Acceder a MainController

Guía de inicio rápido

V1.0.0

Foreword

General

This document elaborates on structure, installation, wiring and WEB operation of the access main controller.

Safety Instructions

The following categorized signal words with defined meaning might appear in the Manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	March 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.

- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Salvaguardias y advertencias importantes

La siguiente descripción es el método de aplicación correcto del dispositivo. Lea la guía detenidamente antes de usarla para evitar peligros y pérdidas materiales. Cumpla estrictamente con la Guía durante la aplicación y consérvela correctamente después de leerla.

Requisito de funcionamiento

- No coloque ni instale el dispositivo en un área expuesta a la luz solar directa o cerca de un dispositivo generador de calor.
- No instale el dispositivo en un área húmeda, polvorienta o fuliginosa.
- Mantenga su instalación horizontal, o instálelo en lugares estables, y evite que se caiga.
- No gotee ni salpique líquidos sobre el dispositivo; No coloque en el dispositivo nada lleno de líquido para evitar que fluyan hacia el dispositivo.
- Instale el dispositivo en lugares bien ventilados; no bloquee su abertura de ventilación.
- Utilice el dispositivo solo dentro del rango nominal de entrada y salida.
- No desmonte el dispositivo de forma arbitraria.
- El dispositivo debe utilizarse con cables de red apantallados.

Requisitos de energía

- Utilice cables eléctricos (cables de alimentación) recomendados por esta área, que deben usarse dentro de su especificación nominal.
- Utilice una fuente de alimentación que cumpla con los requisitos de SELV (voltaje de seguridad muy bajo) y suministre energía con un voltaje nominal que cumpla con la Fuente de energía limitada en IEC60950-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas del dispositivo.
- El acoplador de electrodomésticos es un dispositivo de desconexión. Durante el uso normal, mantenga un ángulo que facilite la operación.
- No corte la fuente de alimentación durante la actualización del dispositivo. La fuente de alimentación se puede cortar solo después de que el dispositivo haya completado la actualización y se haya reiniciado.

Tabla de contenido

1 Overview

Access main controller is a controlling device which compensates video monitoring and visual intercom. It has neat and modern design with strong functionality, suitable for commercial building, corporation property and intelligent community.

Product Highlight

- Support cascade design of CAN bus.
- Overall planning and design of entire route.
- Overall multi-door interlocking.
- Support to connect card readers in the form of fingerprint, IC and password.

Controller Interface

- Locally support 4 groups of lock control output.
- Locally support 8 groups of alarm input and 8 groups of alarm output.
- Locally support 4 groups of exit buttons, 4 groups of door sensor feedback and 4 groups of locking tongue feedback.
- Locally support 4 groups of card readers (four-door one-way 4 groups of RS485 readers or 4 groups of Wiegand readers).

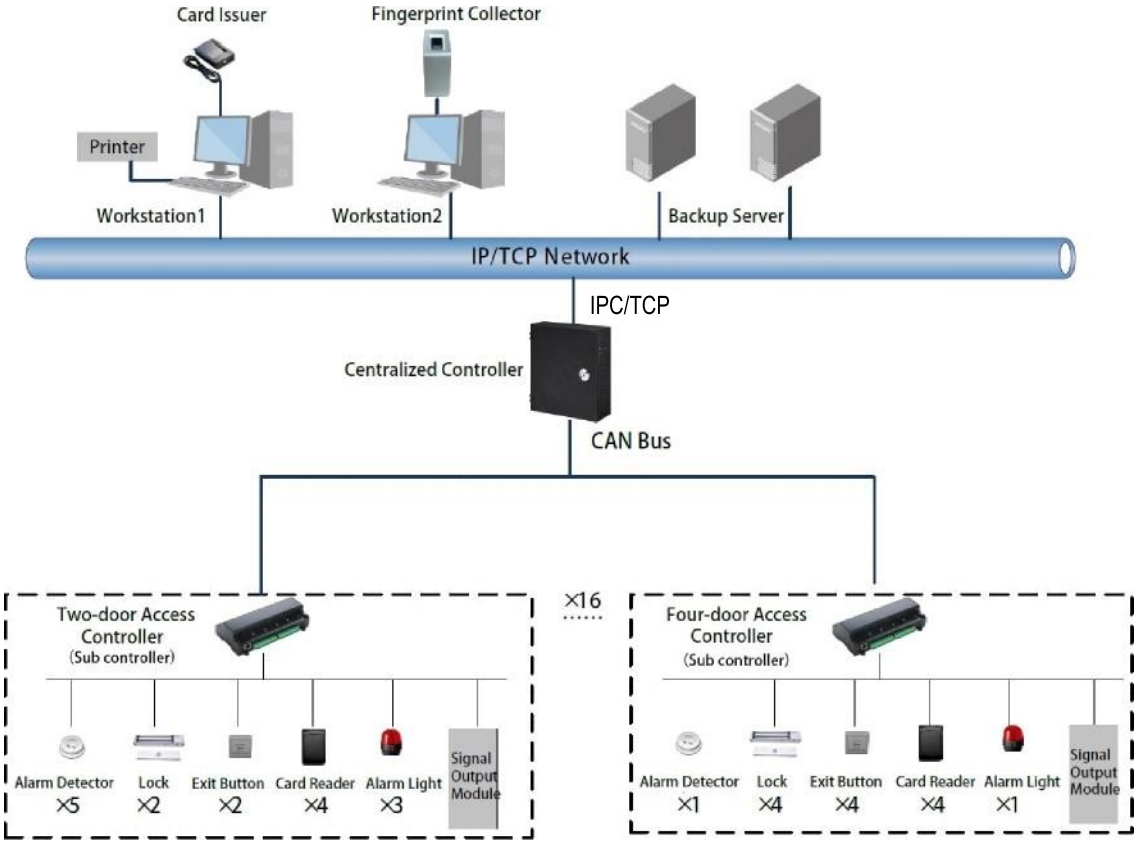
Controller Parameter

- Support three-level network mode of CAN bus, support max. 16 sub controllers and centralized management of 64+4 doors.
- Support max. 200,000 card holders, 150,000 records and 3,000 fingerprints.
- Support illegal intrusion alarm, unlock overtime alarm, tamper alarm, duress alarm and local unlocked alarm.
- Support regional anti-passback and regional AB door.
- Support unlock with multi-card and remote authentication.
- Support VIP card, guest card, patrol card and ordinary card.
- Local web can add, configure and upgrade the sub controllers.
- Support Onvif Profile C/CGI/SDK and third-party platform connection.
- All ports have overcurrent and over-voltage protection.
- Support 128 groups of schedules, 128 groups of periods and 128 groups of holiday schedules.
- Support valid time period setting, password setting and expiration date setting of cards. Regarding guest card, its time of use can be set.
- Permanent data storage during outage, built-in RTC (support DST), online upgrading, NTP (network time protocol) and active registration.
- Working temperature: –30℃ to +60℃ and working humidity: ≤95%.

2 Guía de instalación

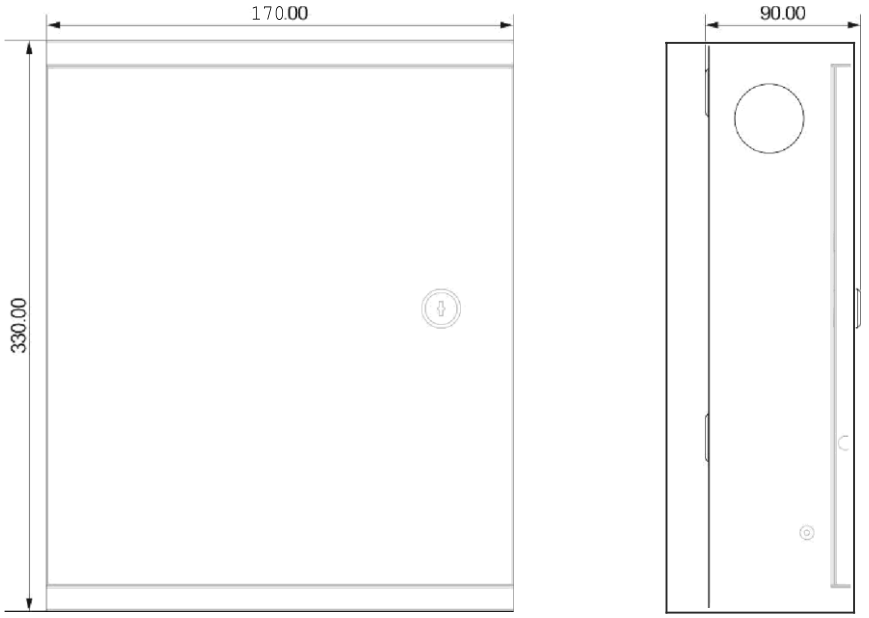
2.1 Estructura del sistema

Figura 2-1 Estructura del sistema



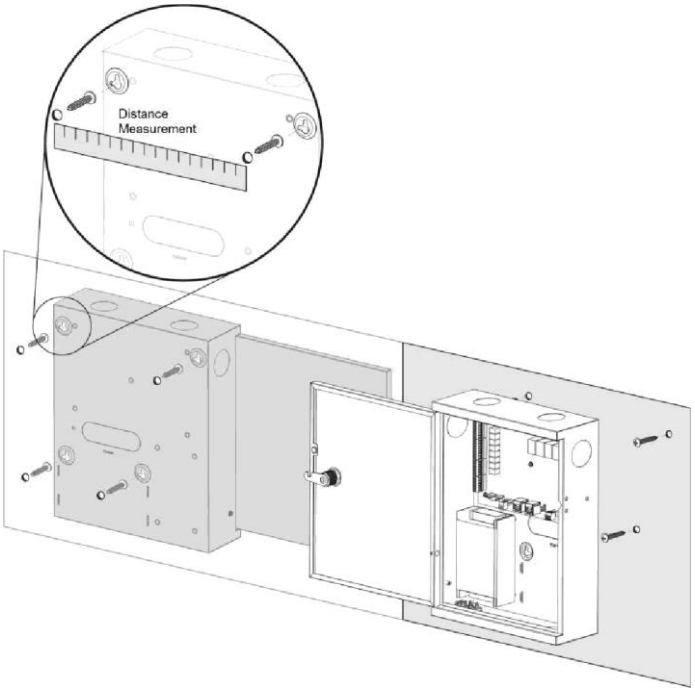
2.2 Dimensión externa

Figura 2-2 Dimensiones (mm)



2.3 Instalación del dispositivo

Figura 2-3 Instalación



Please ensure that device mounting surface is able to bear 3 times as many as the total weight of the device, bracket and accessories.

