Controlador de acceso (C)

Manual de usuario

V1.0.0

Prefacio

General

Este manual presenta la estructura, las funciones y las operaciones del controlador de acceso (en lo sucesivo, "el Controlador").

Las instrucciones de seguridad

Las siguientes palabras de advertencia categorizadas con un significado definido pueden aparecer en el manual.

Palabras de advertencia	Significado
PELIGRO	Indica un peligro de alto potencial que, si no se evita, provocará la muerte o lesiones graves.
ADVERTENCIA	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, reducción del rendimiento o resultados impredecibles.
CONSEJOS	Proporciona métodos para ayudarlo a resolver un problema o ahorrar tiempo.
NOTA	Proporciona información adicional como suplemento al texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.1	Añadido proceso de inicialización.	diciembre 2021
V1.0.0	Primer lanzamiento.	marzo 2021

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otros, como su rostro, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: Proporcionar una identificación clara y visible para informar a las personas sobre la existencia del área de vigilancia y proporcione la información de contacto requerida.

Sobre el Manual

- El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre el manual y el producto.

- No somos responsables de las pérdidas sufridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y reglamentos de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, use nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede haber errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio al cliente si ocurre algún problema al usar el controlador.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del Controlador, la prevención de riesgos, y prevención de daños a la propiedad. Lea atentamente antes de usar el Controlador, cumpla con las pautas al usarlo, y mantenga el manual seguro para referencia futura.

Requisito de transporte

Transporte el controlador en condiciones de humedad y temperatura permitidas.

Requisito de almacenamiento

Almacene el controlador en condiciones de humedad y temperatura permitidas.

requerimientos de instalación

- No conecte el adaptador de corriente al controlador mientras el adaptador esté encendido.
- Cumpla estrictamente con el código y las normas locales de seguridad eléctrica. Asegúrese de que el voltaje ambiental sea estable y cumple con los requisitos de suministro de energía del controlador.
- No conecte el controlador a dos o más tipos de fuentes de alimentación para evitar daños en el Controlador.
- El uso inadecuado de la batería puede provocar un incendio o una explosión.

- El personal que trabaje en alturas debe tomar todas las medidas necesarias para garantizar su seguridad personal, incluidas usando casco y cinturones de seguridad.
- No coloque el controlador en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el controlador alejado de la humedad, el polvo y el hollín.
- Instale el controlador en una superficie estable para evitar que se caiga.
- Instale el controlador en un lugar bien ventilado y no bloquee su ventilación.
- Utilice un adaptador o una fuente de alimentación de gabinete proporcionada por el fabricante.
- Utilice los cables de alimentación recomendados para la región y cumpla con la potencia nominal especificaciones.

- La fuente de alimentación debe cumplir con los requisitos de ES1 en la norma IEC 62368-1 y no ser más alto que PS2. Tenga en cuenta que los requisitos de la fuente de alimentación están sujetos a la etiqueta del controlador.
- El Controlador es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del controlador esté conectado a una toma de corriente con puesta a tierra de protección.

Tabla de contenido

1.1 Introducción

El Controller es un panel de control de accesos que compensa la videovigilancia y la intercomunicación visual. Tiene un diseño limpio y moderno con una gran funcionalidad, adecuado para edificios comerciales de alta gama, propiedades grupales y comunidades inteligentes.

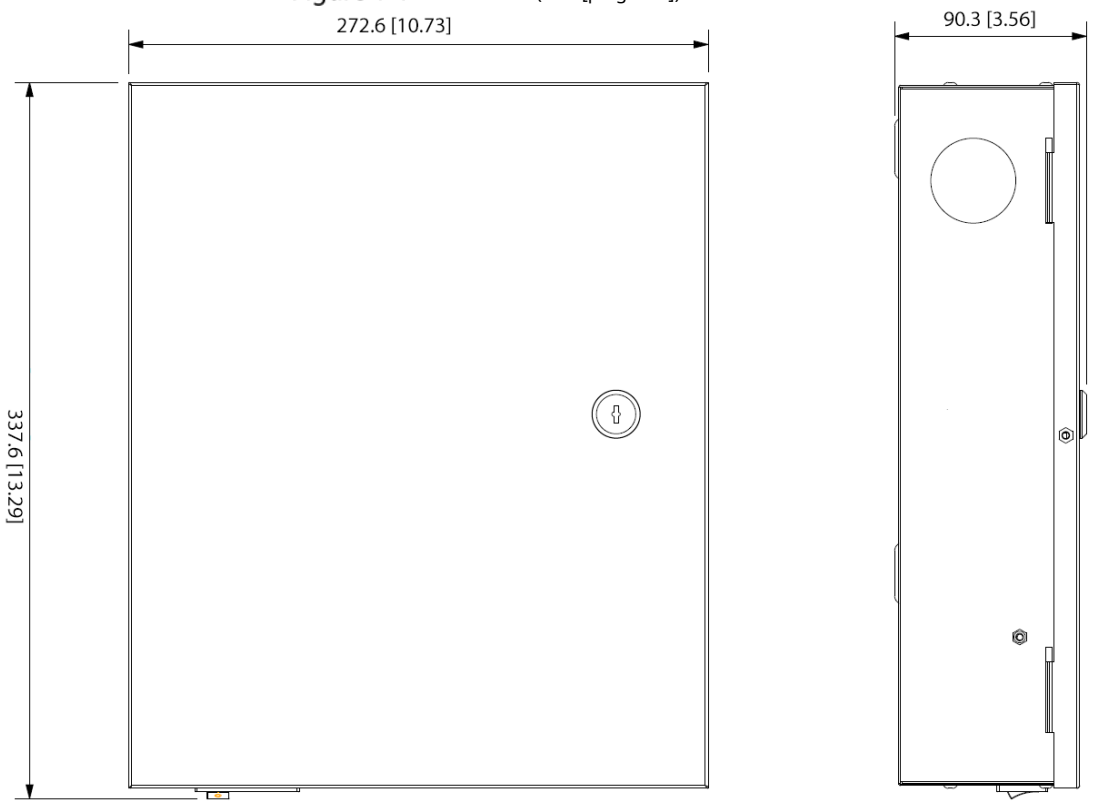
1.1 Características

- Adopta una placa de acero SEEC para brindar una apariencia de alta gama.
- Soporta comunicación de red TCP/IP. Los datos de comunicación están encriptados por seguridad.
- Registro automático.
- Admite el protocolo OSDP.
- Admite desbloqueo de tarjeta, contraseña y huella digital.
- Admite 100 000 usuarios, 100 000 tarjetas, 3000 huellas dactilares y 500 000 registros.
- Admite enclavamiento, anti-passback, desbloqueo multiusuario, desbloqueo de la primera tarjeta, desbloqueo de contraseña de administrador, desbloqueo remoto y más.
- Admite alarma de manipulación, alarma de intrusión, alarma de tiempo de espera del sensor de puerta, alarma de coacción, alarma de lista de bloqueo, alarma de límite de superación de tarjeta no válida, alarma de contraseña incorrecta y alarma externa.
- Admite tipos de usuarios como usuarios generales, usuarios VIP, usuarios invitados, usuarios de listas de bloqueo, usuarios de patrulla y otros usuarios.
- Admite RTC integrado, calibración de hora NTP, calibración de hora manual y funciones de calibración de hora automática.
- Admite la operación fuera de línea, el almacenamiento de registros de eventos y las funciones de carga, y la reposición automática de red (ANR).
- Admite 128 períodos, 128 planes de vacaciones, 128 períodos de vacaciones, períodos normalmente abiertos, períodos normalmente cerrados, períodos de desbloqueo remoto, períodos de desbloqueo de la primera tarjeta y períodos de desbloqueo.
- Admite mecanismo de vigilancia para garantizar la estabilidad de la operación.

1.2 Dimensiones

Hay cinco tipos de controladores de acceso, que incluyen dos puertas unidireccionales, dos puertas bidireccionales, cuatro puertas unidireccionales, cuatro puertas bidireccionales y ocho puertas unidireccionales. Sus dimensiones son las mismas.

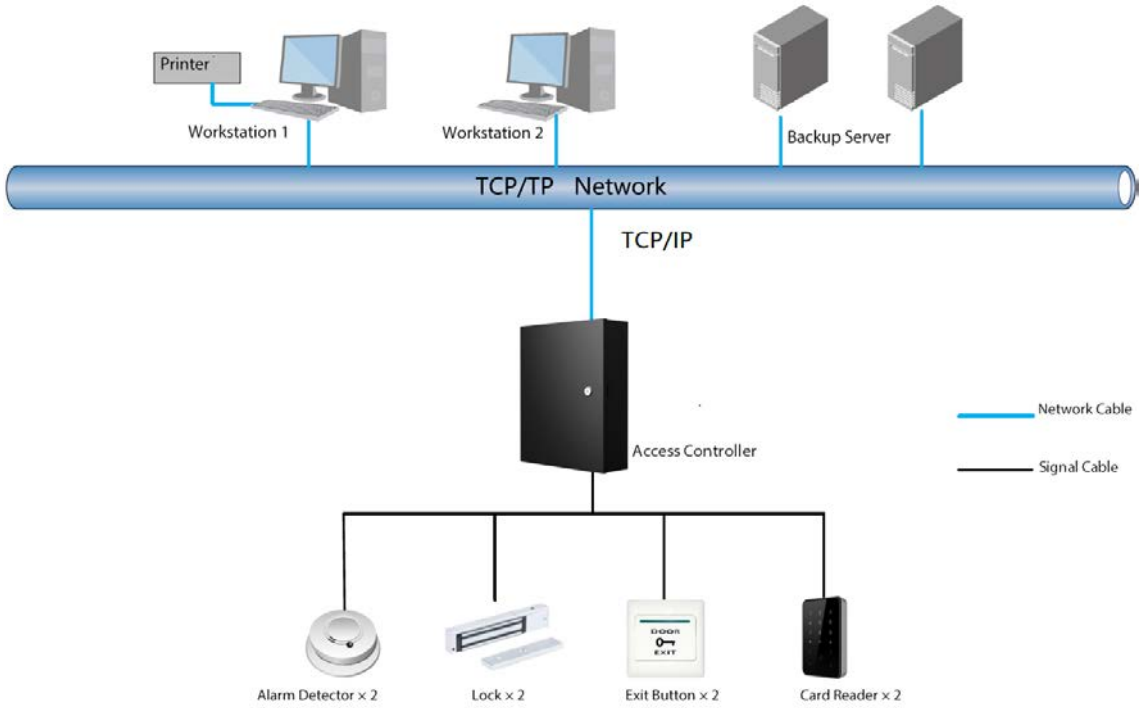
Figure 1-1 Dimensiones (mm [pulgadas])



1.3 Solicitud

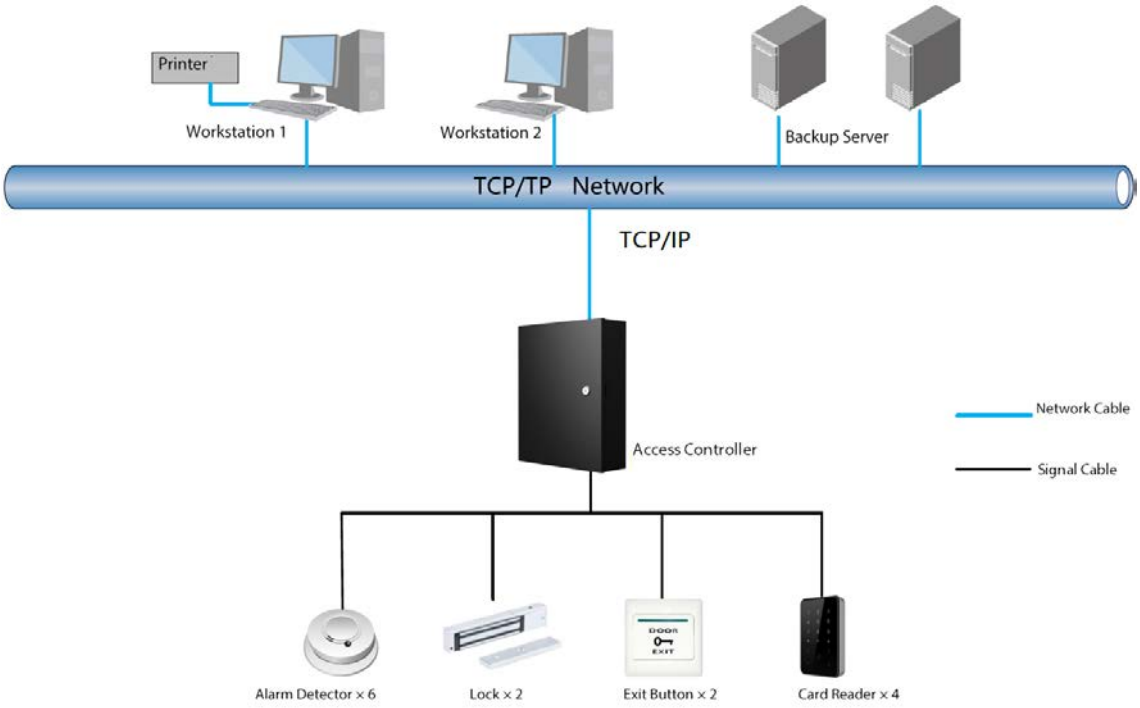
1.3.1 Dos puertas Unidireccional

Figure 1-2 Aplicación del controlador unidireccional de dos puertas



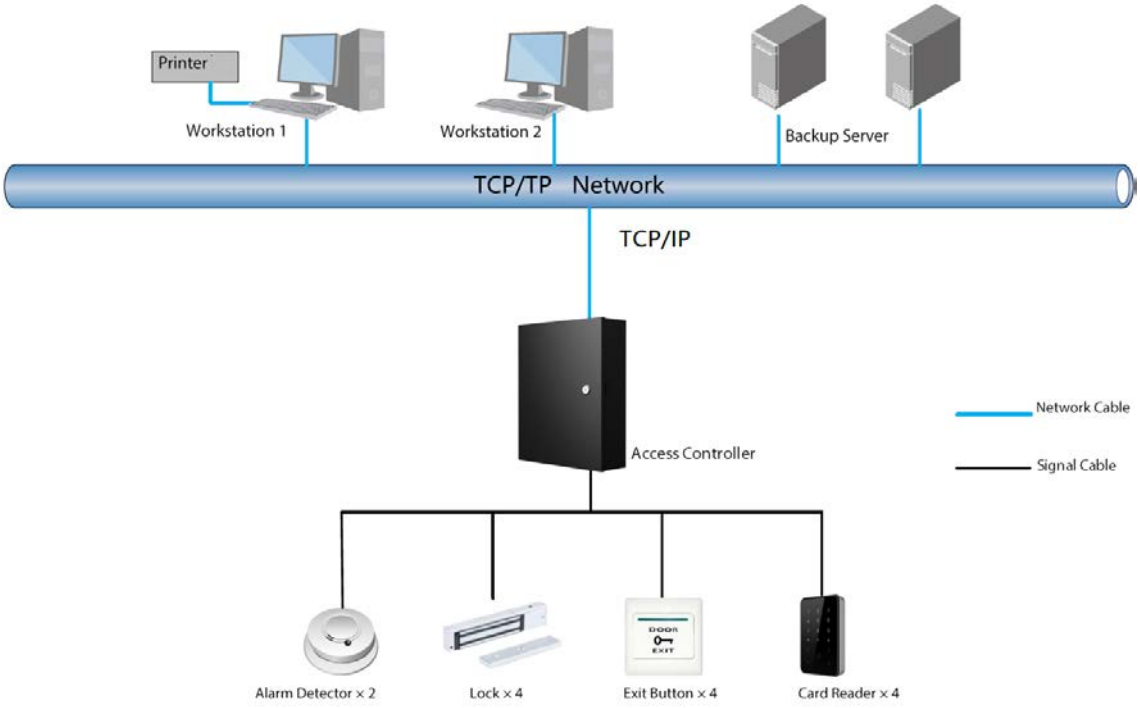
1.3.2 Dos puertas Dos vías

Figure 1-3 Aplicación del controlador bidireccional de dos puertas.



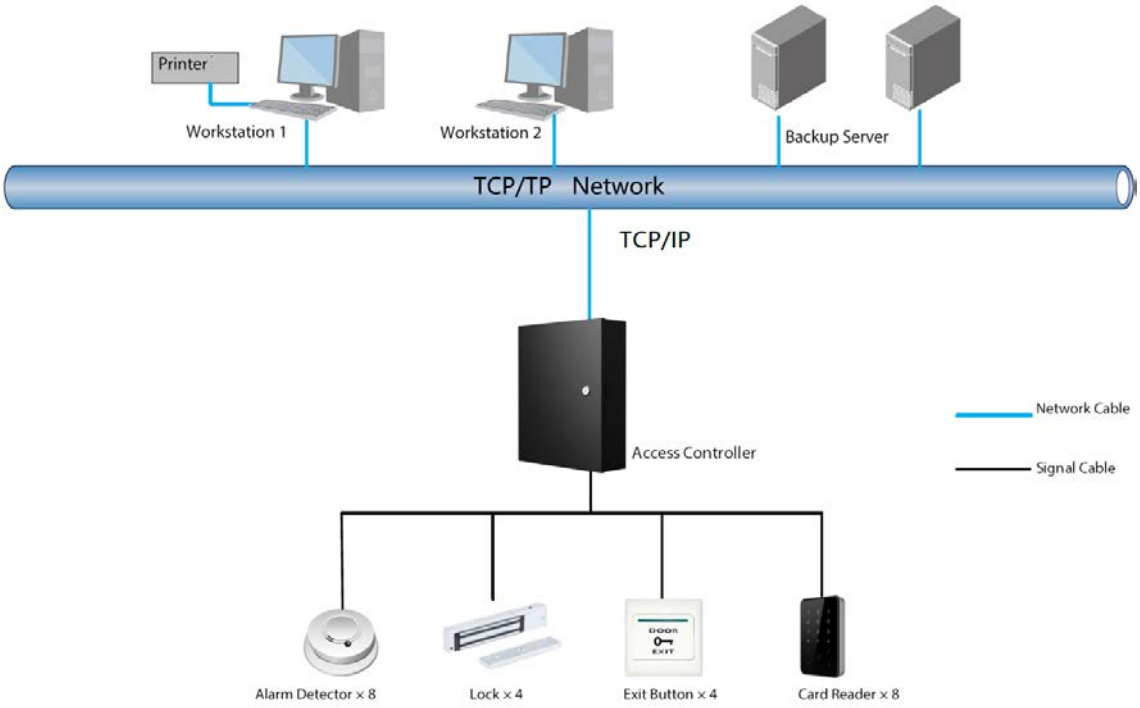
1.3.3 Unidireccional de cuatro puertas

Figure 1-4 Aplicación del controlador unidireccional de cuatro puertas



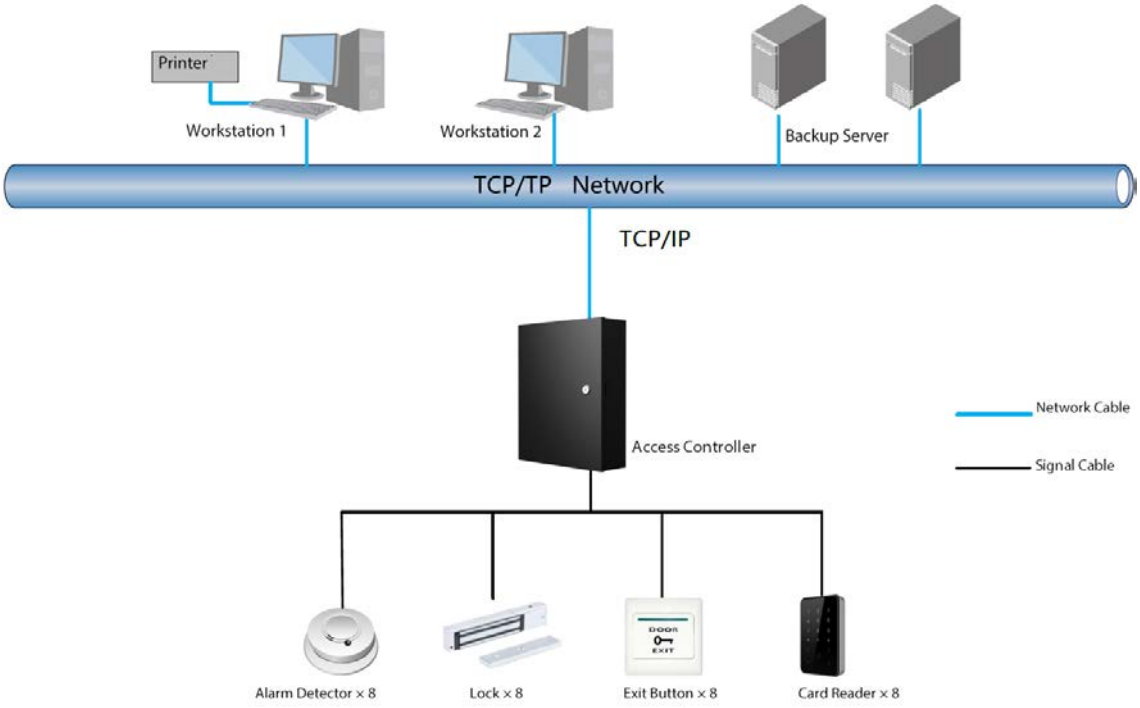
1.3.4 Cuatro puertas Bidireccional

Figure 1-5 Aplicación del controlador bidireccional de cuatro puertas.



