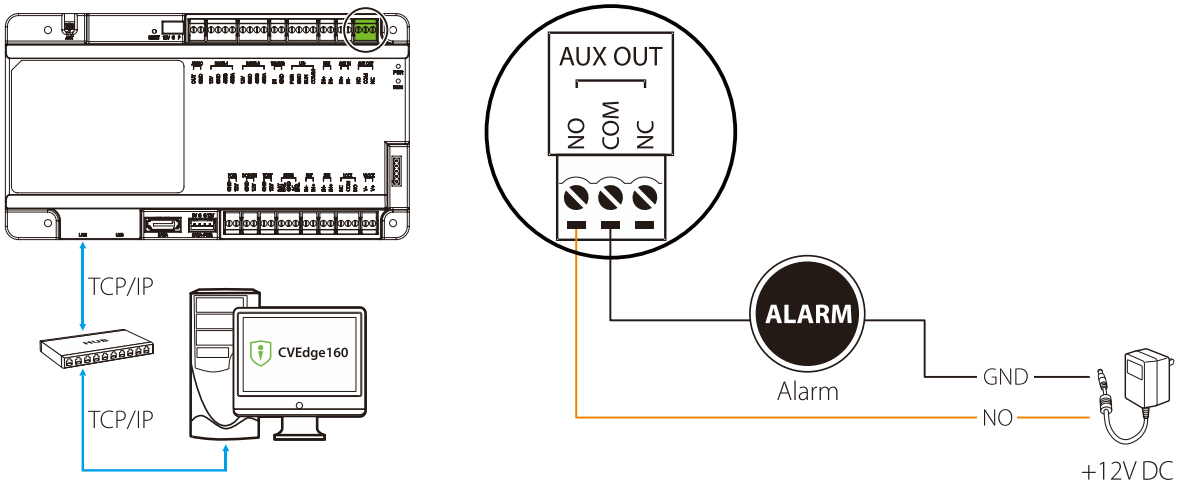
The CVEdge160 provides one auxiliary input interface, which may connect to infrared body detectors, smoke detectors, gas detectors, window magnetic alarms, wireless exit switches, etc. Auxiliary inputs are set through the relevant access control software. Please refer to the relevant user manual for details. The following is an example of wiring with fire alarm only.



5.1.4 Auxiliary Output Wiring

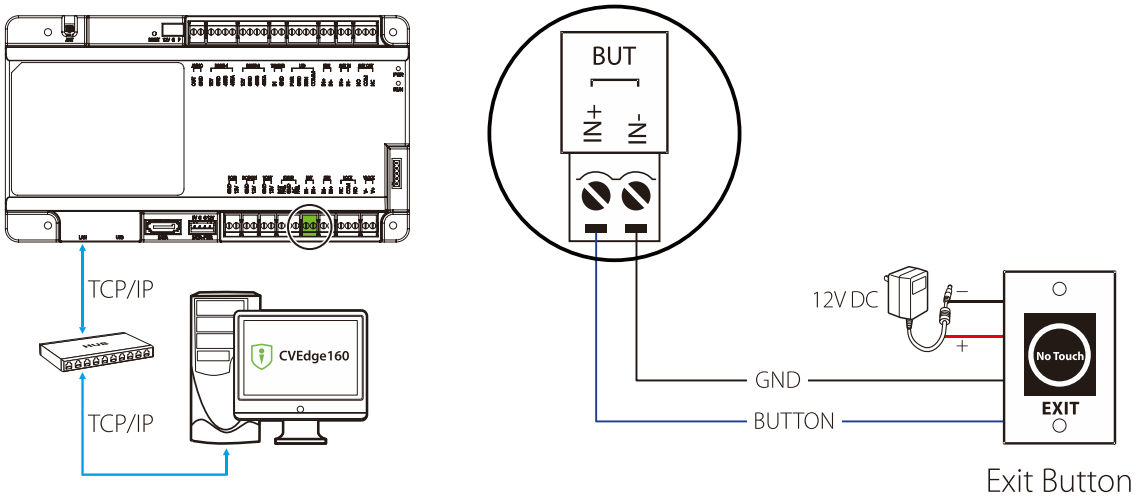
The CVEdge160 has two relays (one used as control lock by default, and the other one used as auxiliary output).

The relays for auxiliary outputs may connect to monitors, alarms, doorbells, etc. Auxiliary outputs are set through the relevant access control software. Please refer to the respective software manual for details. The following is an example of wiring with alarm only.



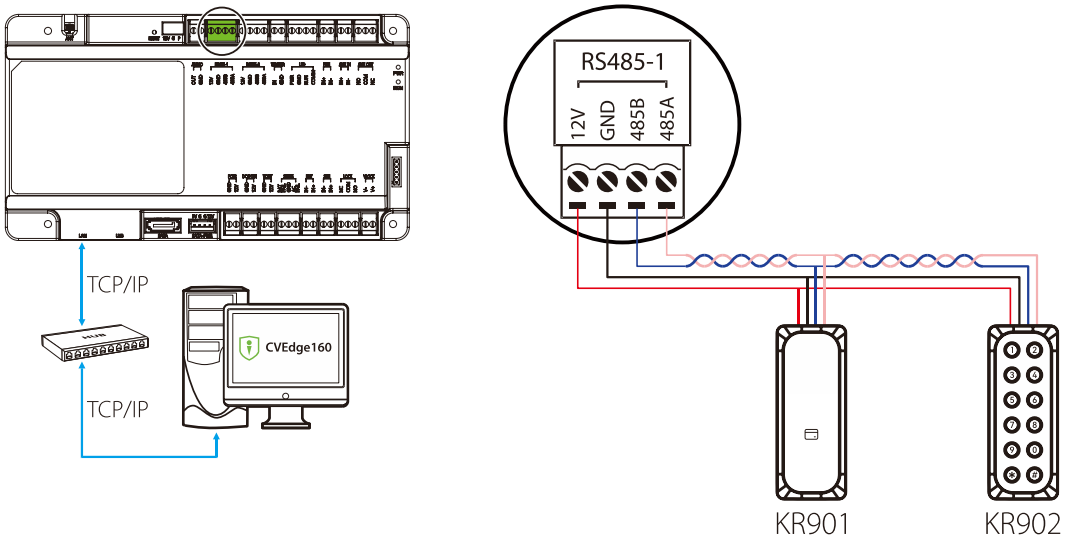
5.1.5 Exit Button Wiring

An exit switch is a switch installed indoor to open a door. When it is switched on, the door will be opened. An exit button is fixed at the height of about 1.4m above the ground. Ensure it is located in the right position without slant, and its connection is correct and secure.



5.1.6 RS485 Reader Wiring

The CVEdge160 can connect two RS485 readers in the one-door two-way mode.



Setting the RS485 Address:

RS485 reader connection: Set the RS485 address (device number) of the reader by DIP switch or software.

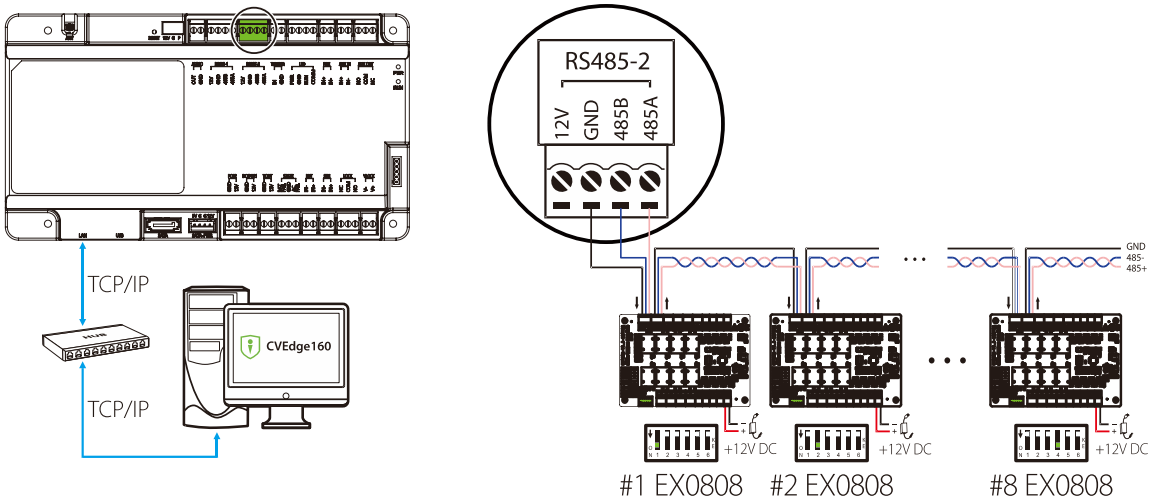
Controller \ RS485 Address	1	2
CVEdge160	#1 Door IN	#1 Door OUT

5.1.7 RS485 Extension Communication Wiring

The CVEdge160 can be connected to the EX0808 expansion board via RS485.

What is EX0808?

EX0808 is an extended module for controllers which is used for connecting more number of auxiliary devices.



Important Notes:

1. Configure the ZK485 protocol through the RS485 port to connect up to eight EX0808 expansion boards to expand a certain number of auxiliary inputs and auxiliary outputs.

   Note: *Set DIP switch **#5** of the expansion board to the **OFF** position.*

2. Configure the **OSDP** protocol through the RS485 port to connect up to eight EX0808 expansion boards to expand a certain number of auxiliary inputs and auxiliary outputs.

   Note: *Set DIP switch **#5** of the expansion board to the **ON** position.*

3. The RS485/OSDP address of each EX0808 is set via the DIP switch before power is applied.
4. Each EX0808 requires a separate power supply. Up to eight auxiliary input devices and eight auxiliary output devices can be connected to one EX0808.

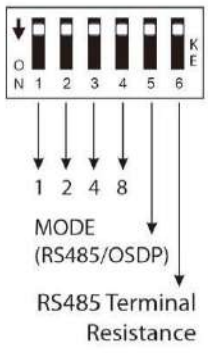
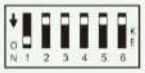
- **DIP Switch Setting for RS485/OSDP Communication**

There are six DIP switches on the EX0808 expansion board and their functions are:

1. Switches 1-4 are used to set the RS485/OSDP addresses.
2. Switch **5** is for RS485/OSDP mode switching. When set to **OFF**, RS485 mode is used, and when set to **ON**, OSDP mode is used.

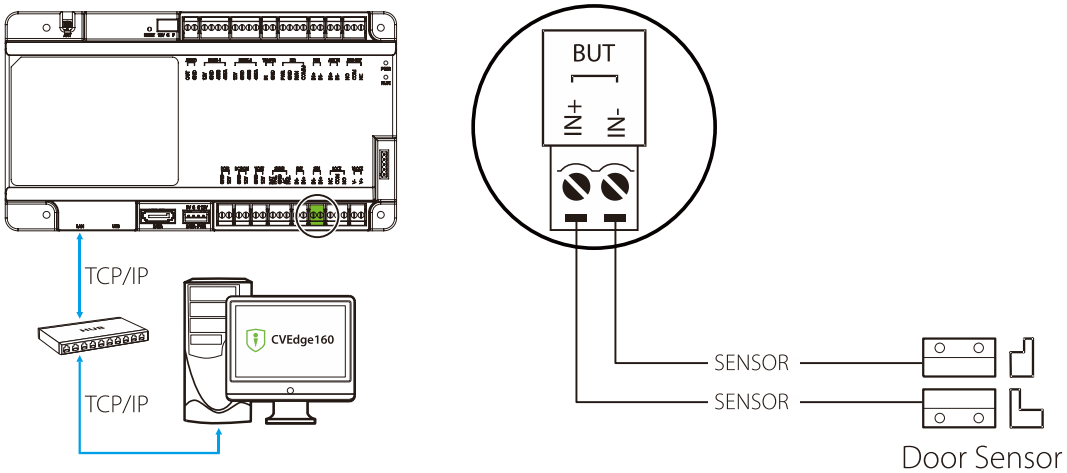
3. If the cable length is more than 200 meters, the switch **6** should be **ON** for noise reduction on long RS485 cables.
4. The detailed settings of the DIP switches are shown in the table 4-1 below.

Table 5-1 - DIP Switch Setting for RS485/OSDP Communication

Description	RS485 Address	DIP Switch	RS485 Address	DIP Switch	RS485 Address	DIP Switch
	1		6		11	
	2		7		12	
	3		8		13	
	4		9		14	
	5		10		15	

5.1.8 Door Sensors Wiring

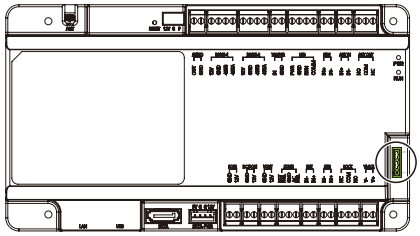
A Door Sensor is used to sense the open/close status of a door. With a door sensor switch, an access control panel can detect the unauthorized opening of a door and will trigger the output of alarm. Moreover, if a door is not closed within a specified period after it is opened, the door control panel will also raise the alarm. It is recommended to select two-core wires with a gauge over 0.22 mm^2. A door sensor can be omitted if it is unnecessary to monitor the open/closed status of a door, raise the alarm when the door is not closed for a long time, monitor if there is unauthorized access, and use the interlock function.

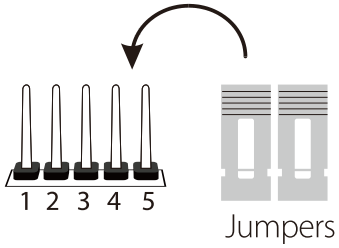


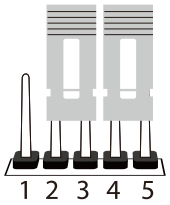
5.1.9 Lock Relay Wiring

1. The CVEdge160 provides one electronic lock outputs. The COM and NO terminals apply to the locks that are unlocked when power is connected and locked when power is disconnected. The COM and NC terminals use the locks that are locked when power is connected and unlocked when power is disconnected.
2. To protect the access control system against the self-induced electromotive force generated by an electronic lock at the instant of switching off/on, it is necessary to connect a diode in parallel (please use **FR107** delivered with the system) with the electronic lock to release the self-induced electromotive force during the onsite connection for application of the access control system.
3. By setting the jumper terminal, you can select the device power supply or lock power supply for the lock (that is, the wet mode or dry mode). The factory default jumper setting is Web Mode.

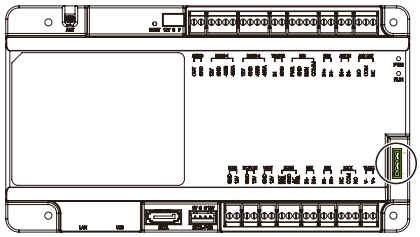
- **Dry mode jumper setting:** short 2-3 and 4-5  , and the device power supply will be used for the relay output.

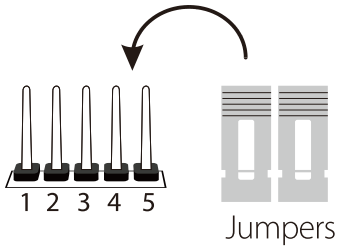


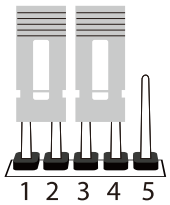




- **Wet mode jumper setting:** short 1-2 and 3-4  , and the lock power supply will be used for the relay output.



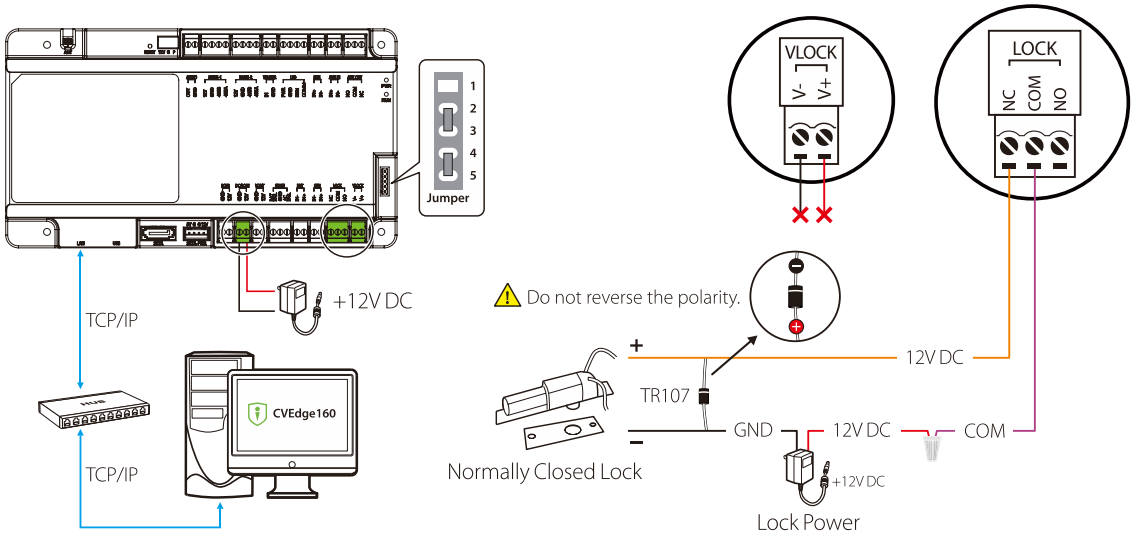




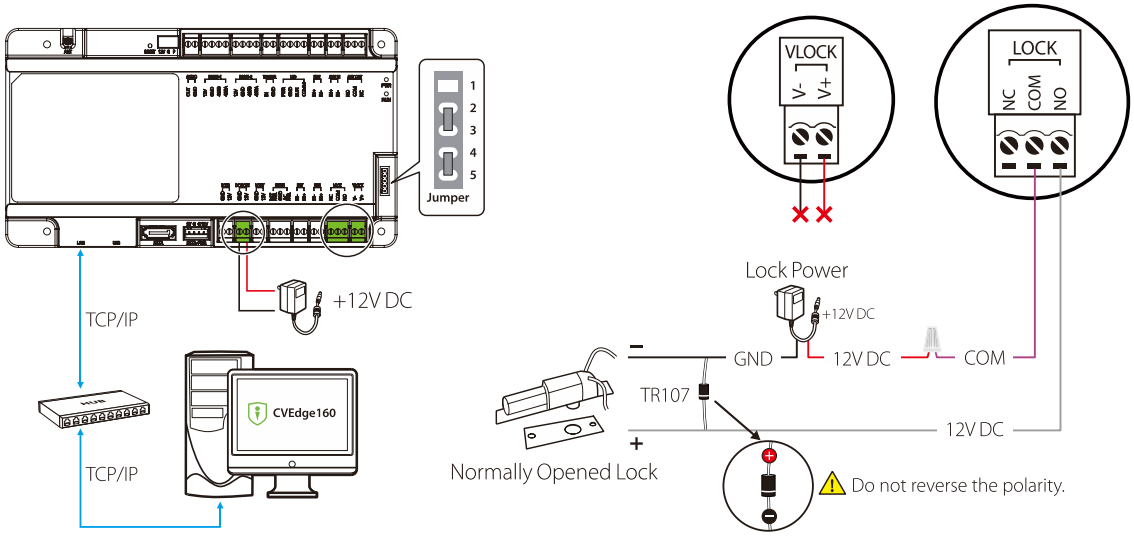
The system supports both **Normally Opened Lock** and **Normally Closed Lock**. The **NO LOCK** (normally opened at power on) is connected with '**NO**' and '**COM**' terminals, and the **NC LOCK** (normally closed at power on) is connected with '**NC**' and '**COM**' terminals. The wiring is as shown in the figure below:

- **Controller not sharing power with the lock(Dry Connect)**

Normally Closed Lock Powered From Lock Terminal:

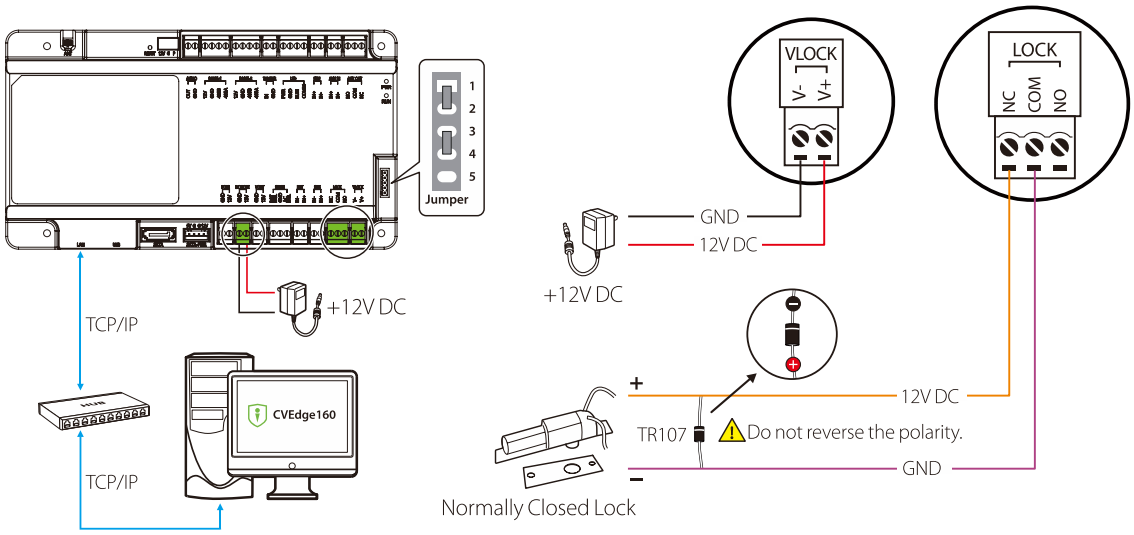


Normally Opened Lock Powered From Lock Terminal:

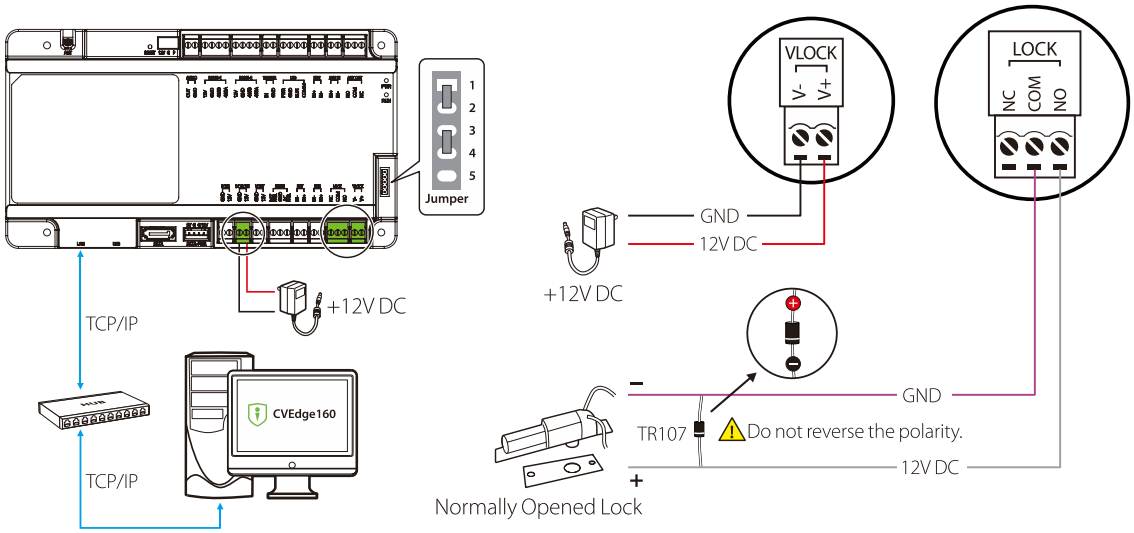


- **Controller sharing power with the lock (Wet Connect)**

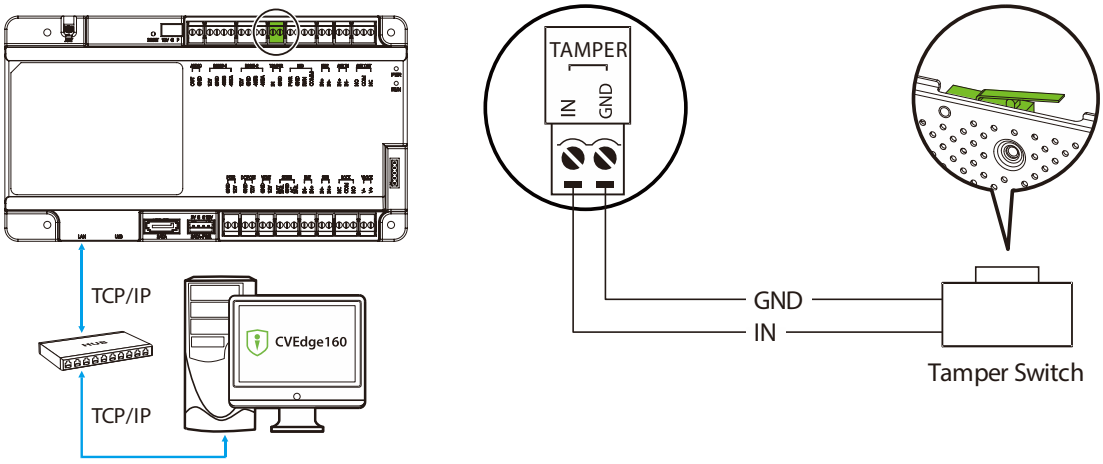
Normally Closed Lock Powered From Lock Terminal:



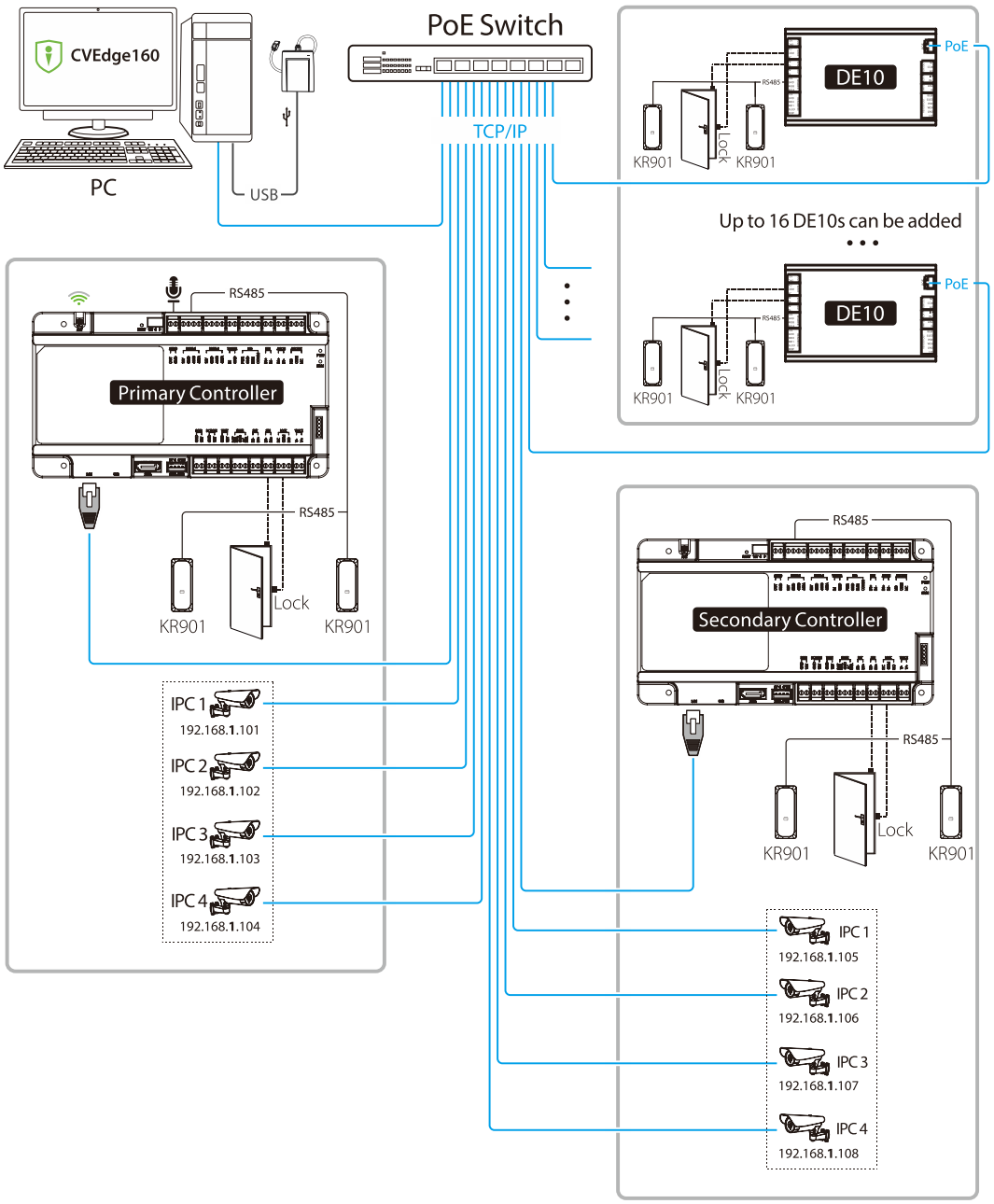
Normally Opened Lock Powered From Lock Terminal:



5.1.10 Tamper Switch Wiring



5.2 Network Topology Diagram



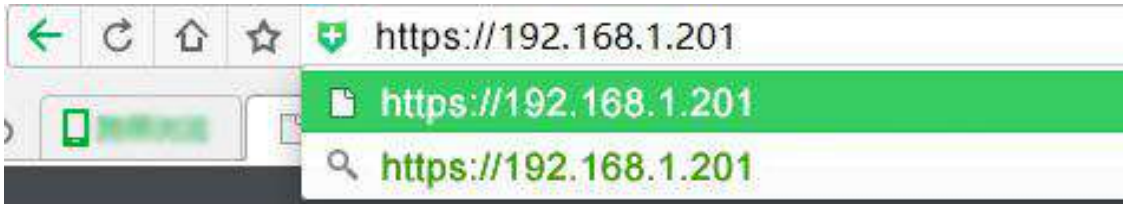
1. The CVEdge160 (primary controller) connects directly to the reader and lock via RS485, and binds 4 IPC cameras through TCP/IP.
2. The CVEdge160 (primary controller) adds another CVEdge160 (secondary controller) through device management to function as a door control unit. The secondary controller cannot expand the number of doors; it can only connect to readers and locks, along with 4 IPC cameras.
3. The CVEdge160 (primary controller) expands the number of doors by adding DE10 door control units through device management. The DE10 then connects to readers and locks. Connect up to 16 doors.

6 Connect to the Web Server

To help users conveniently manage the controller, the controller has a on-board web console. Using this feature, users can connect to the controller via a PC and enter the controller's IP address to access the Web. users can also use the Web server feature to configure parameters such as network configuration, application configuration, application scene, and system management.

6.1 Login to the Web Server

1. Connect the controller to the network or PC, start the browser, enter the IP address of the controller, which is **https://192.168.1.201** by default. Then you can visit the Web Server.



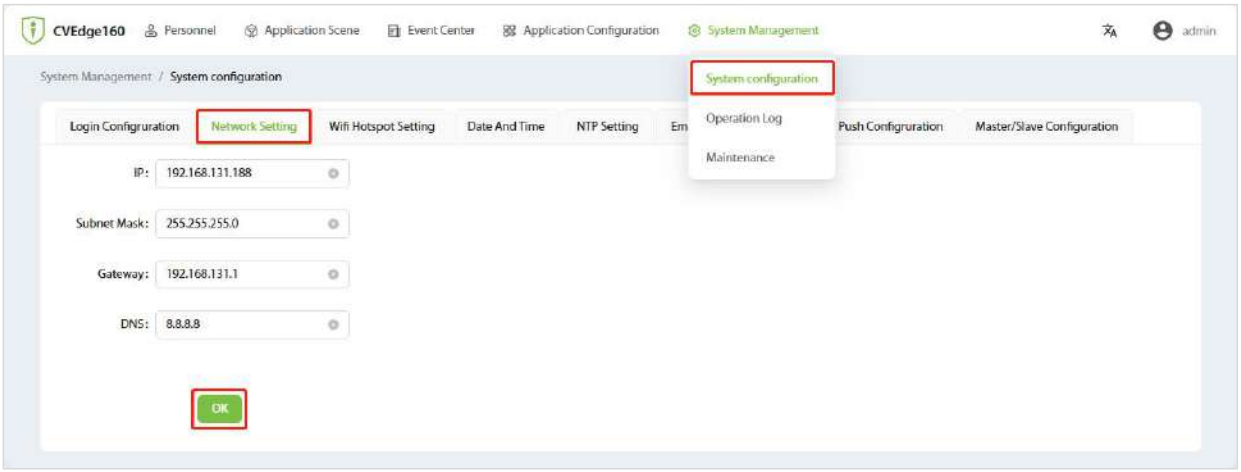
2. After entering the login screen, enter the default administrator account and password. The default “user name” is **admin** and the default “password” is **Zk@123**.

3. Click **Login** to access the Web Server.

Note:*IP addresses of both the server (PC) and the controller must be in the same network segment.*

6.2 Network Settings

1. Click [**System Management**] - [**System configuration**] in the top menu bar to enter the parameter setting interface. Then click [**Network Setting**] to modify the IP address of the controller.



Function introduction:

IP: the default IP is 192.168.1.201, and you can modify according to the actual.

Subnet Mask: the default subnet mask is 255.255.255.0, and you can modify according to the actual.

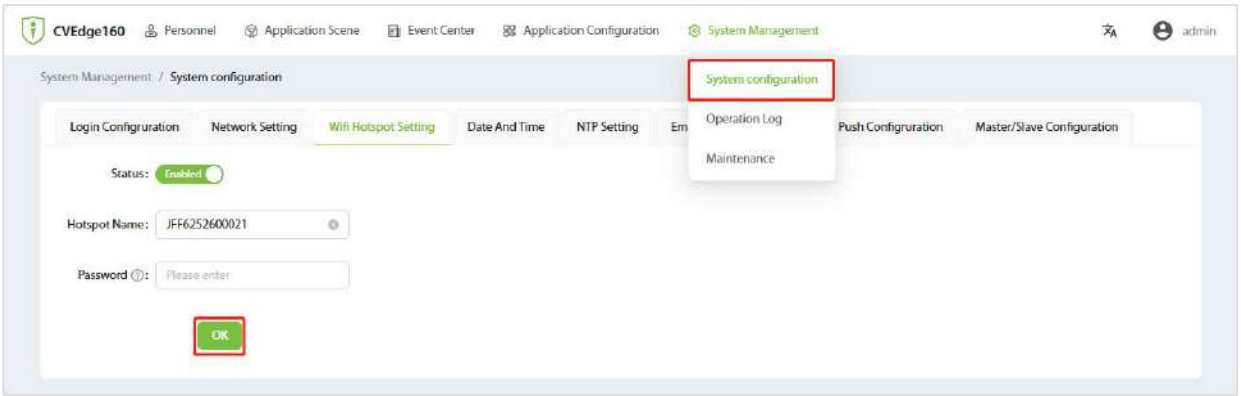
Gateway: the default gateway is 0.0.0.0, and you can modify it according to the actual.

DNS: the default value is null, and you can set its value.

2. Click [**OK**] to write parameters into the device. Please restart the device by manual.

6.3 WiFi Hotspot Setting

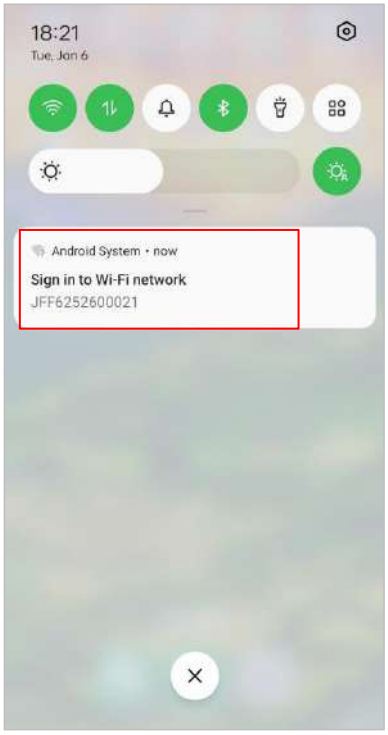
1. Click [**System Management**] - [**System configuration**] in the top menu bar to enter the parameter setting interface. Then click [**WiFi Hotspot Setting**] to set the Wi-Fi hotspot of the controller.



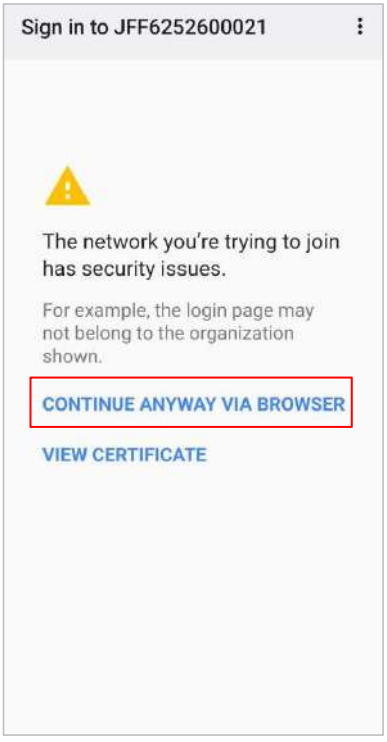
2. Enter the hotspot name and password and click [**OK**].

Access CVEdge160 software via mobile phone:

1. After completing the setup, enable the Wi-Fi function on your smartphone and connect to this hotspot.

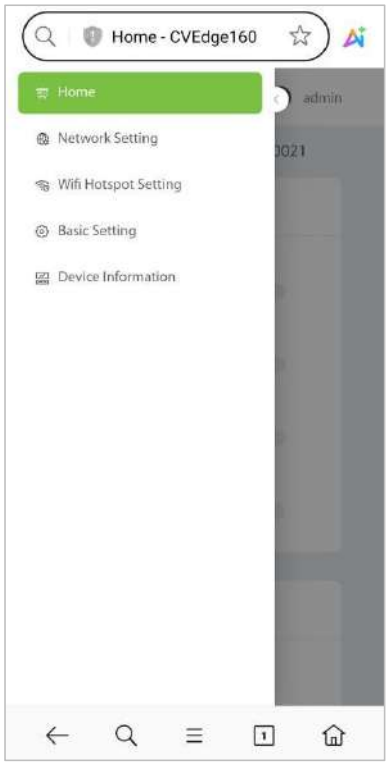


2. Connect to the hotspot as prompted, then proceed to the CVEdge160 login screen.



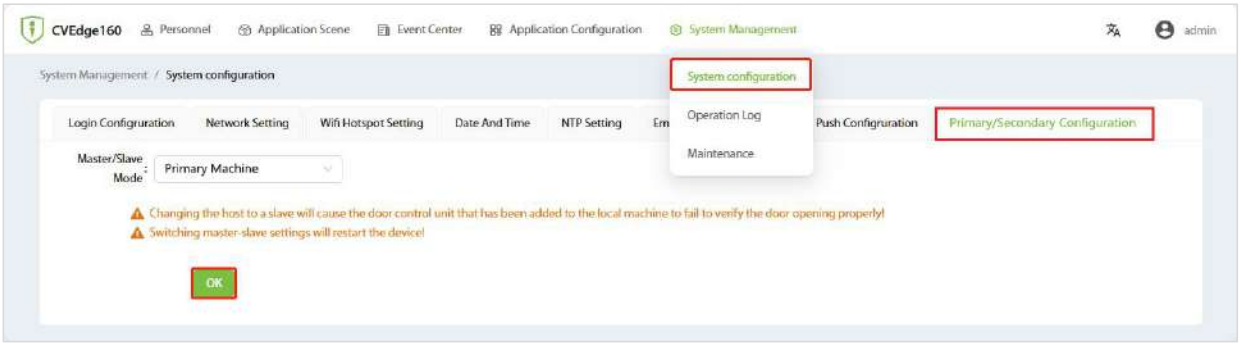
3. Enter your username and password. The default username is admin, and the default password is **Zk@123**.

4. After logging in, you can view or configure certain parameters.



6.4 Primary/Secondary Configuration

1. Click [**System Management**] - [**System Configuration**] in the top menu bar to enter the parameter setting interface. Then click [**Primary/Secondary Configuration**] to switch the primary/ secondary settings.



2. Click [**OK**] and the device reboots to take effect.

Notes:

*1) The device factory defaults to the primary controller. Switching primary-*secondary *settings will restart the device.*

2) Changing the primary to the secondary will cause the door control unit that has been added to the local unit to not be able to verify the door opening normally.

3) The secondary controller is only used as a door control unit, it is not allowed to expand the number of doors, but it supports the use of connecting expansion boards.

4) The secondary can only view the personnel list, and cannot make any editing.

6.5 Add Device

The types of devices that can be added are secondary controllers, door unit exboard, I/O expansion boards, and IPC. There are two ways to add by searching and adding manually, depending on the device.

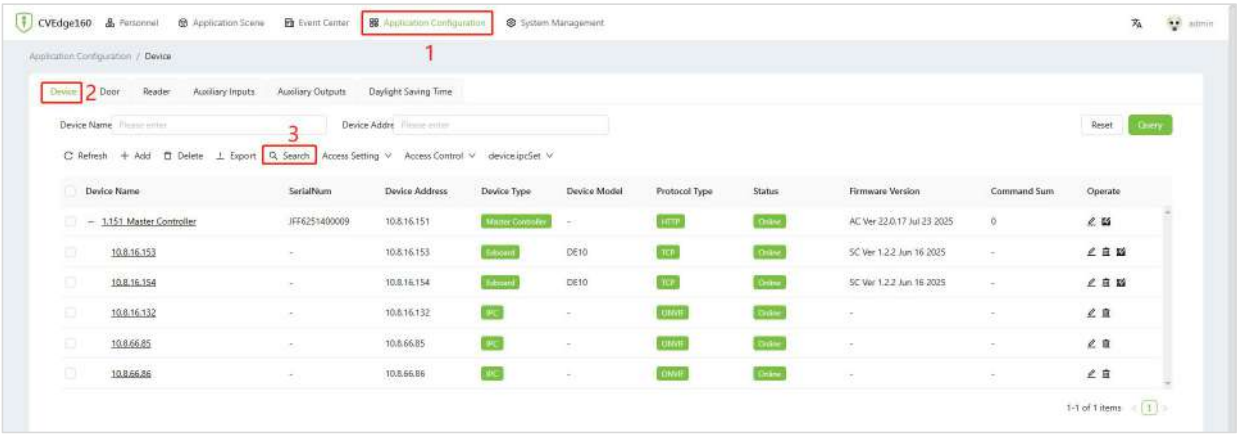
Note: *I/O expansion boards can now only be added via new additions. When spanning subnets, subcontrollers can be searched and added if configured with this host address.*

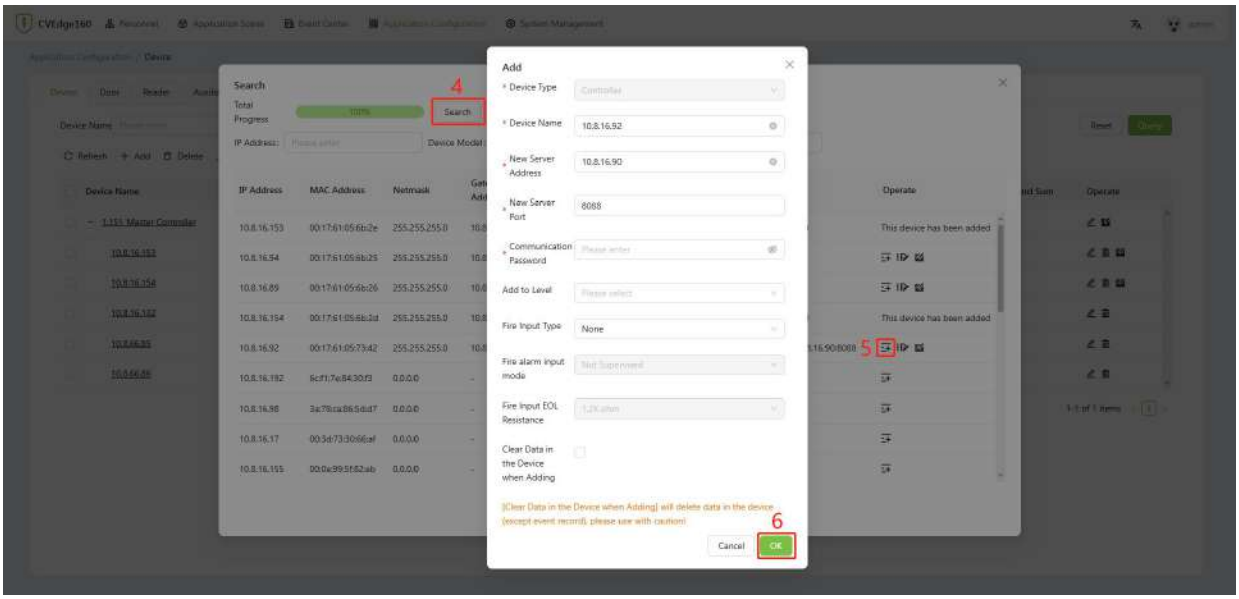
Add the device by searching. The process is as follows:

1. Click [**Application Configuration**] - [**Device**] - [**Search**], to open the Search interface in the Web server. (1, 2, 3)
2. Click [**Search**], and it will prompt Searching……(4)
3. After searching, the list and total number of device will be displayed.

4. In the list of searched devices, select the device you want to add (including Secondary Controller, Door Unit Exboard, I/O Exboard, IPC), click the **Add** icon, and then enter the relevant parameters in the pop-up window and click [**OK**]. (5, 6)

5. After the addition is successful, the device will be displayed in the device list.

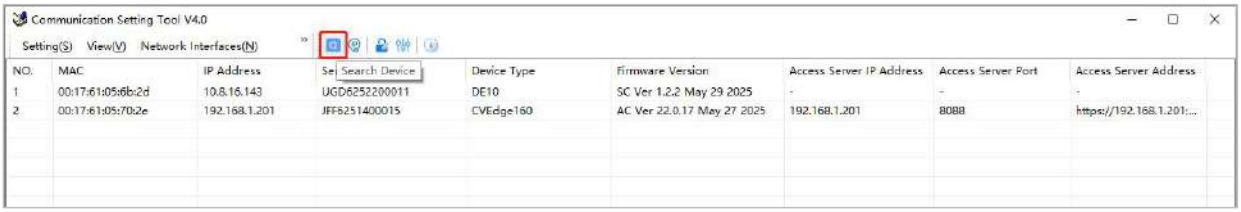




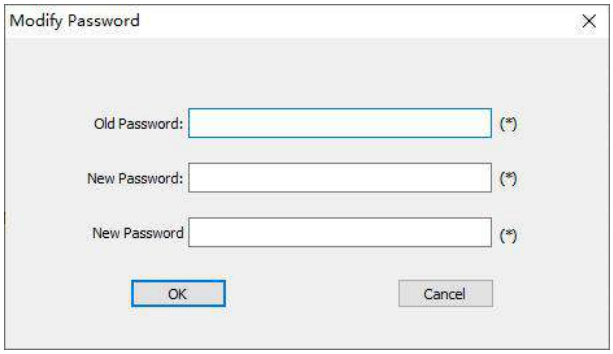
Important Notes:

Before adding **DE10**, you need to change the communication password of DE10. Refer to the following method to modify it.