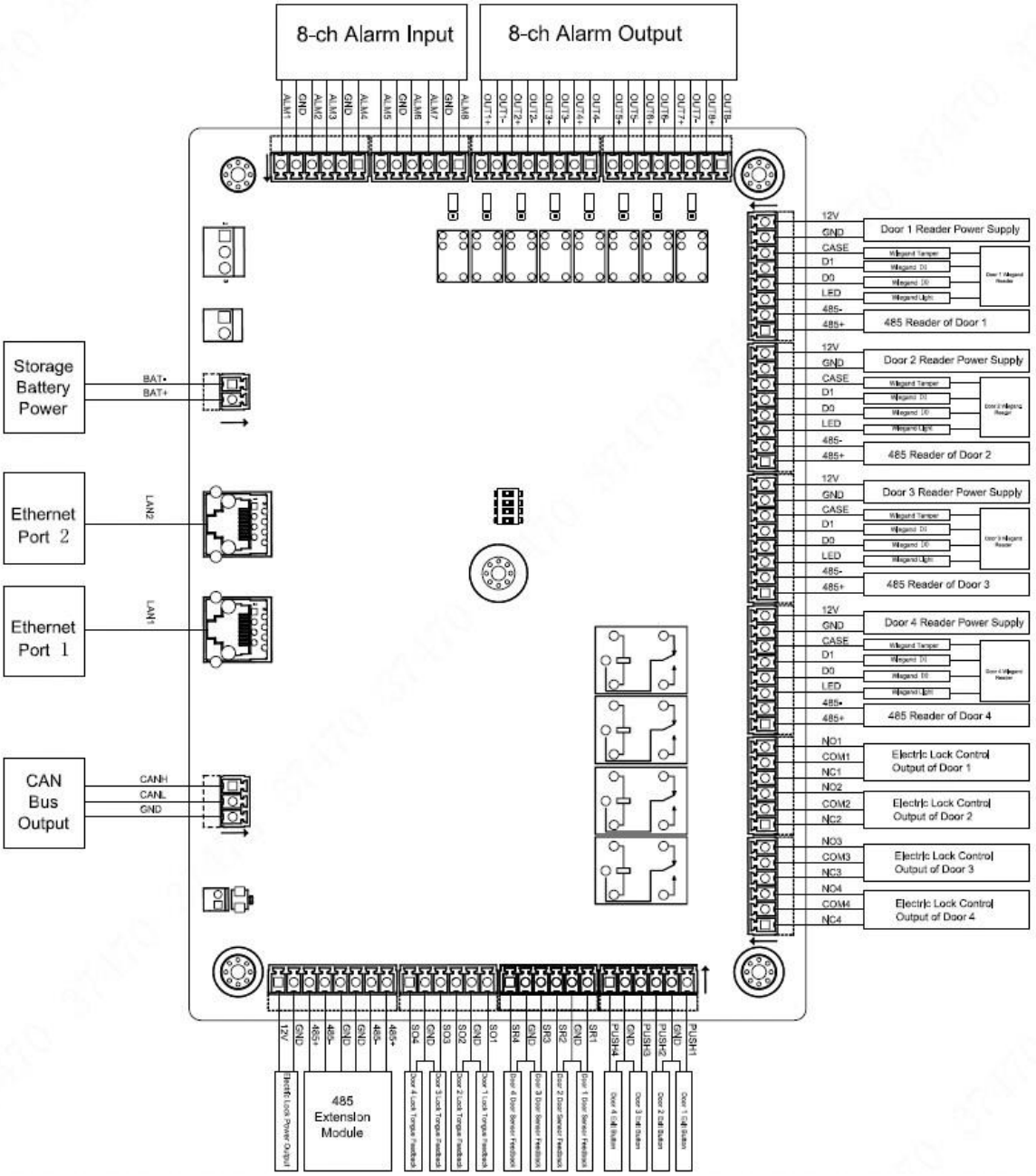
Paso 1 Mida la distancia y posición de cada orificio de acuerdo con los orificios de la carcasa trasera del dispositivo; Taladre agujeros en la pared de acuerdo con las posiciones medidas.

Step 2 Embed expansion nuts and fix screws into the wall.

Step 3 Hang the whole device onto the screws.

2.4 Wiring Diagram

Figure 2-4 Wiring diagram



2.4.1 Description of CAN Bus Wiring

Cable Requirement

- Shielded twisted pair cables (AWG20 or AWG18) are recommended. See Table 3-1 for details.

- If network cable is used, oxygen-free copper cable whose resistance is less than 10 Ω is needed.

Table 2-1 Cable requirement

Cable length	Resistance	Cable cross section area	Cable type
300 m–600 m	<40 mΩ/m	0.5 mm^2–0.6 mm^2	AWG20
600 m–1000 m	<20 mΩ/m	0.75 mm^2–0.8 mm^2	AWG18

Access main controller and sub controllers are connected by CAN bus, see Figure 2-5. For descriptions about wiring terminals, see Table 2-2. For communication distance, see Table 2-1. Data transfer rate can be set through DIP switch, for details, see "2.5 DIP Switch."

Figure 2-5 Use CAN bus to connect main and sub controllers

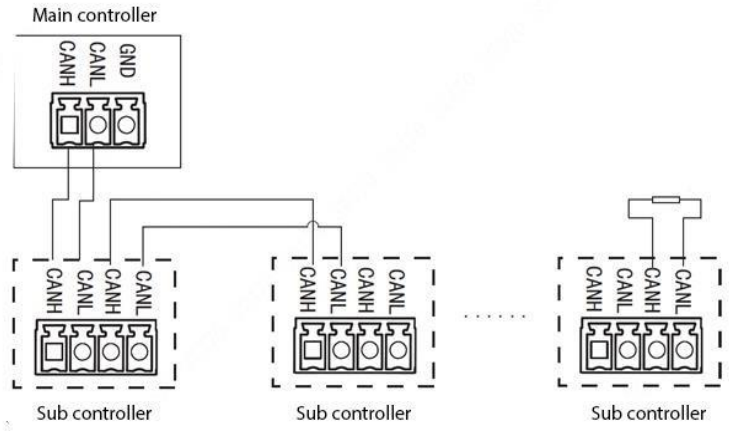


Table 2-2 Communication distance

Interface	Wiring Terminal	Description
CAN Bus	CANH	CAN bus communication
	CANL	

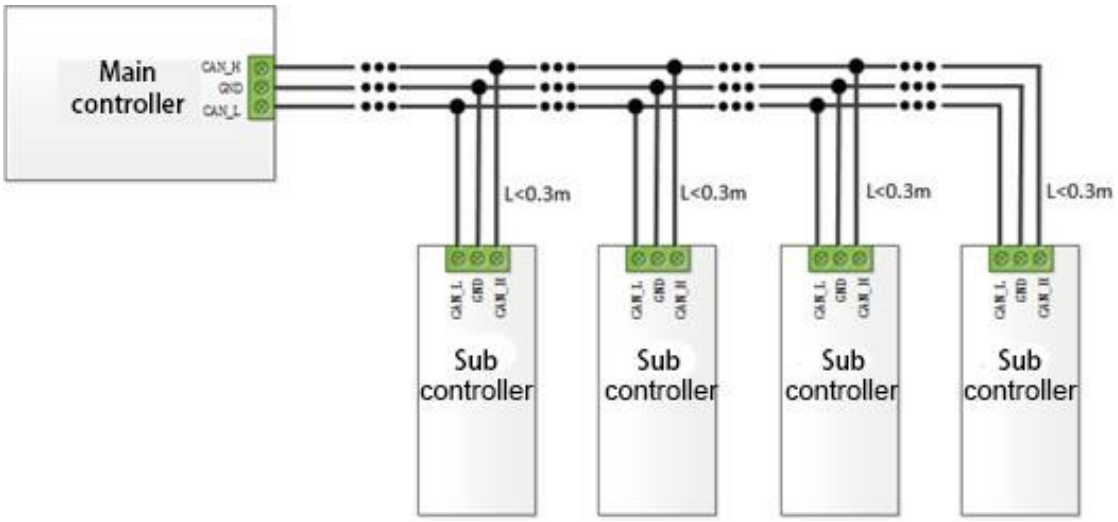
Table 2-3 Data transfer rate

Speed	Distance
50 kb/s	600 m
80 kb/s	400 m
100 kb/s	400 m
125 kb/s	200 m

CAN Connection Mode

"Hand-in-Hand" Connection

Figure 2-6 Hand-in-hand connection



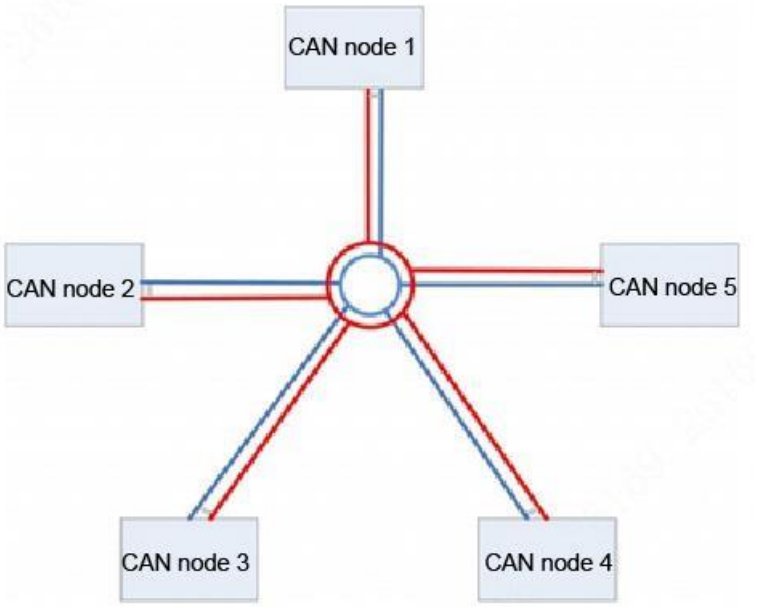
- Connect main controllers and sub controllers by terminal resistance, and 200Ω or 220Ω resistances are recommended. Do not connect peripheral terminal resistances to the main controller because there are already resistances integrated in the main controller. In certain cases, peripheral terminal resistances are needed to do minor adjustment.
- When connecting cables, if T-shaped branch cable layout appears, the T-shaped cable length is not allowed to exceed 0.3 m.
- If network cables are used to transmit data, the cables not used in the network must be all connected to ground cables (no less than two cores). When using one-layer network cable, the shielded layer can be connected to the GND.