1.3.5 Ocho puertas unidireccional

Figure 1-6 Aplicación del controlador unidireccional de ocho puertas



2 Estructura

2.1 Alambrado

⚠

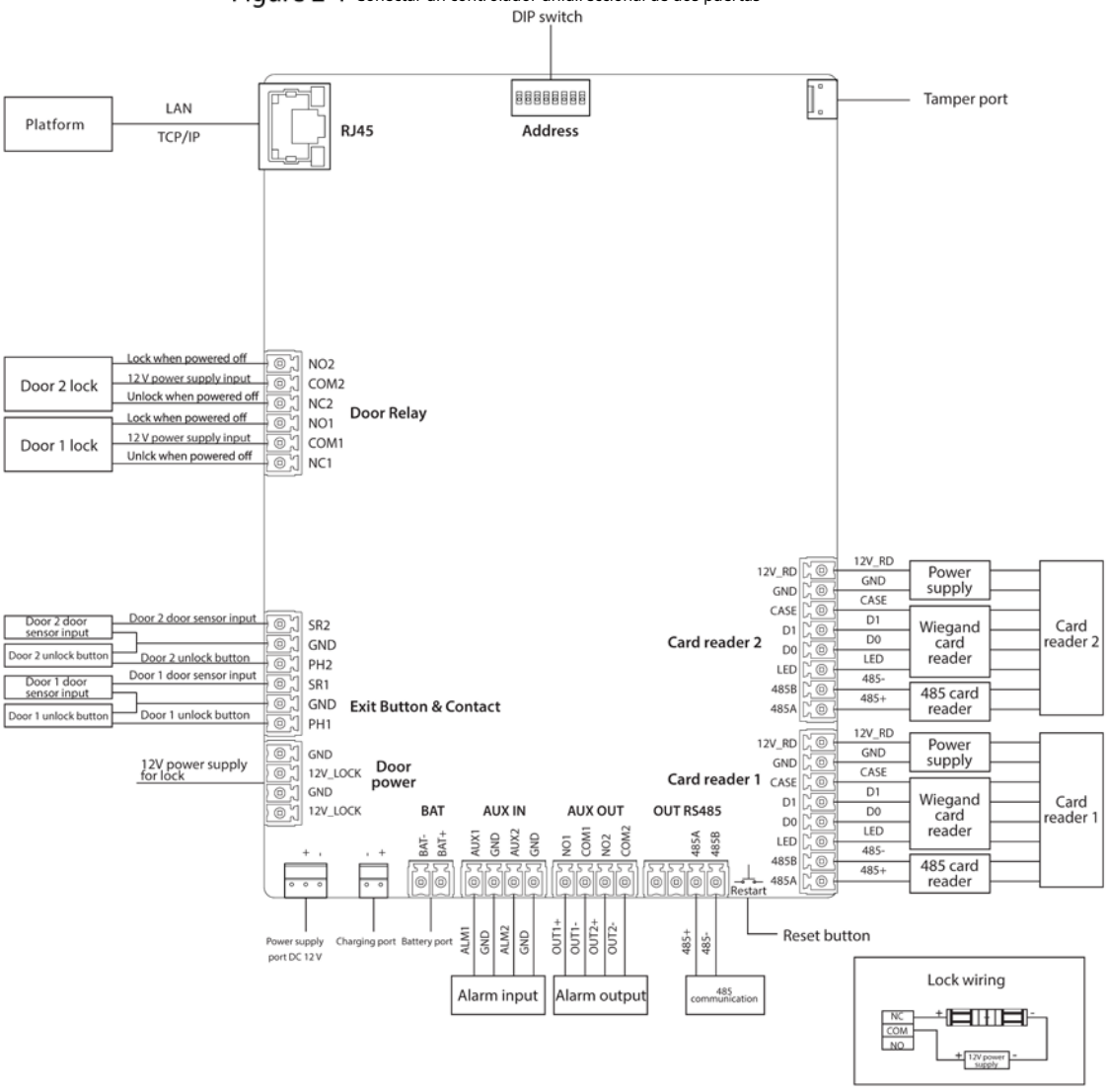
- Conecte los cables solo cuando esté apagado.
- Asegúrese de que el enchufe de la fuente de alimentación esté conectado a tierra.
- 12 V: la corriente máxima para un módulo de extensión es de 100 mA. 12 V_RD: La
- corriente máxima para un lector de tarjetas es de 2,5 A.
- 12 V_LOCK: La corriente máxima para una cerradura es de 2 A.

Tabla 2-1 Especificación de cables

Dispositivo	Cable	Área transversal de cada núcleo	Observaciones
Lector de tarjetas	Cat5 de 8 núcleos blindado par trenzado	≥ 0,22 mm²	Sugerido ≤ 100 m
Cable de ethernet	Cat5 de 8 núcleos blindado par trenzado	≥ 0,22 mm²	Sugerido ≤ 100 m
Botón	2 núcleos	≥ 0,22 mm²	–
Contacto de puerta	2 núcleos	≥ 0,22 mm²	–

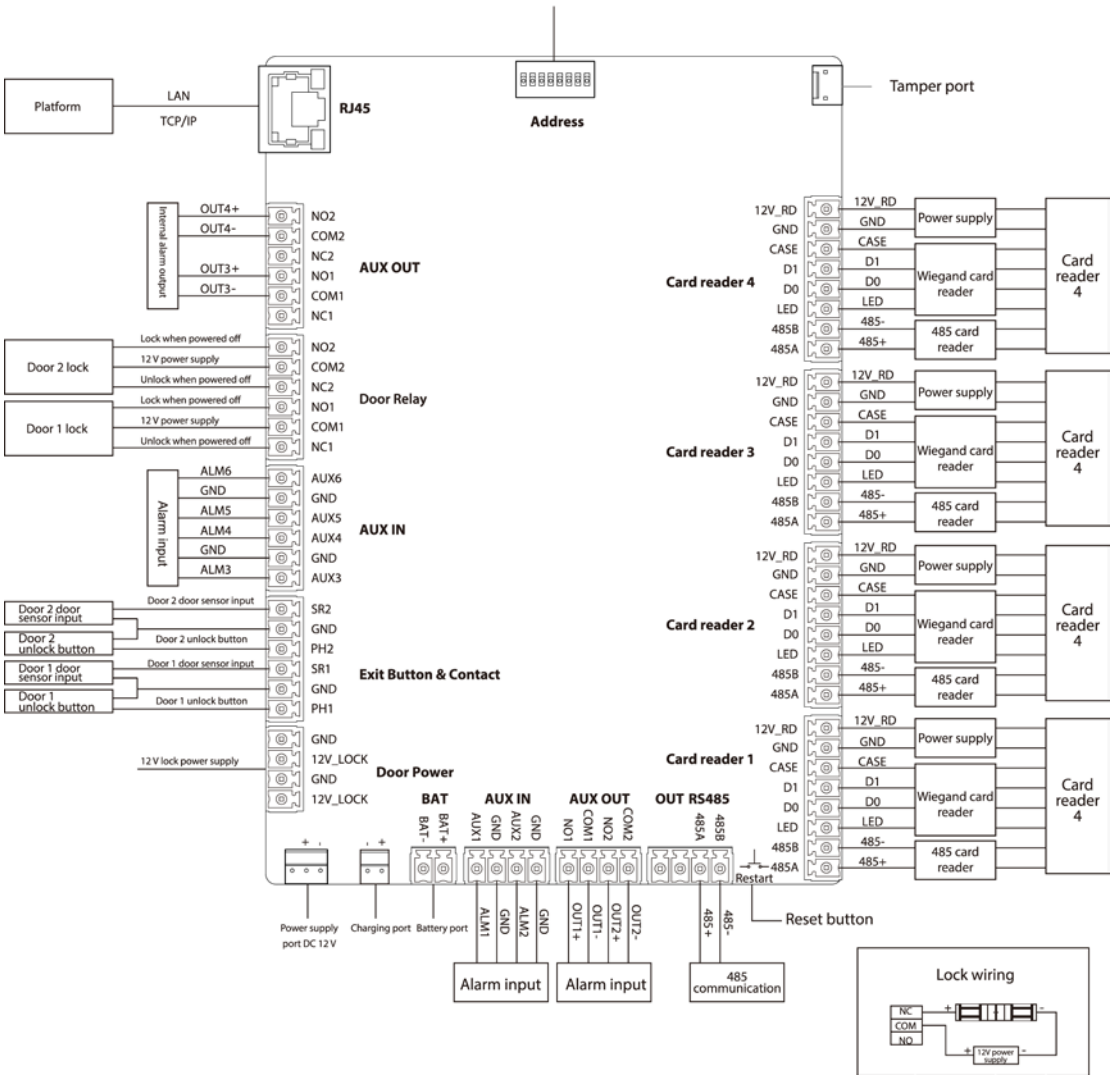
2.1.1 Dos puertas Unidireccional

Figure 2-1 Conectar un controlador unidireccional de dos puertas



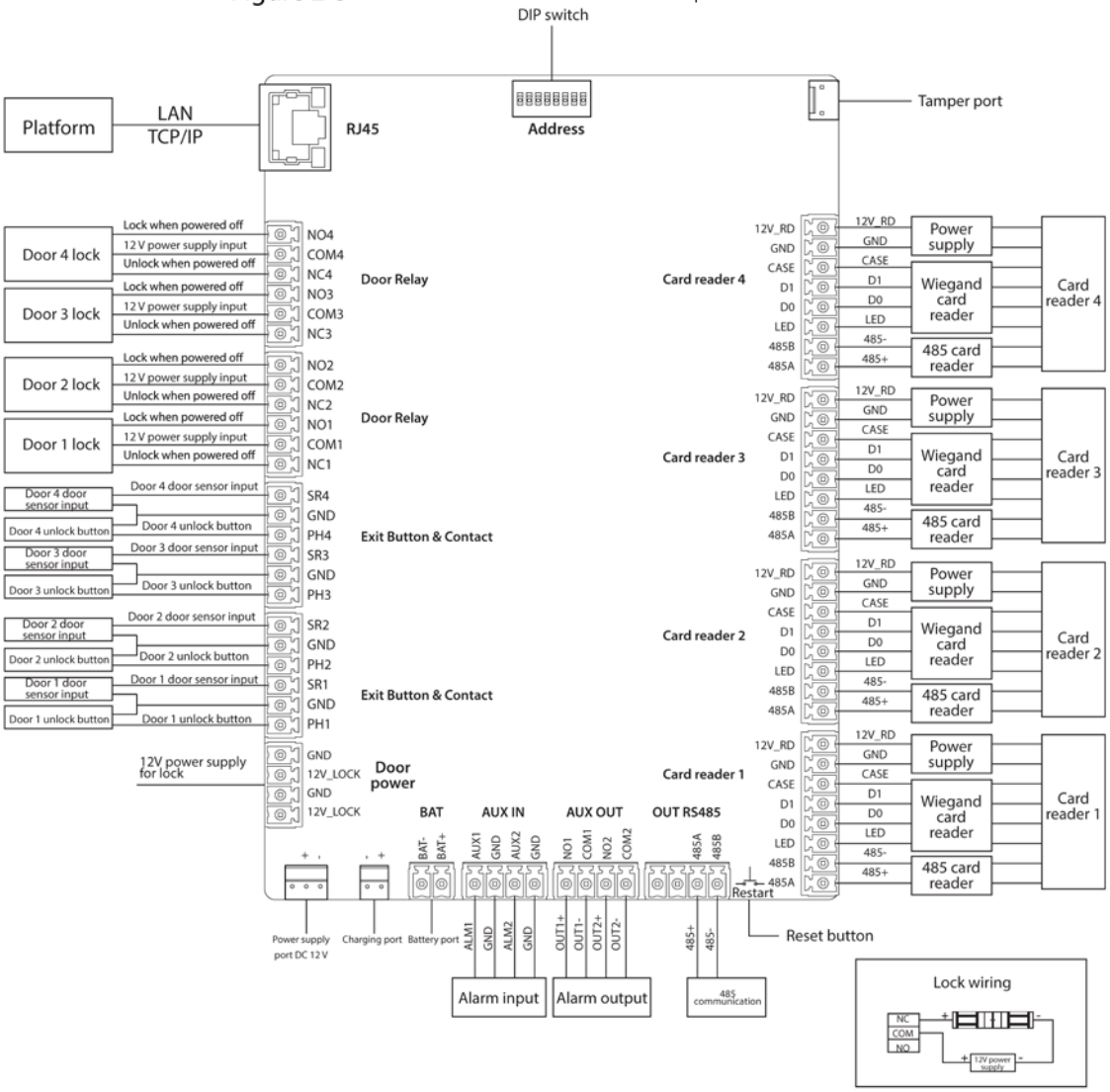
2.1.2 Dos puertas Dos vías

Figure 2-2 Conectar un controlador bidireccional de dos puertas



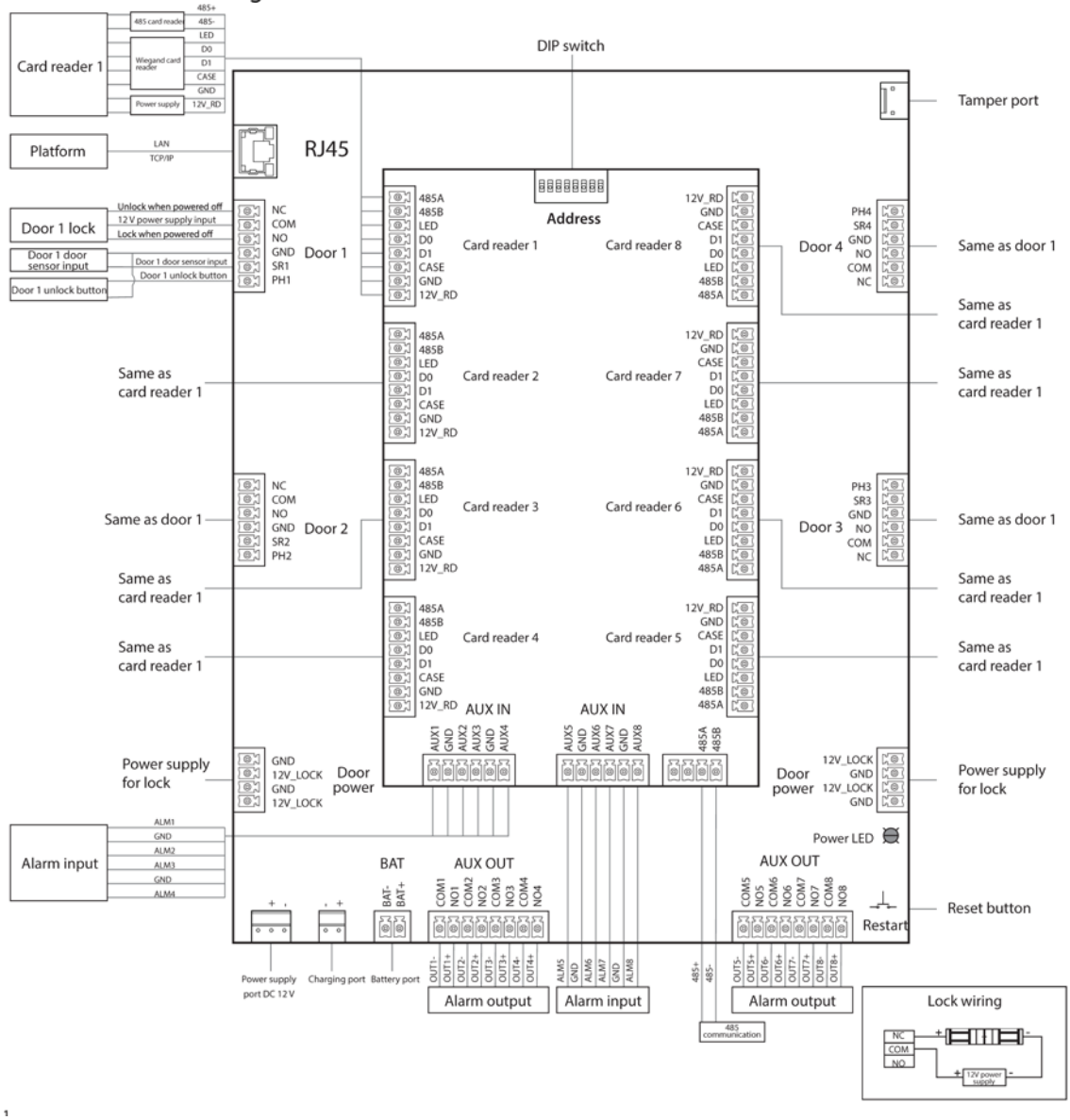
2.1.3 Unidireccional de cuatro puertas

Figure 2-3 Conectar un controlador unidireccional de cuatro puertas



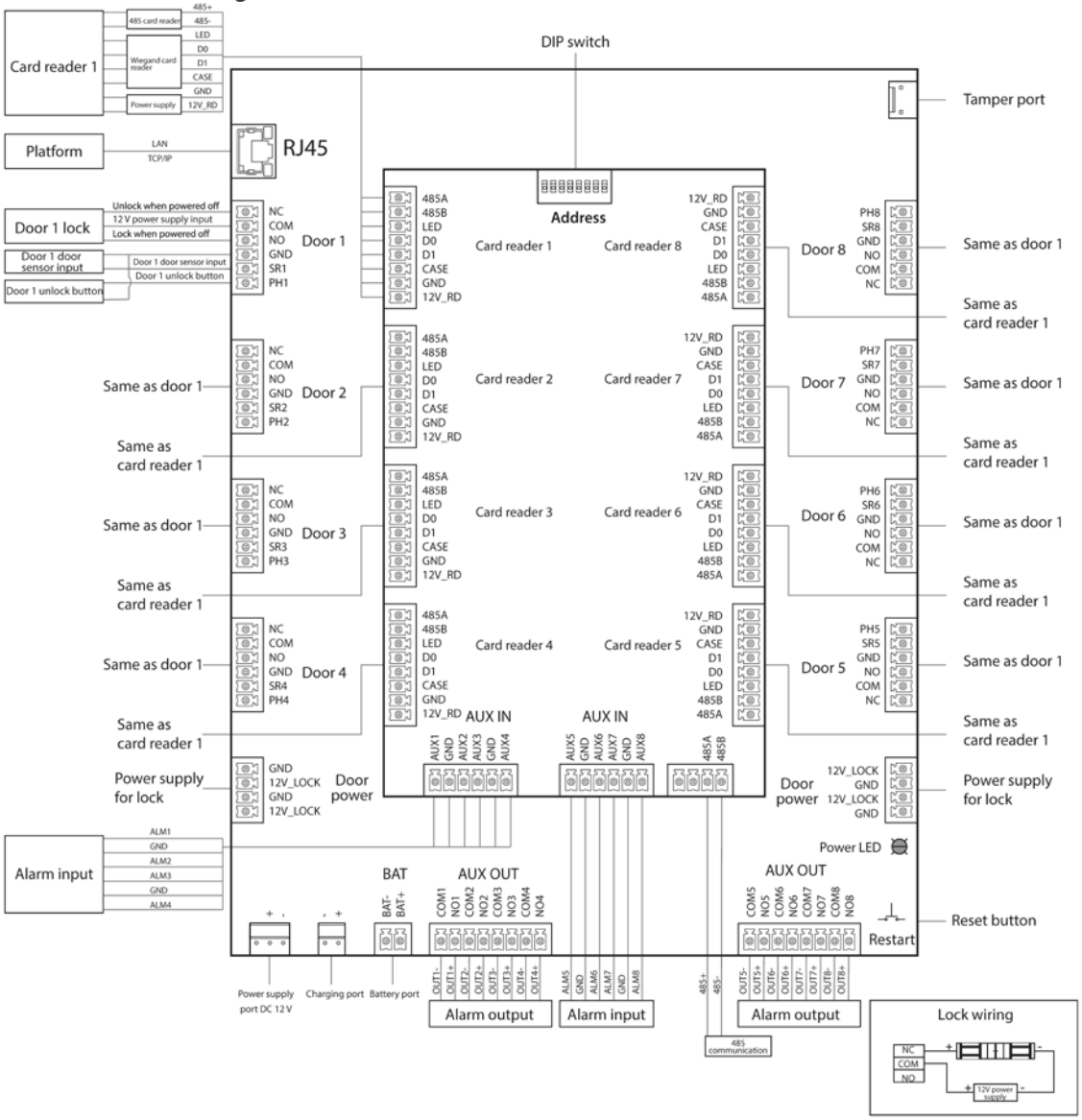
2.1.4 Dos vías de cuatro puertas

Figure 2-4 Conectar un controlador bidireccional de cuatro puertas



2.1.5 Unidireccional de ocho puertas

Figure 2-5 Conectar un controlador unidireccional de ocho puertas



2.1.6 Bloqueo

Seleccione el método de cableado de acuerdo con su tipo de cerradura.