1. Search for devices using the DeviceSettingTool V4.0 search tool. Click the icon to search for devices.



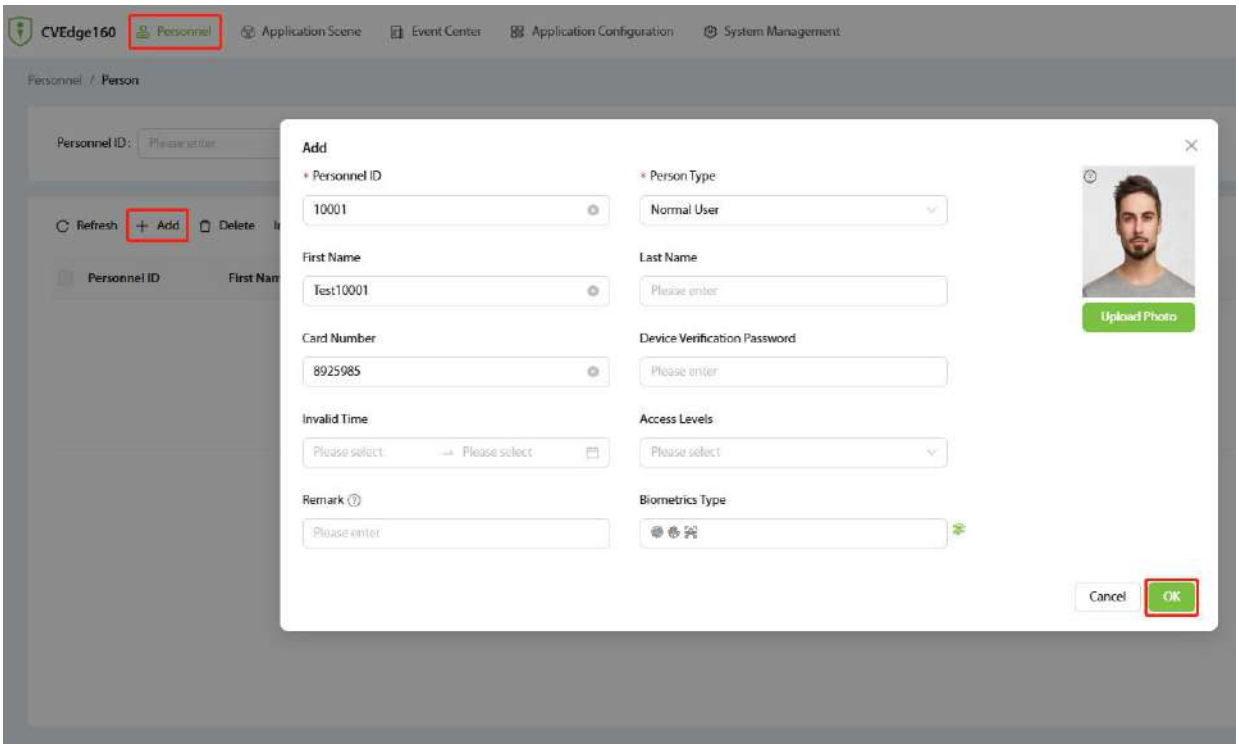
2. Select the searched device and click the icon to change the communication password. For the first time to change the password, the default communication password is **Zk@123**, and the new password is a combination of **2~6** digit alphabetic characters.



Note: *If the communication password is forgotten, the device can be reset to its factory settings, and the password will automatically revert to the default value.*

6.6 Add Personnel

1. Click [**Personnel**] - [**Person**] - [**Add**] to register users in the Web server.

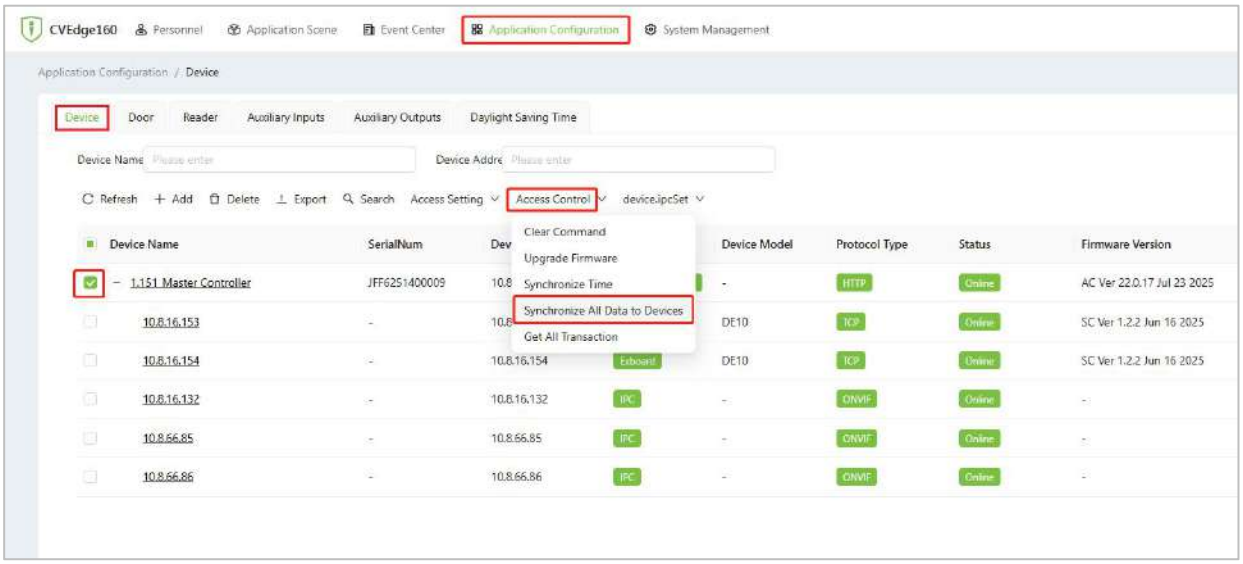


2. Fill in all the required fields of the user and click and select Fingerprint to enter the online fingerprint registration interface.

3. Click [**Driver Download**] to install the driver first.

Note: *The device only supports the ZKFinger 13.0 fingerprint algorithm.*

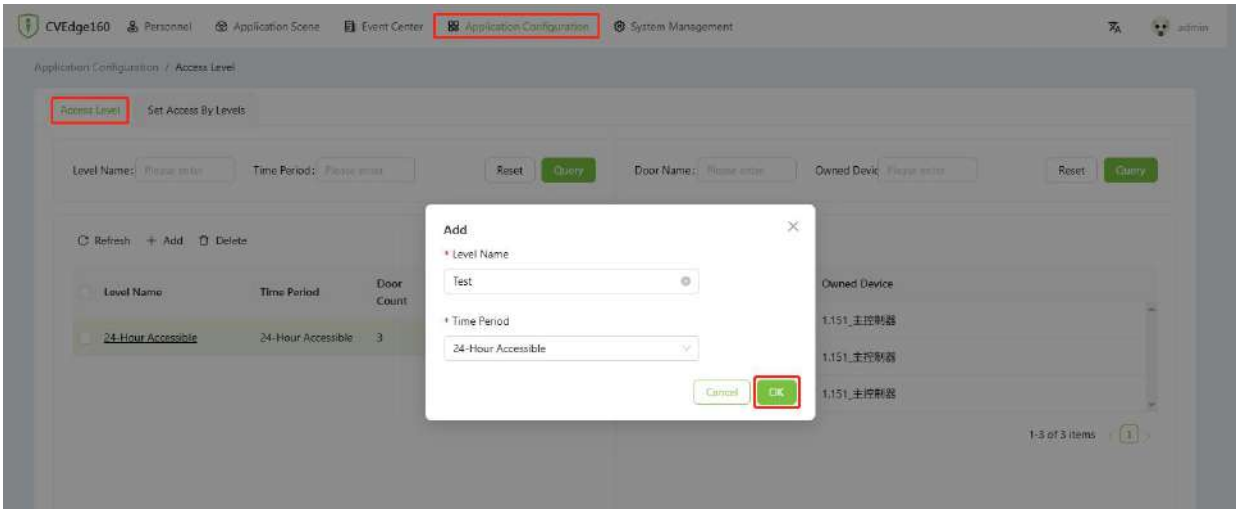
4. Click [**Application Configuration**] - [**Device**] to enter the device list interface. Select the device and click [**Access Control**] - [**Synchronize All Data to Devices**] to synchronize all the data to the device including the new users.



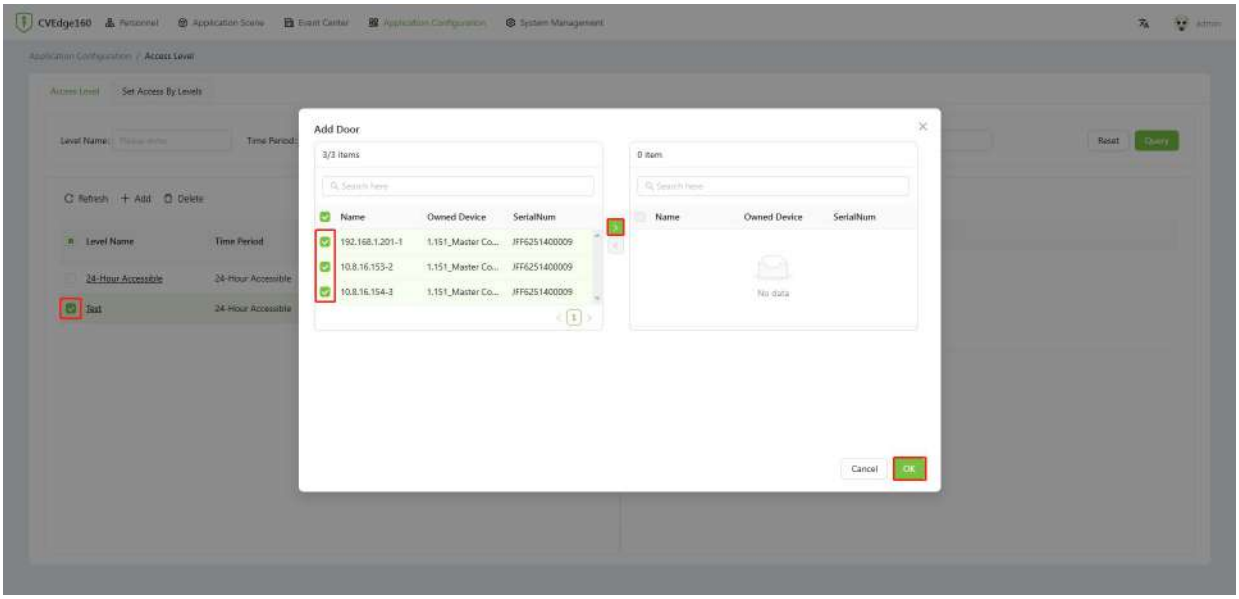
6.7 Set the Control Rules

6.7.1 Set the Access Level Group

1. Click [**Application Configuration**] - [**Access Level**] - [**Access Level**] to enter the setting interface.
2. Click [**Add**] to add a new access level group.
3. Enter the level name and time period, then click [**OK**] to confirm and exit.



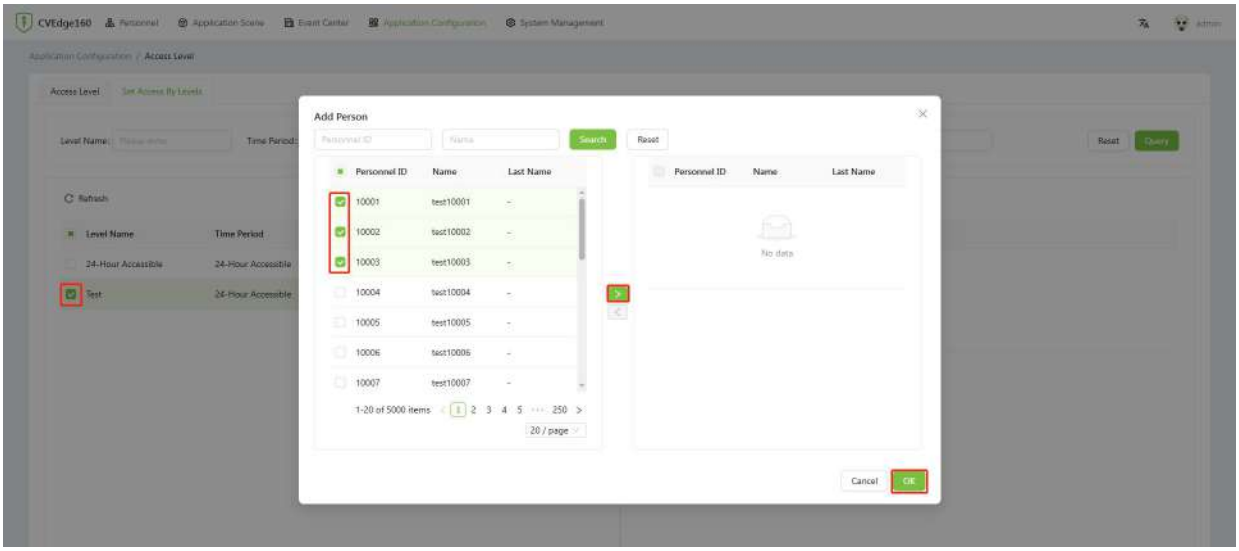
4. After adding successfully, check the levels group.
5. Click [**Add Door**] icon in the levels group bar to open the settings window.
6. Select the door and then click to move it to the selected column on the right.
7. Click [**OK**] to confirm and exit.



6.7.2 Set Access By Levels

Add personnel to the access level group.

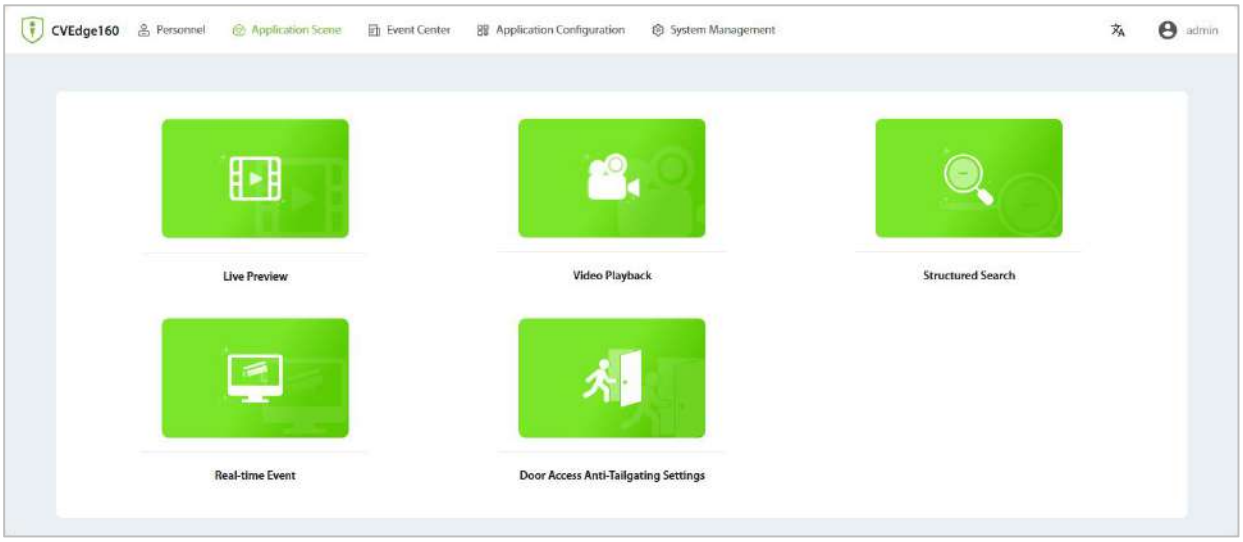
1. Click [**Application Configuration**] - [**Set Access By Levels**] to enter the setting interface.
2. Check the levels group and click the [**Add Person**] icon in its bar to open the settings window.
3. Select the person and then click to move it to the selected column on the right.
4. Click [**OK**] to confirm and exit.



6.8 Application Scene

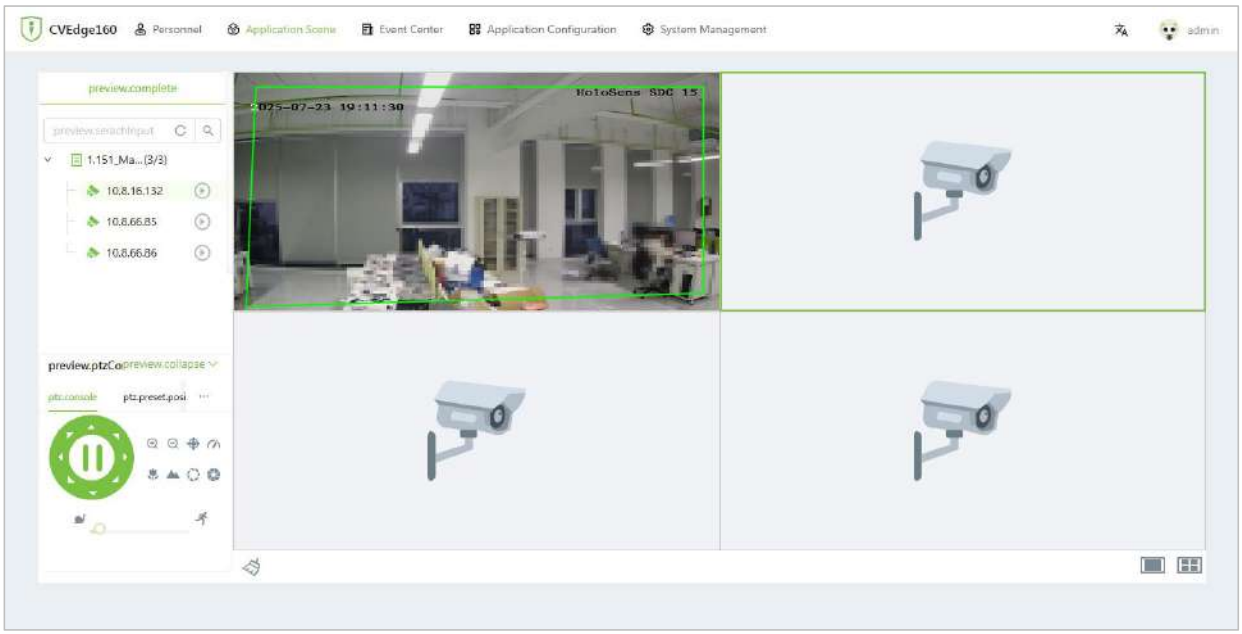
Click [**Application Scene**] in the top menu bar to enter the application scene setting interface.

Under the Application Scenarios menu, parameters such as live preview, video playback, structured search, real-time event and door access anti-tailgating settings can be set.



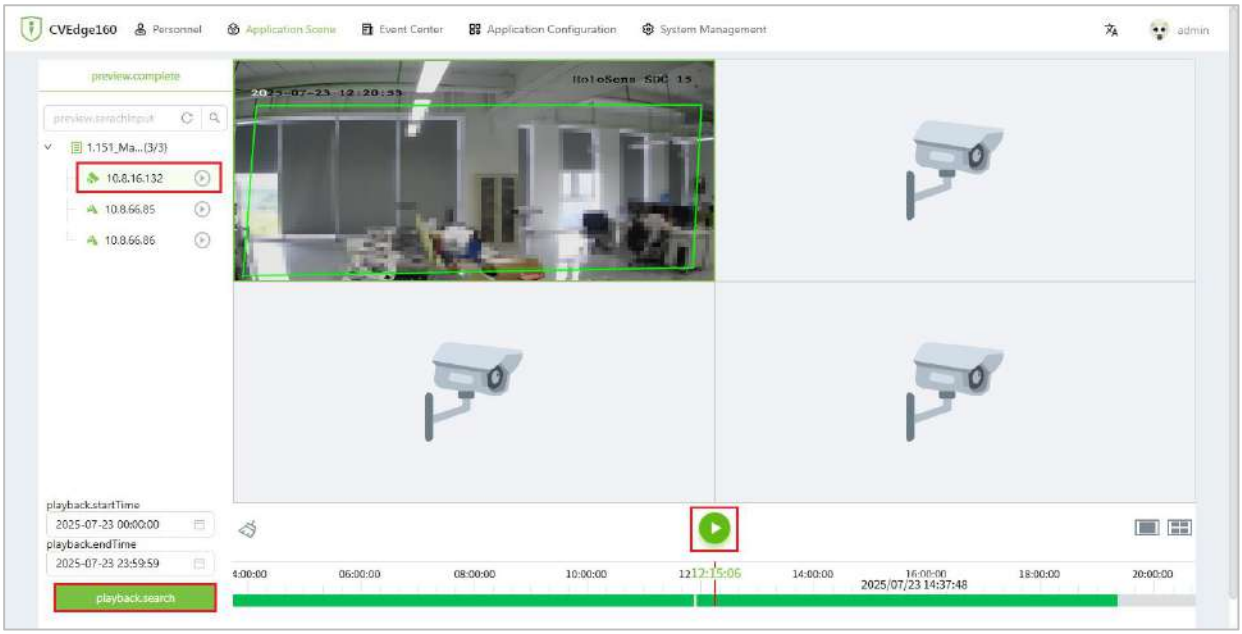
6.8.1 Live Preview

Click [**Application Scene**] - [**Live Preview**] to enter the live preview interface. In this interface users can select the camera in the left menu bar, and then double-click the play button for live preview.



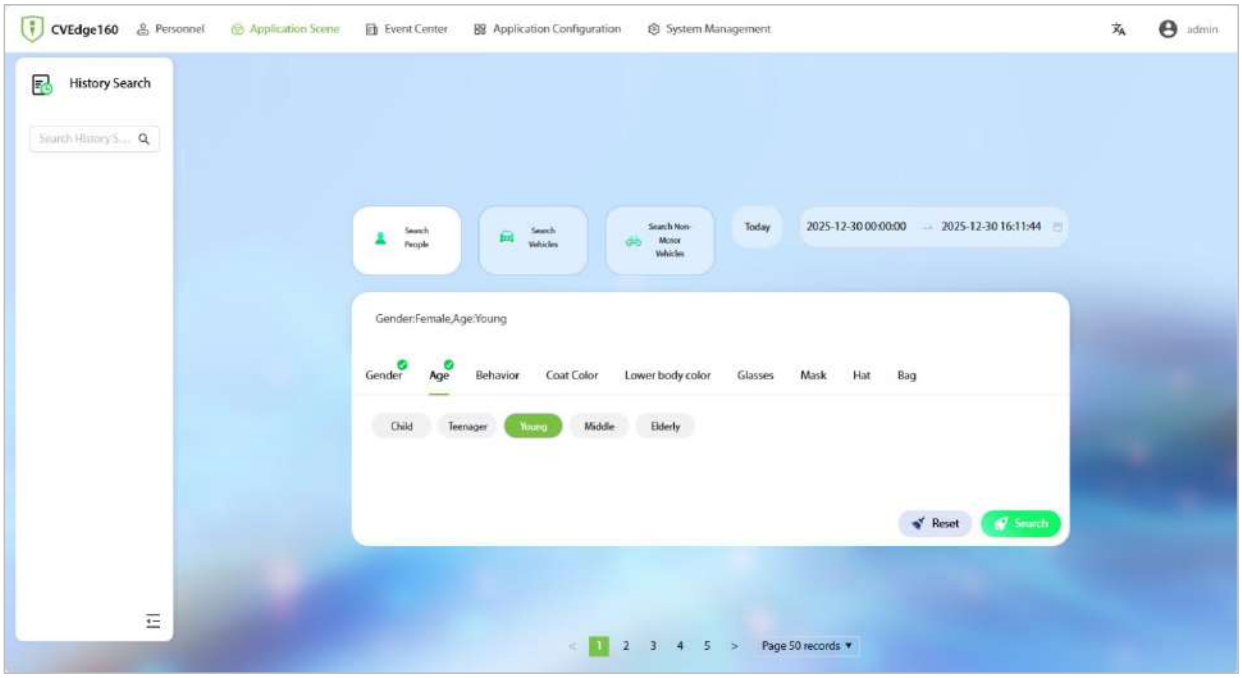
6.8.2 Video Playback

1. Click [**Application Scene**] - [**Video Playback**] to enter the video playback interface.
2. In the list of cameras on the left, check the camera you want to view.
3. Enter the playback start time and playback end time and click [**playback. search**].
4. Time periods with video playback will be marked with a green bar.
5. Click the icon to open the video playback.