- When the distance between main controller and sub controllers is too short, and if there is great common-mode voltage difference and common-mode interference, you can only use CANL and CANH to transfer data without connecting GND.
- When the distance between main controller and sub controllers is far and power supply mode is complex, GND cable must be connected and the GND cable resistance should be as low as possible.

"Non-Hand-in-Hand" Connection

- For the star-shaped cable connection, if the cable lengths are equal, concentrators are not necessary. You just need to adjust terminal resistance.
- R=n×60Ω (R refers to terminal resistance of each branch, and n refers to branch number).

Figure 2-7 Non-hand-in-hand connection



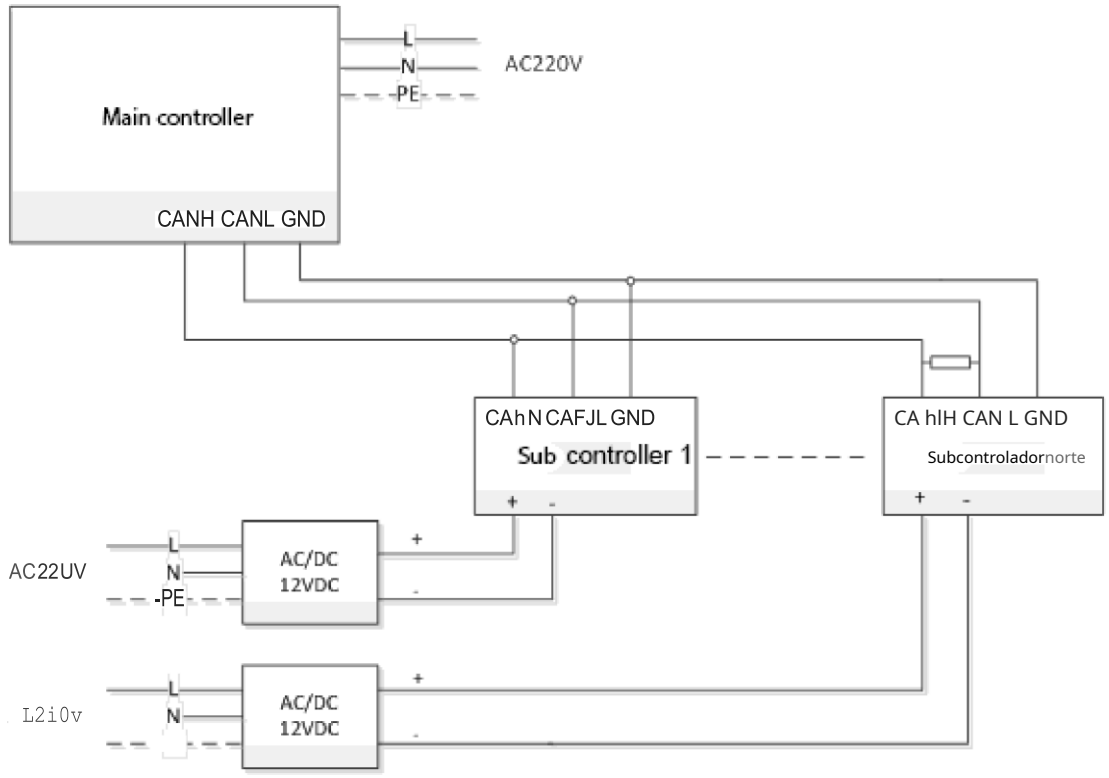
Power Cable Connection

There is a power adapter within the main controller. To provide power for the main controller, connect the main controller to 220V AC power source. Sub controllers are without power adapters. You need to connect them to 12V DC power source.

- In the CAN bus, there must be only one power negative GND connected to PE; otherwise electrical ground loop might occur.
- Currently, PE and GND of the main controller are connected, but PE and GND of sub controllers cannot be connected. When earth leakage protection occurs, you must disconnect the main controller from the PE cable.

- Use a multimeter to test whether there is electric current between negative electrode of the main controller and power adapter cover. If there is no electric current between them, power negative GND was not connected to PE.
- Generally, earth leakage will not occur to the main controller because the current of the main controller is low. You need to pay attention to earth leakage when the main controller and peripheral devices share the GND.

Figura 2-8 Conexión del cable de alimentación



After connecting the CAN bus, stability test must be done for each device. The stability test period must not be less than three days.

2.4.2 Descripción del cableado de la entrada de alarma externa

Admite puertos de entrada de alarma externa de 8 canales.

Figura 2-9 Entrada de alarma externa

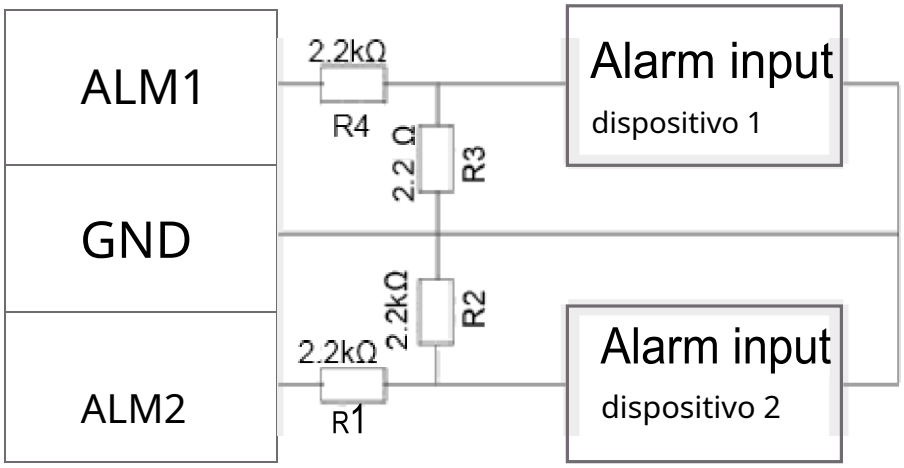


Tabla 2-4 Descripción del terminal

Interface	Wiring Terminal		Description
Entrada de alarma externa	ALM1	Puerto de entrada de alarma 1	Los puertos de entrada de alarma
	GND	Puerto de entrada de alarma 1 y 2	externa conectan detectores de humo y

Interface	Wiring Terminal		Description
	ALM2	Puerto de entrada de alarma 2	Detectores de infrarrojos y más.
	ALM3	Puerto de entrada de alarma 3	
	GND	Puerto de entrada de alarma 3 y 4	
	ALM4	Puerto de entrada de alarma 4	
	ALM5	Puerto de entrada de alarma 5	
	GND	Puerto de entrada de alarma 5 y 6	
	ALM6	Puerto de entrada de alarma 6	
	ALM7	Puerto de entrada de alarma 7	
	GND	Puerto de entrada de alarma 7 y 8	
	ALM8	Puerto de entrada de alarma 8	

Tabla 2-5 Solución de problemas de conexión

Status	ALMIN Value	Description
Circuito abierto	ALMIN = 3,0 V	El cable conectado a los dispositivos de entrada de alarma periféricos no está conectado.
	ALMIN = 0V	El cable conectado a los dispositivos de entrada de alarma periféricos está en cortocircuito.
Normal	ALMIN = 1,5 V	Los dispositivos de entrada de alarma periféricos están conectados correctamente y no hay eventos de alarma.
Alarma	ALMIN = 1.0V	Los dispositivos de entrada de alarma periféricos están conectados correctamente y hay eventos de alarma.

2.4.3 Descripción del cableado de la salida de alarma externa

Hay dos modos de conexión de salida de alarma externa, según el dispositivo de alarma. Por ejemplo, IPC puede usar el Modo 1, mientras que la sirena visual y audible puede usar el Modo 2.

Figura 2-10 Salida de alarma externa (1)

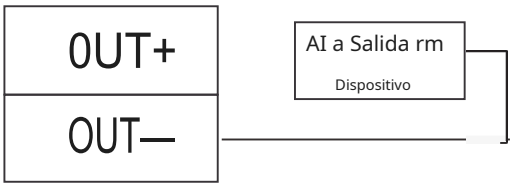


Figura 2-11 Salida de alarma externa (2)

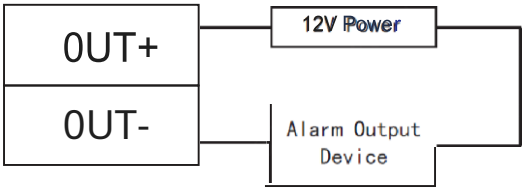


Tabla 2-6 Descripción del terminal

Interface	Wiring Terminal	Description
Externo Alarma Producción	SALIDA1 +	Los puertos de salida de alarma externa conectan sirena visual y audible, etc.
	OUT1-	

2.4.4 Descripción del cableado del lector

1 puerta solo admite la conexión de un tipo de lector: 485 o Wiegand.

Consulte la Tabla 2-7 para obtener descripciones de los terminales de cableado correspondientes a los lectores. Tome la Puerta 1, por ejemplo, y otros lectores son iguales a la Puerta 1. Consulte la Tabla 2-8 para obtener descripciones de las especificaciones y la longitud del cable de video.

Tabla 2-7 Descripción del terminal

Interfaz	Terminal de cableado	Color del cable	Descripción
Lector de entrada de Puerta 1	12V	rojo	Fuente de alimentación del lector
	GND	Negro	
	CASO	Azul	Lector Wiegand
	D1	blanco	
	D0	Verde	
	DIRIGIÓ	marrón	
	485-	Amarillo	485 lector
	485+	Púrpura	

Tabla 2-8 Especificación y longitud del cable

Tipo de lector	Modo de conexión	Largo
Lector 485	Cable de red CAT5e, conexión 485	100 metros
Lector Wiegand	Cable de red CAT5e, conexión Wiegand	30 m

2.4.5 Descripción del cableado de la cerradura

Admite 4 grupos de salidas de control de bloqueo; los números de serie después de los terminales representan las puertas correspondientes. Elija un modo de conexión adecuado según el tipo de bloqueo, como se muestra en la Figura 2-12, Figura 2-13 y Figura 2-14. Consulte la Tabla 2-9 para obtener descripciones de los terminales de cableado.