Figure 2-6 cerradura electrica

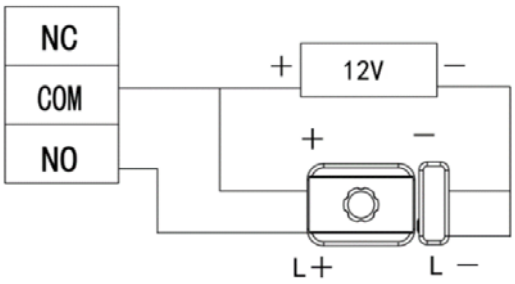


Figure 2-7 Cerradura magnética

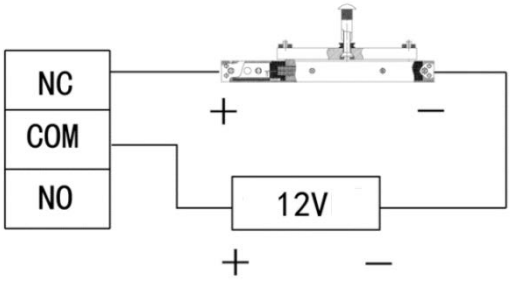
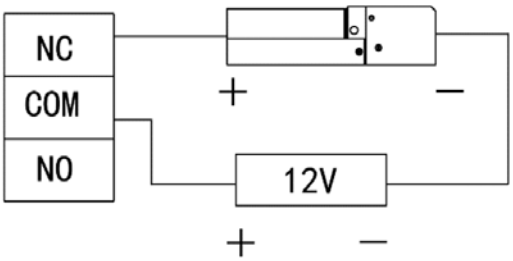


Figure 2-8 Perno eléctrico



2.1.7 Entrada de alarma

El puerto de entrada de alarma se conecta a dispositivos de alarma externos, como detectores de humo y detectores de infrarrojos. Algunas alarmas en los puertos pueden vincular el estado de apertura/cierre de la puerta.

Tabla 2-2 Cableado de entrada de alarma

Tipo	Número de Entrada de alarma Canales	Descripción
Dos puertas De una sola mano	2	Estado de la puerta enlazable: ● Enlaces de alarma externa AUX1 normalmente abiertos para todas las puertas. ● Enlaces de alarma externa AUX2 normalmente cerrados para todas las puertas.
Dos puertas bidireccional	6	Estado de la puerta enlazable: ● Enlaces de alarma externa AUX1–AUX2 Normalmente abierto para todas las puertas. ● Enlaces de alarma externa AUX3–A UX4 normalmente cerrados para todas las puertas.
cuatro puertas De una sola mano	2	Estado de la puerta enlazable: ● Enlaces de alarma externa AUX1 normalmente abiertos para todas las puertas. ● Enlaces de alarma externa AUX2 normalmente cerrados para todas las puertas.
cuatro puertas bidireccional	8	Estado de la puerta enlazable: ● AUX1–AUX2 alarma externa l tintas normalmente abiertas para todas las puertas. ● Enlaces de alarma externa AUX3–A UX4 normalmente cerrados para todas las puertas.
ocho puertas De una sola mano	8	Estado de la puerta enlazable: ● Enlaces de alarma externa AUX1–AUX2 normalmente abiertos para todas las puertas ● Enlaces de alarma externa AUX3–A UX4 normalmente cerrados para todas las puertas.

2.1.8 Salida de alarma

Cuando se activa una alarma desde el puerto de entrada de alarma interno o externo, el dispositivo de salida de alarma informará la alarma y la alarma durará 15 s.

Al cablear el dispositivo de doble puerta bidireccional al dispositivo de salida de alarma interna, seleccione NC/NO según el estado Siempre abierto o Siempre cerrado.

- NC: Normalmente Cerrado.
- NO: Normalmente Abierto.

Tabla 2-3 Cableado de salida de alarma

Tipo	Número de Salida de alarma Canales	Descripción	
Dos puertas De una sola mano	2	NO1	● AUX1 activa la salida de alarma. ● Tiempo límite de puerta y salida de alarma de intrusión para la puerta 1. ● Lector de tarjetas 1 salida de alarma antisabotaje.
		COM1	
		NO2	● AUX2 activa la salida de alarma. ● Tiempo límite de puerta y salida de alarma de intrusión para la puerta 2. ● Lector de tarjetas 2 salida de alarma antisabotaje.
		COM2	
Dos puertas bidireccional	2	NO1	AUX1/AUX2 activa la salida de alarma.
		COM1	
		NO2	AUX3/AUX4 activa la salida de alarma.
		COM2	
	2	NC1	● Lector de tarjetas 1/2 salida de alarma antisabotaje. Tiempo de ● espera de la puerta 1 y salida de alarma de intrusión.
		COM1	
		NO1	
		NC2	● Lector de tarjetas 3/4 salida de alarma antisabotaje. Tiempo de ● espera de la puerta 2 y salida de alarma de intrusión.
		COM2	
		NO2	
cuatro puertas De una sola mano	2	NO1	● AUX1 activa la salida de alarma. ● Tiempo límite de puerta y salida de alarma de intrusión. Salida de ● alarma de manipulación del lector de tarjetas.
		COM1	
		NO2	AUX2 activa la salida de alarma.
		COM2	
cuatro puertas bidireccional	8	NO1	● AUX1 activa la salida de alarma. ● Lector de tarjetas 1/2 salida de alarma antisabotaje. Tiempo de ● espera de la puerta 1 y salida de alarma de intrusión. Salida de ● alarma de manipulación del dispositivo.
		COM1	
		NO2	● AUX2 activa la salida de alarma. ● Lector de tarjetas 1/2 salida de alarma antisabotaje. Tiempo de ● espera de la puerta 2 y salida de alarma de intrusión.
		COM2	
		NUMERO 3	● AUX3 activa la salida de alarma. ● Lector de tarjetas 5/6 salida de alarma antisabotaje. Tiempo de ● espera de la puerta 3 y salida de alarma de intrusión.
		COM3	
		NO. 4	● AUX4 activa la salida de alarma. ● Salida de alarma antisabotaje del lector de tarjetas 7/8. Tiempo de ● espera de la puerta 4 y salida de alarma de intrusión.
		COM4	
		NUMERO 5	AUX5 activa la salida de alarma.
		COM5	
		NO6	AUX6 activa la salida de alarma.
		COM6	
		NO7	AUX7 activa la salida de alarma.
		COM7	
		NO8	AUX8 activa la salida de alarma.
		COM8	

Tipo	Número de Salida de alarma Canales	Descripción	
ocho puertas De una sola mano	8	NO1 COM1	● AUX1 activa la salida de alarma. Lector de tarjetas 1 salida de alarma antisabotaje. Tiempo de espera de la puerta 1 y salida de alarma de intrusión. Salida de alarma de manipulación del dispositivo.
		NO2 COM2	● AUX2 activa la salida de alarma. Lector de tarjetas 2 salida de alarma antisabotaje. Tiempo de espera de la puerta 2 y salida de alarma de intrusión.
		NUMERO 3 COM3	● AUX3 activa la salida de alarma. Lector de tarjetas 3 salida de alarma antisabotaje. Tiempo de espera de la puerta 3 y salida de alarma de intrusión.
		NO. 4 COM4	● AUX4 activa la salida de alarma. Lector de tarjetas 4 salida de alarma antisabotaje. Tiempo de espera de la puerta 4 y salida de alarma de intrusión.
		NUMERO 5 COM5	● AUX5 activa la salida de alarma. Lector de tarjetas 5 salida de alarma antisabotaje. Tiempo de espera de la puerta 5 y salida de alarma de intrusión.
		NO6 COM6	● AUX6 activa la salida de alarma. Lector de tarjetas 6 salida de alarma antisabotaje. Tiempo de espera de la puerta 6 y salida de alarma de intrusión.
		NO7 COM7	● AUX7 activa la salida de alarma. Lector de tarjetas 7 salida de alarma antisabotaje. Tiempo de espera de la puerta 7 y salida de alarma de intrusión.
		NO8 COM8	● AUX8 activa la salida de alarma. Lector de tarjetas 8 salida de alarma antisabotaje. Tiempo de espera de la puerta 8 y salida de alarma de intrusión.

2.1.9 Lector de tarjetas

Una puerta solo puede conectar lectores de tarjetas del mismo tipo, ya sea RS-485 o Wiegand.

Tabla 2-4 Descripción de la especificación del cable del lector de tarjetas

Tipo de lector de tarjetas	Método de cableado	Largo
Lector de tarjetas RS-485	Conexión RS-485. La impedancia de un solo cable debe estar dentro de los 10 Ω.	100 metros
Tarjeta Wiegand lector	Conexión Wiegand. La impedancia de un solo cable debe estar dentro de los 2Ω.	80 metros

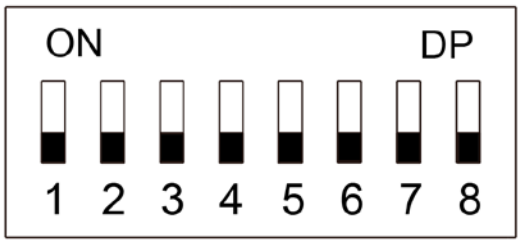
2.2 Indicador de encendido

- Verde fijo: Normal.
- Rojo: Anormal.
- Parpadea en verde: cargando.
- Azul: el controlador está en el modo de arranque.

2.3 Dip switch

(ENCENDIDO) indica 1; indica 0.

Figure 2-9 Dip switch



- Cuando 1–8 se cambian todos a 0, el controlador se inicia normalmente después del encendido. Cuando 1–8
- se cambian todos a 1, el controlador ingresa al modo BOOT después de que se inicia.
- Cuando 1, 3, 5 y 7 se cambian a 1 y los demás son 0, el controlador se restablece a los valores predeterminados de fábrica después de reiniciarse.
- Cuando 2, 4, 6 y 8 se cambian a 1 y los demás a 0, el controlador se restablece a los valores predeterminados de fábrica pero conserva la información del usuario después de que se reinicia.

2.4 Fuente de alimentación

2.4.1 Puerto de alimentación de bloqueo de puerta

El voltaje nominal del puerto de alimentación de la cerradura de la puerta es de 12 V y la salida de corriente máxima es de 2,5 A. Si la carga de energía excede la corriente nominal máxima, proporcione una fuente de alimentación adicional.

2.4.2 Puerto de alimentación del lector de tarjetas

- Controladores unidireccionales de dos puertas, bidireccionales de dos puertas y unidireccionales de cuatro puertas: el voltaje nominal del puerto de alimentación del lector de tarjetas (12V_RD) es de 12 V y la salida de corriente máxima es de 1,4 A
- Controladores bidireccionales de cuatro puertas y unidireccionales de ocho puertas: el voltaje nominal del puerto de alimentación del lector de tarjetas (12V_RD) es de 12 V y la salida de corriente máxima es de 2,5 A.

3 Configuración de CA de SmartPSS

Puede administrar el controlador a través de SmartPSS AC. Esta sección presenta principalmente configuraciones rápidas del controlador. Para obtener más información, consulte el manual del usuario de SmartPSS AC.

Las capturas de pantalla del cliente Smart PSS AC en este manual son solo para referencia y pueden diferir de el producto real.

3.1 Acceso

Step 1 Instale el SmartPSS AC.

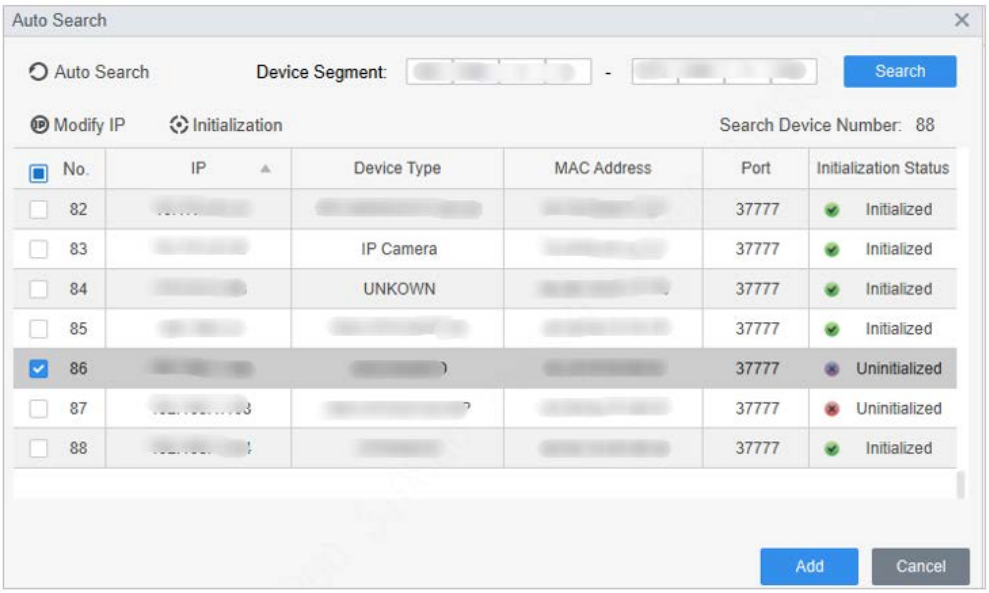
Step 2 Haga doble clic y luego siga las instrucciones para finalizar la inicialización e iniciar sesión.

3.2 Inicialización

Antes de la inicialización, asegúrese de que el controlador y la computadora estén en la misma red.

Step 1 En la página de inicio, seleccione**Administrador de dispositivos**y luego haga clic en**Auto búsqueda**.

Figure 3-1 Auto búsqueda



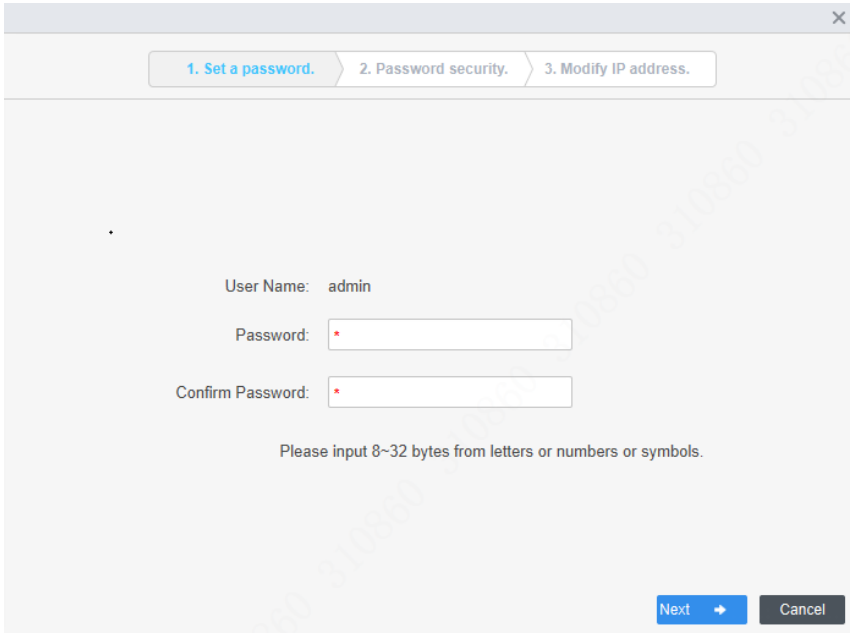
Step 2 Ingrese un rango de segmento de red y luego haga clic en**Búsqueda**.

Step 3 Seleccione el dispositivo y luego haga clic en**Inicialización**. Establezca la

Step 4 contraseña de administrador y luego haga clic en**próximo**.

Si olvida la contraseña, use el interruptor DIP para restaurar los valores predeterminados de fábrica.

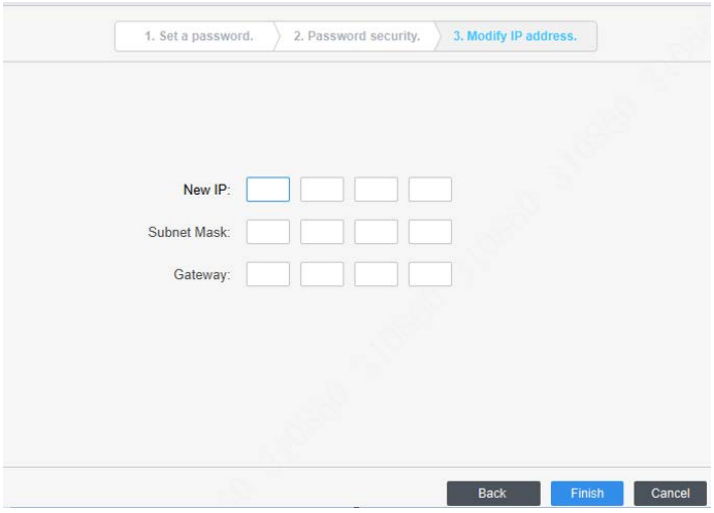
Figure 3-2 Configurar la clave



Step 5 Asocie el número de teléfono y luego haga clic en**próximo**. Ingrese la

Step 6 nueva IP, máscara de subred y puerta de enlace.

Figure 3-3 Modificar dirección IP



Step 7 Hacer clic**Terminar**.

3.3 Adición de dispositivos

Debe agregar el controlador a SmartPSS AC. Puedes hacer clic**Auto búsqueda**para agregar y hacer clic**Agregar**para agregar dispositivos manualmente.

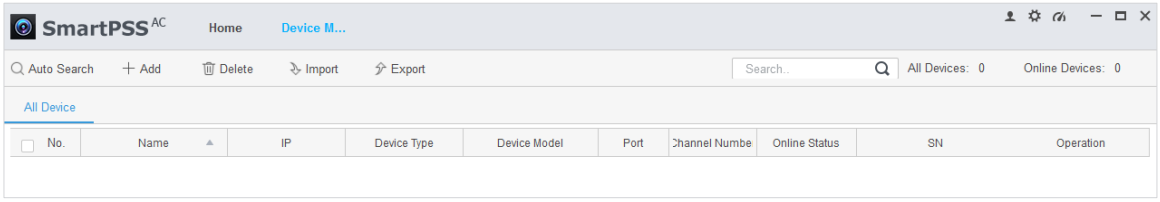
3.3.1 Búsqueda automática

Recomendamos agregar dispositivos mediante búsqueda automática cuando necesite agregar dispositivos en lotes dentro del mismo segmento de red, o cuando el segmento de red está claro pero la dirección IP del dispositivo no está clara.

Step 1 Inicie sesión en SmartPSS AC.