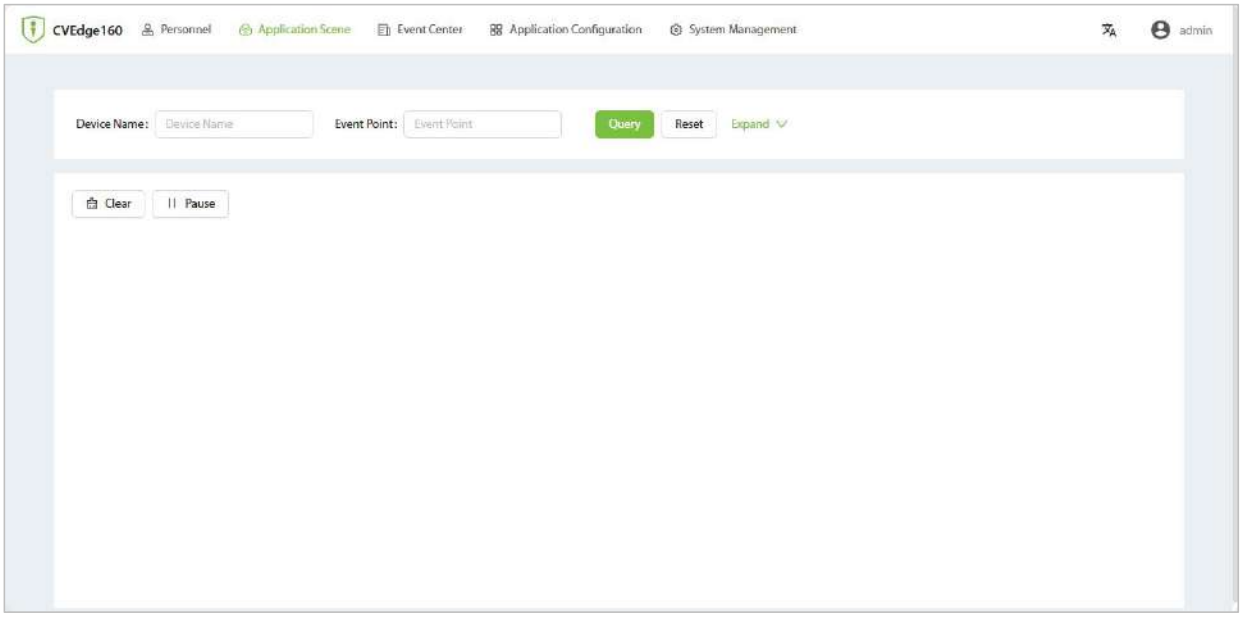
6.8.3 Structured Search(Coming Soon)

Click [**Application Scene**] - [**Structured Search**] to enter the structured search interface. In this interface, you can locate people, vehicles, and non-motor vehicles within a video by defining key information and setting a time range for the search.



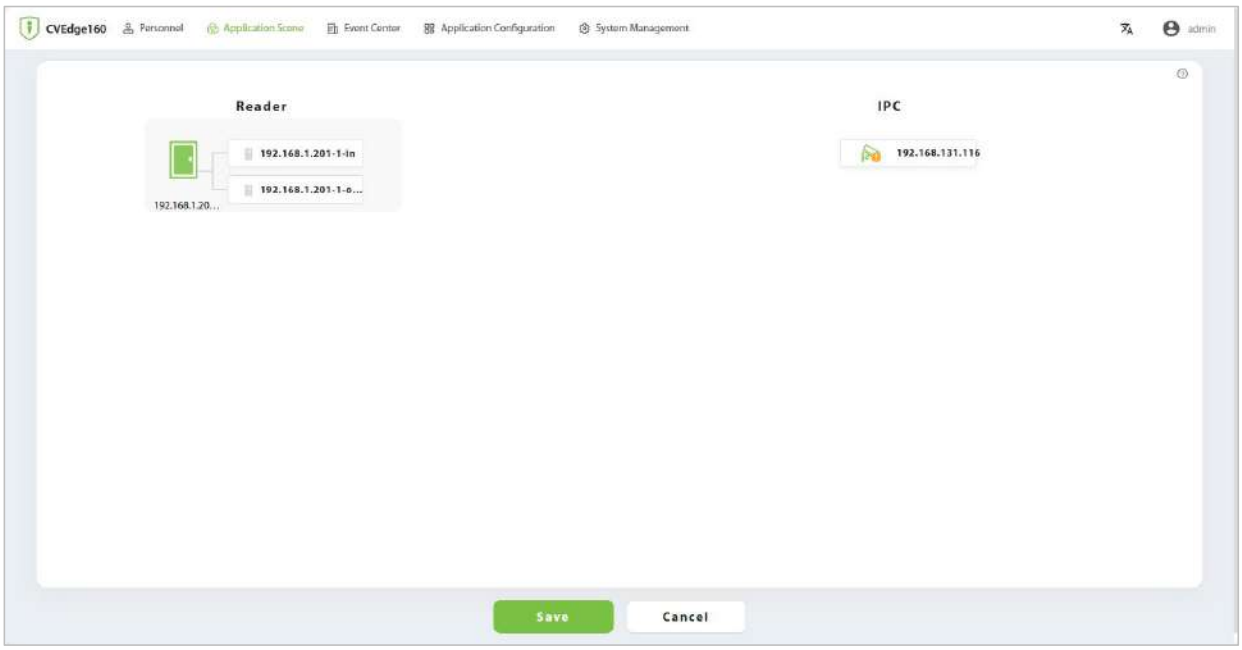
6.8.4 Real-time Event

Click [**Application Scene**] - [**Real-time Event**] to enter the real-time event interface.

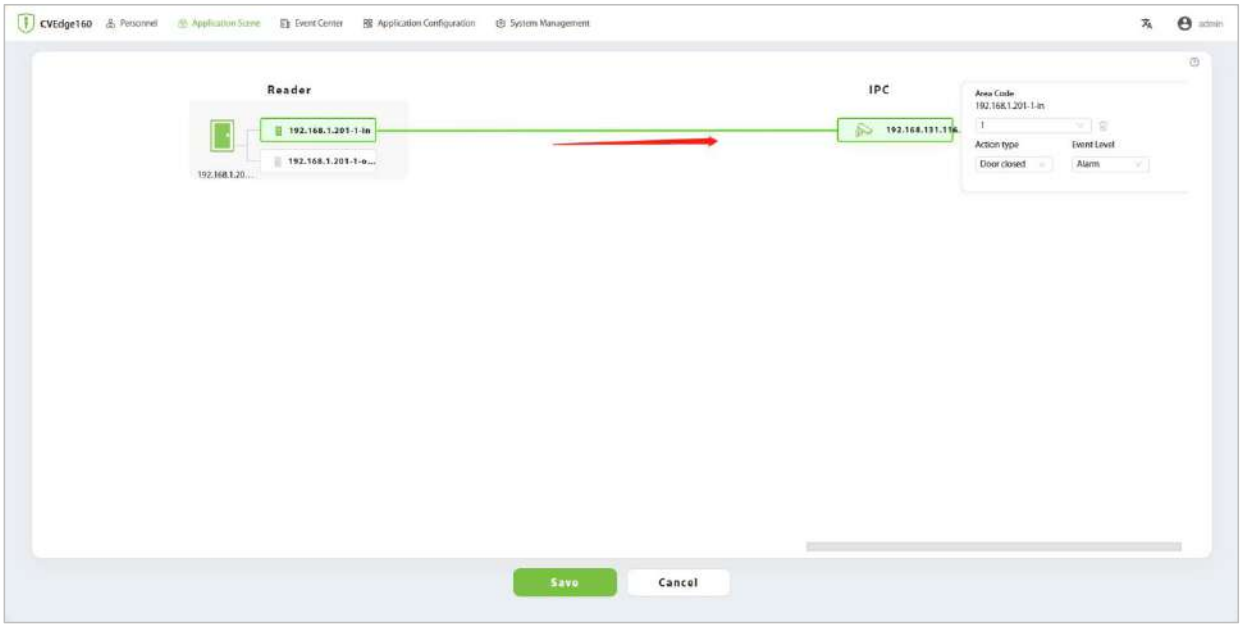


6.8.5 Door Access Anti-Tailgating Settings

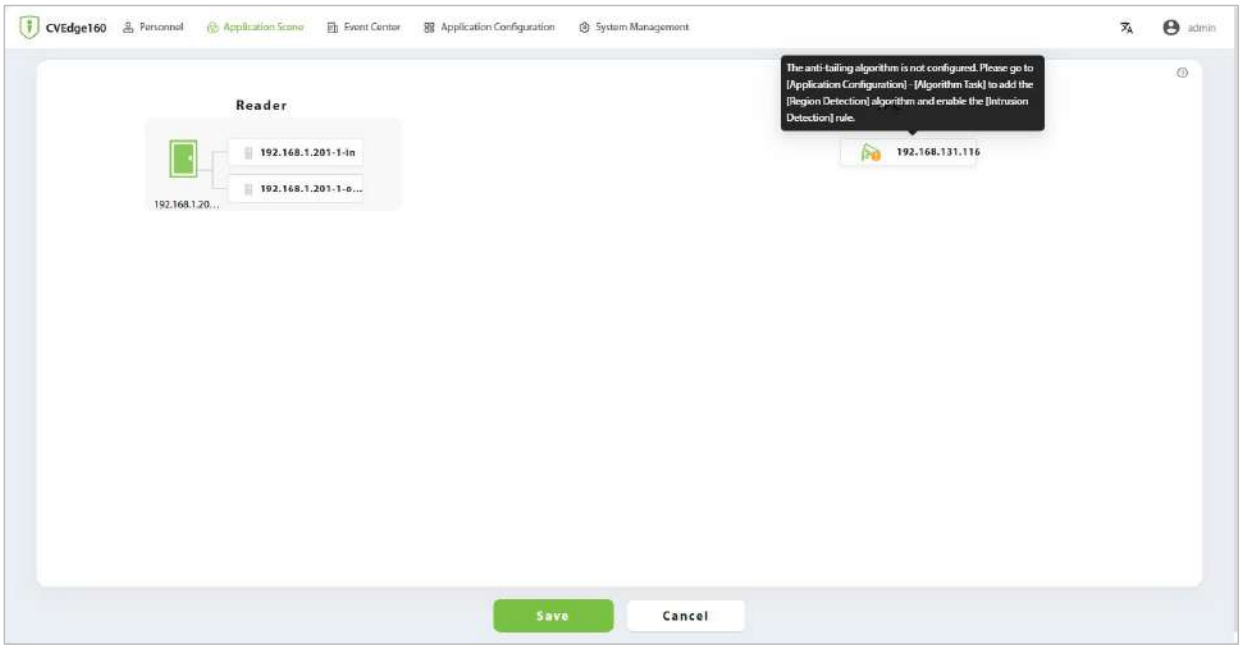
1. Before using the anti-tailgating feature, you must complete the steps in Section 6.7 Set the Control Rules to configure access levels and access level groups.
2. Then click [**Application Scene**] - [**Door Access Anti-Tailgating Settings**] to enter the door access anti-tailgating settings interface.



3. Click the reader connection corresponding to the IPC to select the area code, which serves as the algorithm rule number. You can click **Delete** Connection to remove the configured binding. **Note:** Only one IPC may be configured per reader.



If no corresponding IPC intrusion detection task is configured, the following prompt will appear during connection: The anti-tailing algorithm is not configured. Please go to [**Application Configuration**] - [**Algorithm Task**] to add the [**Region Detection**] algorithm and enable the **[Intrusion Detection**] rule.

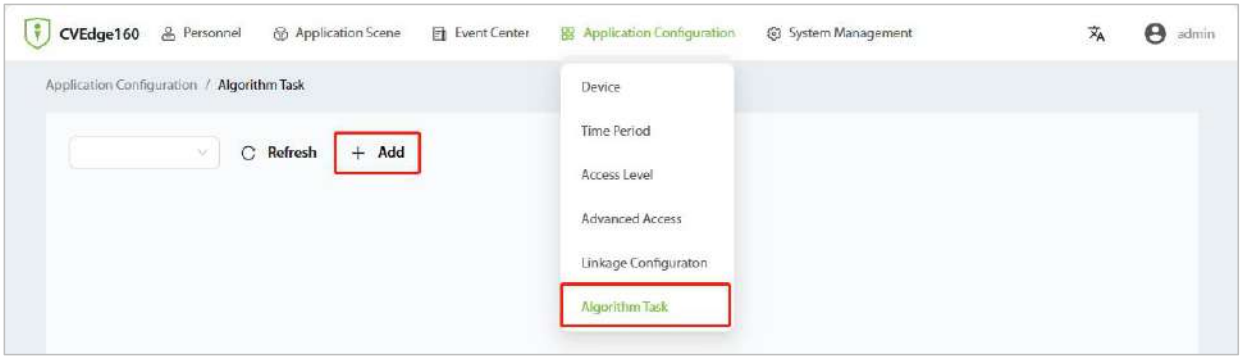


Follow these steps to configure the corresponding IPC intrusion detection task.

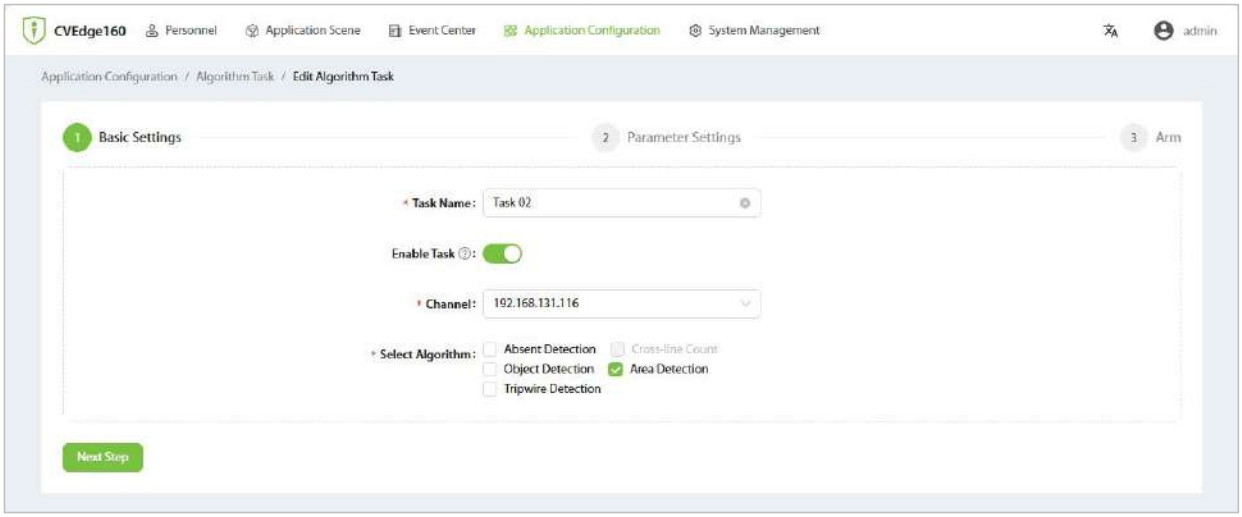
Set up the corresponding IPC intrusion detection task, configure the detection area, and specify the maximum and minimum target sizes along with the polygonal detection area.

Operating Steps:

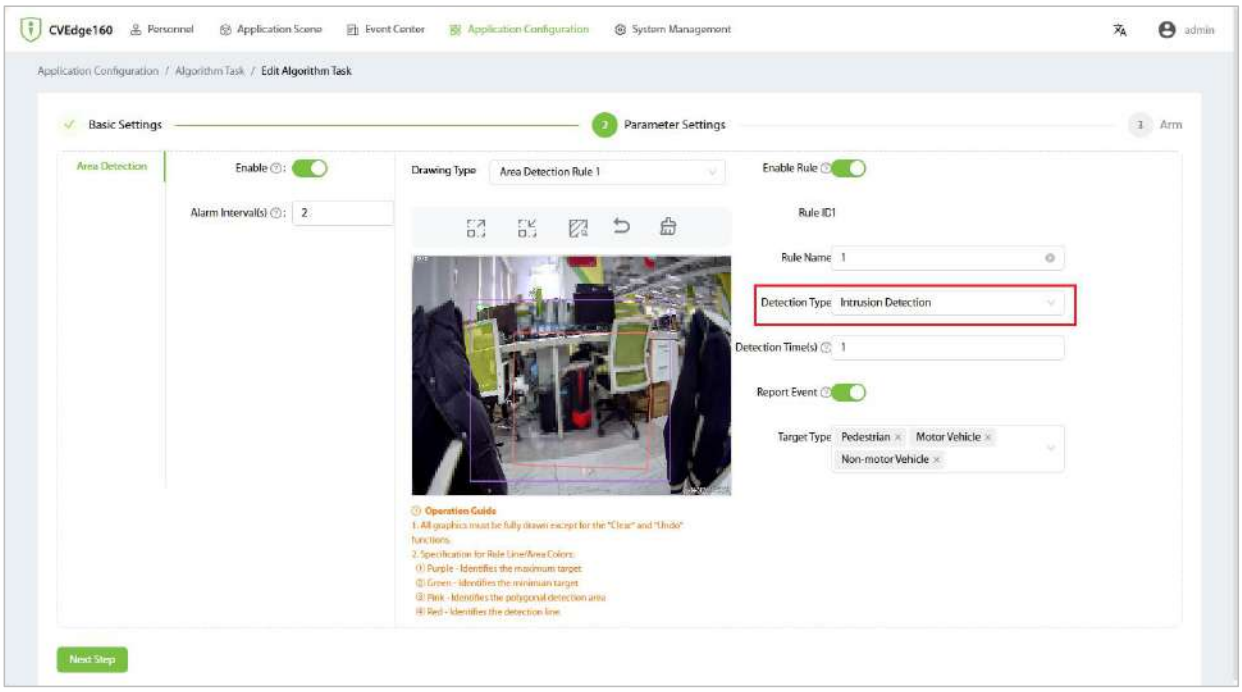
Step 1: On the Web Server homepage, select [**Application Configuration**] - [**Algorithm Task**] - [**Add**].



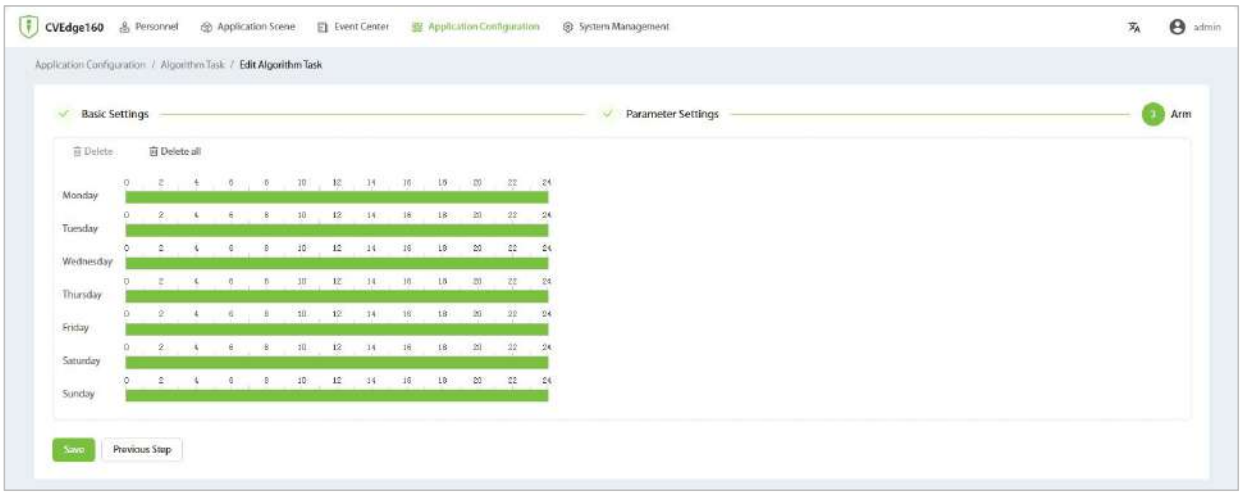
Step 2: Choose the channel of the algorithm task that needs to be configured under a specific device, and then select the Area Detection algorithm. After completing the settings, click [**Next Step**].



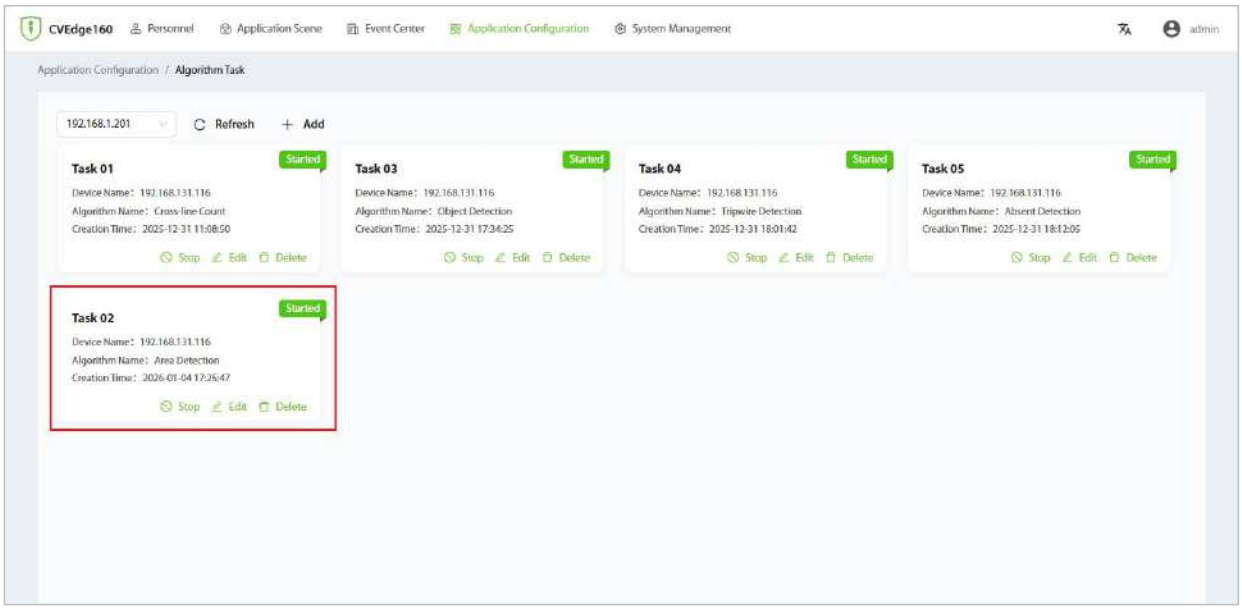
Step 3: Enable the intrusion detection algorithm and set up related detection configurations. Click on the drawing icon above the preview window to draw the area.



Step 4: Set the arming time. Only events triggered within the arming time will be reported as alarms.



Upon completion, it will appear in the list as shown below.



6.9 Algorithm Task Configuration Operations

The following algorithm tasks, except for object detection, allow users to view detection areas and lines in real-time after successful configuration. The triggering of events can be judged by the flashing of the detection area and lines. All reported events can be viewed in detail in both the **Real-time Events** and **Event Center**.

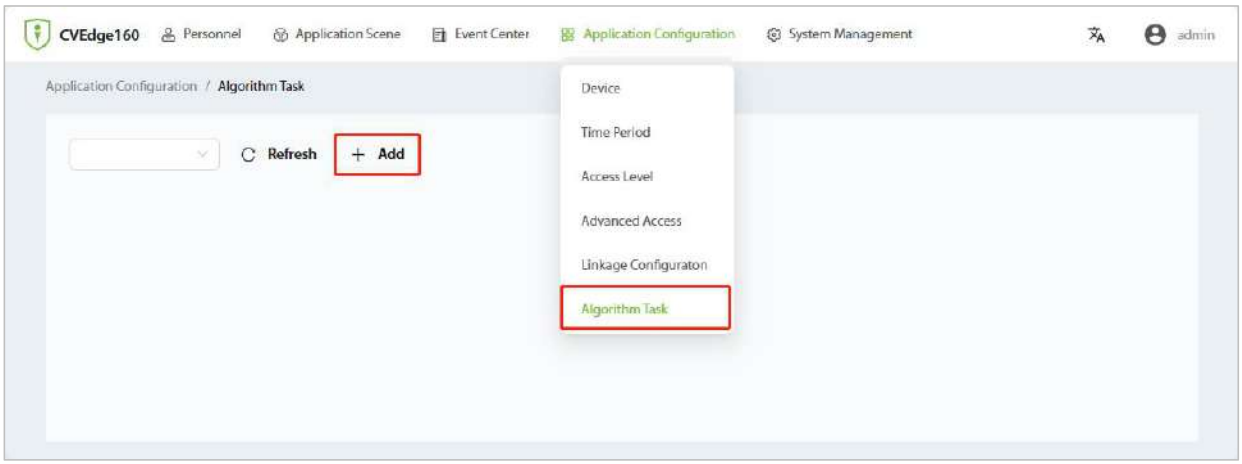
Click [**Application Configuration**] - [**Algorithm Task**] to enter the algorithm task settings interface.