Figura 2-12 Modo de conexión (1)

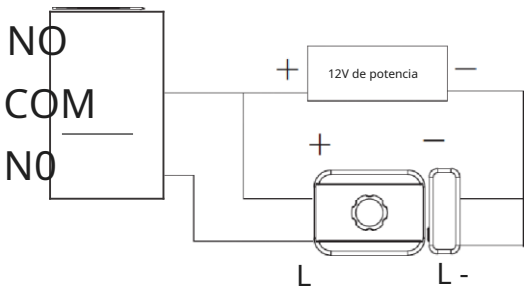


Figura 2-13 Modo de conexión (2)

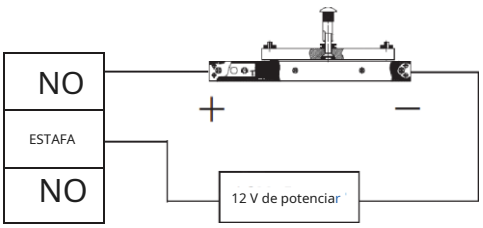


Figura 2-14 Modo de conexión (3)

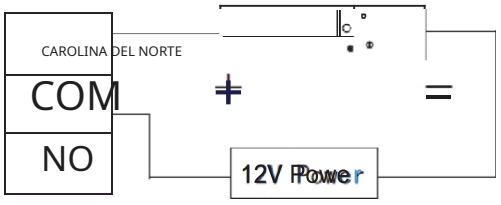


Tabla 2-9 Descripción del terminal

Interfaz	Terminal de cableado	Descripción
Bloquear salida de control Interfaz	NC1	Control de bloqueo de la puerta 1
	COM1	
	NO1	
	NC2	Control de bloqueo de la puerta 2
	COM2	
	NO2	
	NC3	Control de bloqueo de la puerta 3
	COM3	
	NUMERO 3	
	NC4	Control de bloqueo de la puerta 4
	COM4	
	NO. 4	

2.4.b Descripción del cableado del botón de salida

Los terminales de cableado correspondientes del botón de salida se muestran en la Figura 2-15.

Figura 2-15 Terminales del botón de salida del cableado

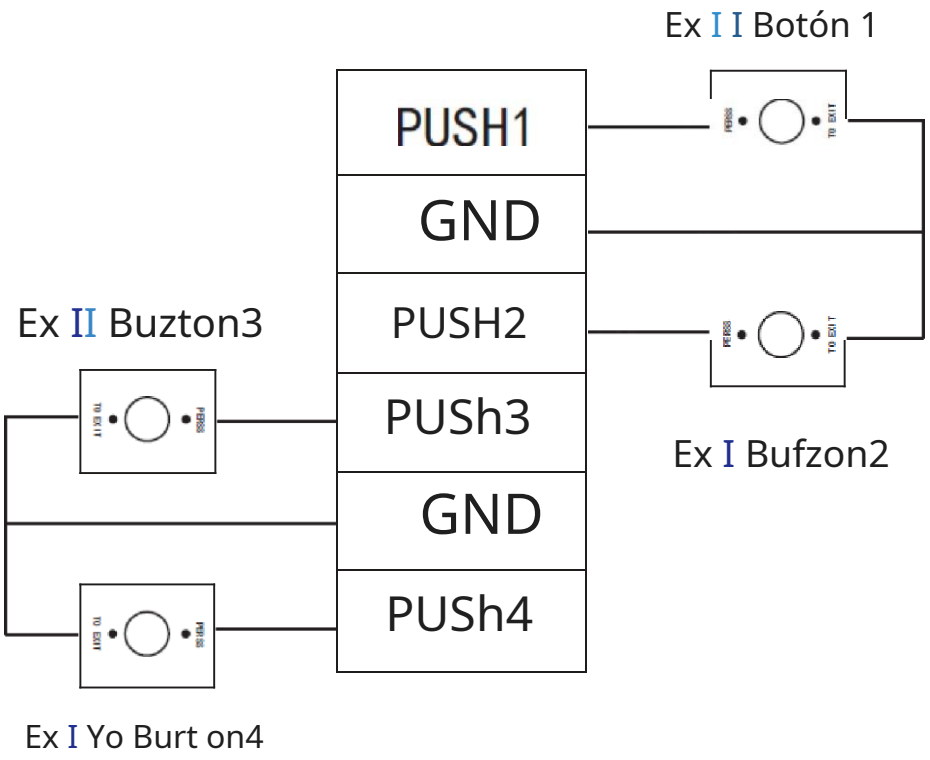


Tabla 2-10 Descripción del terminal

Interfaz	Terminal de cableado	Descripción
Control del botón de salida Interfaz	PUSH1	Botón de salida de la puerta 1
	GND	Compartido por puerta 1 y 2
	PUSH2	Botón de salida de la puerta 2
	PUSH3	Botón de salida de la puerta 3
	GND	Compartido por puerta 3 y 4
	PUSH4	Botón de salida de la puerta 4

2.4.7 Descripción del cableado del sensor de puerta

Consulte la figura siguiente para conocer los terminales de cableado del sensor de puerta.

Tabla 2-11 Cableado de terminales del sensor de la puerta

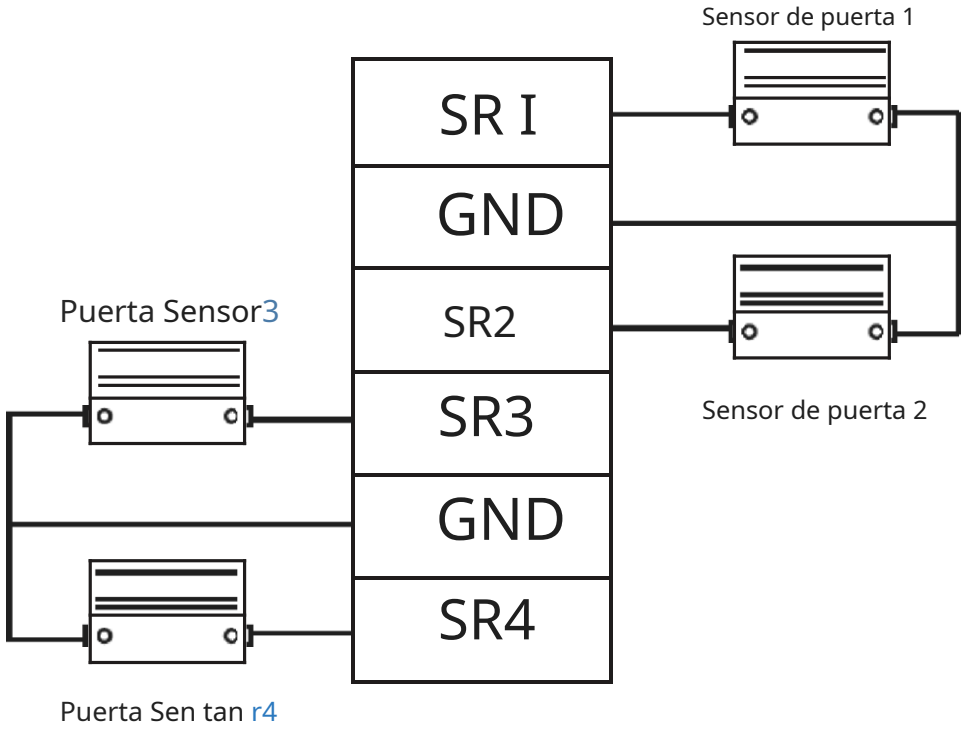


Tabla 2-12 Descripción del terminal

Interfaz	Terminal de cableado	Descripción
Sensor de puerta Interfaz de retroalimentación	SR1	Respuesta del sensor de puerta n. ° 1
	GND	Compartido por puerta 1 y 2
	SR2	Retroalimentación del sensor de puerta n. ° 2
	SR3	Respuesta del sensor de puerta n. ° 3
	GND	Compartido por puerta 3 y 4
	SR4	Respuesta del sensor de puerta n. ° 4

2.5 DIP Switch

Set device number and speed with DIP switch. Speed of access main controller must be consistent with access sub controller.

-  the switch is at ON position, meaning 1.
-  the switch is at the bottom, meaning 0.

Figure 2-16 DIP switch

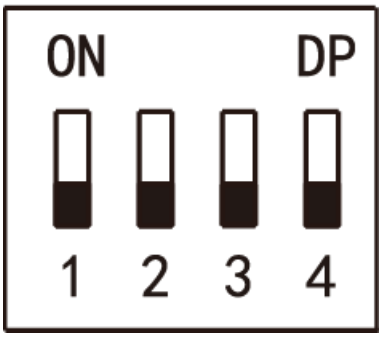
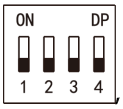
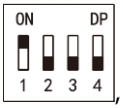
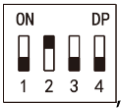


Table 2-13 Function description

Function	No.	Description
Speed	1–4	Set the speed. ● All of them are at the bottom  , transmission speed is 50 kb/s. ● Only digit 6 is at ON position  , transmission speed is 80 kb/s. ● Only digit 7 is at ON position  , transmission speed is 100 kb/s. ● Digits 6 and 7 are at ON position  , transmission speed is 125 kb/s.

2.6 Reset

Insert a needle into RESET hole, and press and hold for a few seconds to restart the controller.

3 Web Configuration

Default IP address of access main controller is 192.168.1.109. During the first use, connect PC with the device directly, modify and ensure that IP address of PC and IP address of the device are in the same network segment, in order to login WEB for operations.

3.1 Initialization

During the first use, please set admin username and password (default administrator username is admin).

To ensure device safety, please keep admin login password properly after device initialization, and modify it regularly.

Step 1 Open IE explorer, input IP address of access main controller in the address bar, and press Enter.

Figure 3-1 Device initialization

Step 2 Set admin login password and Email.

- The password can be set with 8–32 digits of characters, and must include at least two types of number, letter and ordinary character (expect “‘”, “””, “;”, “:” and “&”).
- Bind Email. Scan QR code, input the reserved Email to receive a security code, and thus reset admin password.

- Without reserved Email or in order to modify the Email, please set at **System > User Management** interface. Please refer to the user's manual for details.

Step 3 Click **Next**.

Step 4 Click **OK**.

3.2 Login

Step 1 Open IE explorer, input IP address of access main controller in the address bar, and press Enter.