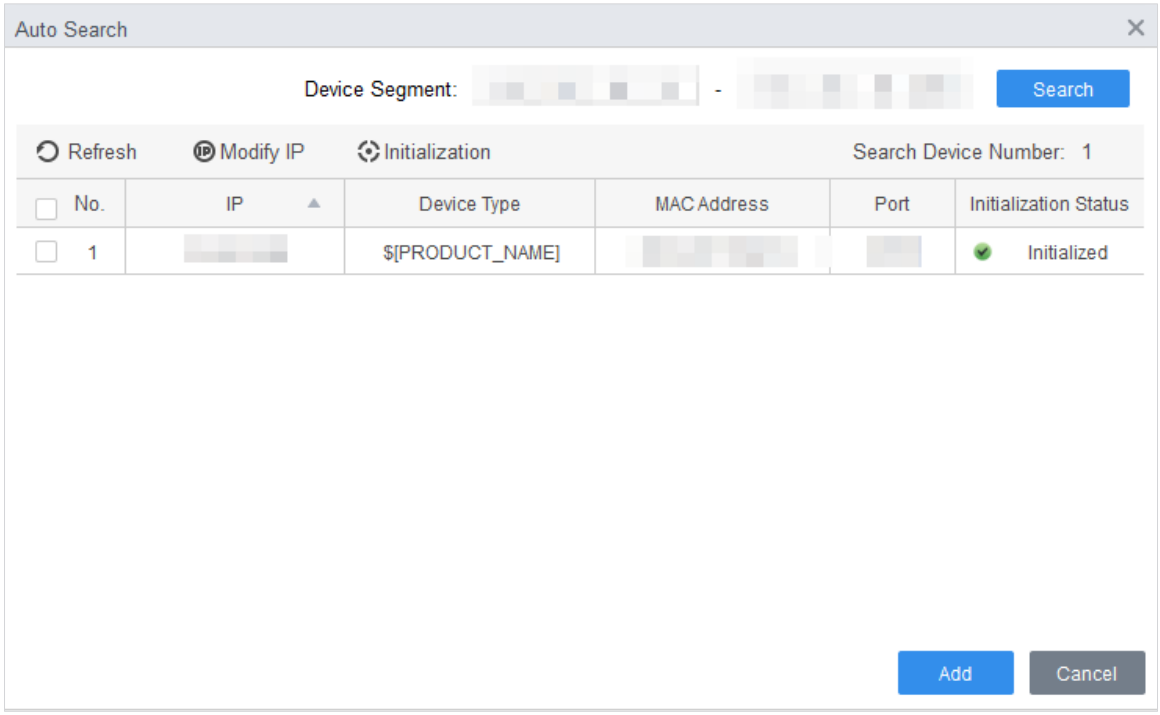
Step 2 Hacer clic**Administrador de dispositivos**en la esquina inferior izquierda.

Figure 3-4 Dispositivos



Step 3 Hacer clic**Auto búsqueda**.

Figure 3-5 Auto búsqueda



Step 4 Ingrese el segmento de red y luego haga clic en**Búsqueda**. Se mostrará una lista de resultados de búsqueda.

- Hacer clic**Actualizar**para actualizar la información del dispositivo.
- Seleccione un dispositivo, haga clic en**Modificar IP**para modificar la dirección IP del dispositivo.

Step 5 Seleccione los dispositivos que desea agregar a SmartPSS AC y luego haga clic en**Agregar**. Ingrese el

Step 6 nombre de usuario y la contraseña de inicio de sesión para iniciar sesión.

Puede ver los dispositivos agregados en la**Dispositivos**página.

- El nombre de usuario es admin y la contraseña es admin123 por defecto. Recomendamos cambiar la contraseña después de iniciar sesión.
- Después de agregar, SmartPSS AC inicia sesión en el dispositivo automáticamente. Después de un inicio de sesión exitoso, el pantallas de estado**En línea**. De lo contrario, muestra**Desconectado**.

3.3.2 Adición manual

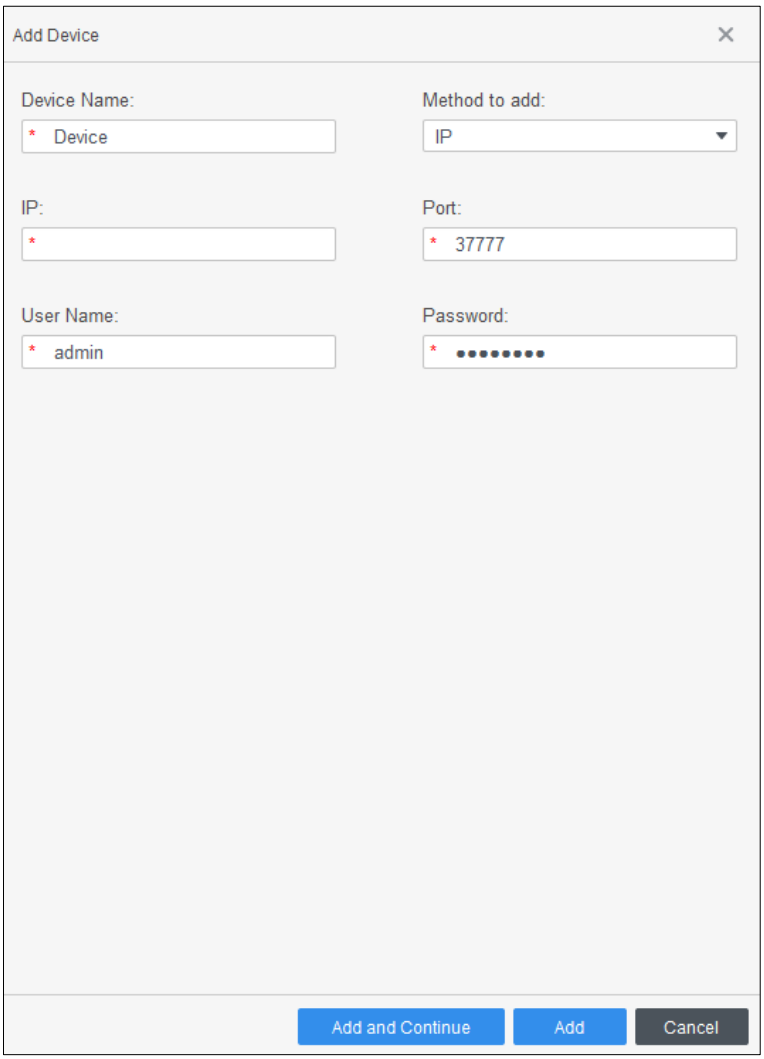
Puede agregar dispositivos manualmente. Debe conocer las direcciones IP y los nombres de dominio de los controladores de acceso que desea agregar.

Step 1 Inicie sesión en SmartPSS AC.

Step 2 Hacer clic**Administrador de dispositivos**en la esquina inferior izquierda. Hacer

Step 3 clic**Agregar**sobre el**Administrador de dispositivos**página.

Figure 3-6 Adición manual



Step 4 Ingrese información detallada del Controlador.

Tabla 3-1 Parámetros

Parámetro	Descripción
Nombre del dispositivo	Introduzca un nombre del controlador. Le recomendamos que asigne al controlador el nombre de su área de instalación para una fácil identificación.
Método para agregar	Seleccione**IP**para agregar el Controlador a través de la dirección IP.
IP	Introduzca la dirección IP del controlador. Es 192.168.1.108 por defecto.
Puerto	Introduzca el número de puerto del dispositivo. El número de puerto es 37777 por defecto.
Nombre de usuario, Clave	Ingrese el nombre de usuario y la contraseña del Controlador. El nombre de usuario es admin y la contraseña es admin123 por defecto. Le recomendamos que cambie la contraseña después de iniciar sesión.

Step 5 Hacer clic**Agregar**.

El dispositivo agregado está en el**Dispositivos**página.

Después de agregar, SmartPSS AC inicia sesión en el dispositivo automáticamente. Después de un inicio de sesión exitoso, el pantallas de estado**En línea**. De lo contrario, muestra**Desconectado**.

3.4 Gestión de usuarios

Agregue usuarios, asígneles tarjetas y configure sus permisos de acceso.

3.4.1 Configuración del tipo de tarjeta

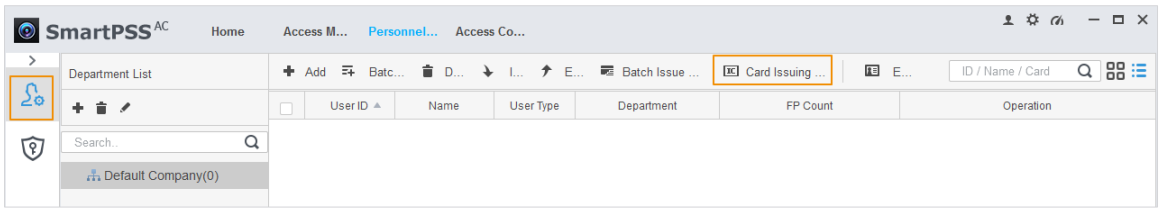
Antes de asignar una tarjeta, establezca primero el tipo de tarjeta. Por ejemplo, si la tarjeta asignada es una tarjeta de identificación, seleccione el tipo como tarjeta de identificación.

El tipo de tarjeta seleccionado debe ser el mismo que el tipo de tarjeta asignado real; de lo contrario números de tarjeta no se puede leer

Step 1 Inicie sesión en SmartPSS AC.

Step 2 Hacer clic**Gerente de Personal**.

Figure 3-7 gerente de personal

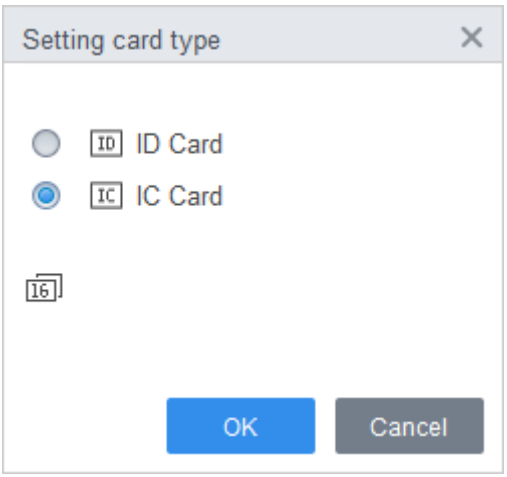


Step 3 Sobre el**Gerente de Personal**página, haga clic , luego haga clic .

Step 4 Sobre el**Configuración del tipo de tarjeta**ventana, seleccione un tipo de tarjeta.

Step 5 Hacer clic para seleccionar el método de visualización del número de tarjeta en decimal o en hexadecimal.

Figure 3-8 Configuración del tipo de tarjeta



Step 6 Hacer clic**DE ACUERDO**.

3.4.2 Agregar usuario

3.4.2.1 Agregar individualmente

Puede agregar usuarios individualmente.

Step 1 Inicie sesión en SmartPSS AC.

Step 2 Hacer clic**Gerente de Personal**>**Usuario**>**Agregar**.

Step 3 Añadir información básica del usuario.

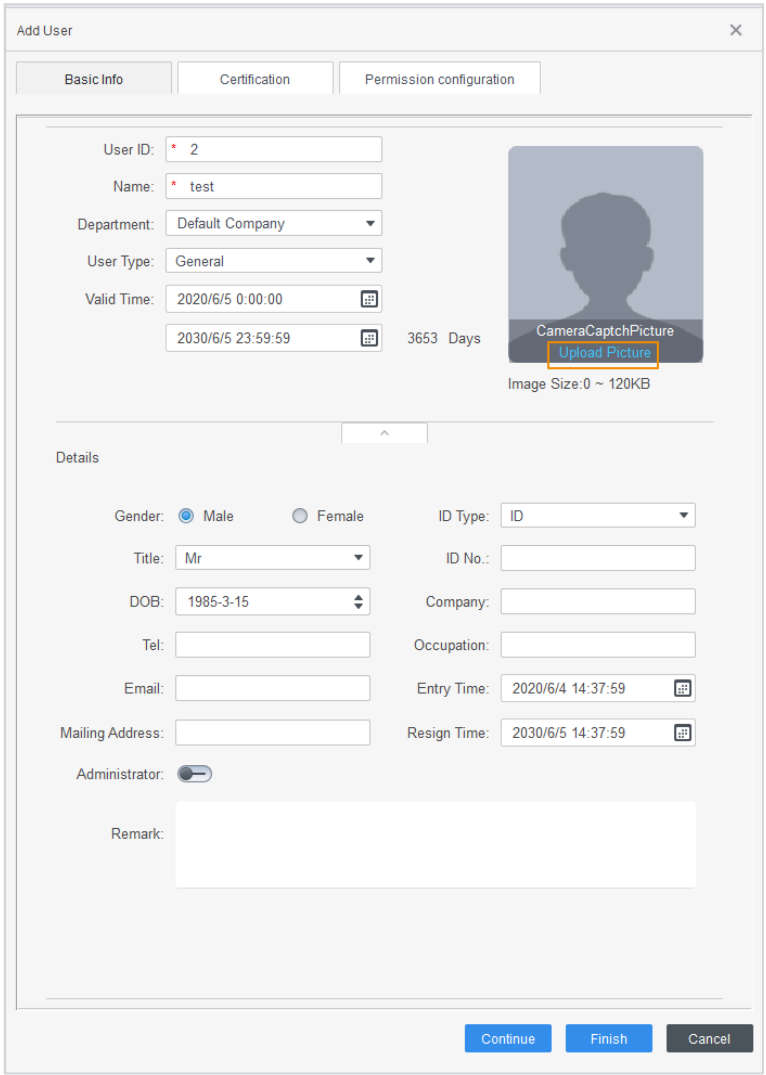
1) Haga clic en el**Información básica**pestaña en el**Agregar usuario**página, y luego agregue información básica del usuario.

2) Haga clic en la imagen y luego haga clic en**Subir foto**para agregar una imagen de la cara.

La imagen de la cara cargada se mostrará en el cuadro de captura.

Asegúrese de que los píxeles de la imagen tengan más de 500 × 500; el tamaño de la imagen es inferior a 120 KB.

Figure 3-9 Agregar información básica



Step 4 Haga clic en el**Certificación**pestaña para agregar información de certificación del usuario.

- Configurar contraseña.

  Configurar la clave. Para los controladores de acceso de segunda generación, establezca la contraseña de personal; para otros dispositivos, configure la contraseña de la tarjeta. La nueva contraseña debe constar de 6 dígitos.

- Configurar tarjeta.

El número de tarjeta puede leerse automáticamente o introducirse manualmente. Para leer el número de tarjeta automáticamente, seleccione un lector de tarjetas y luego coloque la tarjeta en el lector de tarjetas.

1) Haga clic establecer**Dispositivo**o**Emisor de la tarjeta**al lector de tarjetas.

2) Se debe agregar el número de tarjeta si se utiliza el controlador de acceso que no es de segunda generación.

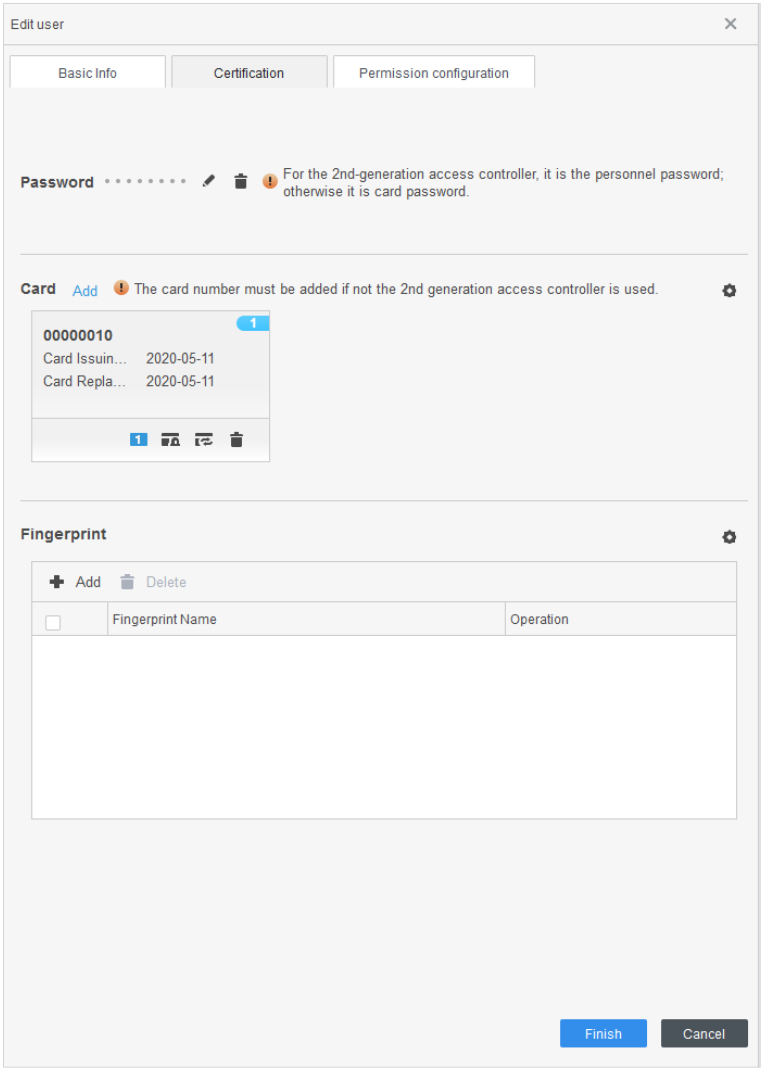
3) Después de agregar, puede configurar la tarjeta como tarjeta principal o tarjeta de coacción, o reemplazar la tarjeta por una nueva, o eliminar la tarjeta.

- Configurar huella dactilar.

1) Haga clic establecer**Dispositivo**o**Escáner de huellas dactilares**al recolector de huellas dactilares.

2) Haga clic**Agregar huella digital**y presione su dedo en el escáner tres veces seguidas.

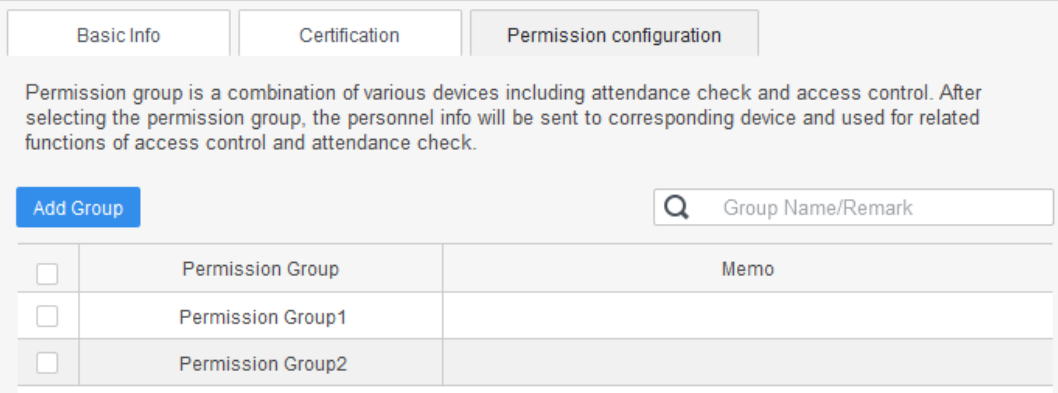
Figure 3-10 Configurar certificación



Step 5 Configurar permisos para el usuario.

Para obtener más información, consulte "3.5 Configuración de permisos".

Figure 3-11 Configuración de permisos



Step 6 Hacer clic**Terminar**.

3.4.2.2 Adición de lotes

Puede agregar usuarios en lotes.

Step 1 Inicie sesión en SmartPSS AC.

Step 2 Hacer clic**Gerente de Personal**>**Usuario**>**Agregar lote**.

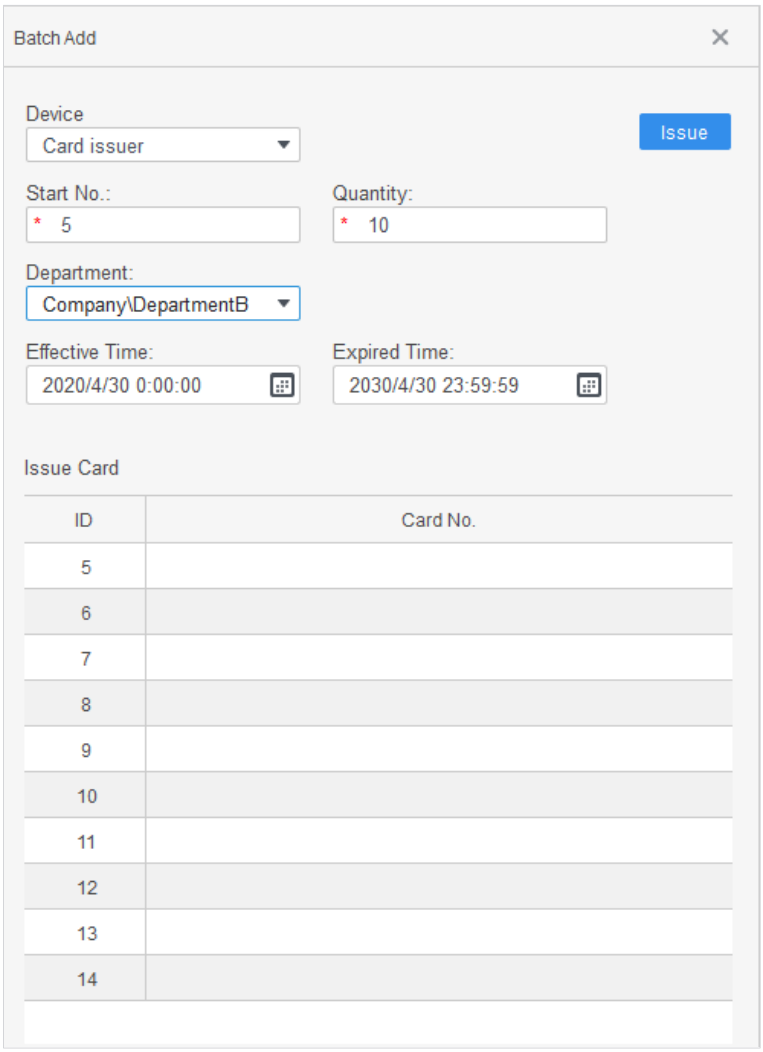
Step 3 Seleccione el lector de tarjetas y el departamento de usuario. Establezca el número de inicio, la cantidad de tarjetas, el tiempo efectivo y el tiempo de vencimiento de la tarjeta.