6.9.1 Cross-line Count

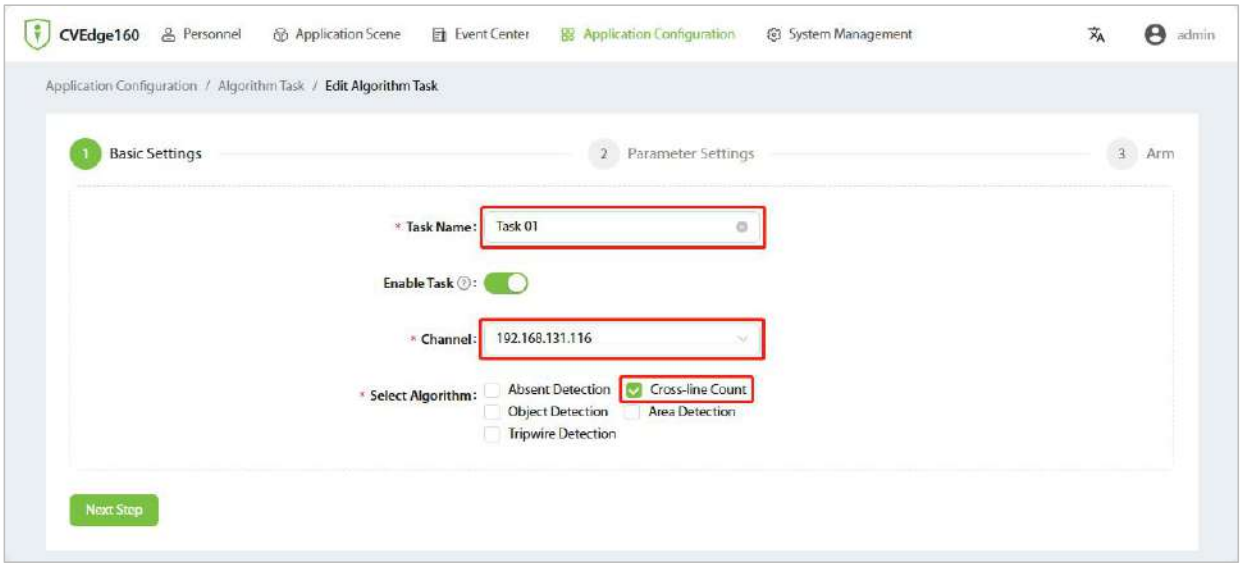
Users can set up detection lines within a detection area to count the number of people entering and exiting the detection line.

Operating Steps:

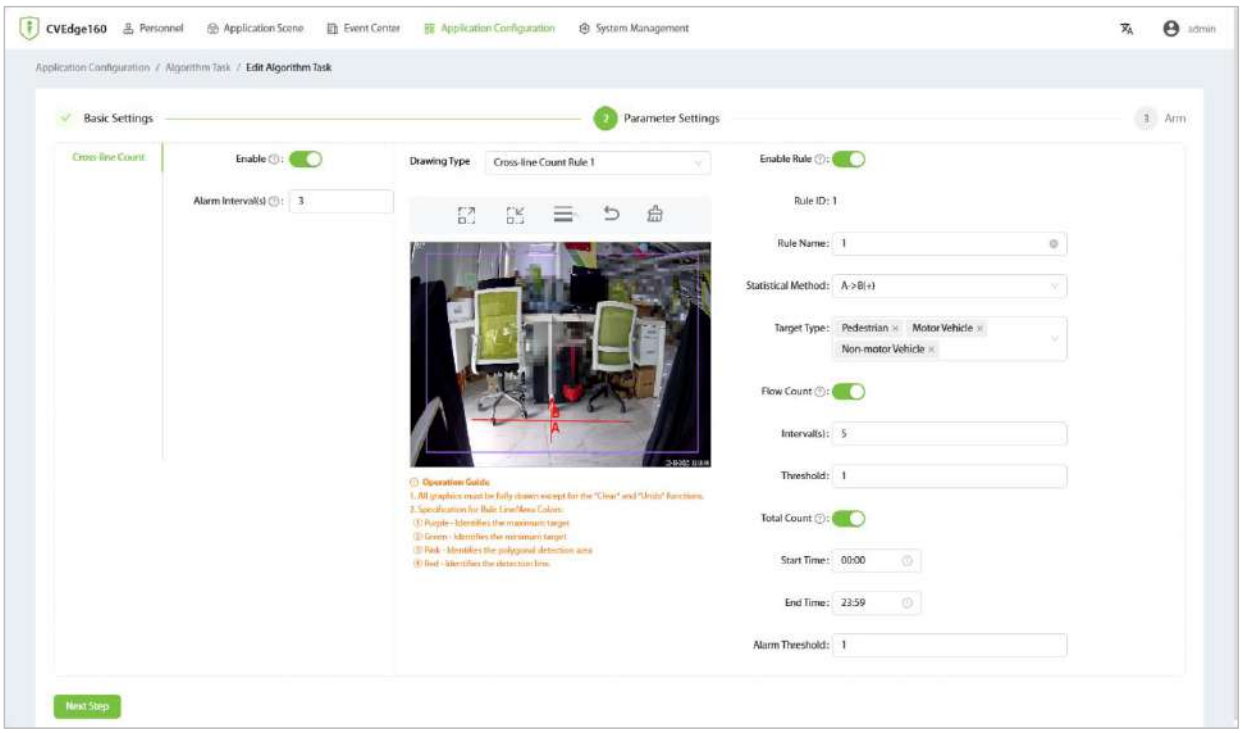
Step 1: On the Web Server homepage, select [**Application Configuration**] - [**Algorithm Task**] - [**Add**].



Step 2: Choose the channel of the algorithm task that needs to be configured under a specific device, and then select the Cross-line Count algorithm. After completing the settings, click [**Next Step**].



Step 3: Enable the cross-line count algorithm and configure the detection settings. Click the drawing icon above the preview window to draw the detection area.



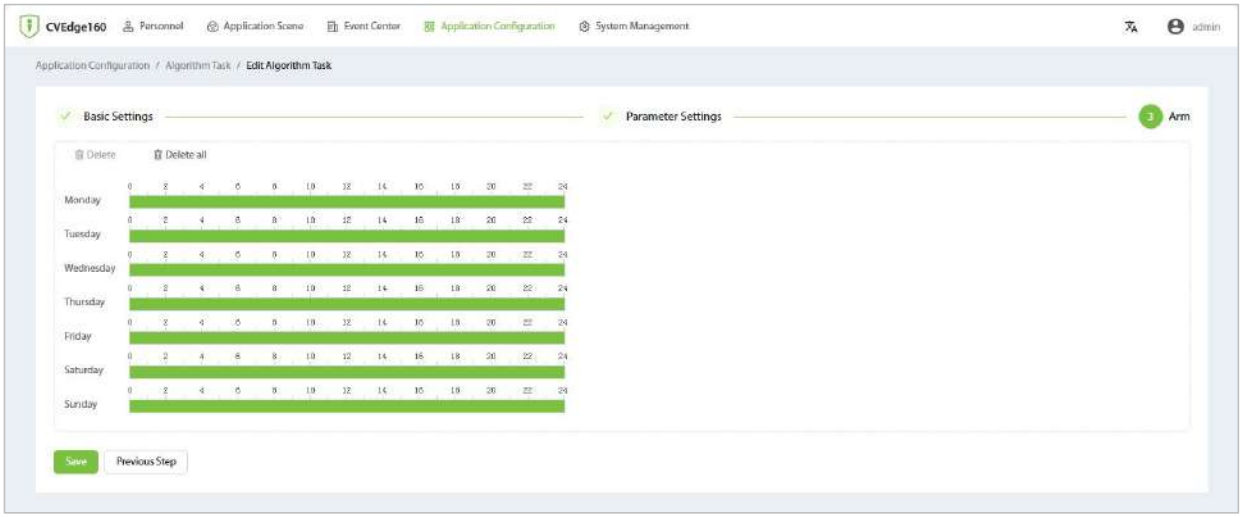
Note: *For cross-line count detection, it is necessary to draw the maximum and minimum targets and detection lines (default maximum and minimum targets are provided, which can be modified by clicking on the target frames according to actual conditions).*

Parameter Configuration Descriptions

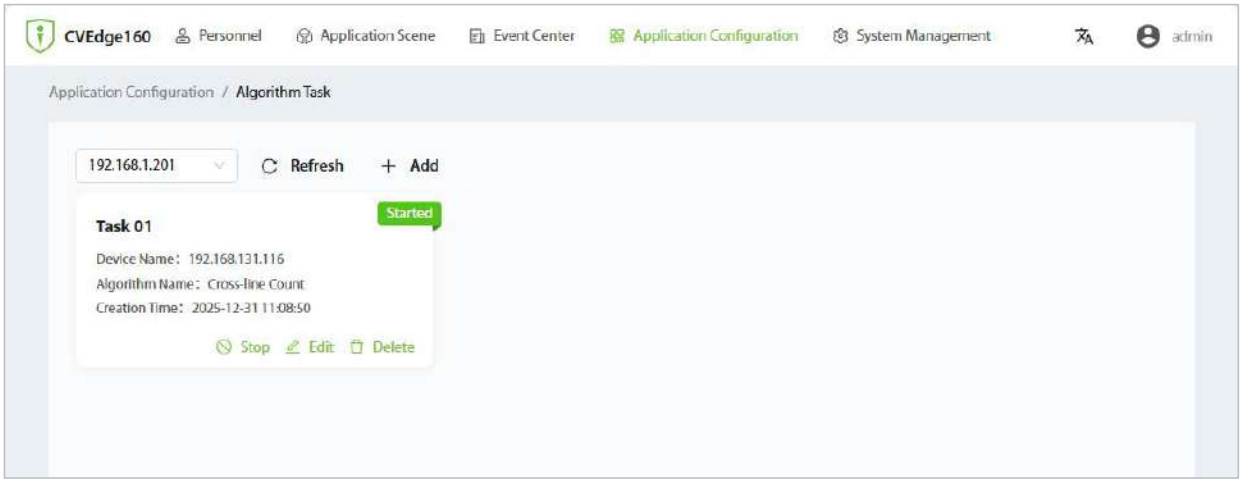
Parameter	Descriptions
Alarm Interval(s)	For the same event and rule, only one alert is triggered within the alert interval; if both traffic and total statistics are enabled, cross-reporting will occur for the statistical figures in the reported data. **Note:** To prevent alarm storms, if multiple alarms occur within the detection interval, only one alarm will be reported.
Drawing Type (Cross-Line Detection Rules)	A target counting algorithm can configure four detection rules. These rules operate independently of each other, and all four rules remain active when simultaneously configured.
Direction	Specify the effective direction for pedestrians crossing the detection line.
Maximum Target	No alarm will be triggered if the detected target is larger than the set size.
Minimum Target	No alarm will be triggered if the detected target is smaller than the set size.
Undo	Undo the previous drawing operation.
Clear	Clear all current drawing content.

Rule ID	The detection rule corresponding to the drawn type.
Rule Name	Name the detection rule for quick event search in the Event Center.
Statistical Method	**A->B(+):** If the target crosses the detection line from A to B, the target count will increase. **A->B(+)B->A(-):** If the target crosses the detection line from A to B, the target count will increase; if it crosses from B to A, the target count will decrease. **A<->B(+):** If the target crosses the detection line in either direction (from A to B or from B to A), the target count will increase.
Target Type	Select the type of detection target according to user needs: 1. Pedestrian, 2. Motor Vehicle, 3. Non-Motor Vehicle.
Flow Count	Traffic statistics serves to measure traffic within a statistical interval (differentiated by target type), with an alarm event triggered upon reaching the statistical threshold. **Note:** If both traffic statistics and total volume statistics of the same rule are triggered simultaneously, only one alarm event will be reported randomly.
Counting Interval(s)	The time interval for traffic statistics to generate alarms. Traffic is counted at regular intervals, and once the counting period ends, the next counting cycle begins.
Counting Threshold	If the statistical threshold is reached within the statistical interval, an alarm event will be reported.
Total Count	Total volume statistics is designed to calculate the total amount within a specified time period (differentiated by target type), and an alarm event will be triggered when the alarm threshold is met.
Start / End Time	The total number of targets is counted within the specified time period, and counting stops after the end time is exceeded. **Note:** If the end time is set to be greater than the start time, the counting will not take effect.
Alarm Threshold	If the number of targets counted within the time period reaches the alarm threshold, an alarm event will be reported. If the number of targets continues to increase consistently after exceeding the alarm threshold, an alarm will be generated each time there is an increase until the number of targets falls below the threshold.

Step 4: Set the arming time. Only events triggered within the arming time will be reported as alarms.



Upon completion, it will appear in the list as shown below.



6.9.2 Area Detection

Area Entry: Detects whether a target has entered the detection area. If a target enters, an alarm is triggered. Staff then observe the video feed and dispatch personnel to handle the situation to prevent losses.

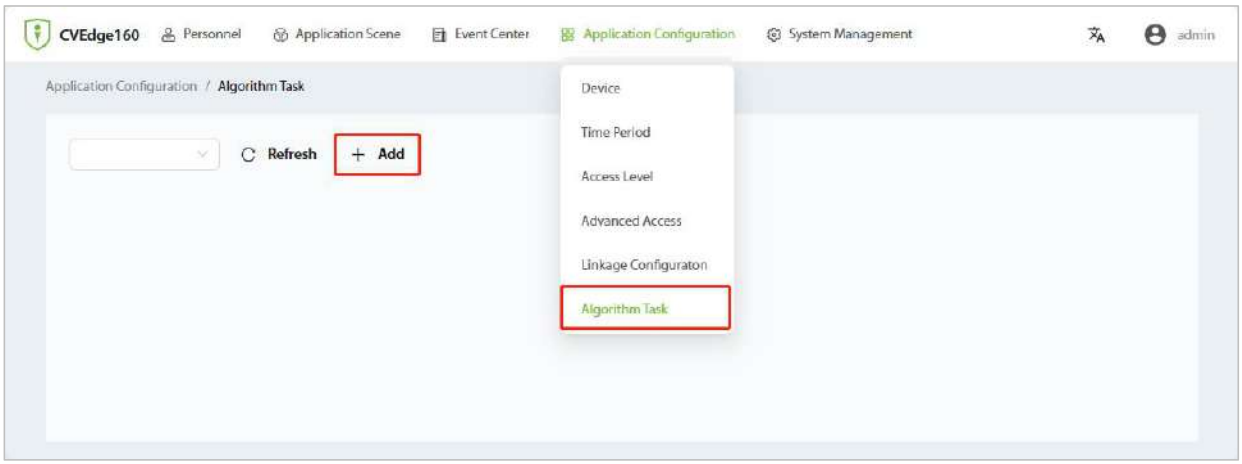
Area Exit: Detects whether a target has exited the detection area. If a target exits, an alarm is triggered. Staff then observe the video feed and dispatch personnel to handle the situation to prevent losses.

Intrusion Detection: Detects whether a target has entered the alert zone. If a target enters, an alarm is triggered. Staff then observe the video feed and dispatch personnel to handle the situation to prevent losses.

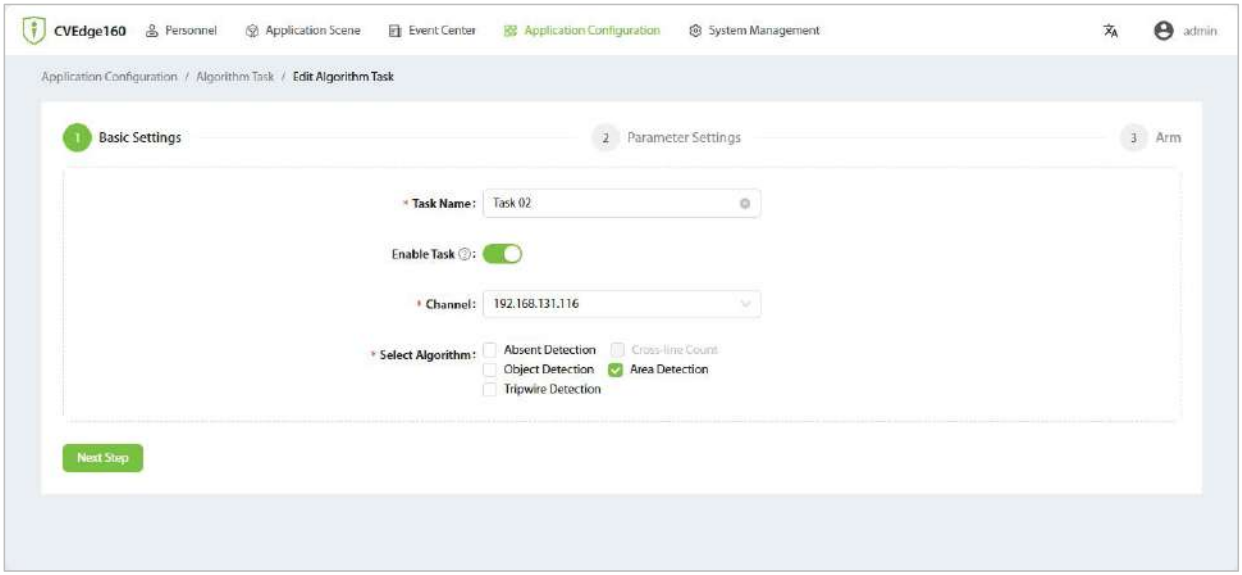
Loitering Detection: Detects whether a target has loitered in the alert zone for a specified duration. If the duration is exceeded, an alarm is triggered. Staff then observe the video feed and dispatch personnel to handle the situation to prevent harmful behavior.

Operating Steps:

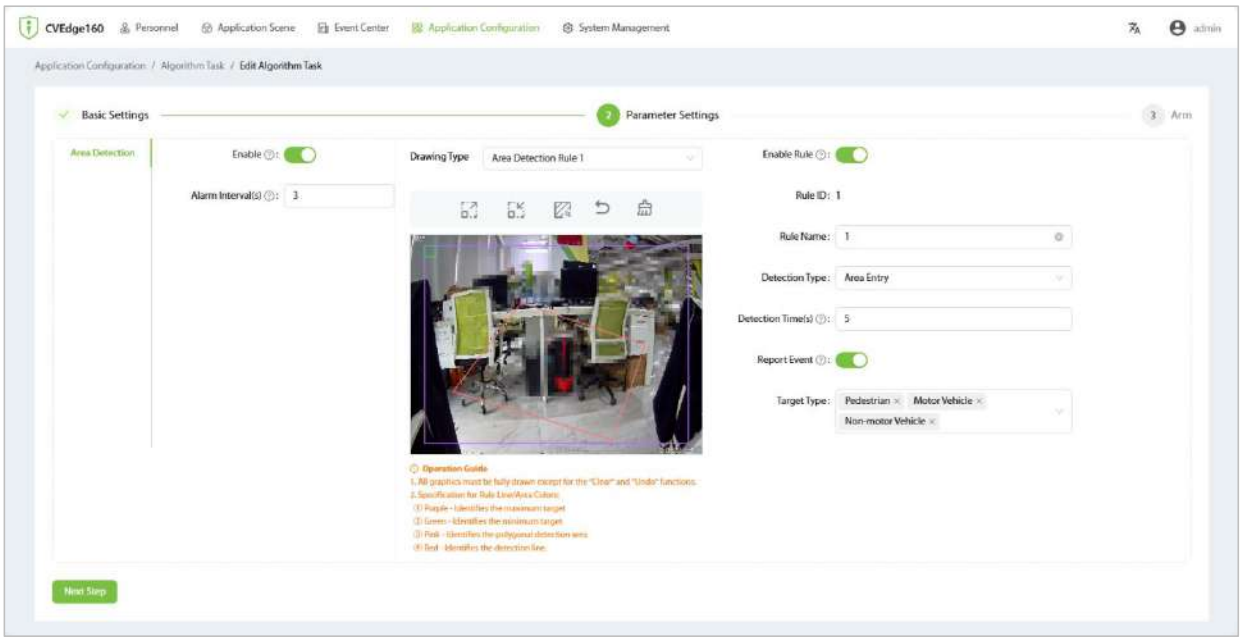
Step 1: On the Web Server homepage, select [**Application Configuration**] - [**Algorithm Task**] - [**Add**].



Step 2: Choose the channel of the algorithm task that needs to be configured under a specific device, and then select the Area Detection algorithm. After completing the settings, click [**Next Step**].



Step 3: Enable the area detection algorithm and set up related detection configurations. Click on the drawing icon above the preview window to draw the area.



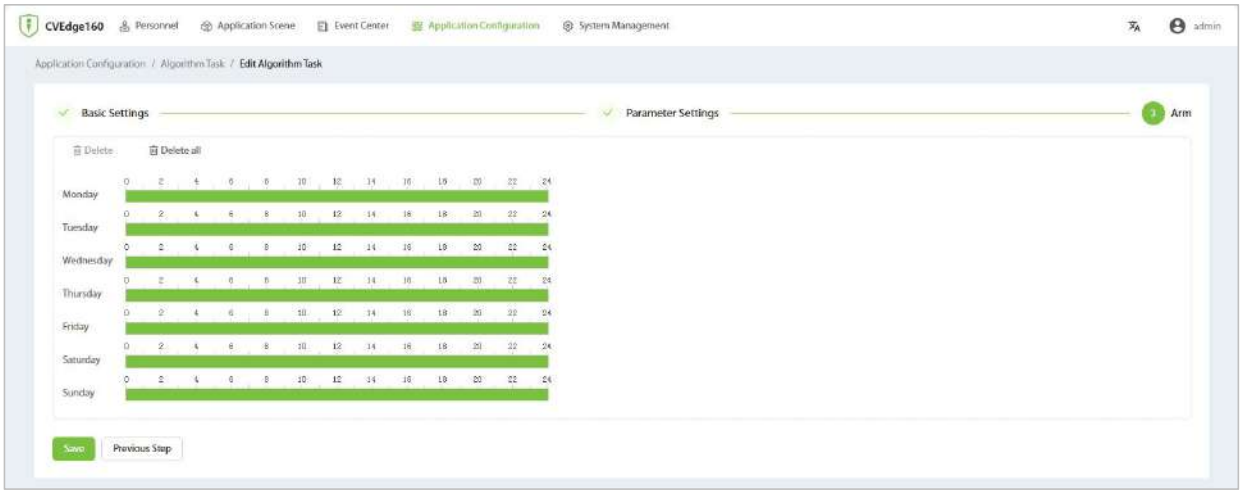
Note: *For area detection, it is necessary to draw the maximum and minimum targets and the polygonal area (default maximum and minimum targets are provided, which can be modified by clicking on the target frames according to actual conditions).*

Parameter Configuration Descriptions

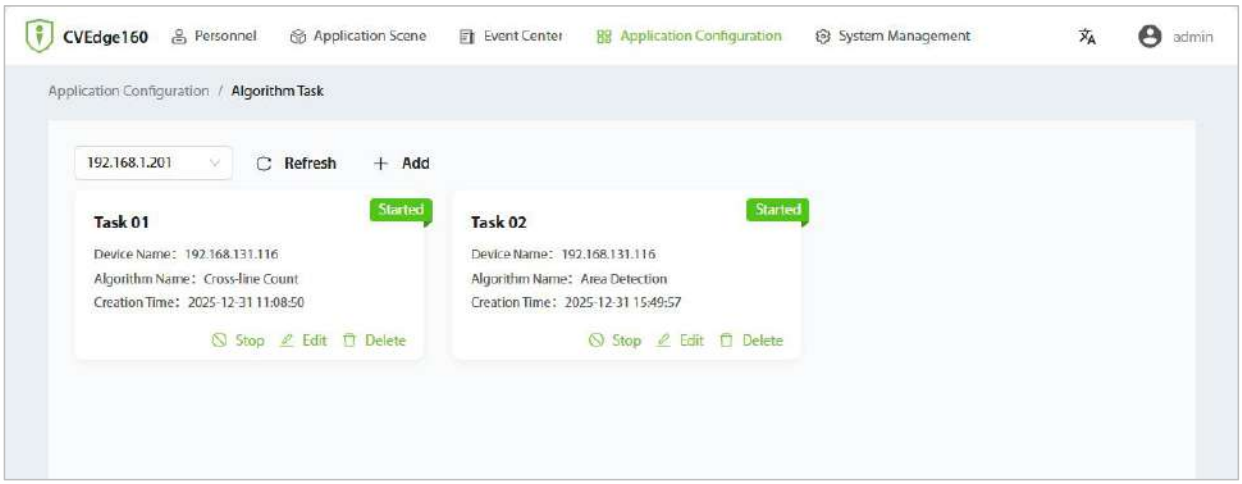
Parameter	Descriptions
Alarm Interval(s)	For the same event and rule, only one alert is triggered within the alert interval. **Note:** To prevent alarm storms, if multiple alarms occur within the detection interval, only one alarm will be reported.
Drawing Type (Cross-Line Detection Rules)	A single area detection algorithm can set up to 8 detection rules. These eight rules do not affect each other, and it is possible to activate four rules simultaneously.
Polygonal Area	The detection area defines the scope for target detection, and only targets within this area will be detected. By clicking on the border of the detection area, you can edit the shape and size of the area.
Maximum Target	No alarm will be triggered if the detected target is larger than the set size.
Minimum Target	No alarm will be triggered if the detected target is smaller than the set size.
Undo	Undo the previous drawing operation.
Clear	Clear all current drawing content.
Rule ID	The detection rule corresponding to the drawn type.
Rule Name	Name the detection rule for quick event search in the Event Center.