Step 2 Input username and password.

- Default administrator username is admin, whereas password is the login password set during device initialization. For the sake of safety, it is suggested that you modify admin password regularly and keep it properly.
- If you forget the login password, click **Forget Password** to reset it. Please refer to the user's manual for details.

Step 3 Click **Login**.

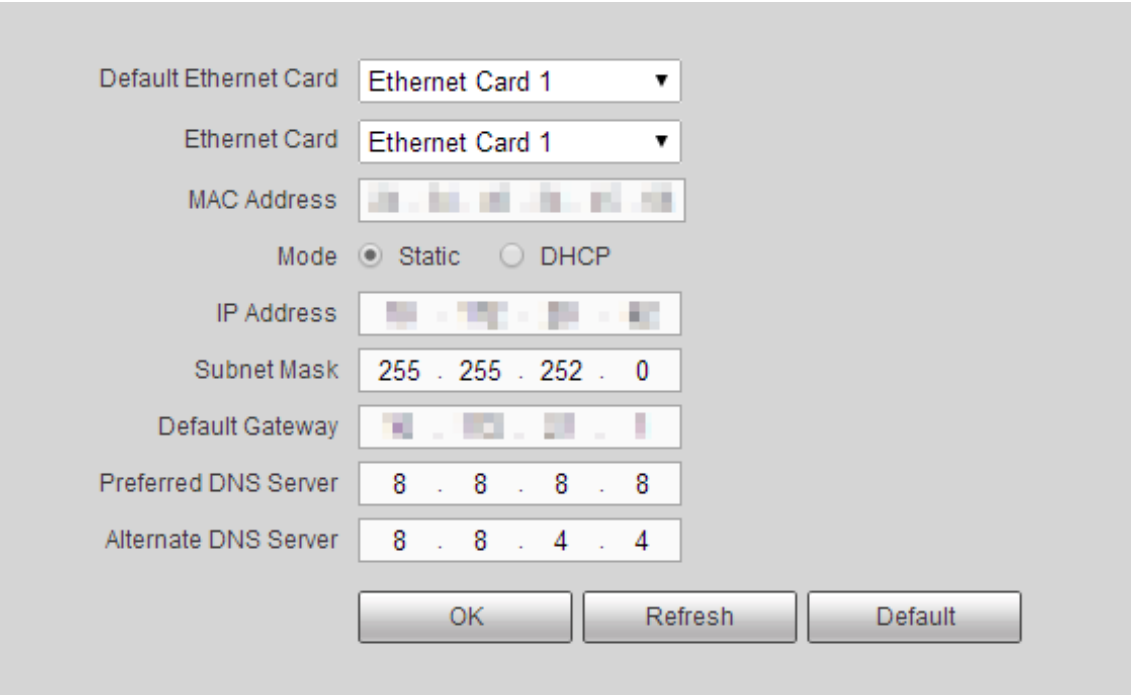
The **Preview** interface is displayed.

3.3 Set Network

Set IP address and DNS server of access main controller, in order to connect with other devices in the network.

Step 1 Select **System > Network > TCP/IP**.

Figure 3-2 TCP/IP



Step 2 Set TCP/IP parameters.

Table 3-1 Parameter description

Parameter	Description
Default Ethernet Card and Ethernet Card	They cannot be modified. Default one is Ethernet Card 1.
MAC Address	Display MAC address of the device.
Mode	• Static Set IP address, subnet mask and gateway manually. • DHCP Obtain IP function automatically. When DHCP is enabled, IP address, subnet mask and gateway cannot be set. □ If present DHCP takes effect, IP/subnet mask/gateway displays the value obtained by DHCP. Otherwise, they display 0. □ To view the manual set IP, if DHCP is not effective, please disable DHCP; display IP info that is not obtained by DHCP. If DHCP takes effect, previous IP info cannot be displayed by disabling DHCP, but IP parameters must be set again. □ When PPPoE is enabled, IP address, subnet mask, default gateway and DHCP cannot be modified.
IP Address	Input numbers to modify IP address; set subnet mask and default gateway corresponding to IP address.  IP address and default gateway must be in the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS Server	IP address of DNS server.
Alternate DNS Server	IP address of alternate DNS server.

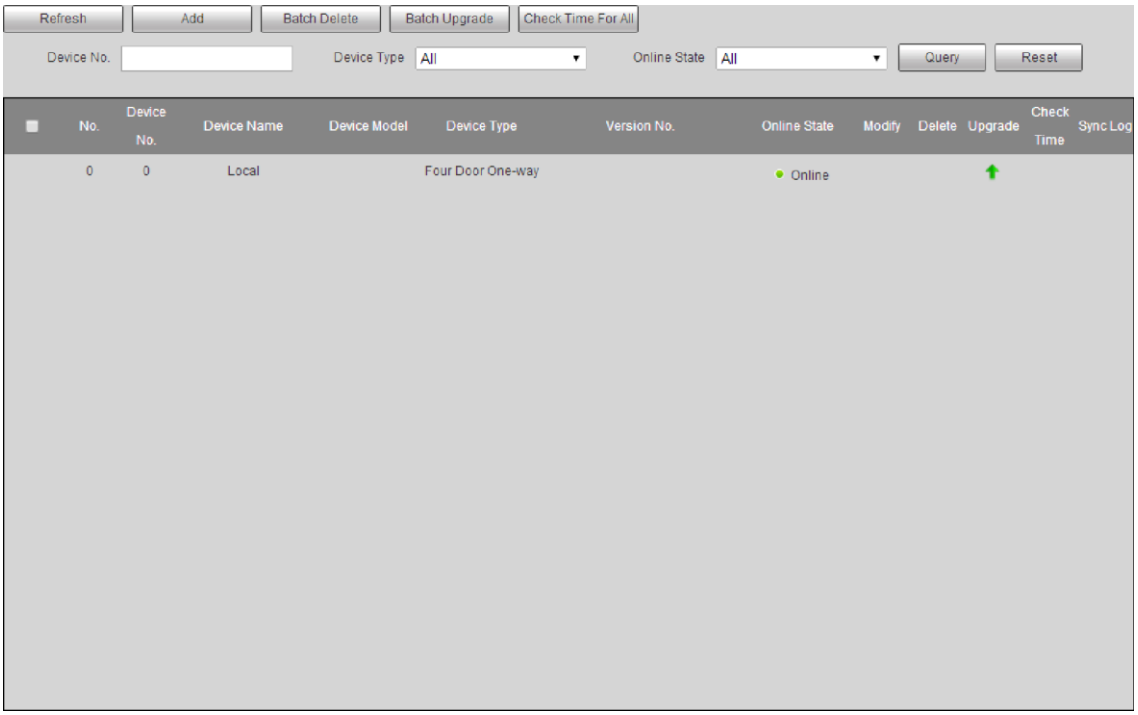
Step 3 Click **OK** to complete setting.

3.4 Add Access Controller

After connecting sub controller with access main controller, add the sub controller to access main controller management system, in order to realize unified management. Maximum 16 controllers can be added.

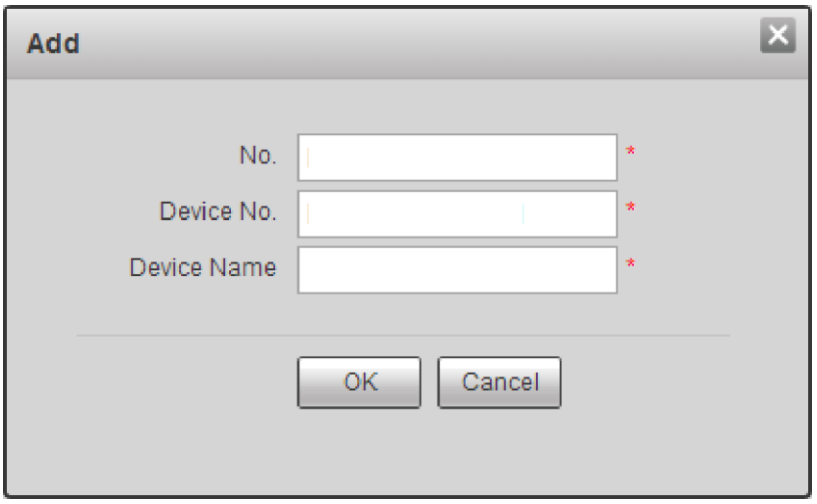
Step 1 Select **Access > Device Management**.

Figura 3-3 Gestión de dispositivos



Paso 2 Haga clic en Agregar.

Figura 3-4 Agregar un dispositivo



Paso 3 Introduzca el número, el número de dispositivo y el nombre del dispositivo.

Tabla 3-2 Descripción de los parámetros

Parameter	Description
No.	Número personalizado que va de 1 a 16. El número no se puede repetir.
No de dispositivo	Es el mismo que el número de subcontrolador agregado. El número de subcontrolador se establece en el interruptor DIP y se puede utilizar después de transformar la codificación binaria en un sistema decimal.
Nombre del dispositivo	Nombre del subcontrolador personalizado, con el fin de facilitar la gestión. El nombre consta de 16 dígitos como máximo, incluida una letra, un número y un carácter especial en inglés. El nombre no se puede repetir.

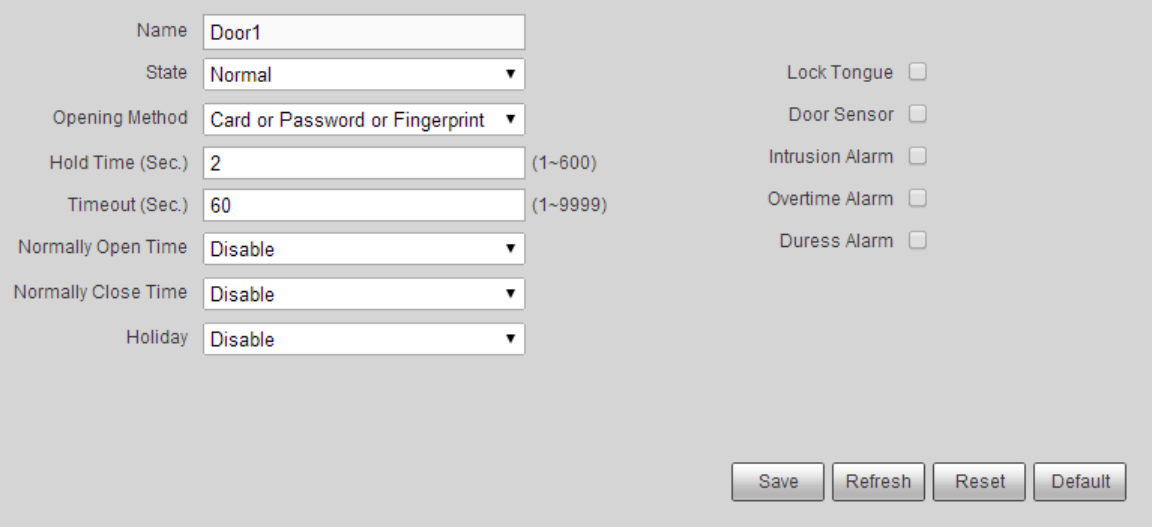
Paso 4 Haga clic en Aceptar.