Step 4 Hacer clic**Tema**a la asignación de tarjetas.

El número de tarjeta se leerá automáticamente. Hacer clic**Detenerse**

Step 5 después de asignar la tarjeta, y luego haga clic en**DE ACUERDO**.

Figure 3-12 Agregar usuarios en lotes



3.5 Configuración de permisos

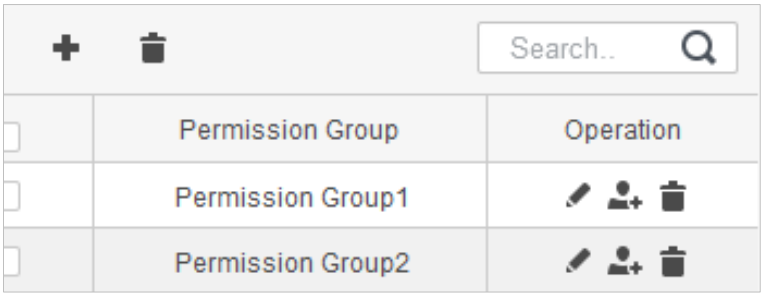
3.5.1 Agregar grupo de permisos

Cree un grupo de permisos que sea una colección de permisos de acceso a puertas.

Step 1 Inicie sesión en SmartPSS AC.

Step 2 Hacer clic**Gerente de Personal**>**Configuración de permisos**.

Figure 3-13 Lista de grupos de permisos



Step 3 Hacer clic para agregar un grupo de permisos.

Step 4 Establecer parámetros de permiso.

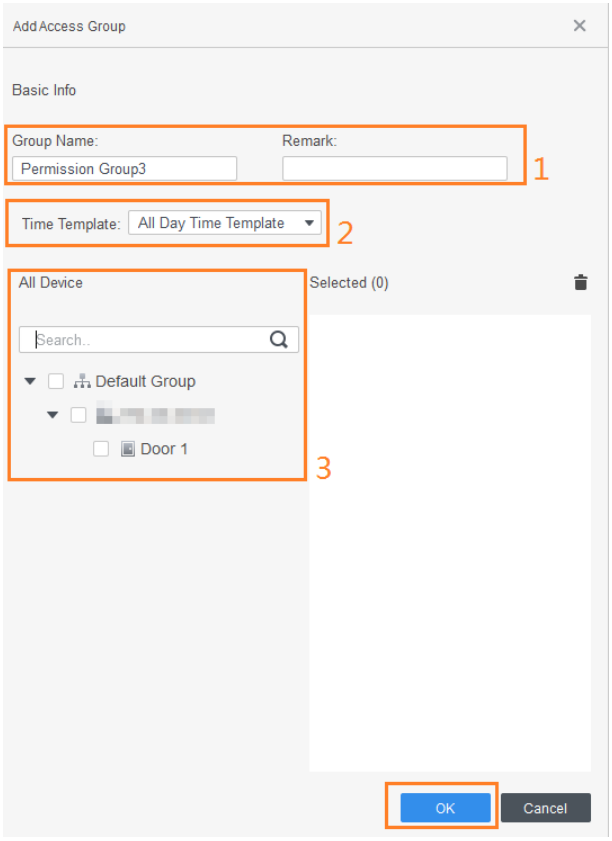
1) Introduzca el nombre del grupo y el comentario.

2) Seleccione la plantilla de tiempo.

Para obtener detalles sobre la configuración de la plantilla de tiempo, consulte el manual del usuario de SmartPSS AC.

3) Seleccione el dispositivo correspondiente, como la puerta 1.

Figure 3-14 Agregar grupo de permisos



Step 5 Hacer clic**DE ACUERDO**.

Operación relacionada

Sobre el**Lista de grupos de permisos**página, puede:

- Haga clic para eliminar el grupo.
- Hacer clic para modificar la información del grupo.
- Haga doble clic en el nombre del grupo de permisos para ver la información del grupo.

3.5.2 Asignación de permiso de acceso

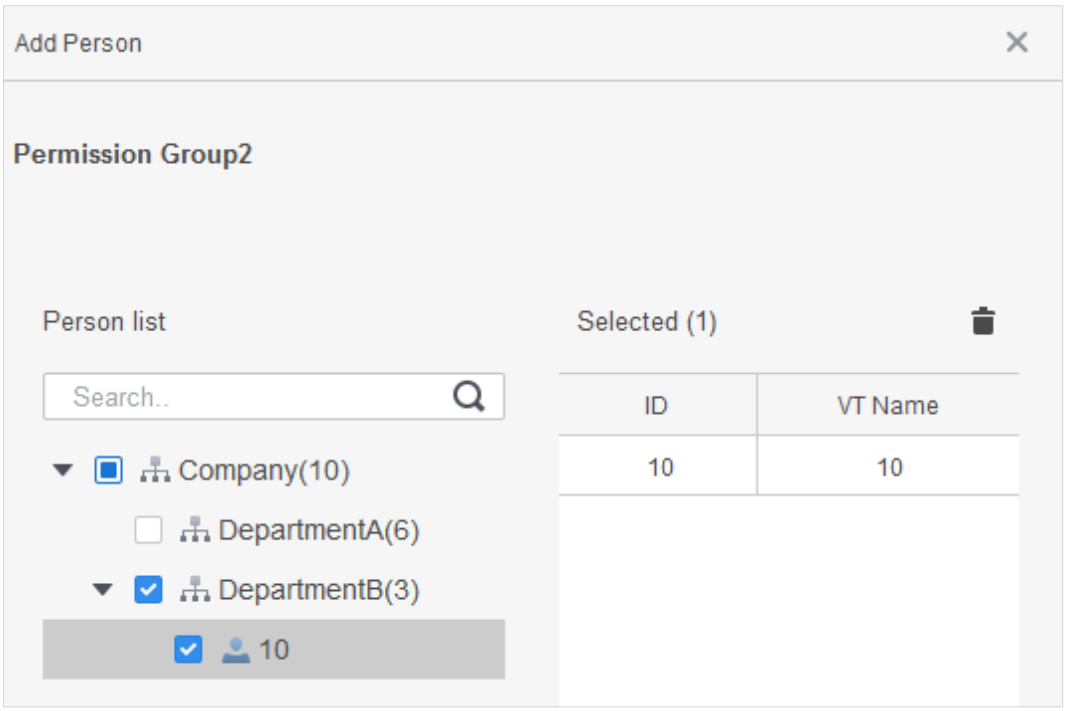
Asocie a los usuarios con los grupos de permisos deseados y luego a los usuarios se les asignarán permisos de acceso a las puertas definidas.

Step 1 Inicie sesión en SmartPSS AC.

Step 2 Hacer clic**Gerente de Personal**>**Configuración de permisos**.

Step 3 Seleccione el grupo de permisos de destino y luego haga clic en .

Figure 3-15 Configurar permiso



Step 4 Seleccione usuarios para asociarlos con el grupo seleccionado. Hacer clic**DE**

Step 5 **ACUERDO**.

3.6 Configuración del controlador de acceso

3.6.1 Configuración de funciones avanzadas

3.6.1.1 Desbloqueo de la primera tarjeta

Otros usuarios pueden deslizar para desbloquear la puerta solo después de que el primer titular de la tarjeta especificado pase la tarjeta. Puede configurar varias primeras tarjetas. Otros usuarios sin primeras tarjetas pueden desbloquear la puerta solo después de que uno de los titulares de la primera tarjeta pase la primera tarjeta.

- La persona a la que se le concederá el primer permiso de desbloqueo de tarjeta deberá ser de la**General**usuario tipo y tener permisos de las puertas determinadas. Establezca el tipo al agregar usuarios. Para más detalles, consulte "3.3.2 Adición de Usuario".
- Para obtener detalles sobre la asignación de permisos, consulte "3.5 Configuración de permisos".

Step 1 Seleccione**Configuración de acceso**>**Configuración avanzada**. Haga clic en el

Step 2 **Desbloqueo de la primera tarjeta**pestaña. Hacer clic**Agregar**.

Step 3

Step 4 Configurar el**Desbloqueo de la primera tarjeta**parámetros y, a continuación, haga clic en**Guardar**.

Figure 3-16 Configuración de desbloqueo de la primera tarjeta

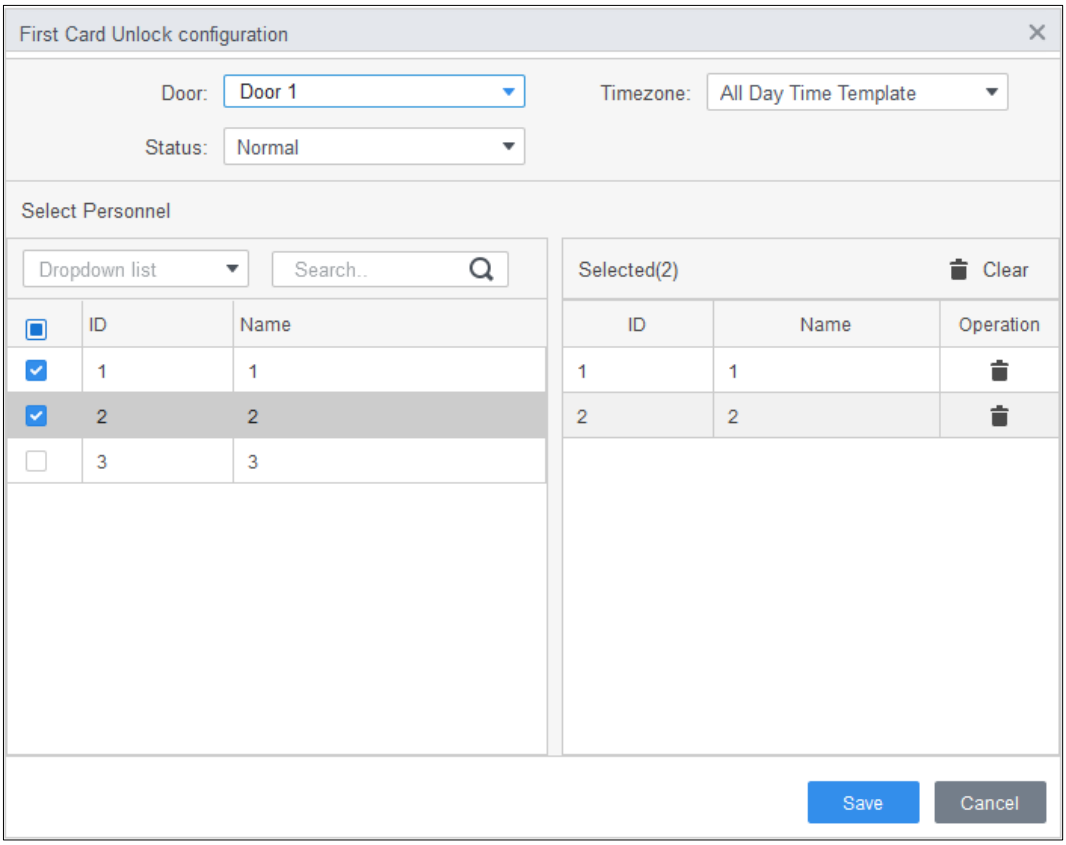


Tabla 3-2 Parámetros de desbloqueo de la primera tarjeta

Parámetro	Descripción
Puerta	Seleccione el canal de control de acceso de destino para configurar el desbloqueo de la primera tarjeta.
Zona horaria	**Desbloqueo de la primera tarjeta**es válido en el período de la plantilla de tiempo seleccionada.
Estado	Después**Desbloqueo de la primera tarjeta**está habilitado, la puerta está en el**Modo normal**o **Modo siempre abierto**.
Usuario	Seleccione el usuario para tener la primera tarjeta. Admite la selección de una cantidad de usuarios para tener las primeras tarjetas. Cualquiera de ellos que pase la primera tarjeta significa que se realiza el desbloqueo de la primera tarjeta.

Step 5 (Opcional) Haga clic en  . El ícono cambiando a  indica**Desbloqueo de la primera tarjeta**está habilitado.

El recién agregado**Desbloqueo de la primera tarjeta**está habilitado de forma predeterminada.

3.6.1.2 Desbloqueo multitarjeta

Los usuarios solo pueden desbloquear la puerta después de que los usuarios o grupos de usuarios definidos otorguen acceso en secuencia.

- Un grupo puede tener hasta 50 usuarios y una persona puede pertenecer a varios grupos.
- Puede agregar hasta cuatro grupos de usuarios con permiso de desbloqueo multitarjeta para una puerta, con hasta 200 usuarios en total y hasta 5 usuarios válidos.

- El desbloqueo de la primera tarjeta tiene prioridad sobre el desbloqueo de múltiples tarjetas, lo que significa que si las dos reglas son ambas activado, el desbloqueo de la primera tarjeta es lo primero. Le recomendamos que no asigne el desbloqueo de varias tarjetas permiso a los titulares de la primera tarjeta.
- No establezca el**VIP**o**Patrulla**escriba para las personas del grupo de usuarios. Para obtener más información, consulte "3.3.2 Agregar usuario".

- Para obtener detalles sobre la asignación de permisos, consulte "3.4 Configuración de permisos".

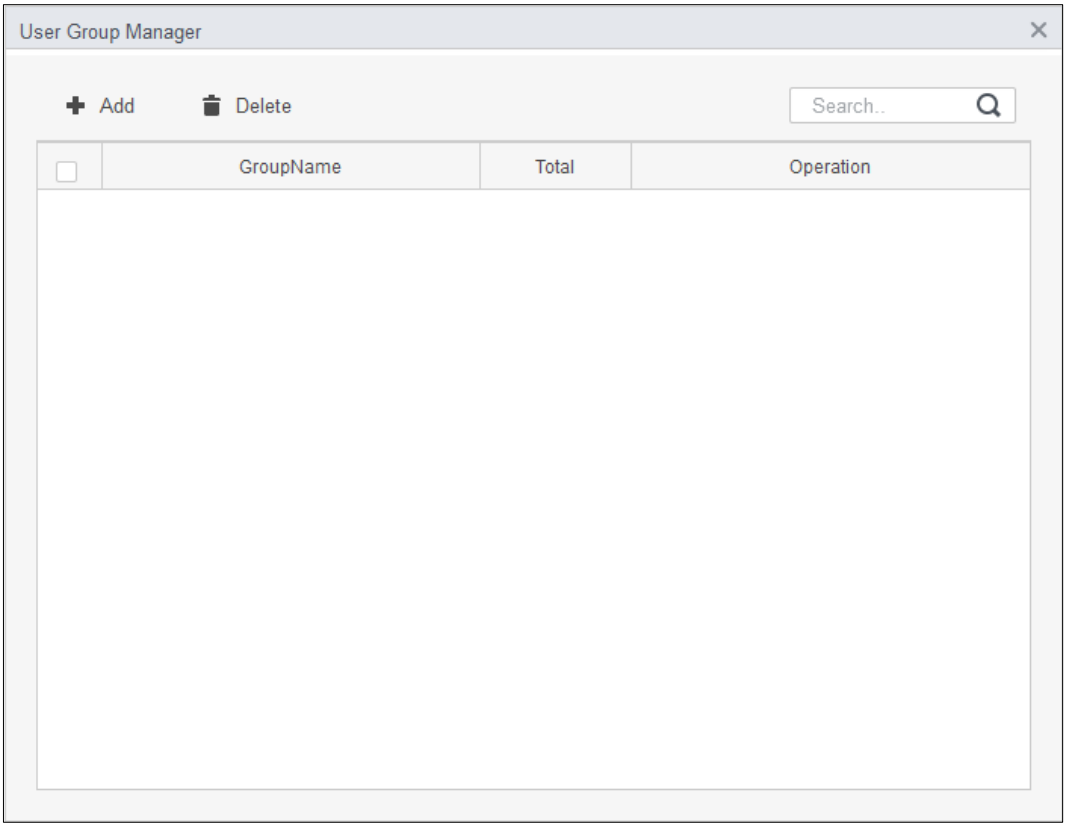
Step 1 Seleccione**Configuración de acceso**>**Configuración avanzada**. Haga clic en

Step 2 el**Desbloqueo de tarjetas múltiples**pestaña. Añadir grupo de usuarios.

Step 3

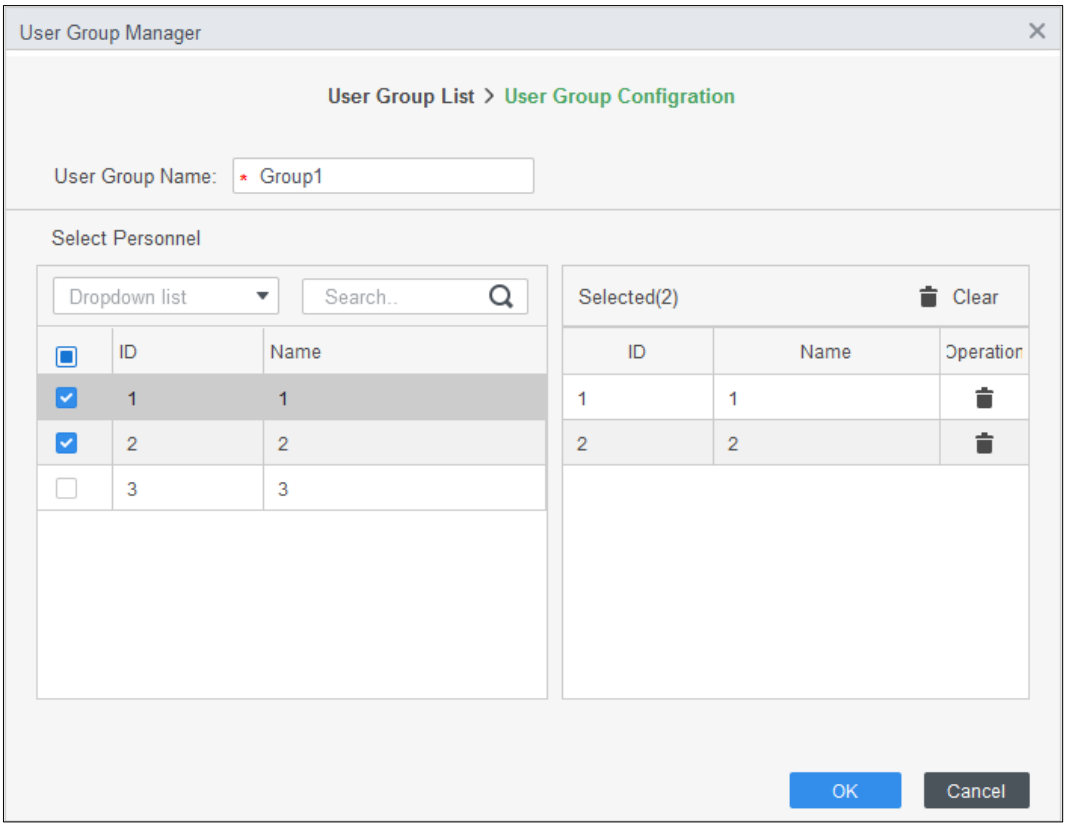
1) Haga clic**Grupo de usuario**.

Figure 3-17 Administrador de grupos de usuarios



2) Haga clic**Agregar**.