Detection Type	**Area Entry:** The target enters the detection area. **Area Exit:** The target leaves the detection area. **Area Entry/Exit:** The target either enters or exits the detection area. **Loitering Detection:** The target moves within the detection area. **Intrusion Detection:** The target enters the detection area and will continue to be detected as long as it remains within the area.
Detection Time(s)	It takes effect solely when the detection type is 'Loitering Detection'. The time interval for generating an alarm after a target loiters. An alarm will be reported if the target remains active within the detection area for longer than the specified detection time.
Report Event	It takes effect solely when the detection type is 'Intrusion Detection'. When disabled, intrusion detection will not report alarm events.
Target Type	Select the type of detection target according to user needs: 1. Pedestrian, 2. Motor Vehicle, 3. Non-Motor Vehicle.

Step 4: Set the arming time. Only events triggered within the arming time will be reported as alarms.



Upon completion, it will appear in the list as shown below.



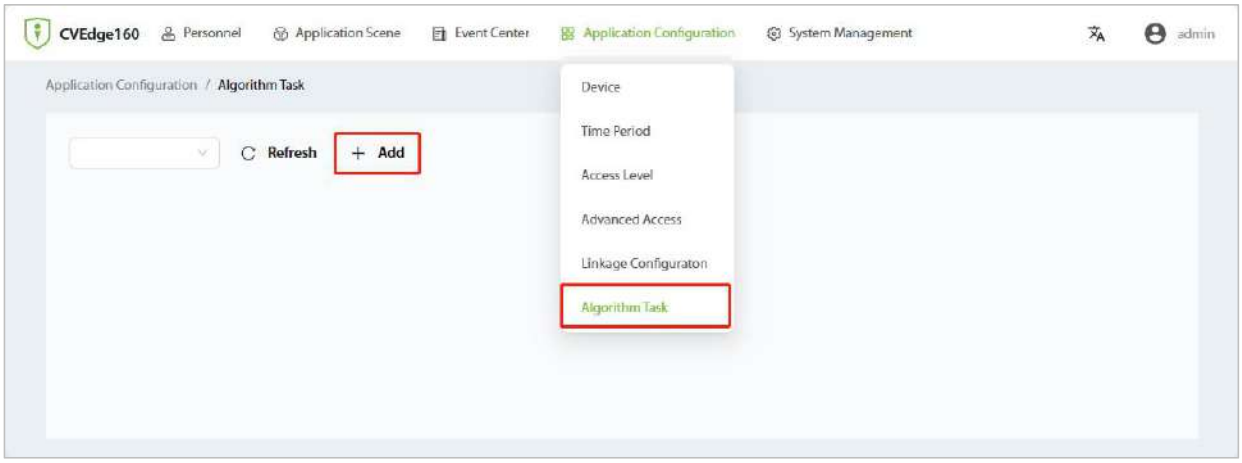
6.9.3 Object Detection

Object Lost: Detects whether a target has been left behind in the alert zone. If an object is left behind, an alarm is triggered. Staff then observe the video feed to assess the impact of the target on the public, and dispatch personnel to handle the situation to protect public interests and safety.

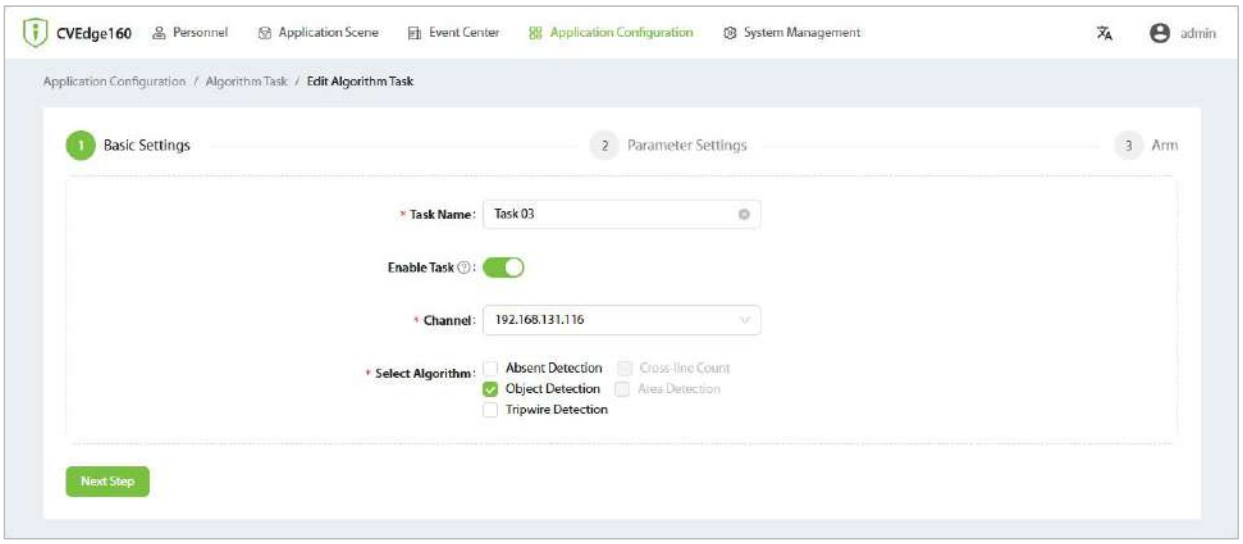
Object Abandon: Detects whether a target within the alert zone has been removed. This is used to protect valuable items such as safes, exhibits, vehicles, etc. If an item is removed, an alarm is triggered. Staff then observe the video feed and dispatch personnel to handle the situation to prevent theft of valuable items.

Operating Steps:

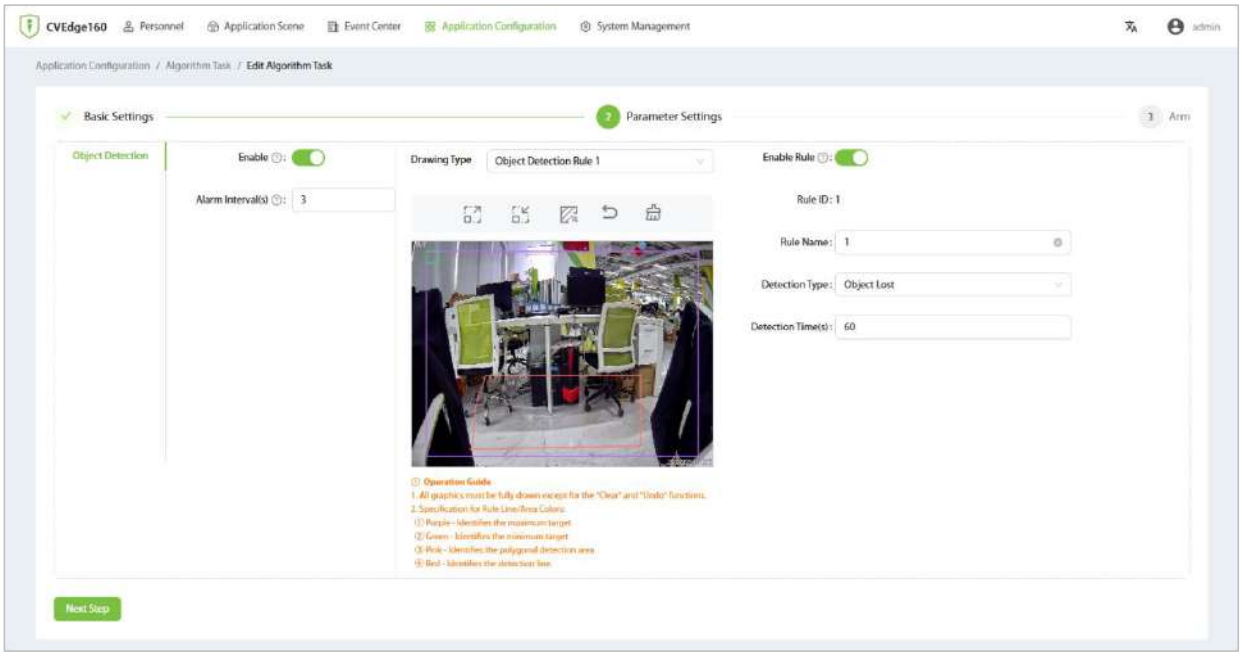
Step 1: On the Web Server homepage, select [**Application Configuration**] - [**Algorithm Task**] - [**Add**].



Step 2: Choose the channel of the algorithm task that needs to be configured under a specific device, and then select the Object Detection algorithm. After completing the settings, click [**Next Step**].



Step 3: Enable the object detection algorithm and set up related detection configurations. Click on the drawing icon above the preview window to draw the area.



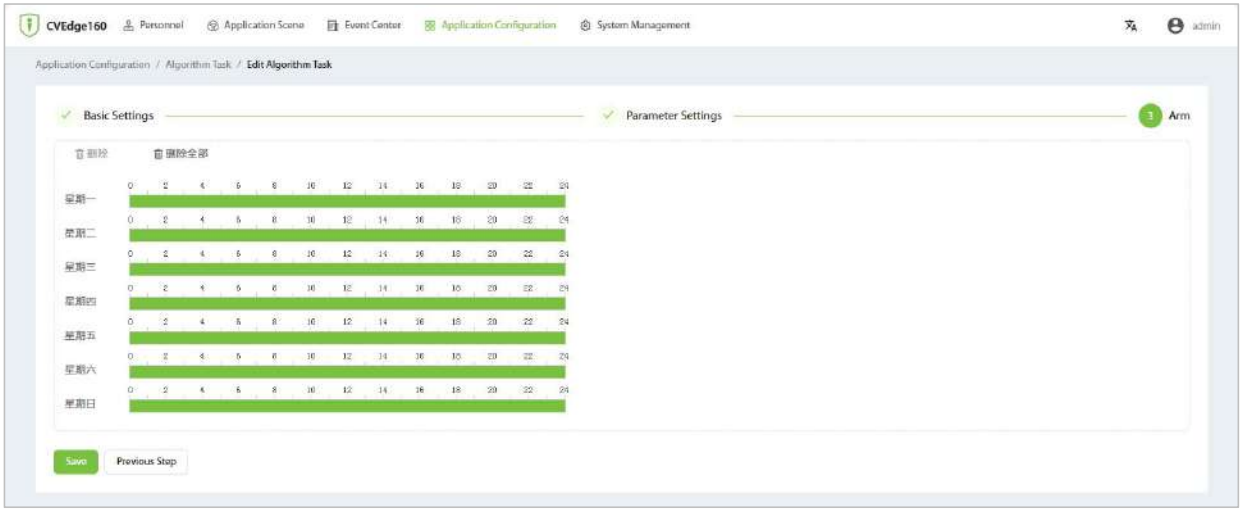
Note: *For object detection, it is necessary to draw the maximum and minimum targets and the polygonal area (default maximum and minimum targets are provided, which can be modified by clicking on the target frames according to actual conditions).*

Parameter Configuration Descriptions

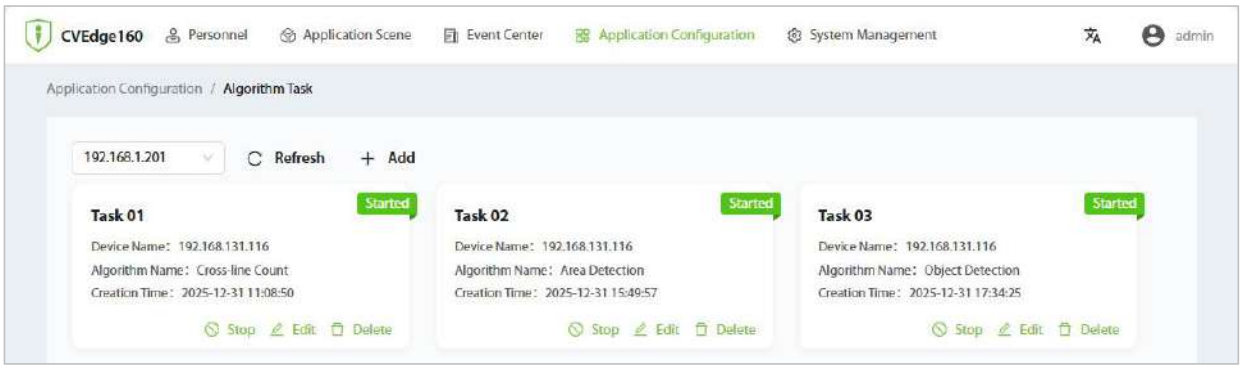
Parameter	Descriptions
Alarm Interval(s)	For the same event and rule, only one alert is triggered within the alert interval. **Note:** To prevent alarm storms, if multiple alarms occur within the detection interval, only one alarm will be reported.
Drawing Type (Cross-Line Detection Rules)	A single area detection algorithm can set up to 8 detection rules. These eight rules do not affect each other, and it is possible to activate four rules simultaneously.
Polygonal Area	The detection area defines the scope for target detection, and only targets within this area will be detected. By clicking on the border of the detection area, you can edit the shape and size of the area.
Maximum Target	No alarm will be triggered if the detected target is larger than the set size.
Minimum Target	No alarm will be triggered if the detected target is smaller than the set size.
Undo	Undo the previous drawing operation.
Clear	Clear all current drawing content.
Rule ID	The detection rule corresponding to the drawn type.

Rule Name	Name the detection rule for quick event search in the Event Center.
Detection Type	**Object Lost:** An object is considered left behind if it remains in the detection area for longer than the detection time. After an event is reported, the object can still be observed in the detection state in the live view, and it will disappear after a while (if someone passes through the detection area during the object left-behind detection, an alarm event may be triggered again after the person leaves). A person in the detection area will not be judged as an object left behind. **Object Abandon:** An object in the detection area is considered missing if it is removed for longer than the detection time. **Object Lost/Abandon**: An object is either removed or left behind in the detection area.
Detection Time(s)	The time interval for generating an alarm after an object is lost or left behind. An alarm will be reported if the object remains lost or left behind for longer than the detection time.

Step 4: Set the arming time. Only events triggered within the arming time will be reported as alarms.



Upon completion, it will appear in the list as shown below.

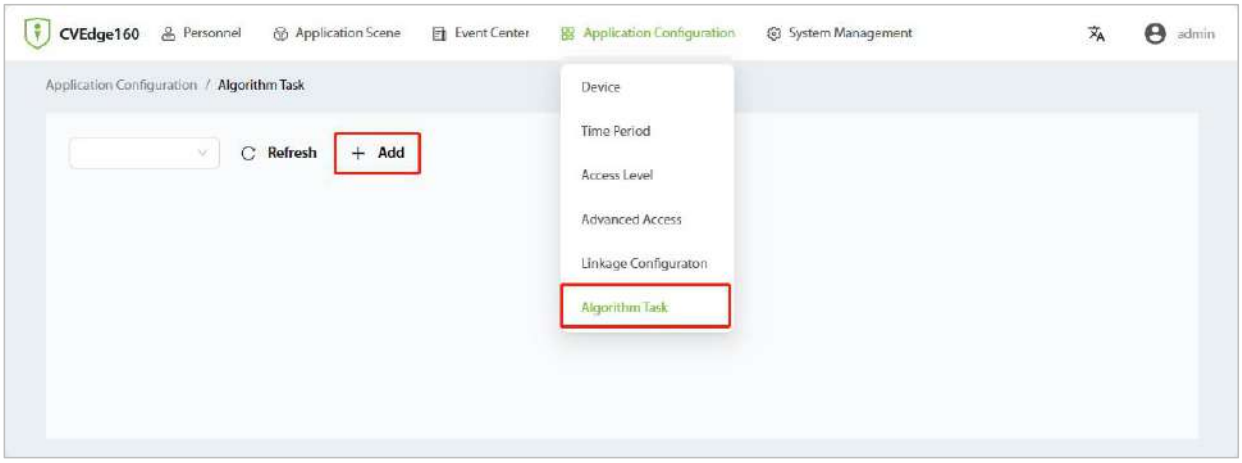


6.9.4 Tripwire Detection

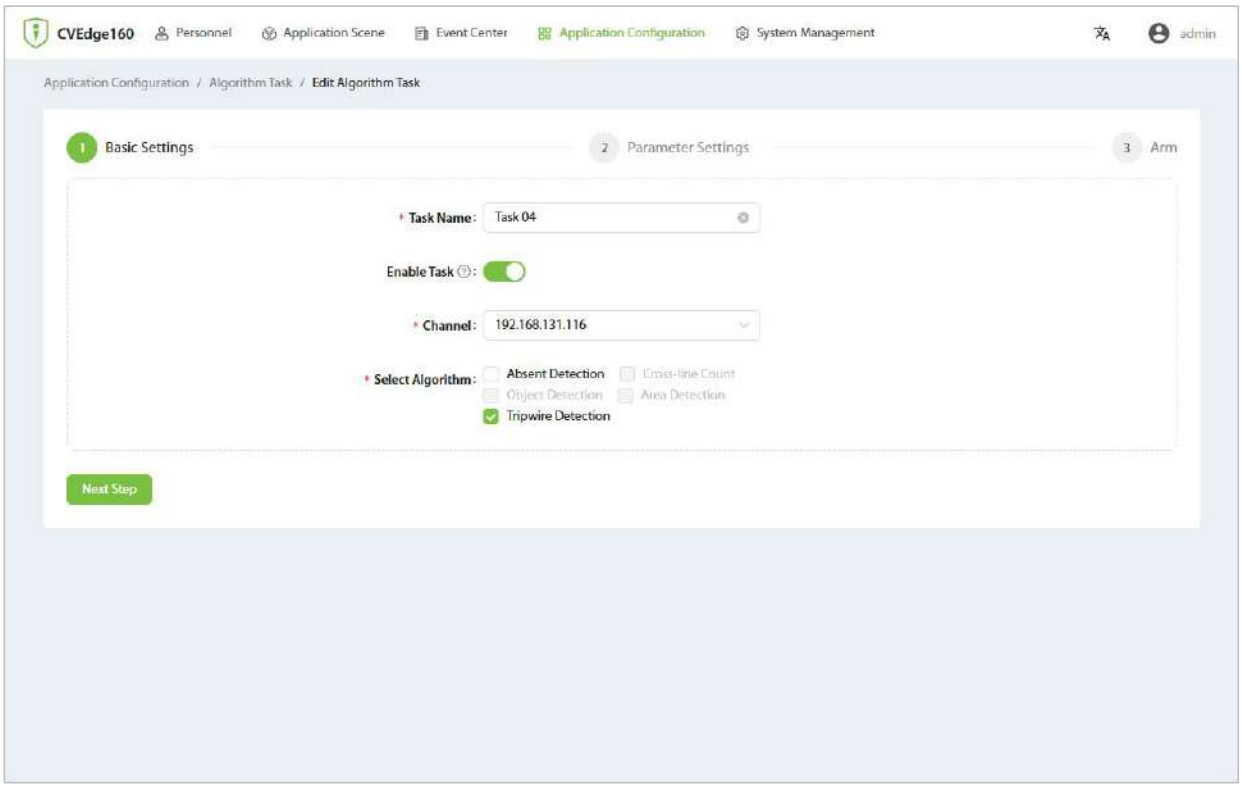
It is used to detect whether there are targets crossing the tripwire in the specified direction. If a target crosses the tripwire in the specified direction, an alarm will be triggered. At this time, the staff will observe the video feed, dispatch personnel to the scene for handling, and prevent the occurrence of harmful events.

Operating Steps:

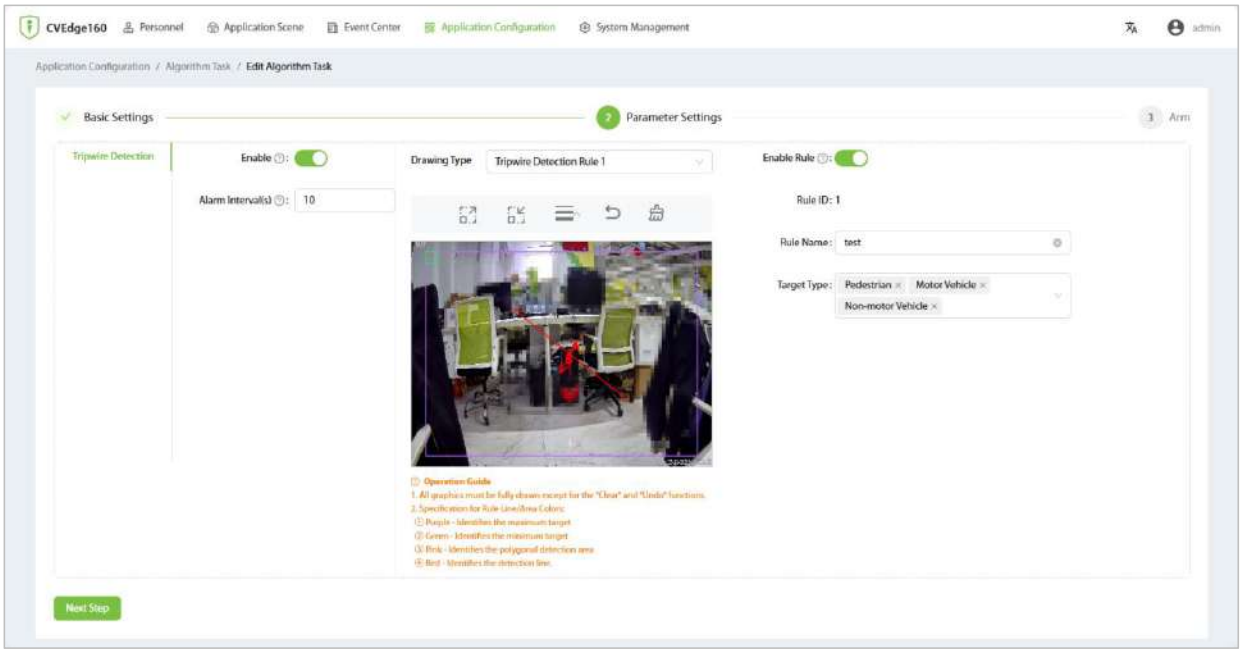
Step 1: On the Web Server homepage, select [**Application Configuration**] - [**Algorithm Task**] - [**Add**].