3.5 Set Door Parameters

Configure parameters of doors under access controller.

Step 1 Select **Access > Door Parameters**.

Figure 3-5 Door parameter



Step 2 Select a door in the device tree in the left, and configure the door parameters.

Table 3-3 Parameter description

Parameter	Description
Name	Display the name of present door.
Status	Select door status, which won't be affected after reboot. ● Normal: open the door in a preset way. ● Normally closed: the door is normally closed and cannot be opened in any way. ● Normally open: the door is normally open and can be entered directly.
Opening Method	Select an opening method. Only the selected method works, while other methods are invalid. ● Password: open the door with password only. ● Card: open the door with card. ● Card and password: open the door with card plus password. ● Period: open the door with corresponding methods within the preset period. ● Fingerprint: open the door with fingerprint only. ● Card or password or fingerprint: open the door with one of the three methods. ● Card and fingerprint: open the door with card plus fingerprint.
Hold Time (Sec.)	Hold time of an open door. The door is closed automatically after hold time.
Timeout (Sec.)	When "overtime alarm" is enabled, upload an alarm if exceeding opening time.
Normally Open Time	The door is normally open within the set time.
Normally Close Time	The door is normally closed within the set time.
Holiday	It is effective within the selected

In the drop-down list, select a synchronously set period in Smart PSS client.

● Disabled: period control is not

Parameter	Description	
	holiday period, and becomes ineffective after the period.	enabled. ● All day: this setting is executed 24 hours a day.
Lock Tongue	Tick the checkbox to enable lock tongue function. Judge and alarm according to lock tongue status.	
Door Sensor	Tick the checkbox to enable door sensor function. Judge and alarm according to door sensor status.	
Intrusion Alarm	Tick the checkbox to enable intrusion alarm function. Upload an alarm in case that door sensor or door tongue is opened when the door is not opened normally.	While the alarm is enabled, corresponding be enabled. Otherwise, door status cannot be judged.
Overtime Alarm	Tick the checkbox to enable overtime alarm function. Upload an alarm in case that opening time exceeds "overtime".	
Duress Alarm	Tick the checkbox to enable duress alarm function. In case of duress, open the door with duress card, duress password or duress fingerprint. The door will be opened normally, but the system will upload alarm info to management center.	

Step 3 Click **Save**.

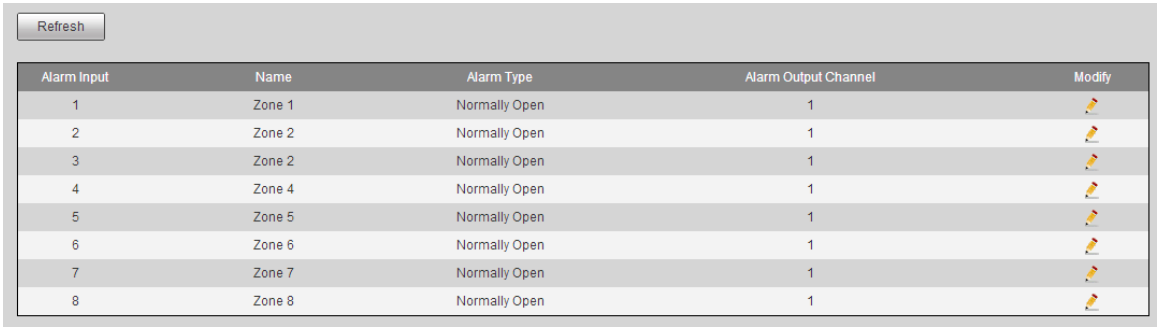
If access main controller connects Smart PSS client, relevant parameters and alarms will be synchronized with the client. Parameters modified in the client will also be synchronized with main controller.

3.6 Set Alarm Linkage

Access main controller supports 8-channel alarm input and output. Set alarm linkage output at this interface.

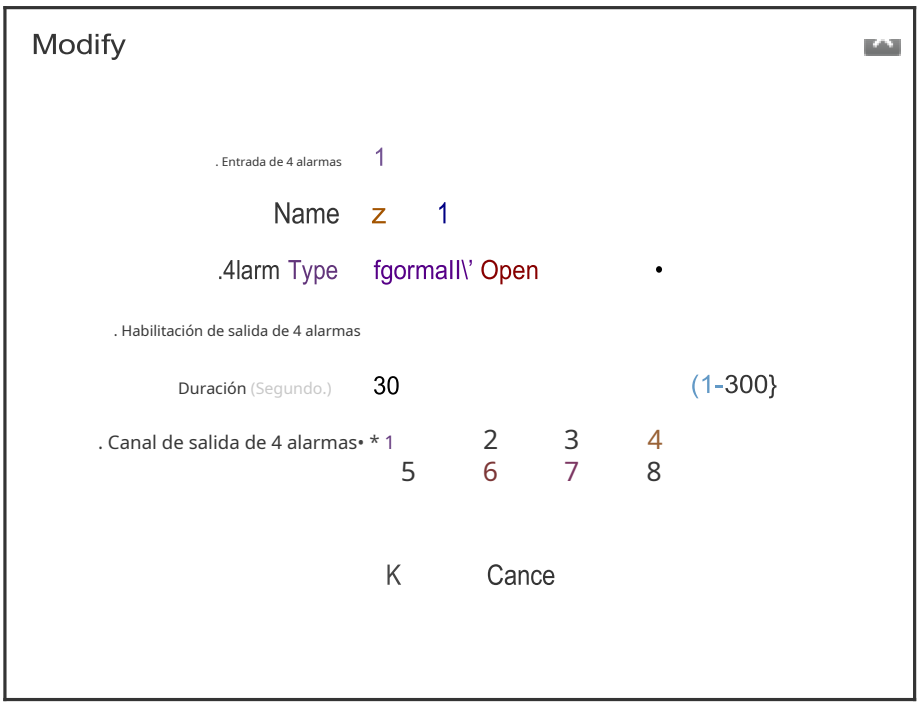
Step 1 Select **Access > Alarm Linkage**.

Figure 3-6 Alarm linkage



Step 2 Click .

Figura 3-7 Modificar la información de la alarma



Paso 3 Configure los parámetros.

Tabla 3-4 Descripción de los parámetros

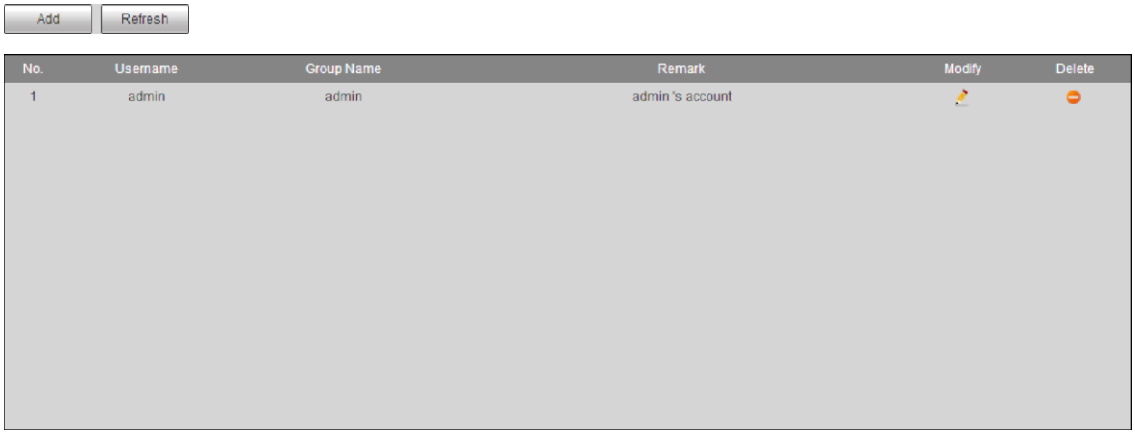
Parámetro	Descripción
Entrada de alarma	Muestra la entrada de alarma actual.
Nombre	Personalice el nombre de la entrada de alarma.
Tipo de alarma	El tipo de alarma es compatible con el terminal.
Habilitar salida de alarma	Marque la casilla de verificación para habilitar la salida de alarma, a fin de cargar la alarma a la plataforma de forma sincrónica.
Duración (seg.)	Duración de la alarma. La alarma desaparecerá después de esta duración.
Canal de salida de alarma	Seleccione el canal de salida de alarma, para que salga el canal designado para alarma.

Paso 4 Haga clic en Aceptar.