Figure 3-18 Configuración del grupo de usuarios



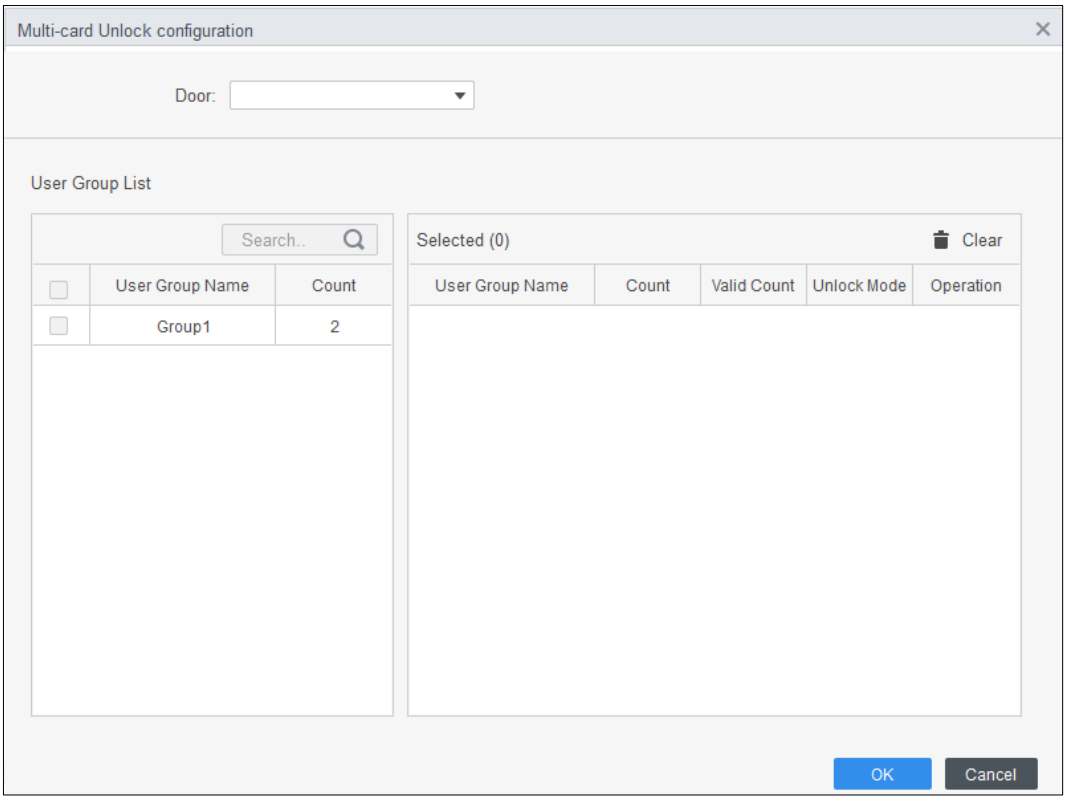
3) Configurar**Nombre del grupo de usuarios**. Seleccionar usuarios de**Lista de usuarios**y haga clic**DE ACUERDO**. Puede seleccionar hasta 50 usuarios.

4) Haga clic en en la esquina superior derecha de la**Administrador de grupos de usuarios**página.

Step 4 Configurar parámetros de desbloqueo multitarjeta.

1) Haga clic**Agregar**.

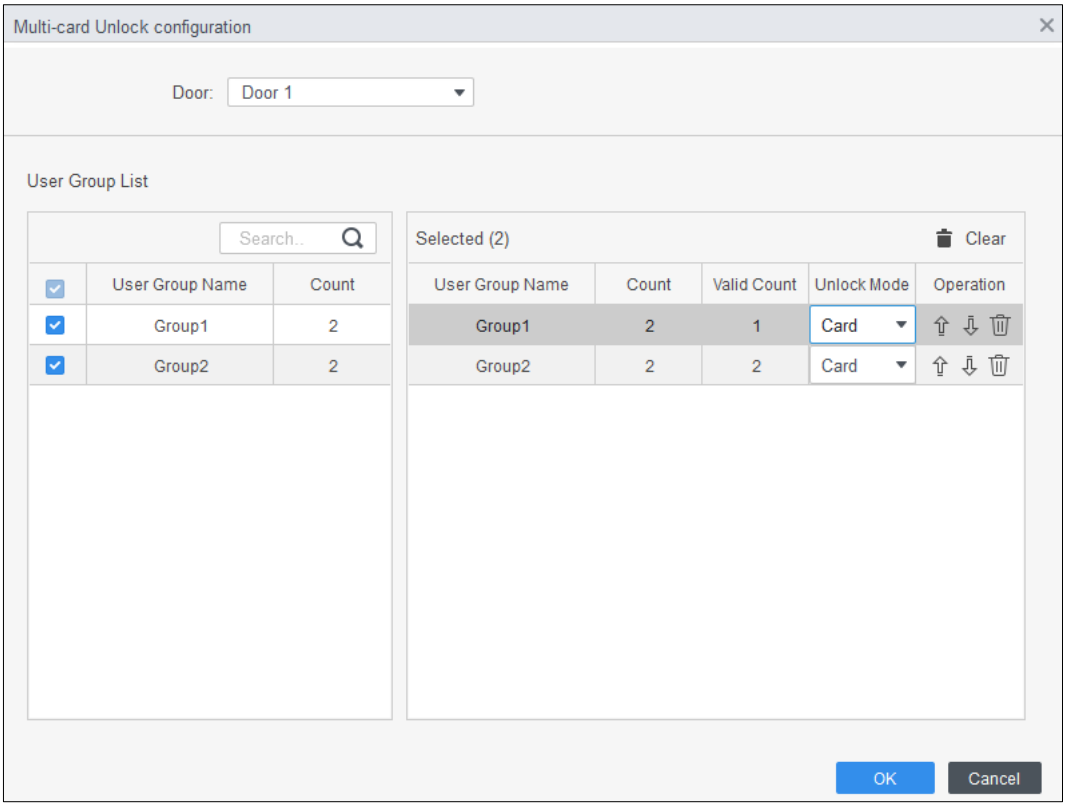
Figure 3-19 Configuración de desbloqueo multitarjeta (1)



2) Seleccione la puerta.

3) Seleccione el grupo de usuarios. Puede seleccionar hasta cuatro grupos.

Figure 3-20 Configuración de desbloqueo multitarjeta (2)



4) Introduzca el**Recuento válido**para que cada grupo esté en el sitio, y luego seleccione el**Modo de desbloqueo**.

Hacer clic o para ajustar la secuencia de grupo para desbloquear la puerta.

- El conteo válido se refiere a la cantidad de usuarios en cada grupo que debe estar en el sitio para deslizar sus tarjetas. Tome la figura 3-17 como ejemplo. La puerta solo se puede desbloquear después de que una persona del grupo 1 y 2 personas del grupo 2 hayan pasado sus tarjetas.
- Se permiten hasta cinco usuarios válidos.

5) Haga clic**DE ACUERDO**.

Step 5 (Opcional) Haga clic en . El ícono cambiando a indica**Desbloqueo de tarjetas múltiples**está habilitado.

El recién agregado**Desbloqueo de tarjetas múltiples**está habilitado de forma predeterminada.

3.6.1.3 Antirretorno

Los usuarios deben verificar sus identidades tanto para la entrada como para la salida; de lo contrario, se activará una alarma. Si una persona ingresa con una verificación de identidad válida y sale sin verificación, se activará una alarma cuando intente ingresar nuevamente y se negará el acceso al mismo tiempo. Si una persona ingresa sin verificación de identidad y sale con verificación, se niega la salida cuando intenta salir.

Step 1 Seleccione**Configuración de acceso**>**Configuración avanzada**. Hacer

Step 2 clic**Agregar**.

Step 3 Configurar parámetros.

1) Seleccione el dispositivo e ingrese el nombre del dispositivo.

2) Seleccione la plantilla de tiempo.

3) Configure el tiempo de descanso y la unidad es minuto.

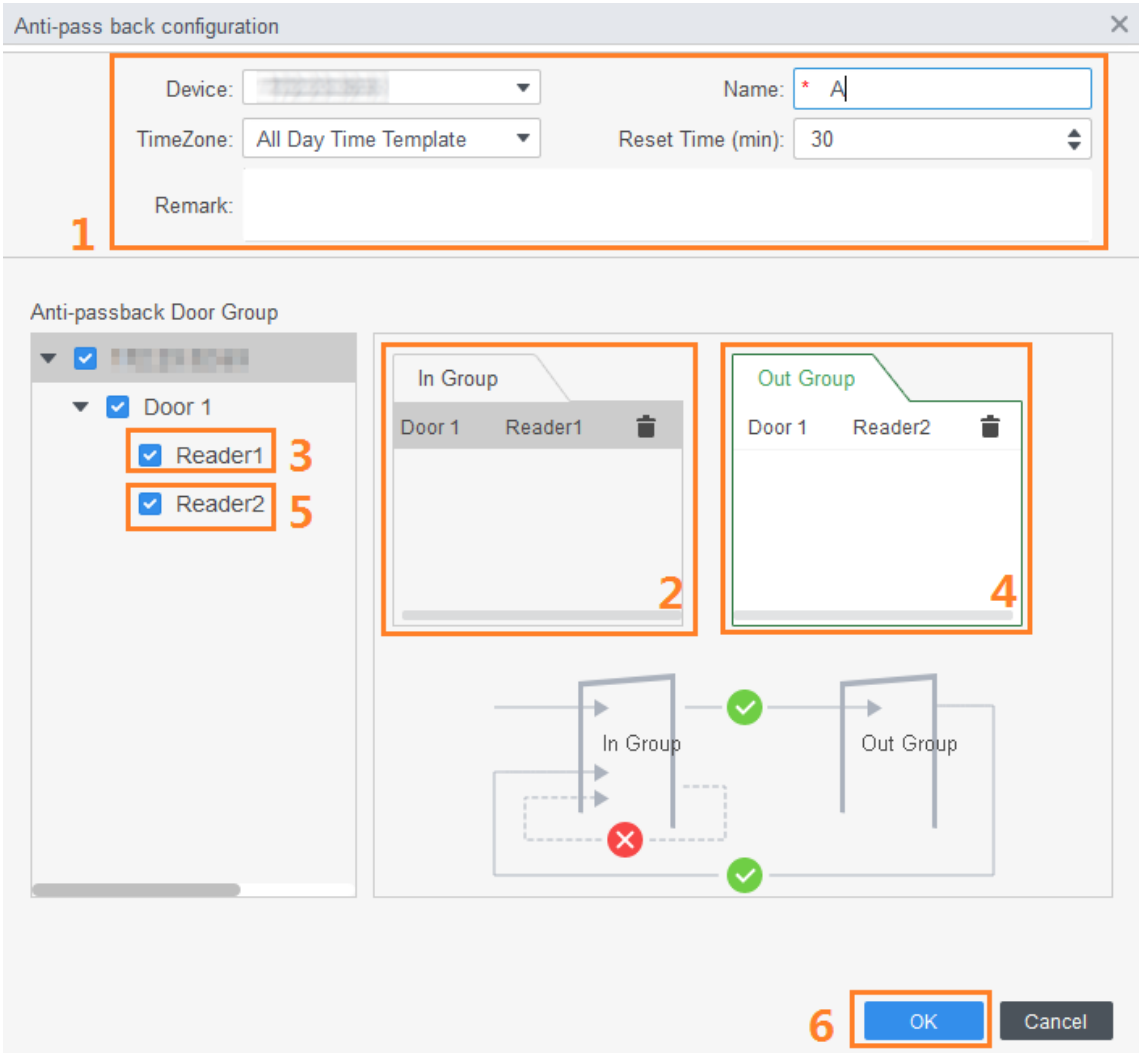
Por ejemplo, establezca el tiempo de reinicio en 30 minutos. Si un pentagrama ha entrado pero no salido, la alarma anti-retroceso se activará cuando este pentagrama tienda a entrar de nuevo dentro de los 30 minutos. El segundo deslizamiento de este personal solo es válido después de 30 minutos más tarde.

4) Haga clic**En grupo**y seleccione el lector correspondiente. Y luego haga clic**fuera del grupo**y seleccione el lector correspondiente.

5) Haga clic**DE ACUERDO**.

La configuración se emitirá al dispositivo y tendrá efecto.

Figure 3-21 Configuración anti-pass back



Step 4 (Opcional) Haga clic en . El ícono cambiando a indica**Anti-passback**está habilitado.

El recién agregado**Anti-passback**está habilitado de forma predeterminada.

3.6.1.4 Cerradura entre puertas

El acceso a través de una o más puertas depende del estado de otra puerta (o puertas). Por ejemplo, cuando dos puertas están bloqueadas, puede acceder a través de una puerta solo cuando la otra puerta está cerrada. Un dispositivo admite dos grupos de puertas con hasta 4 puertas en cada grupo.

Step 1 Seleccione**Configuración de acceso**>**Configuración avanzada**. Haga

Step 2 clic en el**Entrelazar**pestaña. Hacer clic**Agregar**.

Step 3

Step 4 Configure los parámetros y haga clic en**DE ACUERDO**. 1)

Seleccione el dispositivo e ingrese el nombre del dispositivo.

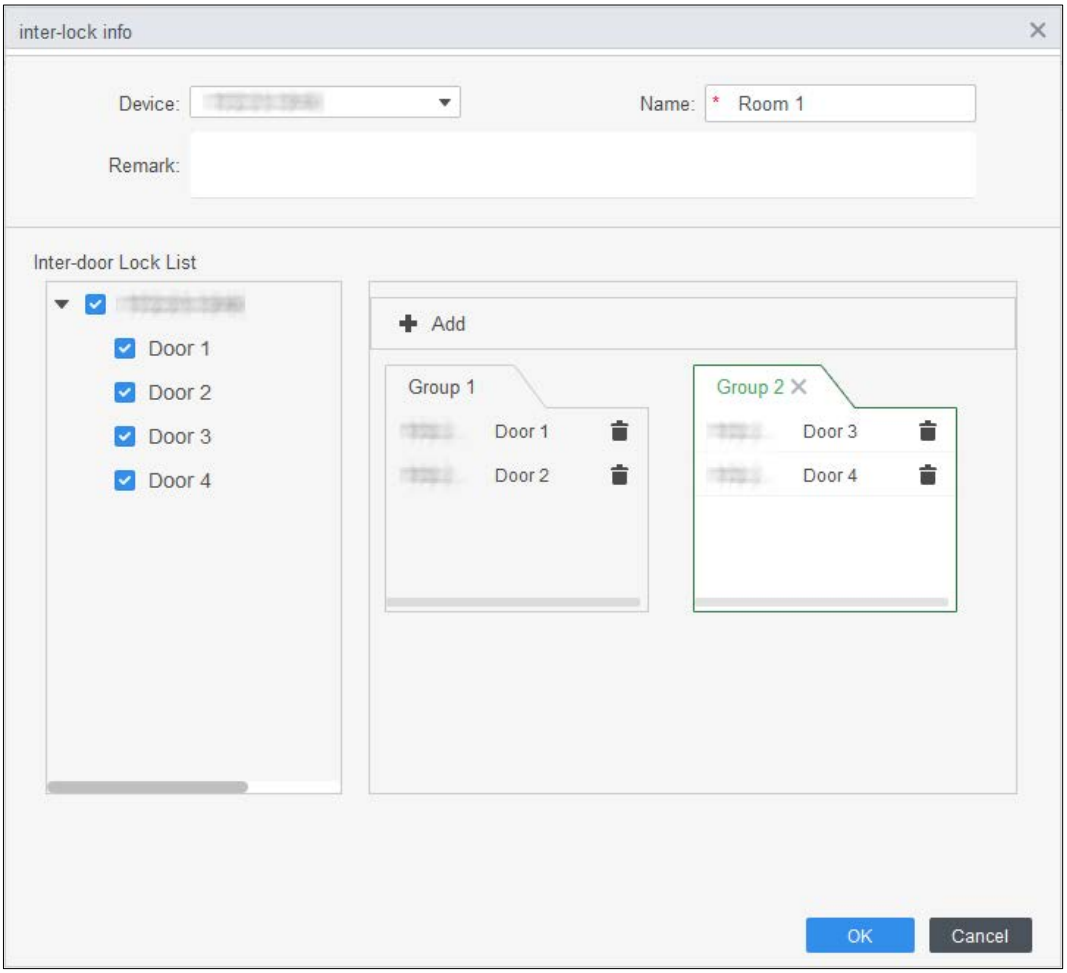
2) Introducir comentario.

3) Haga clic**Agregar**dos veces para agregar dos grupos de puertas.

4) Agregue puertas del controlador de acceso al grupo de puertas necesario. Haga clic en un grupo de puertas y luego haga clic en puertas para agregar.

5) Haga clic**DE ACUERDO**.

Figure 3-22 Configuración de cerradura entre puertas



Step 5 (Opcional) Haga clic en . El ícono cambiando a , lo cual indica**Cerradura entre puertas**es activado.

El recién agregado**Cerradura entre puertas**está habilitado de forma predeterminada.

3.6.2 Configuración del controlador de acceso

Puede configurar la puerta de acceso, como la dirección del lector, el estado de la puerta y el modo de desbloqueo.

Step 1 Seleccione**Configuración de acceso**>**Configuración de**

Step 2 **acceso**. Haga clic en la puerta que debe configurarse.

Step 3 Configurar parámetros.