Step 2: Choose the channel of the algorithm task that needs to be configured under a specific device, and then select the Tripwire Detection algorithm. After completing the settings, click [**Next Step**].



Step 3: Enable the line-crossing detection algorithm and configure the relevant settings. Click the drawing icon at the top of the preview window to draw the detection area.



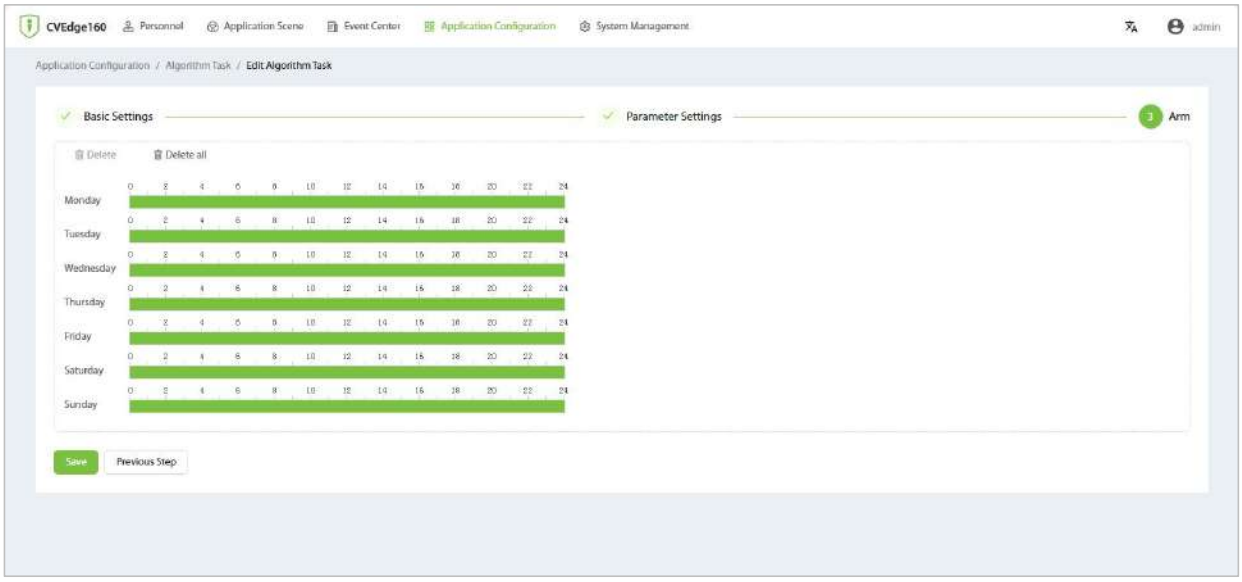
Note: *To set cross-line count detection, you must draw the maximum and minimum target sizes and the detection line. There are default maximum and minimum target sizes, but you can click on the borders of the maximum and minimum targets to modify them according to the actual situation.*

Parameter Configuration Descriptions

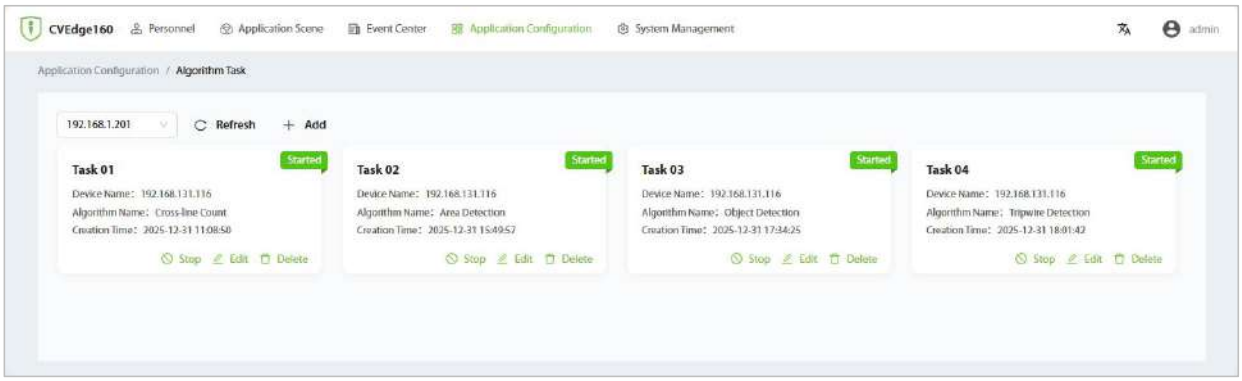
Parameter	Descriptions
Alarm Interval(s)	For the same event and rule, only one alert is triggered within the alert interval. **Note:** To prevent alarm storms, if multiple alarms occur within the detection interval, only one alarm will be reported.
Drawing Type (Cross-Line Detection Rules)	A target counting algorithm can configure four detection rules. These rules operate independently of each other, and all four rules remain active when simultaneously configured.
Direction	Specify the valid direction for pedestrians crossing the detection line. It can be set as bidirectional or unidirectional.
Maximum Target	No alarm will be triggered if the detected target is larger than the set size.
Minimum Target	No alarm will be triggered if the detected target is smaller than the set size.
Undo	Undo the previous drawing operation.
Clear	Clear all current drawing content.

Rule ID	The detection rule corresponding to the drawn type.
Rule Name	Name the detection rule for quick event search in the Event Center.
Target Type	Select the type of detection target according to user needs: 1. Pedestrian, 2. Motor Vehicle, 3. Non-Motor Vehicle.

Step 4: Set the arming time. Only events triggered within the arming time will be reported as alarms.



Upon completion, it will appear in the list as shown below.

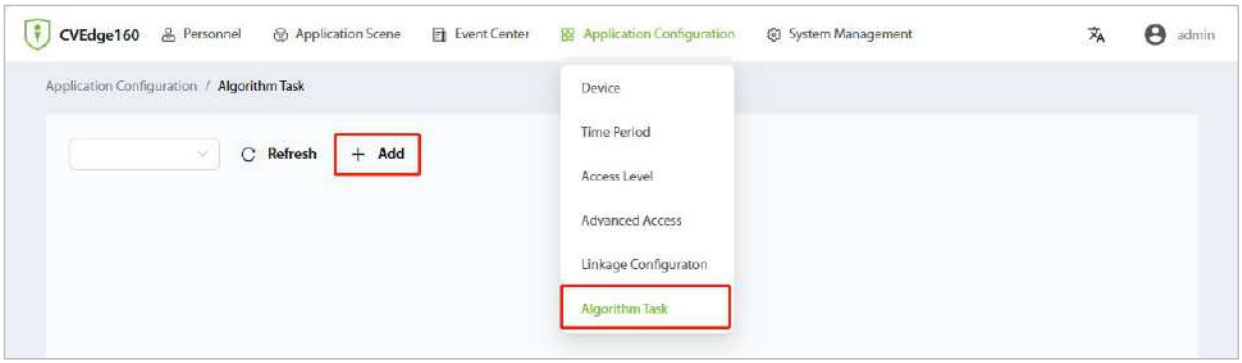


6.9.5 Absent Detection

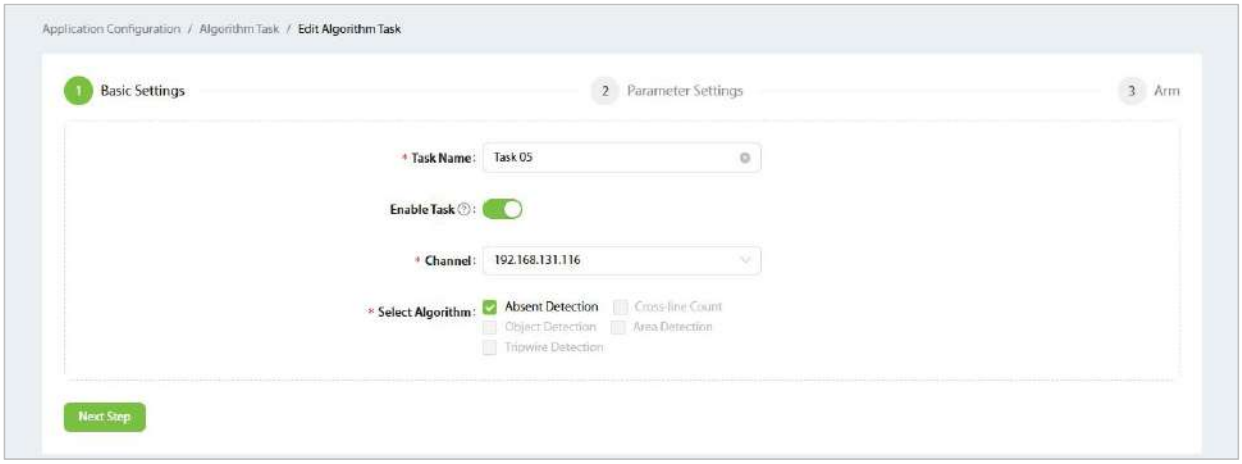
Users can set up a detection area to monitor whether personnel are on duty within the specified area.

Operating Steps:

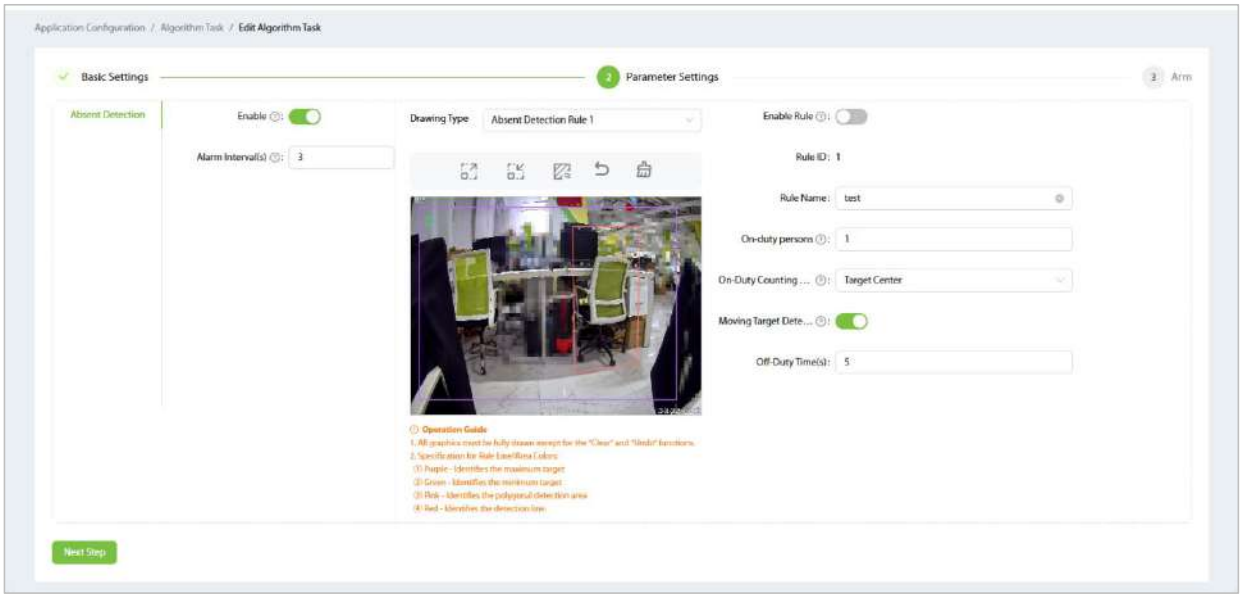
Step 1: On the Web Server homepage, select [**Application Configuration**] - [**Algorithm Task**] - [**Add**].



Step 2: Choose the channel of the algorithm task that needs to be configured under a specific device, and then select the Absent Detection algorithm. After completing the settings, click [**Next Step**].



Step 3: Enable absent detection, configure the detection area and other parameters. Click the drawing icon at the top of the preview window to draw the area (currently, the live detection box does not reflect the off-duty detection status in real time. Please determine the off-duty situation through alarm events).

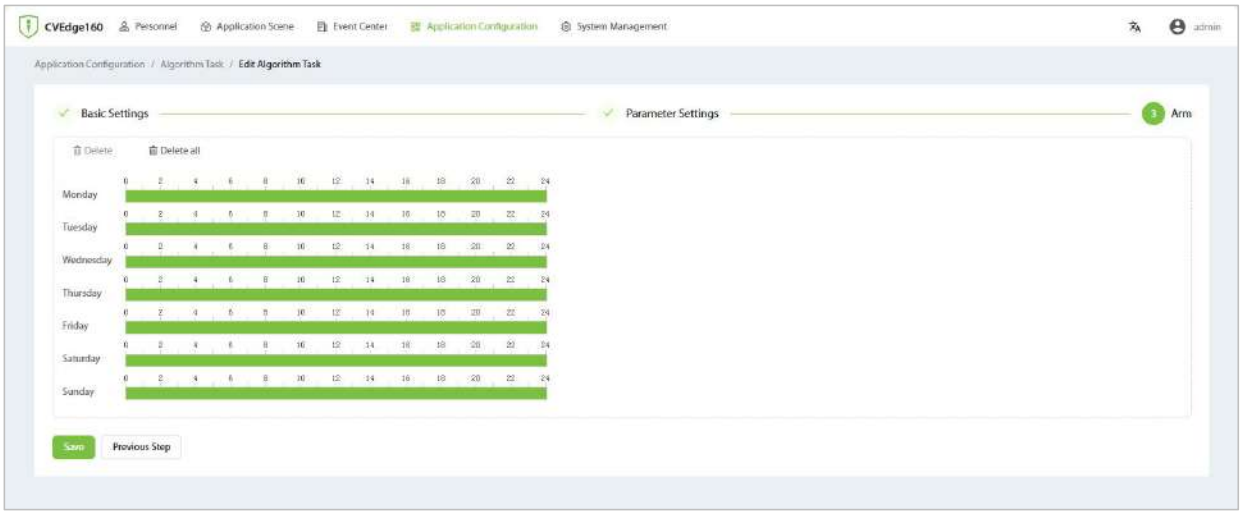


Note: *To set up absent detection, you must draw the maximum and minimum targets and the polygonal area. There are default maximum and minimum targets, but you can click on the borders of the maximum and minimum targets to modify them according to the actual situation.*

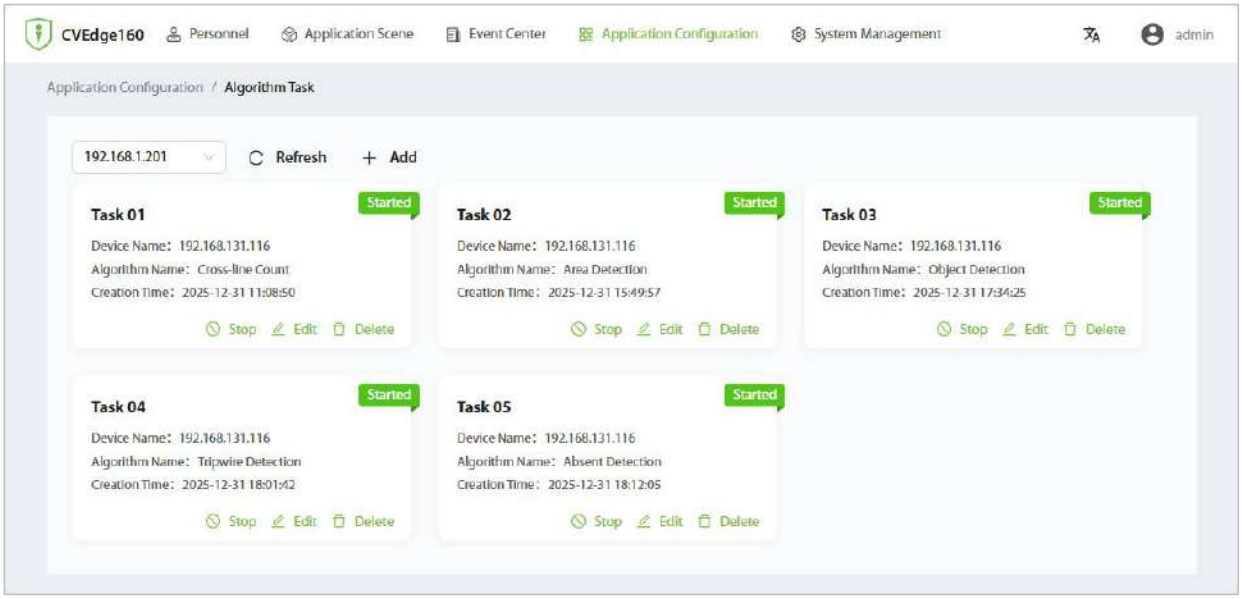
Parameter Configuration Descriptions

Parameter	Descriptions
Alarm Interval(s)	For the same event and rule, only one alert is triggered within the alert interval; if both traffic and total statistics are enabled, cross-reporting will occur for the statistical figures in the reported data. **Note:** To prevent alarm storms, if multiple alarms occur within the detection interval, only one alarm will be reported.
Drawing Type (Cross-Line Detection Rules)	An off-duty detection algorithm can set up to 8 detection rules. These eight rules do not affect each other, and all eight rules can be activated simultaneously.
Polygonal Area	The detection area defines the scope for target detection, and only targets within this area will be detected. By clicking on the border of the detection area, you can edit the shape and size of the area.
Maximum Target	No alarm will be triggered if the detected target is larger than the set size.
Minimum Target	No alarm will be triggered if the detected target is smaller than the set size.
Undo	Undo the previous drawing operation.
Clear	Clear all current drawing content.
Rule ID	The detection rule corresponding to the drawn type.
Rule Name	Name the detection rule for quick event search in the Event Center.
On-duty persons	The specified number of personnel required to be on duty in this area.
On-Duty Counting Method	Target Center Rule: A target will be included in the on-duty count only if the center point of its frame is completely within the detection area; Target Area Intersection Rule: A target will be included in the on-duty count only if its frame has actual overlap (i.e., forms an effective intersection) with the detection area.
Moving Target Detection	When the moving target detection function is enabled, only moving targets will be included in the on-duty count; stationary targets will be excluded.
Off-Duty Time(s)	The time interval for generating an alarm after an off-duty condition is detected.

Step 4: Set the arming time. Only events triggered within the arming time will be reported as alarms.



Upon completion, it will appear in the list as shown below.

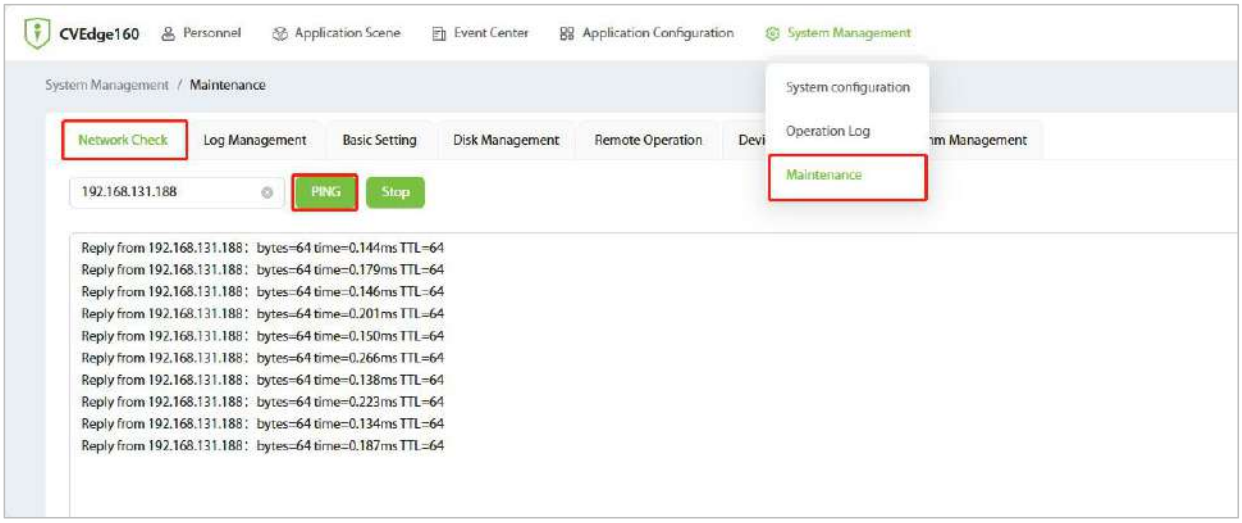


6.10 Maintenance

Within the maintenance management interface, you can perform network check, log management, basic configuration, disk management, remote operations and maintenance, device information management, and algorithm management.

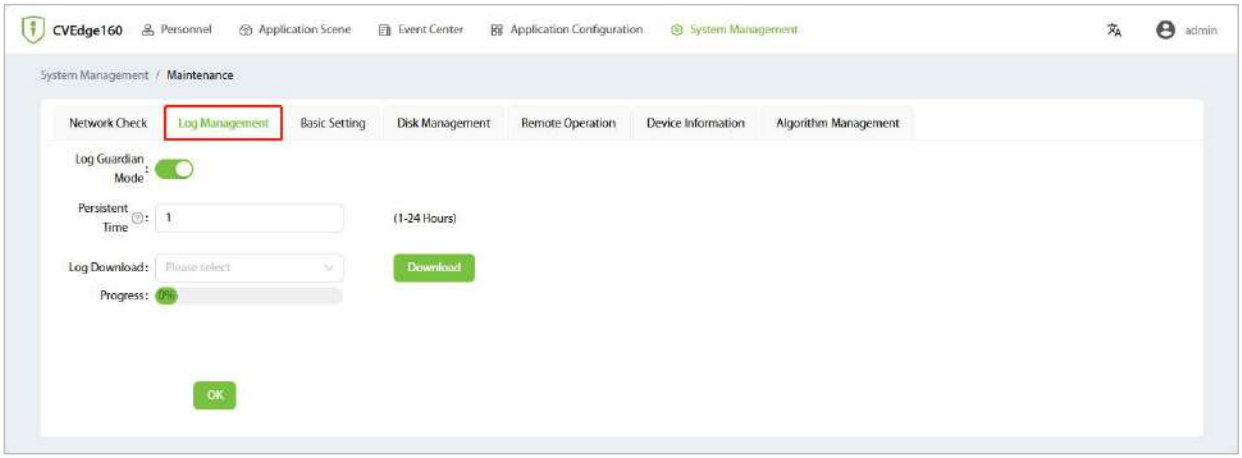
6.10.1 Network Check

1. Click [**System Management**] - [**Maintenance**] in the top menu bar to enter the maintenance setting interface. Then click [**Network Check**] to enter the operation interface.
2. Enter the network IP address and click [**PING**] to run the test, as shown below.



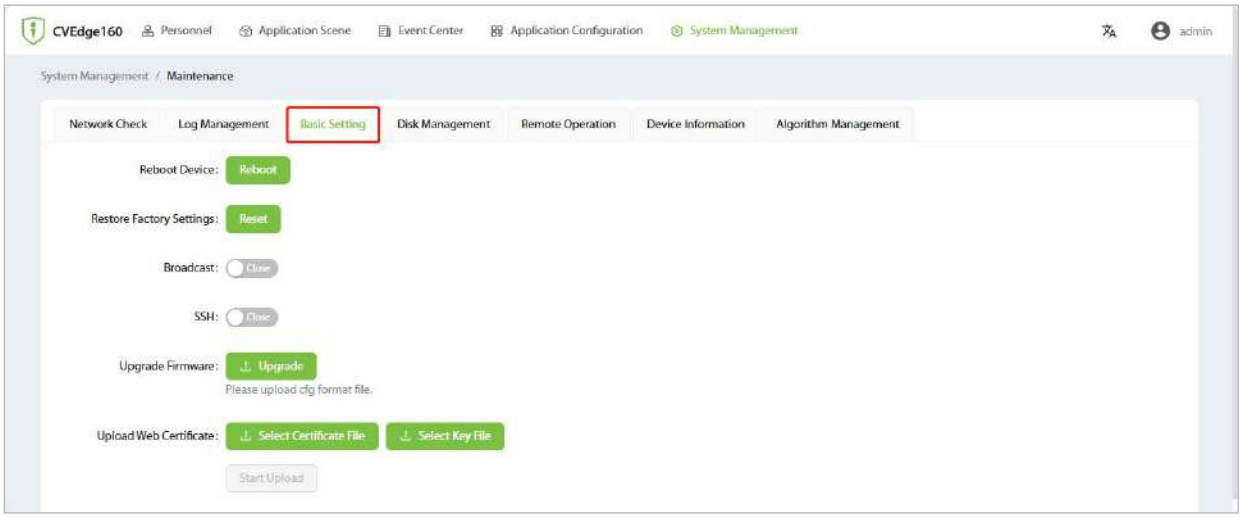
6.10.2 Log Management

1. Click [**System Management**] - [**Maintenance**] in the top menu bar to enter the maintenance setting interface. Then click [**Log Management**] to enter the operation interface.
2. Time to save logs without a USB drive after enabling Guardian Mode.