3.7 Agregar usuario

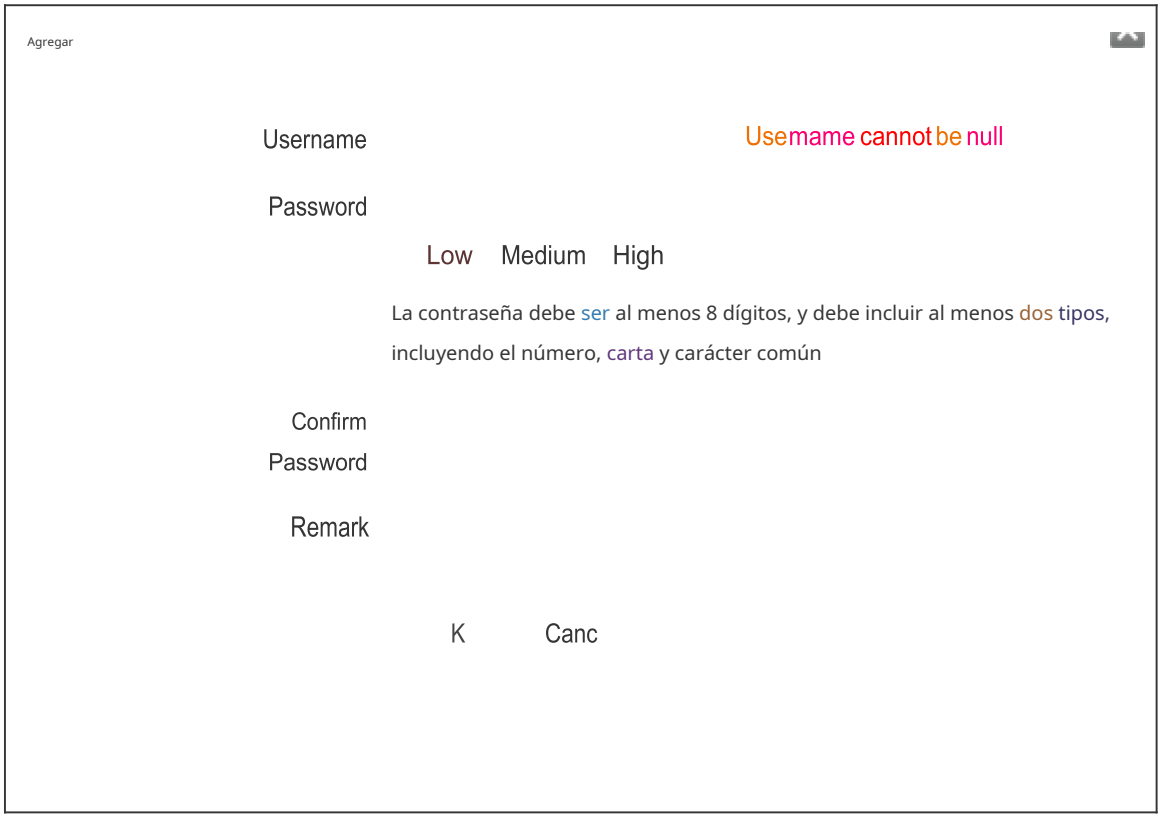
Paso 1 Seleccione Sistema> Gestión de usuarios.

Figura 3-8 Gestión de usuarios



Paso 2 Haga clic en Agregar.

Figura 3-9 Agregar un usuario



Paso 3 Ingrese el nombre de usuario, la contraseña, confirme la contraseña y comente. Paso 4

Haga clic en Aceptar.

4 Configuración de Smart PSS

El controlador de acceso se administra con Smart PSSclient, para realizar el control y la configuración derecha de una puerta y grupos de puertas.

Este capítulo presenta principalmente la configuración rápida. Para operaciones específicas, consulte el Manual del usuario de Smart PSSClient.

El cliente Smart PSS ofrece diferentes interfaces para diferentes versiones. Debe prevalecer la interfaz real.

4.1 Cliente de inicio de sesión

Instale el cliente Smart PSS correspondiente y haga doble clic en la configuración de  correr. Realizar inicialización acuerdo con las indicaciones de la interfaz y complete el inicio de sesión.

4.2 Agregar controlador de acceso

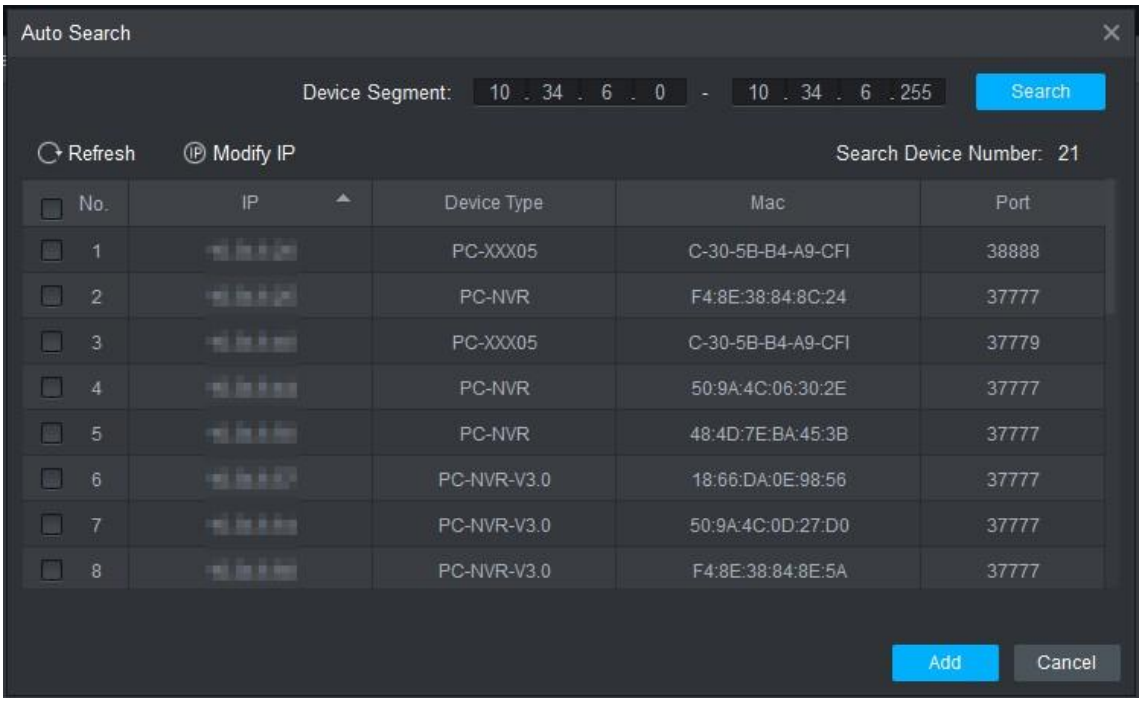
Controlador de Addaccess inSmart PSS; seleccione AutoSearchandAdd.

4.2.1 Búsqueda automática

Los dispositivos deben estar en el mismo segmento de red. Paso 1 En la interfaz de Dispositivos, haga clic en Búsqueda automática.

Figura 4-1 Búsqueda automática

Figure 4-2 Search results



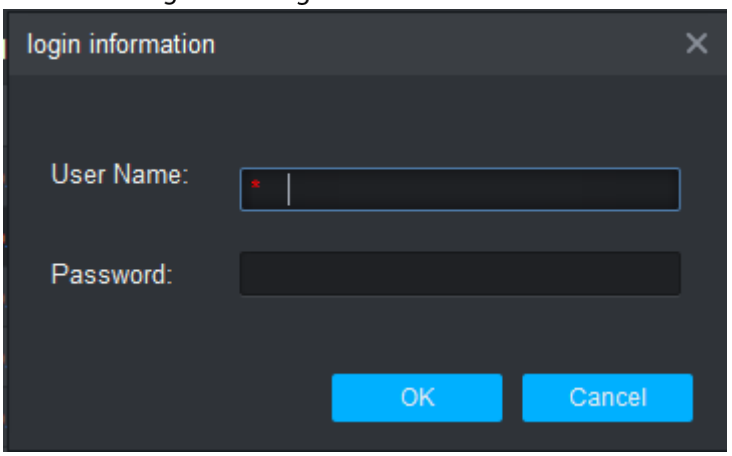
Step 2 Input device segment and click **Search**.

- Click **Refresh** to update device information.
- Select a device, click **Modify IP** to modify IP address of the device. For specific s Manual of Smart PSS Client.

Step 3 Select the device that needs to be added, and click **Add**.

Step 4 Click **OK**.

Figure 4-3 Login information



Step 5 Input user name and password to log in the device, and click **OK**.

- After completing adding, the system continues to stay on the **Auto Search** interface. You can continue to add more devices, or click **Cancel** to exit.
- After completing adding, Smart PSS logs in the device automatically. In case of successful login, online status is **Online**. Otherwise, **Offline** will be displayed.

Figura 4-4 Inicio de sesión

Tabla 4-1 Descripción de los iconos

Icono	Descripción
	Haga clic en este icono para ingresar a la interfaz Modificar dispositivo. La información del dispositivo se puede modificar, incluido el nombre del dispositivo, IP / nombre de dominio, puerto, nombre de usuario y contraseña. Alternativamente, haga doble clic en el dispositivo para ingresar a Modificar dispositivo. interfaz.
	Haga clic en este icono para acceder a la interfaz "Configuración de dispositivo". Configure la cámara del dispositivo, la red, el evento, el almacenamiento y la información del sistema, etc.
and	• Cuando el dispositivo está conectado, aparece el icono. Haga clic en el icono para salir, y el icono cambia a . • Cuando el dispositivo está fuera de línea, aparece el icono. Haga clic en el icono para iniciar sesión en el dispositivo (la información del dispositivo debe ser correcta) y el icono cambios a .
	Haga clic en este icono para eliminar un dispositivo.

4.2.2 Adición manual

Para agregar dispositivos, primero se debe conocer la dirección IP del dispositivo o el nombre de dominio. Paso 1 En la interfaz de Dispositivos, haga clic en Agregar.