Figure 3-23 Configurar puerta de acceso

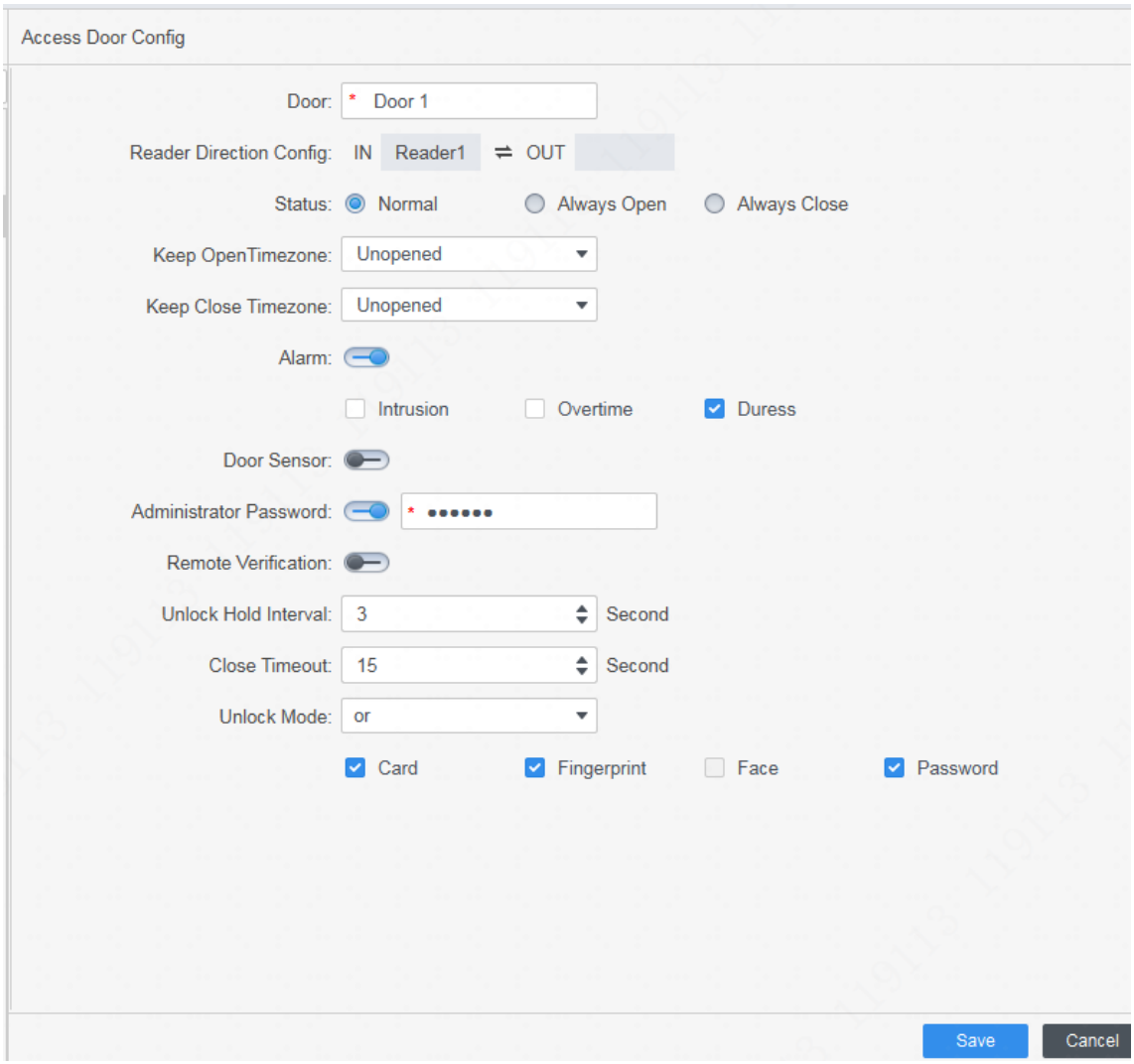


Figure 3-24 Desbloqueo por período de tiempo

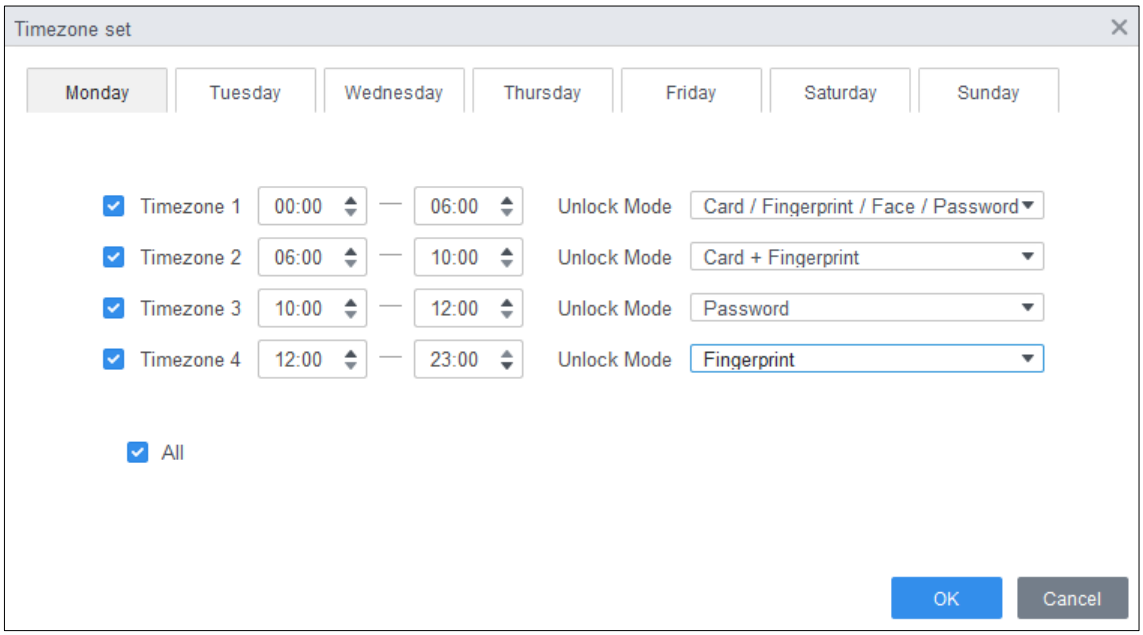


Tabla 3-3 Parámetros de la puerta de acceso

Parámetro	Descripción
Puerta	Introduzca el nombre de la puerta.
Dirección del lector Configuración	Hacer clic ⇌ para establecer la dirección del lector de acuerdo con las situaciones reales.
Estado	Establecer el estado de la puerta, incluido**Normal**,**Siempre abierto**y**Siempre Cerrar**. No es el estado real de la puerta porque SmartPSS-AC solo puede enviar comandos al dispositivo. Si desea conocer el estado real de la puerta, habilite el sensor de puerta.
Mantener zona horaria abierta	Seleccione la plantilla de tiempo cuando la puerta esté siempre abierta.
Mantener cerrada la zona horaria	Seleccione la plantilla de tiempo cuando la puerta esté siempre cerrada.
Alarma	Habilite la función de alarma y configure el tipo de alarma, incluidas intrusión, horas extra y coacción. Cuando la alarma está habilitada, el SmartPSS-AC recibirá un mensaje cargado cuando se active la alarma.
sensor de puerta	Habilite el sensor de puerta para que pueda conocer el estado real de la puerta. Recomendamos habilitar la función.
Administrador Clave	Habilite y establezca la contraseña de administrador. Puede acceder introduciendo la contraseña.
Verificación remota	Habilite la función y configure la plantilla de tiempo, y luego el acceso de la persona debe verificarse de forma remota a través del SmartPSS-AC durante los períodos de la plantilla.
Intervalo de espera de desbloqueo	Configure el intervalo de retención de desbloqueo. La puerta se cerrará automáticamente cuando termine el tiempo.
Cerrar tiempo de espera	Configure el tiempo de espera para la alarma. Por ejemplo, establezca el tiempo de espera de cierre en 60 segundos. Si la puerta no se cierra durante más de 60 segundos, se cargará el mensaje de alarma.
Modo de desbloqueo	Seleccione el modo de desbloqueo según sea necesario. ● Seleccione**Y**y seleccione los métodos de desbloqueo. Puede abrir la puerta combinando los métodos de desbloqueo seleccionados. ● Seleccione**O**y seleccione los métodos de desbloqueo. Puede abrir la puerta de una de las formas que configuró. ● Seleccione**Desbloqueo por período de tiempo**y seleccione el modo de desbloqueo para cada período de tiempo. La puerta solo se puede abrir con los métodos seleccionados dentro del período definido.

Step 4 Hacer clic**Guardar**.

3.6.3 Visualización de eventos históricos

Historial de eventos de puerta incluye eventos tanto en SmartPSS-AC como en dispositivos. Extraiga eventos del historial de los dispositivos para asegurarse de que todos los registros de eventos estén disponibles para su búsqueda.

Step 1 Agregue el personal necesario al SmartPSS-AC.

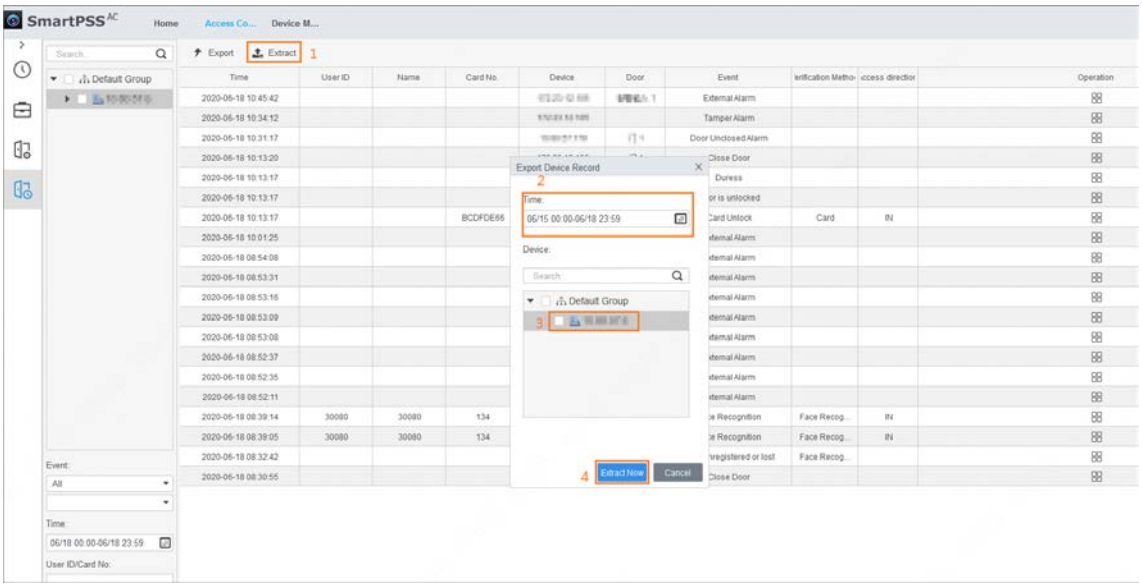
Step 2 Hacer clic**Configuración de acceso**>**Evento de historia**en la página de inicio.

Step 3 Clickea en el**Administrador de acceso**página.

Step 4 Extraiga eventos del dispositivo de puerta al local. Hacer clic**Extracto**, configure la hora, seleccione el dispositivo de la puerta y luego haga clic en**Extraer ahora**.

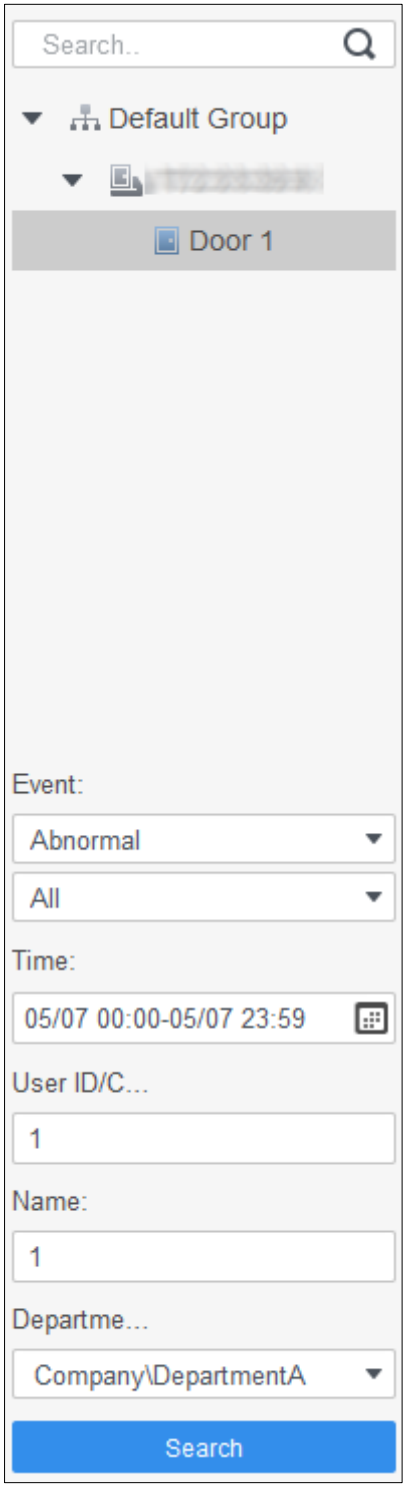
Puede seleccionar varios dispositivos a la vez para extraer eventos.

Figure 3-25 Extraer eventos



Step 5 Establezca las condiciones de filtrado y luego haga clic en**Búsqueda**.

Figure 3-26 Buscar eventos por condiciones de filtrado



3.7 Gestión de Acceso

3.7.1 Apertura y cierre de puertas a distancia

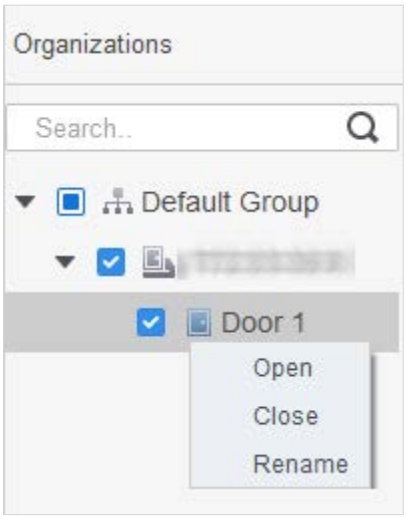
Puede controlar la puerta de forma remota a través de SmartPSS AC.

Step 1 Hacer clic**Administrador de acceso**en la página de inicio. (O haga clic en**Guía de acceso >**) .

Step 2 Controlar remotamente la puerta. Hay dos métodos.

- Método 1: seleccione la puerta, haga clic derecho y seleccione**Abierto**.

Figure 3-27 Control remoto (método 1)



- Método 2: haga clic o para abrir o cerrar la puerta.

Figure 3-28 Control remoto (método 2)

Step 3 Ver el estado de la puerta por**Información del evento**lista.

- Filtrado de eventos: Seleccione el tipo de evento en el**Información del evento**y la lista de eventos muestra eventos de los tipos seleccionados. Por ejemplo, seleccione**Alarma**, y la lista de eventos solo muestra la alarma eventos.
- Bloqueo de actualización de eventos: haga clic en junto a**Información del evento**para bloquear o desbloquear la lista de eventos, y entonces los eventos en tiempo real no se pueden ver.
- Eliminación de eventos: haga clic en junto a**Información del evento**para borrar todos los eventos en la lista de eventos.

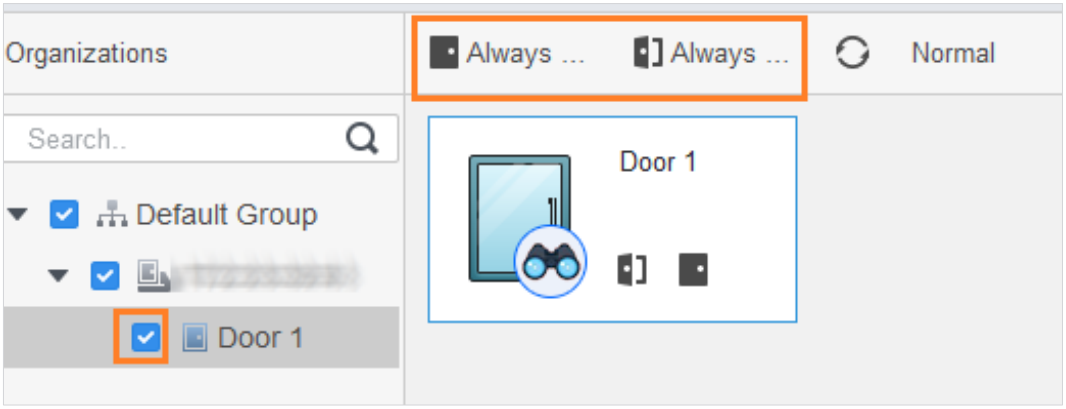
3.7.2 Configuración del estado de la puerta

Después de configurar el estado siempre abierto o siempre cerrado, la puerta permanece abierta o cerrada todo el tiempo. Puedes hacer clic **Normal**para restaurar el estado de la puerta a la normalidad para que los usuarios puedan desbloquear la puerta después de la verificación de identidad.

Step 1 Hacer clic**Administrador de acceso**en la página de inicio. (O haga clic en**Guía de acceso >**) .

Step 2 Seleccione la puerta y luego haga clic en**Siempre abierto**o**Siempre Cerrar**.

Figure 3-29 Establecer siempre abierto o siempre cerrado



3.7.3 Configuración de enlace de alarma

Después de configurar la vinculación de alarmas, se activarán las alarmas. Para obtener más información, consulte el manual de usuario de SmartPss AC. Esta sección utiliza la alarma de intrusión como ejemplo.

- Configure enlaces de alarma externos conectados al controlador de acceso, como una alarma de humo. Configure los
- enlaces de los eventos del controlador de acceso.
  - ◇ Evento de alarma
  - ◇ Evento anormal
  - ◇ Evento normal

Para la función anti-pass back, configure el modo anti-pass back en**Anormal**de**Configuración de eventos**, y luego configurar los parámetros en**Configuración avanzada**. Para obtener más información, consulte "3.5.1 Configuración avanzada Funciones".

Step 1 Hacer clic**Configuración de eventos**en la página de inicio.

Step 2 Seleccione la puerta y seleccione**Evento de alarma**>**Evento de intrusión**. Hacer clic

Step 3 junto a**Alarma de intrusión**para habilitar la función.

Step 4 Configure las acciones de vinculación de la alarma de intrusión según sea necesario.

- Habilitar sonido de alarma.

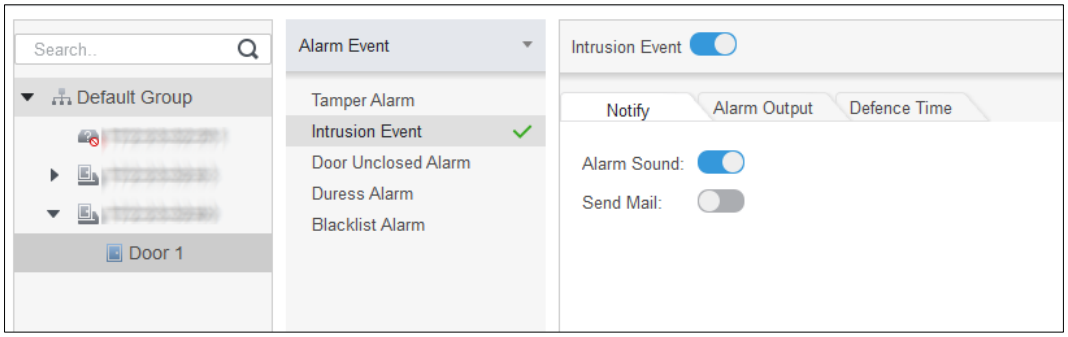
  Haga clic en el**Notificar**pestaña y haga clic en junto a**Sonido de alarma**. Cuando evento de intrusión sucede, el controlador de acceso advierte con un sonido de alarma.

- Enviar correo de alarma.

  1) Habilitar**Enviar correo**y confirme para establecer SMTP. Él**Ajustes del sistema**se muestra la página.

  2) Configure los parámetros SMTP, como la dirección del servidor, el número de puerto y el modo de cifrado. Cuando ocurren eventos de intrusión, el sistema envía notificaciones de alarma a través de correos electrónicos al receptor especificado.

Figure 3-30 Configurar alarma de intrusión



- Configurar E/S de alarma.

1) Haga clic en el**Salida de alarma**pestaña.

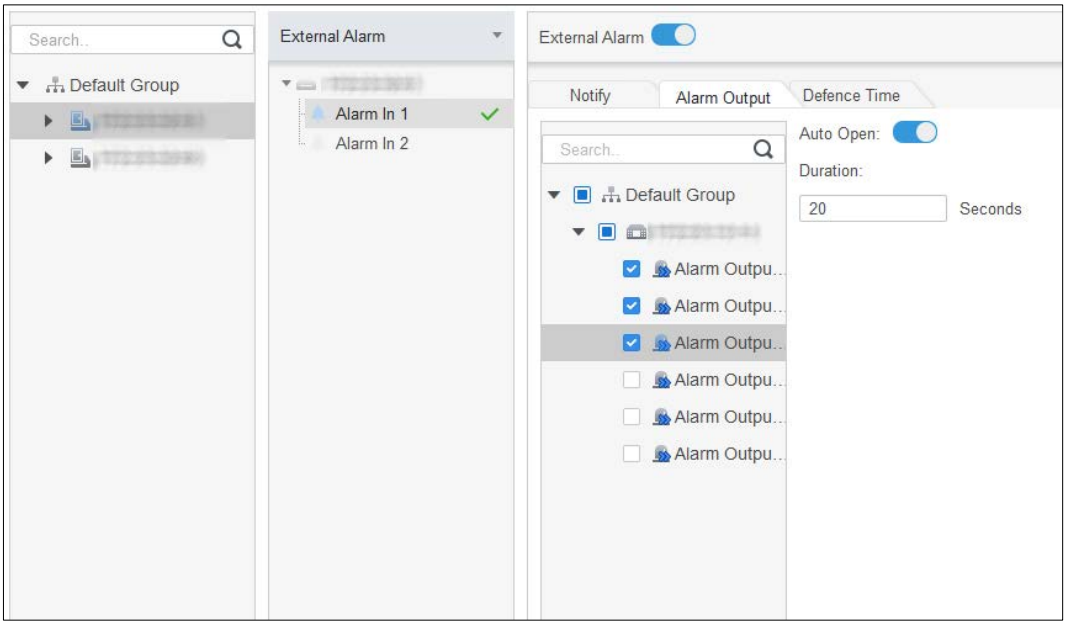
2) Seleccione el dispositivo que admita entrada de alarma, seleccione la interfaz de entrada de alarma y luego habilite **Alarma externa**.

3) Seleccione el dispositivo que admita salida de alarma, luego seleccione la interfaz de salida de alarma.

4) Habilitar**Apertura automática**para el enlace de alarma.

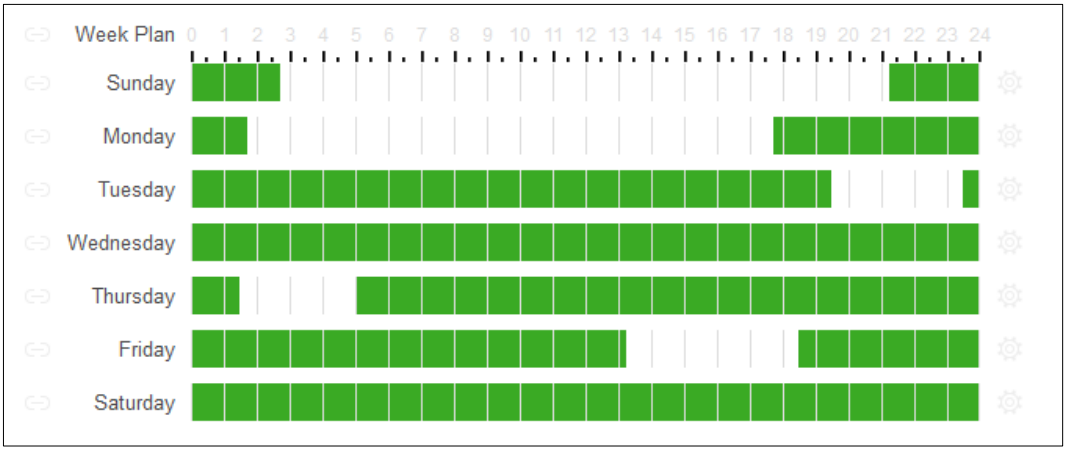
5) Establecer la duración.