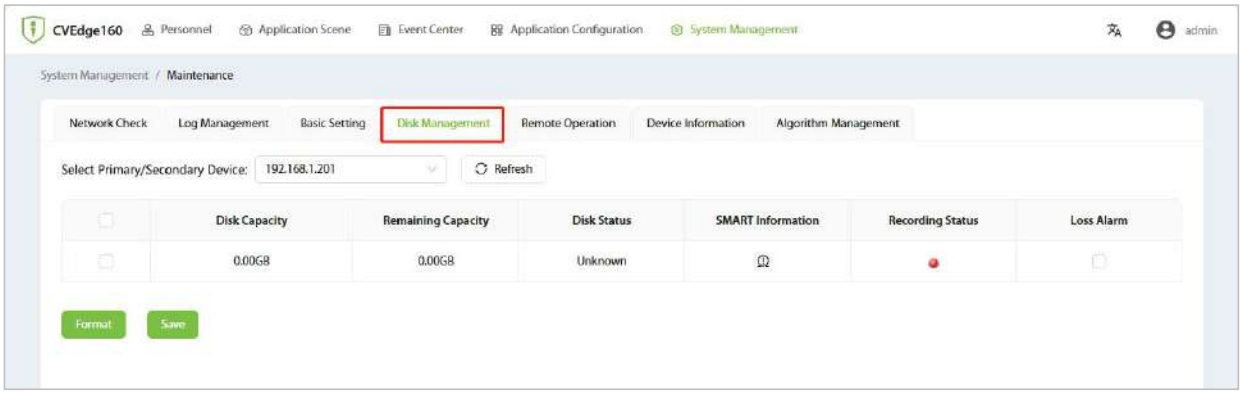
6.10.3 Basic Setting

1. Click [**System Management**] - [**Maintenance**] in the top menu bar to enter the maintenance setting interface. Then click [**Basic Setting**] to enter the operation interface.
2. Users can perform some basic configurations here.



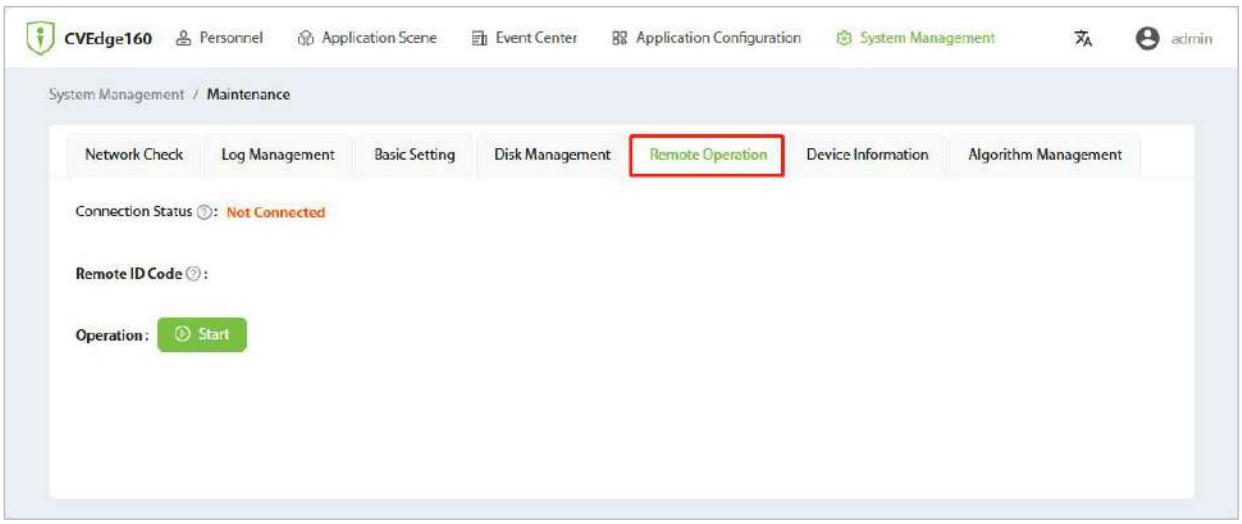
6.10.4 Disk Management

1. Click [**System Management**] - [**Maintenance**] in the top menu bar to enter the maintenance setting interface. Then click [**Disk Management**] to enter the operation interface.
2. After selecting the primary and secondary devices, proceed with the relevant operations.



6.10.5 Remote Operation

1. Click [**System Management**] - [**Maintenance**] in the top menu bar to enter the maintenance setting interface. Then click [**Remote Operation**] to enter the operation interface.
2. Click [**Start**] for remote maintenance. Please provide the Remote ID Code to maintenance personnel to complete the authentication process.



Note: You need to use the **CVEdge160 Remote Maintenance Tool** to perform the operation. The specific steps are as follows:

- **Tool Overview**

CVEdge160 Remote Maintenance Tool is a specialized software designed for technical support personnel to remotely access the web interface of customer devices. It enables technicians to quickly reproduce on-site issues, diagnose faults, and assist with configuration. The tool supports remote login, access, operation, and log analysis of devices over the network, accelerating troubleshooting efficiency.

- **System Environment Requirements**

Client Environment:

✧ Operating System: Windows 10/11 (64-bit)

✧ Hardware Requirements: No specific requirements

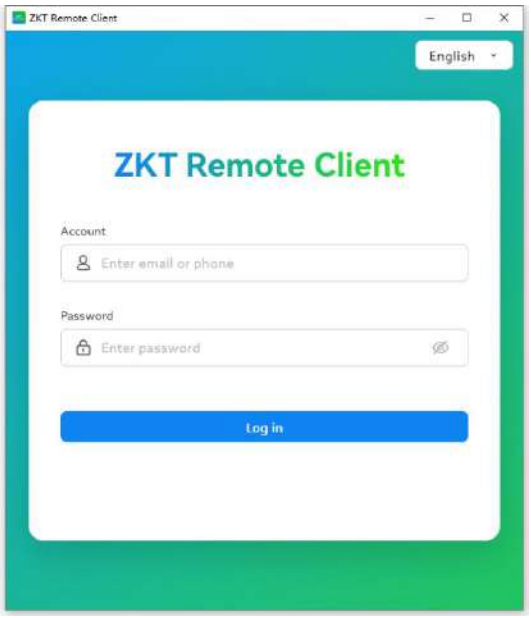
✧ Network Requirements: Stable internet connection (recommended bandwidth ≥ 10Mbps), supports wired/wireless access

- **Installation and Initialization**

Client Installation:

1. Double-click the installation package ZKTRemoteClient_Install_v1_20260126.exe to complete the installation.

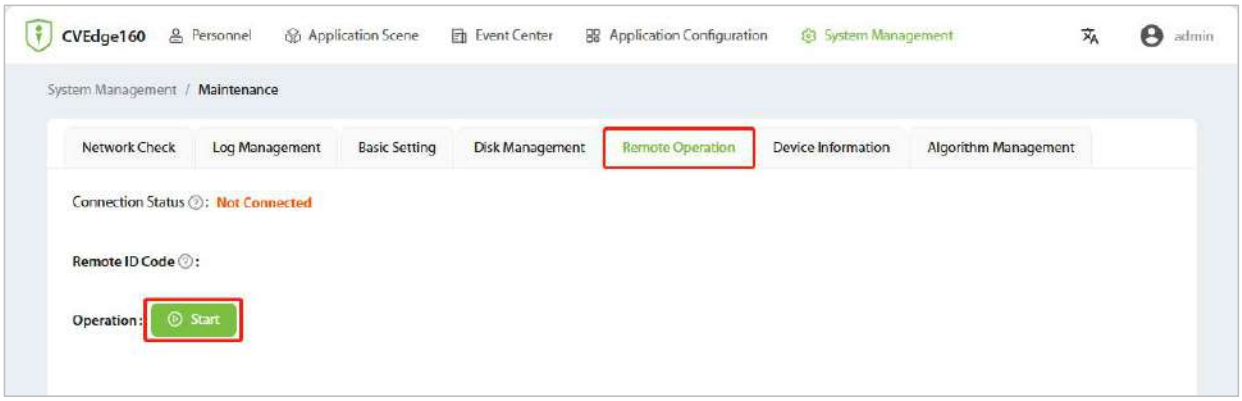
2. After installation, launch the software. The login interface appears as follows:



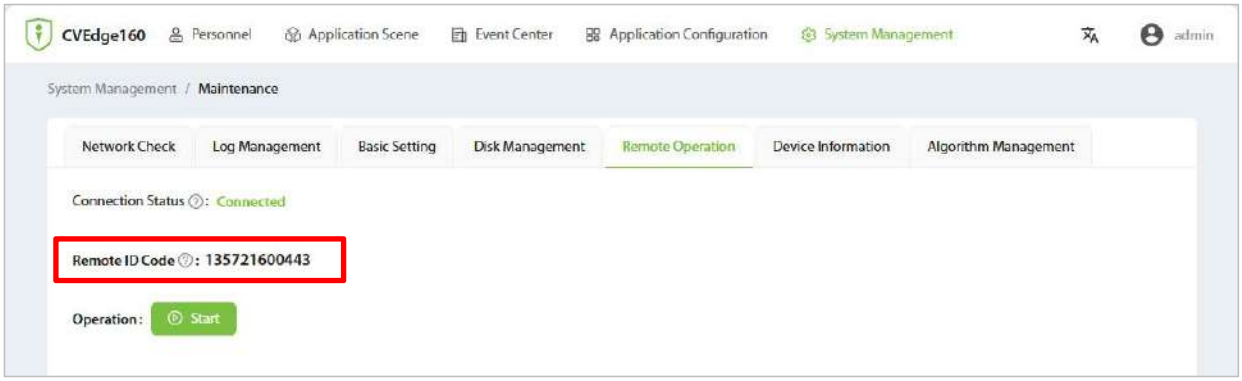
Functional Operation Guide

1. Device Side:

1. Enable "Remote Operations": Click [**System Management**] - [**Maintenance**] - [**Remote Operation**] - [**Start**] for remote maintenance.



2. After enabling this feature, you will receive a remote identification code, as shown in the figure below.



Notes:

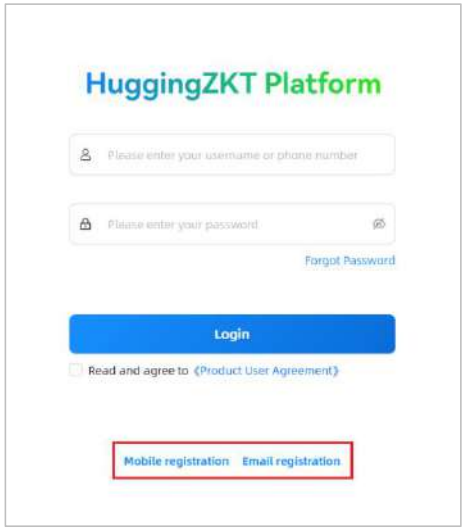
1) To use the remote maintenance feature, ensure the customer's device (CVEdge160) has access to the wide area network;

2) If no connection activity occurs for over 30 minutes, the system will automatically suspend the remote maintenance feature.

2. Client Side:

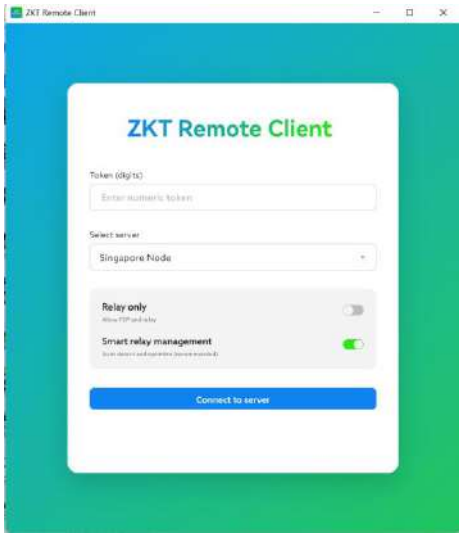
1) Registering an Account:

First-time users must register a new account at http://hugging.minervaiotstaging.com, as shown below:



2) Login Client Tool:

a. After successfully registering a new account, you can log in to the operations and maintenance tool client. Upon login, you will need to configure the information for the device you wish to access remotely. The specific interface is as follows:



Notes:

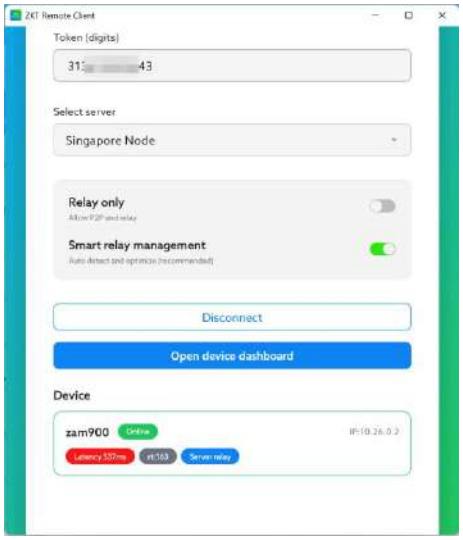
✧ **Token:** Enter the device's "Remote Identification Code".

✧ **Select Server:** Singapore node.

✧ **Relay Connection Only:** Enable to route traffic through the server.

✧ **Smart Relay Management:** Enable to automatically switch to relay mode upon detecting connection timeouts when the first option is disabled.

b. After entering the token, click "Connect to Server." If the connection is successful as shown below, click "Enter Device Backend" to access the device's web interface:



c. After completing remote maintenance, click "Disconnect" to terminate the remote connection with the device.

3) Remote Control

After establishing a successful remote connection, you can log in to the device via remote web access to perform operations and troubleshoot issues.

Troubleshooting Common Issues

1. Remote operation and maintenance cannot be enabled on the device:

✧ Check if the device is connected to the network.

✧ Verify that the device's IP address has internet access permissions.

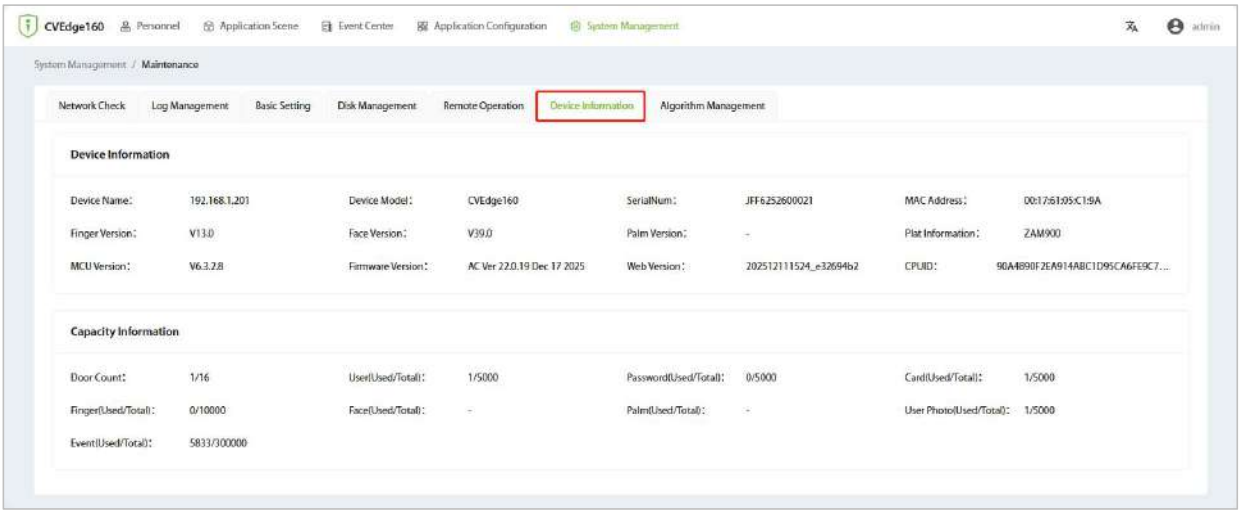
2. Client tool can connect to device, but web login fails:

✧ Browser authentication fails due to security vulnerabilities. Temporary workaround: install browser plugins. Refer to "Install ModHeader Plugin and Remove Referer Request Header.pdf".

✧ Currently, only installation guides for Edge and Firefox plugins are available.

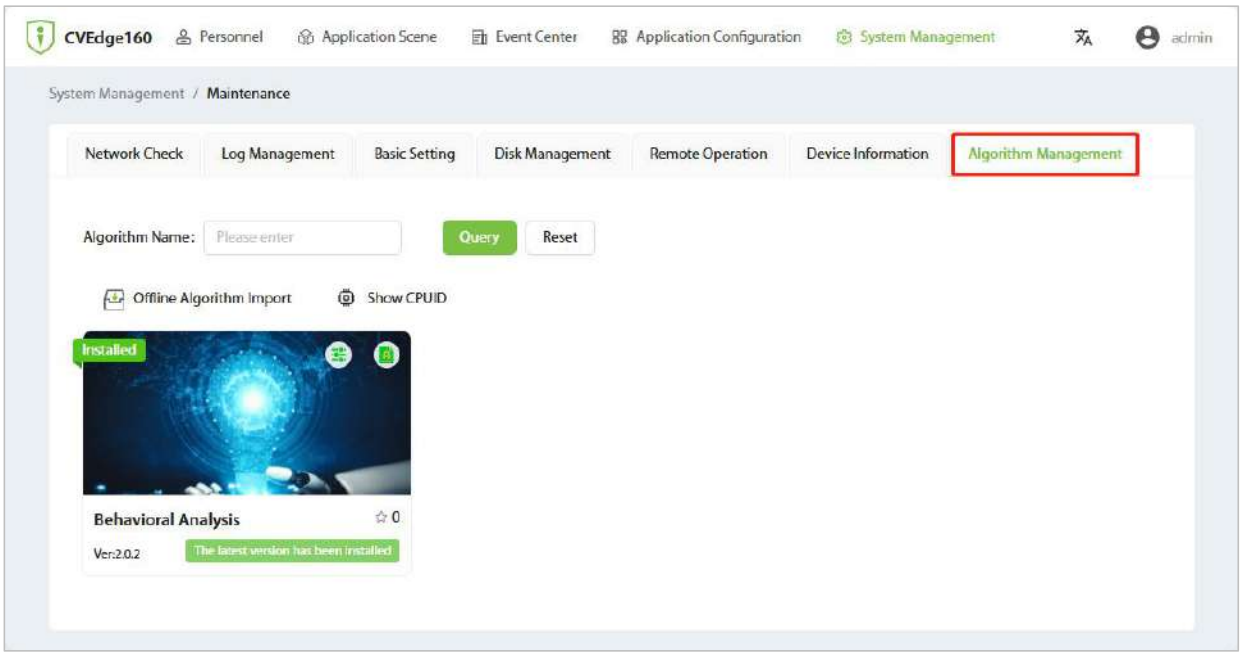
6.10.6 Device Information

Click [**System Management**] - [**Maintenance**] in the top menu bar to enter the maintenance setting interface. Then click [**Device Information**] to enter the device information interface. You can view device information and capacity details here.

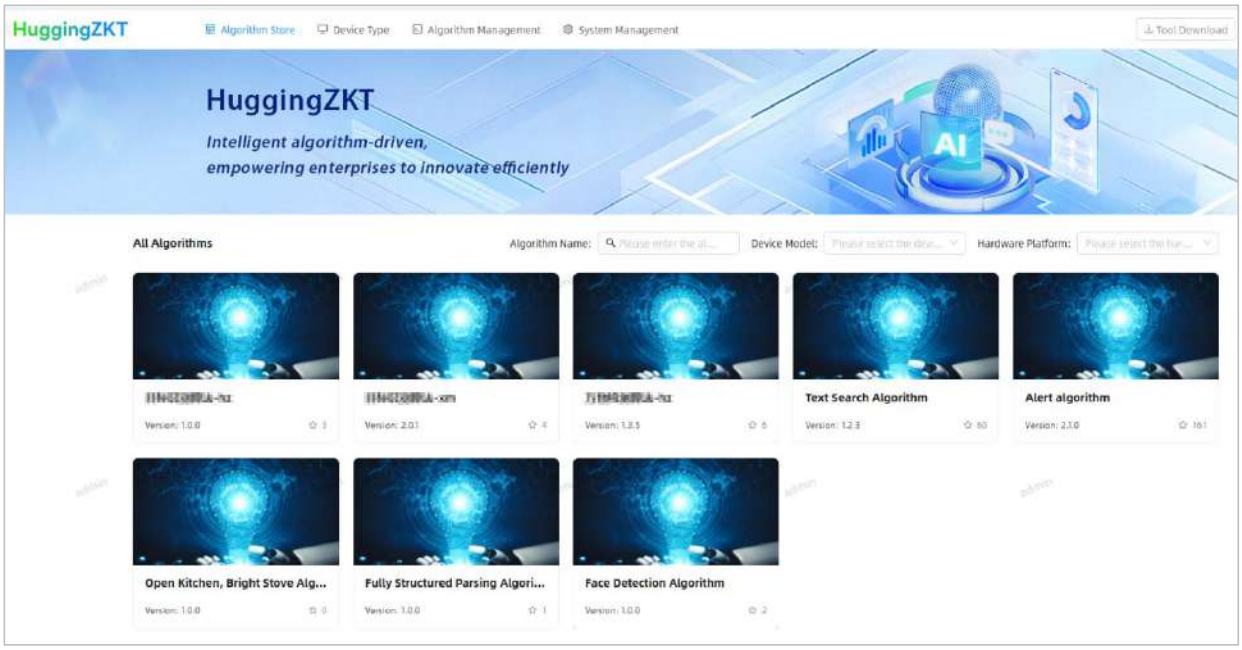


6.10.7 Algorithm Management(Coming Soon)

1. Click [**System Management**] - [**Maintenance**] in the top menu bar to enter the maintenance setting interface. Then click [**Algorithm Management**] to enter the Algorithm Management interface.
2. On this interface, you can import offline algorithm files and view information such as CPUI.



Note: Offline algorithm files must be purchased from the Algorithm Store and downloaded locally. The image below shows the Algorithm Store.



7 Privacy Policy

Notice:

To help you better use the products and services of ZKTeco and its affiliates, hereinafter referred as "we", "our", or "us", the smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.

I. Collected Information

To ensure the normal product operation and help the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

1. **User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.

2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**

2. All the functions of displaying the biometric information are disabled in our products by default.

You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**

4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**

5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.

6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. How we handle personal information of minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.
We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.
Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

IV. Others

You can visit https://www.zkteco.com/cn/index/Index/privacy_protection.html to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

8 Eco-friendly Operation

The product's "eco-friendly operational period" refers to the time period during which this product will not discharge any toxic or hazardous substances when used in accordance with the prerequisites in this manual.

The eco-friendly operational period specified for this product does not include batteries or other components that are easily worn down, and must be periodically replaced. The battery's eco-friendly operational period is 5 years.

Hazardous or Toxic substances and their quantities

Component Name	Hazardous/Toxic Substance/Element					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent chromium (Cr6+)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
Chip Resistor	×	○	○	○	○	○
Chip Capacitor	×	○	○	○	○	○
Chip Inductor	×	○	○	○	○	○
Diode	×	○	○	○	○	○
ESD component	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in SJ/T 11363—2006.

× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in SJ/T 11363—2006.

Note: 80% of this product's components are manufactured using non-toxic and eco-friendly materials. The components which contain toxins or harmful elements are included due to the current economic or technical limitations which prevent their replacement with non-toxic materials or elements.

ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com