Figure 4-5 Manually add a device

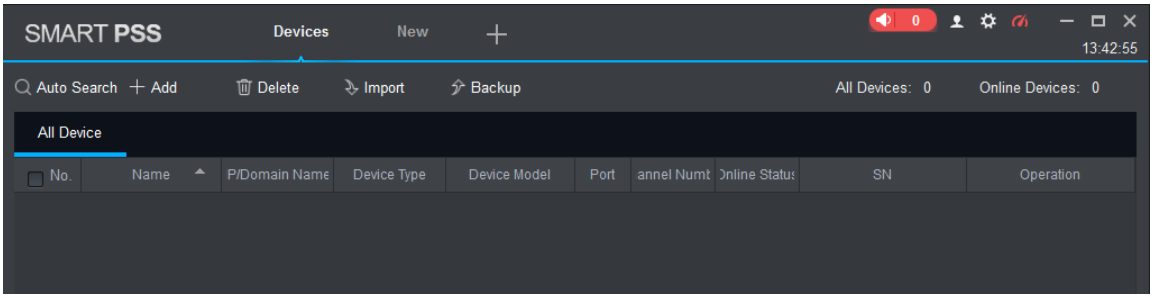
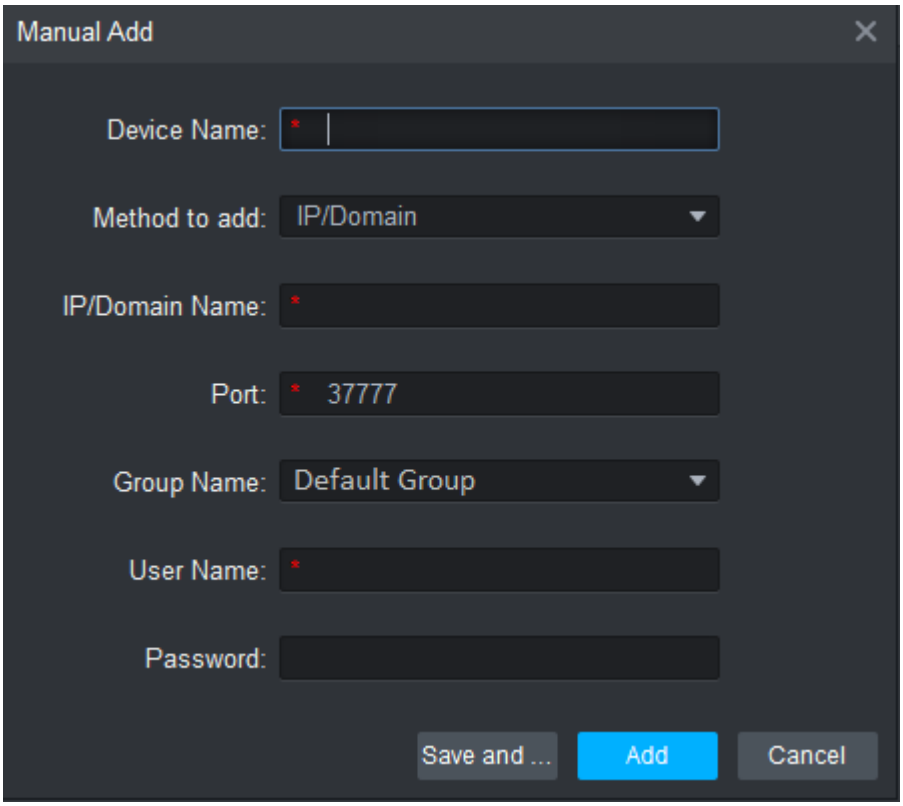


Figure 4-1 Enter information



Step 2 Set device parameters.

Table 4-2 Parameter description

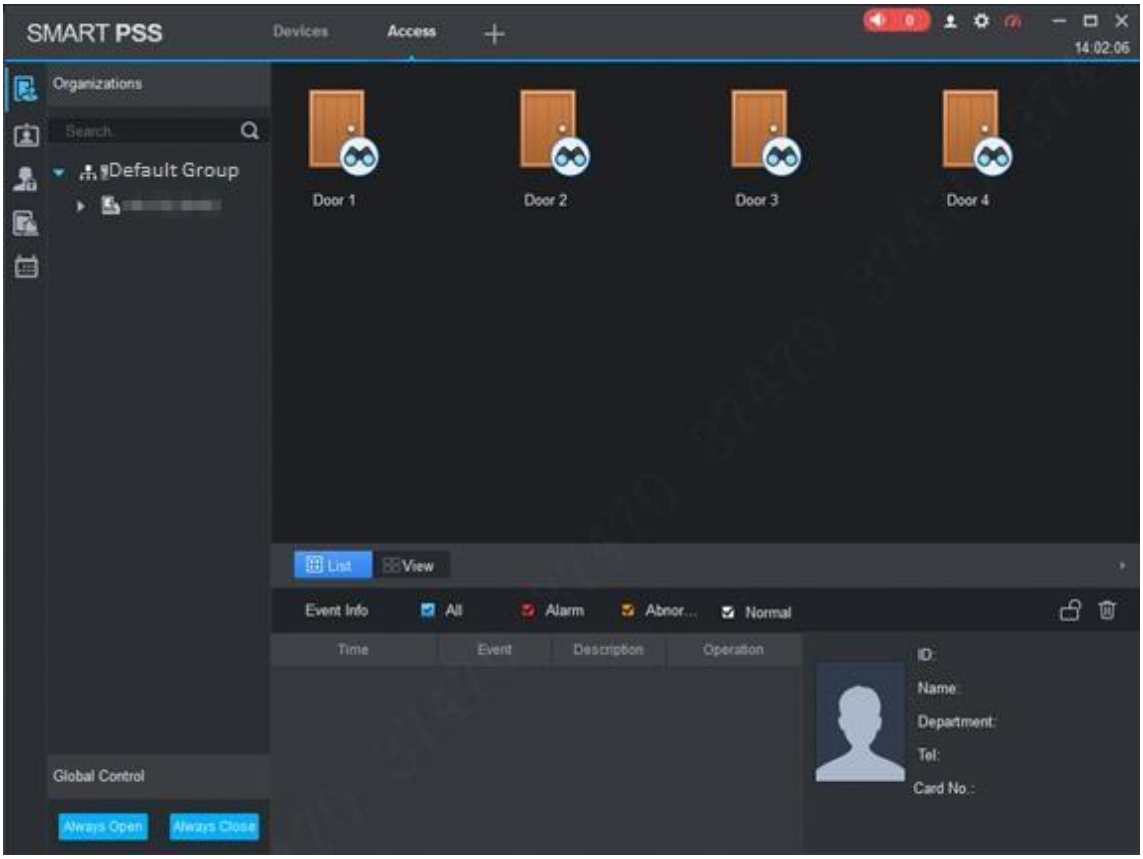
Parameter	Description
Device Name	It is suggested that device name should be named by the monitoring zone, so as to facilitate maintenance.
Method to add	Select **IP/Domain Name**. Add devices according to device IP address or domain name.
IP/Domain Name	IP address or domain name of the device.
Port	Port number of the device. Default port number is 37777. Please fill in according to actual conditions.
Group Name	Select the group of the device.
User Name and Password	User name and password of the device.

Step 3 Click **Add** to add a device.

- To add more devices, click **Save and Continue** to add devices.

- To cancel the adding, click **Cancel** to exit **Manual Add** interface.
- After completing adding, Smart PSS logs in to the device automatically. In case of successful login, online status is **Online**. Otherwise, **Offline** will be displayed.

Figure 4-6 Automatically log in to the device



Apéndice 1 Lista de empaque

Apéndice Tabla 1-1 Lista de empaque

No.	Name	Quantity
1	Controlador de acceso	1
2	Cable de suministro de energía	1
3	Cable de batería de almacenamiento	1
4	Llave	1
5	Kit de accesorios (tornillo, tubo de expansión y terminal de cableado)	1
6	Guía de inicio rápido	1
7	Certificado de Cualificación	1

Apéndice 2 Recomendaciones de ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que pertenece a todos los dispositivos que están conectados a Internet. La videovigilancia IP no es inmune a los riesgos cibernéticos, pero tomar medidas básicas para proteger y fortalecer las redes y los dispositivos en red los hará menos susceptibles a los ataques. A continuación, se muestran algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias que se deben tomar para la seguridad básica de la red del dispositivo: 1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de personajes; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;
- No incluya el nombre de la cuenta o el nombre de la cuenta en orden inverso;
- No utilice caracteres continuos, como 123, abc, etc .;
- No utilice caracteres superpuestos, como 111, aaa, etc .;

2. Actualice el firmware y el software cliente inTime

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su dispositivo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. para habilitar la función de "verificación automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware publicadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software cliente.

Recomendaciones "Es bueno tener" para mejorar la seguridad de la red de su dispositivo: 1. Protección física

Le sugerimos que realice una protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras especial y gabinete, e implemente permisos de control de acceso bien hechos y administración de claves para evitar que el personal no autorizado lleve a cabo contactos físicos como daños en el hardware, conexión no autorizada de dispositivos extraíbles (como un disco flash USB). , puerto serie), etc.

2. Cambie las contraseñas con regularidad

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de ser adivinado o descifrado.

3. Establecer y actualizar la información de restablecimiento de contraseñas oportunamente

El dispositivo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluido el buzón del usuario final y las preguntas sobre protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar las preguntas de protección por contraseña, se sugiere no utilizar aquellas que se puedan adivinar fácilmente.

4. Habilite el bloqueo de cuenta

La función de bloqueo de cuenta está habilitada de forma predeterminada y le recomendamos que la mantenga activada para garantizar la seguridad de la cuenta. Si un atacante intenta iniciar sesión con la contraseña incorrecta varias veces, la cuenta correspondiente y la dirección IP de origen se bloquearán.

5. Cambiar HTTP predeterminado y otros puertos de servicio

Le sugerimos que cambie el HTTP predeterminado y otros puertos de servicio en cualquier conjunto de números entre 1024-65535, reduciendo el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.

6. Habilite HTTPS

Le sugerimos que habilite HTTPS, para que visite el servicio web a través de un canal de comunicación seguro.

7. Enlace de dirección MAC

Le recomendamos que vincule la dirección IP y MAC de la puerta de enlace al dispositivo, reduciendo así el riesgo de falsificación de ARP.

8. Asignar cuentas y privilegios de forma razonable

De acuerdo con los requisitos comerciales y de administración, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

9. Deshabilite los servicios innecesarios y elija modos seguros

Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir los riesgos.

Si es necesario, se recomienda encarecidamente que utilice modos seguros, incluidos, entre otros, los siguientes servicios:

- SNMP: elija SNMP v3 y configure contraseñas de cifrado y contraseñas de autenticación seguras.
- SMTP: elija TLS para acceder al servidor de buzones de correo.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

10.Transmisión encriptada de audio y video

Si su contenido de datos de audio y video es muy importante o sensible, le recomendamos que utilice la función de transmisión encriptada, para reducir el riesgo de robo de datos de audio y video durante la transmisión.

Recordatorio: la transmisión cifrada provocará una pérdida en la eficiencia de la transmisión.

1 1. Auditoría segura

- Verificar usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo está conectado sin autorización.
- Verificar el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se utilizaron para iniciar sesión en sus dispositivos y sus operaciones clave.

12. Registro de red

Debido a la capacidad de almacenamiento limitada del dispositivo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, se recomienda que habilite la función de registro de red para asegurarse de que los registros críticos estén sincronizados con el servidor de registro de red para su seguimiento.

13. Construya un entorno de red seguro

Para garantizar mejor la seguridad del dispositivo y reducir los posibles riesgos cibernéticos, recomendamos:

- Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde una red externa.
- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere utilizar VLAN, red GAP y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP / MAC para limitar el rango de hosts permitidos para acceder al dispositivo.