Figure 3-31 Configurar enlace de alarma



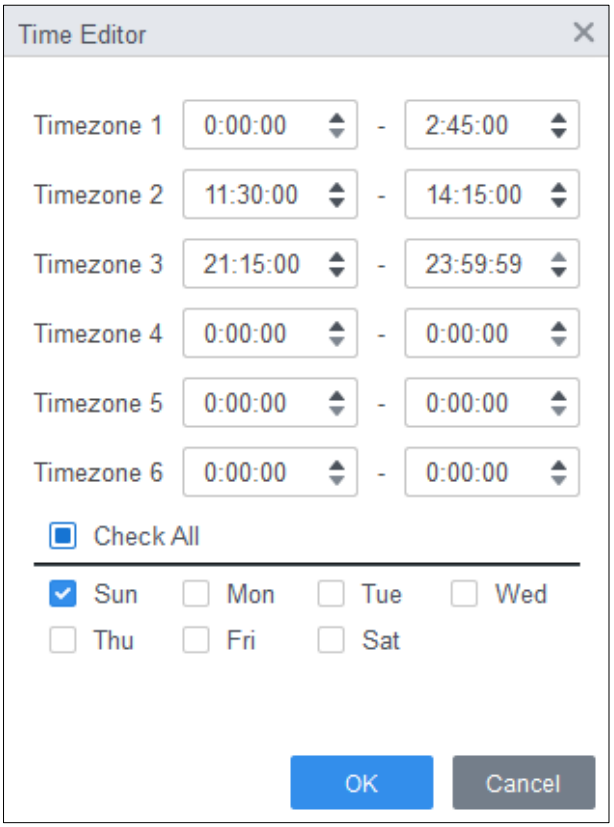
- Establecer el tiempo de armado. Hay dos métodos.
  - Método 1: Mueva el cursor para establecer períodos. Cuando el cursor es un lápiz, haga clic para agregar puntos; cuando el cursor es borrador, haga clic para eliminar puntos. El área verde son los períodos de armado

Figure 3-32 Establecer el tiempo de armado (método 1)



-Método 2: haga clic  para establecer períodos y, a continuación, haga clic en**DE ACUERDO**.

Figure 3-33 Establecer el tiempo de armado (método 2)



Step 5 (Opcional) Si desea configurar los mismos períodos de armado para otro controlador de acceso, haga clic en**Copiar a**, seleccione el controlador de acceso y luego haga clic en**DE ACUERDO**. Hacer clic**Guardar**.

Step 6

4 Configuración de la herramienta de configuración

ConfigTool se utiliza principalmente para configurar y mantener el dispositivo.

No use ConfigTool y SmartPSS AC al mismo tiempo, de lo contrario puede causar resultados anormales cuando buscas dispositivos.

4.1 Inicialización

Antes de la inicialización, asegúrese de que el controlador y la computadora estén en la misma red.

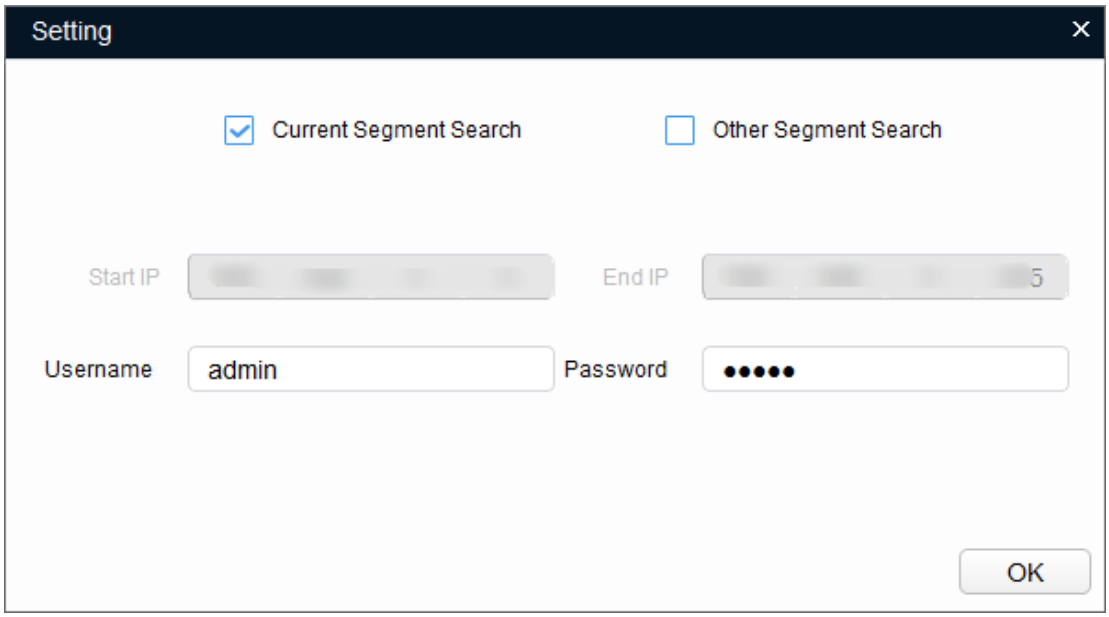
Step 1 Busque el controlador a través de ConfigTool. 1)

Haga doble clic en ConfigTool para abrirlo.

2) Haga clic**Configuración de búsqueda**, ingrese el rango del segmento de red y luego haga clic en Aceptar.

3) Seleccione el controlador no inicializado y luego haga clic en Inicializar.

Figure 4-1 Buscar el dispositivo



Step 2 Seleccione el controlador no inicializado y luego haga clic en**Inicializar.** Hacer clic**DE**

Step 3 **ACUERDO**.

El sistema inicia la inicialización. indica el éxito de la inicialización, indica inicialización falló.

Step 4 Hacer clic**Terminar**.

4.2 Adición de dispositivos

Puede agregar uno o varios dispositivos según sus necesidades reales.

Asegúrese de que el dispositivo y la PC donde está instalado ConfigTool estén conectados; de lo contrario el

La herramienta no puede encontrar el dispositivo.

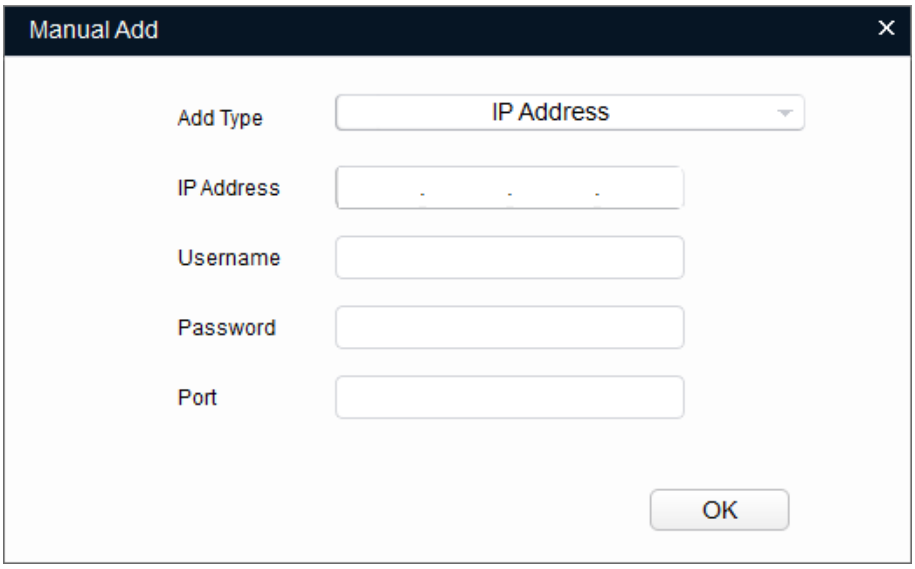
4.2.1 Agregar dispositivo individualmente

Step 1 Hacer clic .

Step 2 Hacer clic**Adición manual**.

Step 3 Seleccione**Dirección IP**desde**Añadir tipo**.

Figure 4-2 Adición manual (dirección IP)



Step 4 Configure los parámetros del controlador.

Tabla 4-1 Parámetros de adición manual

Añadir método	Parámetro	Descripción
Dirección IP	Dirección IP	La dirección IP del dispositivo. Es 192.168.1.108 por defecto.
	Nombre de usuario	El nombre de usuario y la contraseña para iniciar sesión en el dispositivo.
	Clave	
	Puerto	El número de puerto del dispositivo.

Step 5 Hacer clic**DE ACUERDO**.

El dispositivo recién agregado se muestra en la lista de dispositivos.

4.2.2 Adición de dispositivos en lotes

Puede agregar varios dispositivos mediante la búsqueda de dispositivos o la importación de la plantilla.

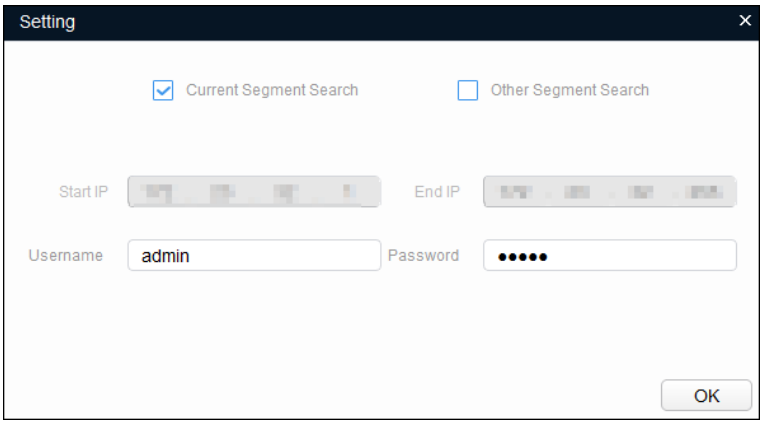
4.2.2.1 Adición mediante búsqueda

Puede agregar varios dispositivos buscando en el segmento actual o en otros segmentos.

Puede establecer las condiciones de filtrado para buscar rápidamente el dispositivo deseado.

Step 1 Hacer clic Search setting.

Figure 4-3 Entorno



Step 2 Seleccione la forma de búsqueda. Las dos formas siguientes se seleccionan de forma predeterminada.

- Buscar segmento actual

  Seleccione**Búsqueda de segmento actual**. Introduzca el nombre de usuario y la contraseña. El sistema buscará los dispositivos correspondientes.

- Buscar otro segmento

  Seleccione**Búsqueda de otro segmento**. Ingrese la dirección IP inicial y la dirección IP final. Introduzca el nombre de usuario y la contraseña. El sistema buscará los dispositivos correspondientes.

- Si selecciona ambos**Búsqueda de segmento actual**y**Búsqueda de otro segmento**, el sistema busca dispositivos en ambos segmentos.
- El nombre de usuario y la contraseña son los que se utilizan para iniciar sesión cuando desea modificar IP, configure el sistema, actualice el dispositivo, reinicie el dispositivo y más.

Step 3 Hacer clic**DE ACUERDO**para comenzar a buscar dispositivos.

Los dispositivos buscados se mostrarán en la lista de dispositivos.

- Hacer clic para actualizar la lista de dispositivos.
- El sistema guarda las condiciones de búsqueda al salir del software y reutiliza las mismas condiciones cuando se inicie el software la próxima vez.

4.2.2.2 Adición mediante importación de plantilla de dispositivo

Puede agregar los dispositivos importando una plantilla de Excel. Puede importar hasta 1000 dispositivos.

Cierre el archivo de plantilla antes de importar los dispositivos; de lo contrario, la importación fallará.

Step 1 Hacer clic , seleccione un dispositivo y luego haga clic en**Exportar**para exportar una plantilla de dispositivo.

Step 2 Siga las instrucciones en pantalla para guardar el archivo de plantilla localmente.

Step 3 Abra el archivo de plantilla, cambie la información del dispositivo existente a la información de los dispositivos que desea agregar.

Step 4 Importar la plantilla. Hacer clic**Importar**, seleccione la plantilla y haga clic en**Abierto**. El sistema comienza a importar los dispositivos.

Step 5 Hacer clic**DE ACUERDO**.

Los dispositivos recién importados se muestran en la lista de dispositivos.

4.3 Configuración del controlador de acceso

Las capturas de pantalla y los parámetros pueden ser diferentes según los tipos y modelos de dispositivos.

Step 1 Hacer clic en el menú principal.

Step 2 Haga clic en el controlador de acceso que desea configurar en la lista de dispositivos y luego haga clic en**Obtener información del dispositivo**.

Step 3 (Opcional) Si aparece la página de inicio de sesión, ingrese el nombre de usuario y la contraseña, y luego haga clic en**DE ACUERDO**.

Step 4 Establecer los parámetros del controlador de acceso.

Figure 4-4 Configurar controlador de acceso

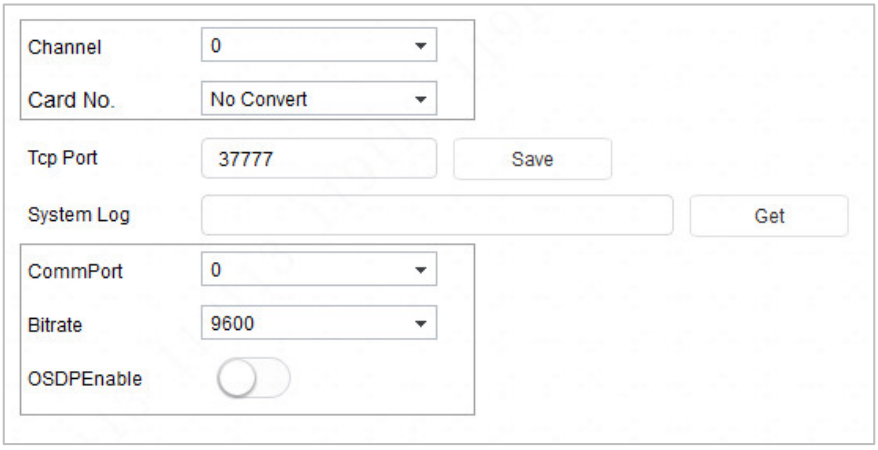


Tabla 4-2 Parámetros del controlador de acceso

Parámetro	Descripción
Canal	Seleccione el canal para configurar los parámetros.
número de tarjeta	Configure la regla de procesamiento del número de tarjeta del controlador de acceso. Está**Sin conversión**por defecto. Cuando el resultado de la lectura de la tarjeta no coincida con el número de tarjeta real, seleccione **Reversión de bytes**o**Convertir HIDpro**. ● **Reversión de bytes**: Cuando el controlador de acceso funciona con lectores de terceros y el número de tarjeta leído por el lector de tarjetas está en orden inverso al número de tarjeta real. Por ejemplo, el número de tarjeta leído por el lector de tarjetas es hexadecimal 12345678 mientras que el número de tarjeta real es hexadecimal 78563412, y puede seleccionar**Reversión de bytes**.

Parámetro	Descripción
	• **Convertir HIDpro**: Cuando el controlador de acceso funciona con lectores HID Wiegand y el número de tarjeta leído por el lector de tarjetas coincide con el número de tarjeta real, puede seleccionar HIDpro Revert para que coincidan. Por ejemplo, el número de tarjeta leído por el lector de tarjetas es hexadecimal 1BAB96 mientras que el número de tarjeta real es hexadecimal 78123456,
Puerto TCP	Modifique el número de puerto TCP del dispositivo.
Registro del sistema	Hacer clic**Conseguir**para seleccionar una ruta de almacenamiento para los registros del sistema.
Puerto de comunicaciones	Seleccione el lector para establecer la tasa de bits y habilitar OSDP.
tasa de bits	Si la lectura de la tarjeta es lenta, puede aumentar la tasa de bits. Es 9600 por defecto.
Habilitar OSDP	Cuando el controlador de acceso funciona con lectores de terceros a través del protocolo ODSP, habilite ODSP.

Step 5 (Opcional) Haga clic en**Aplicar para**, seleccione los dispositivos con los que necesita sincronizar los parámetros configurados y luego haga clic en**Configuración**.

Si tiene éxito, se muestra en el lado derecho del dispositivo; si falla, puede hacer se visualiza. Tú clic en el icono para ver información detallada.

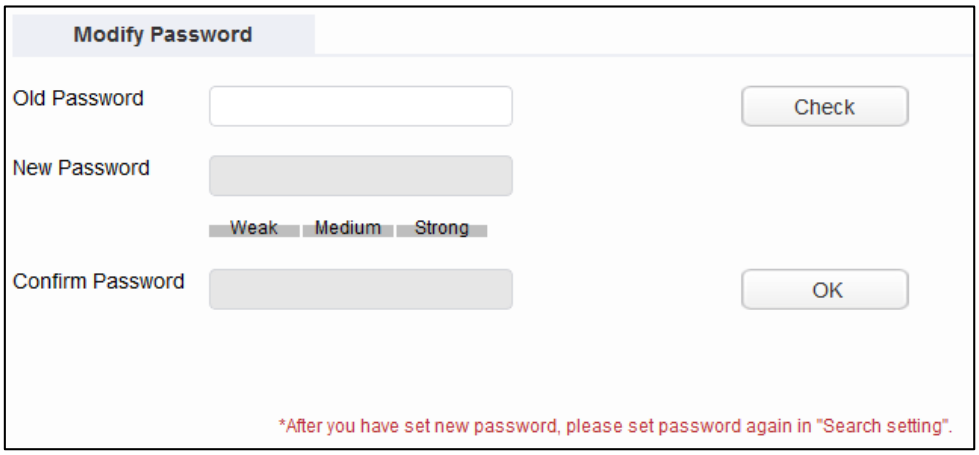
4.4 Cambiar la contraseña del dispositivo

Puede modificar la contraseña de inicio de sesión del dispositivo.

Step 1 Hacer clic en la barra de menú.

Step 2 Haga clic en el**Contraseña del dispositivo**pestaña.

Figure 4-5 Contraseña del dispositivo



Step 3 Hacer clic junto al tipo de dispositivo y luego seleccione uno o varios dispositivos.

Si selecciona varios dispositivos, las contraseñas de inicio de sesión deben ser las mismas.

Step 4 Establezca la contraseña.

Siga la sugerencia del nivel de seguridad de la contraseña para establecer una nueva contraseña.

Tabla 4-3 Parámetros de contraseña

Parámetro	Descripción
Contraseña anterior	Introduzca la contraseña antigua del dispositivo. Para asegurarse de que la contraseña anterior se ingresó correctamente, puede hacer clic en**Cheque**para verificar.
Nueva contraseña	Introduzca la nueva contraseña para el dispositivo. Hay una indicación de la seguridad de la contraseña. La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excepto ' " ; : &).
confirmar Contraseña	Confirme la nueva contraseña.

Step 5 Hacer clic**DE ACUERDO**para completar la modificación.

Appendix 1 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 presentan algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias a tomar para la seguridad de la red de equipos básicos: 1.

Usar contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de caracteres; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;
- No contenga 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 del cliente a tiempo

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

Recomendaciones "agradables de tener" para mejorar la seguridad de su red de equipos: 1. Protección física

Le sugerimos que realice protección física a los equipos, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en un gabinete y una sala de computadoras especiales, e implemente un control de permisos y administración de claves bien hecho para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, conectar equipos extraíbles (como discos flash USB, puerto), etc

2. Cambie las contraseñas regularmente

Le sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinadas o descifradas.

3. Establezca y actualice la información de restablecimiento de contraseñas a tiempo

El equipo 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 de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección de contraseña, se sugiere no utilizar aquellas que se pueden adivinar fácilmente.

4. Habilitar 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 varias veces con la contraseña incorrecta, 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 a cualquier conjunto de números entre 1024 y 65535, lo que reduce el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.

6. Habilitar 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 vincular la dirección IP y MAC de la puerta de enlace al equipo, reduciendo así el riesgo de suplantación de ARP.

8. Asigne cuentas y privilegios de manera razonable

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios razonablemente 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.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de encriptación WPA2-PSK y configure contraseñas seguras.

10. Transmisión encriptada de audio y video

Si el contenido de sus datos de audio y video es muy importante o confidencial, 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 encriptada causará cierta pérdida en la eficiencia de la transmisión.

11. Auditoría segura

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

12. Registro de red

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

13. Construya un entorno de red seguro

Para garantizar mejor la seguridad de los equipos y reducir los posibles riesgos cibernéticos, recomendamos:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de 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 usar VLAN, GAP de red 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 que pueden acceder al dispositivo.