Controlador de acceso (C)

Manual de usuario

V1.0.2

Prefacio

General

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

Instrucciones de seguridad

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

Palabras de advertencia	Significado
PELIGRO	Indica un alto riesgo 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, reducciones en el rendimiento o resultados impredecibles.
CONSEJOS	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
NOTA	Proporciona información adicional como complemento al texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.2	Imagen de cableado actualizada.	junio 2022
V1.0.1	Proceso de inicialización agregado.	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 otras personas, 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 proporcionar la información de contacto requerida.

Acerca del Manual

- El manual es sólo para referencia. Pueden encontrarse ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas incurridas 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 regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es sólo para referencia. Es posible que se encuentren ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones de productos pueden provocar que aparezcan algunas diferencias entre el producto real y el manual. Comuníquese con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Pueden existir 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 otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en este manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si ocurre algún problema durante el uso del Controlador.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de dar una explicación final.

Salvaguardias y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del Controlador, prevención de riesgos, y prevención de daños a la propiedad. Lea atentamente antes de utilizar el Controlador, cumpla con las siga las pautas al usarlo y guarde el manual en un lugar seguro para consultarlo en el futuro.

Requisito de transporte

Transporte el controlador en condiciones permitidas de humedad y temperatura.

Requisito de almacenamiento

Guarde el controlador en condiciones permitidas de humedad y temperatura.

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 al Controlador.
- El uso inadecuado de la batería podría provocar un incendio o una explosión.

- El personal que trabaja en alturas debe tomar todas las medidas necesarias para garantizar la 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 sobre 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 fuente de alimentación de gabinete proporcionado 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 el estándar IEC 62368-1 y no ser más alto que PS2. Tenga en cuenta que los requisitos de suministro de energía 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 protección a tierra.

- El controlador debe estar conectado a tierra cuando esté conectado a una red eléctrica de 220 V.

Tabla de contenido

1.1 Introducción

El Controlador es un panel de control de acceso que compensa la videovigilancia y el intercomunicador visual. Tiene un diseño limpio y moderno con una gran funcionalidad, adecuado para edificios comerciales de alto nivel, propiedades grupales y comunidades inteligentes.

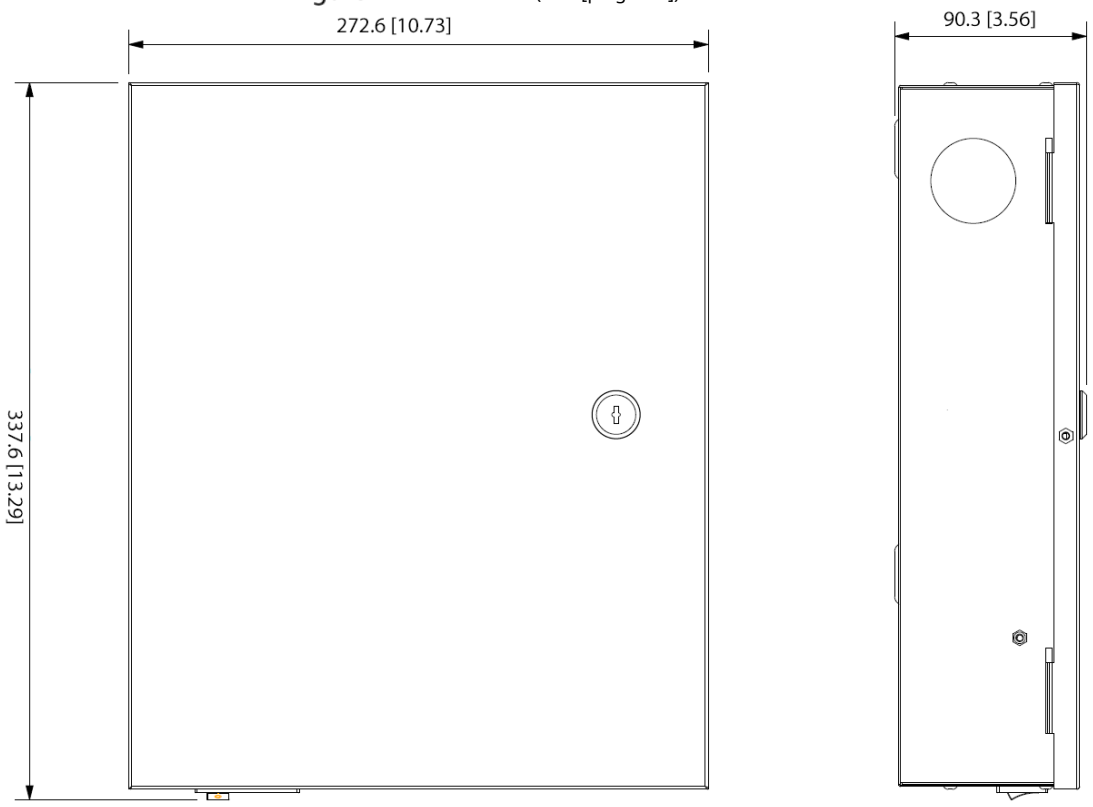
1.1 Características

- Adopta un tablero de acero SEEC para brindar una apariencia de alta gama.
- Admite comunicación de red TCP/IP. Los datos de comunicación están cifrados por seguridad. Registro
- automático.
- Soporta protocolo OSDP.
- Admite desbloqueo de tarjeta, contraseña y huella digital.
- Admite 100.000 usuarios, 100.000 tarjetas, 3.000 huellas dactilares y 500.000 registros.
- Admite interbloqueo, anti-passback, desbloqueo multiusuario, desbloqueo de 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 tarjeta no válida que excede el umbral, 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 funciones integradas de RTC, calibración de hora NTP, calibración de hora manual y calibración de hora automática.
- Admite operación fuera de línea, funciones de carga y almacenamiento de registros de eventos y reabastecimiento automático 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 desbloqueo en períodos.
- Admite el mecanismo de vigilancia para garantizar la estabilidad de la operación.

1.2 Dimensiones

Hay cinco tipos de controladores de acceso, incluidos unidireccional de dos puertas, unidireccional de dos puertas, unidireccional de cuatro puertas, unidireccional de cuatro puertas y unidireccional de ocho puertas. Sus dimensiones son las mismas.

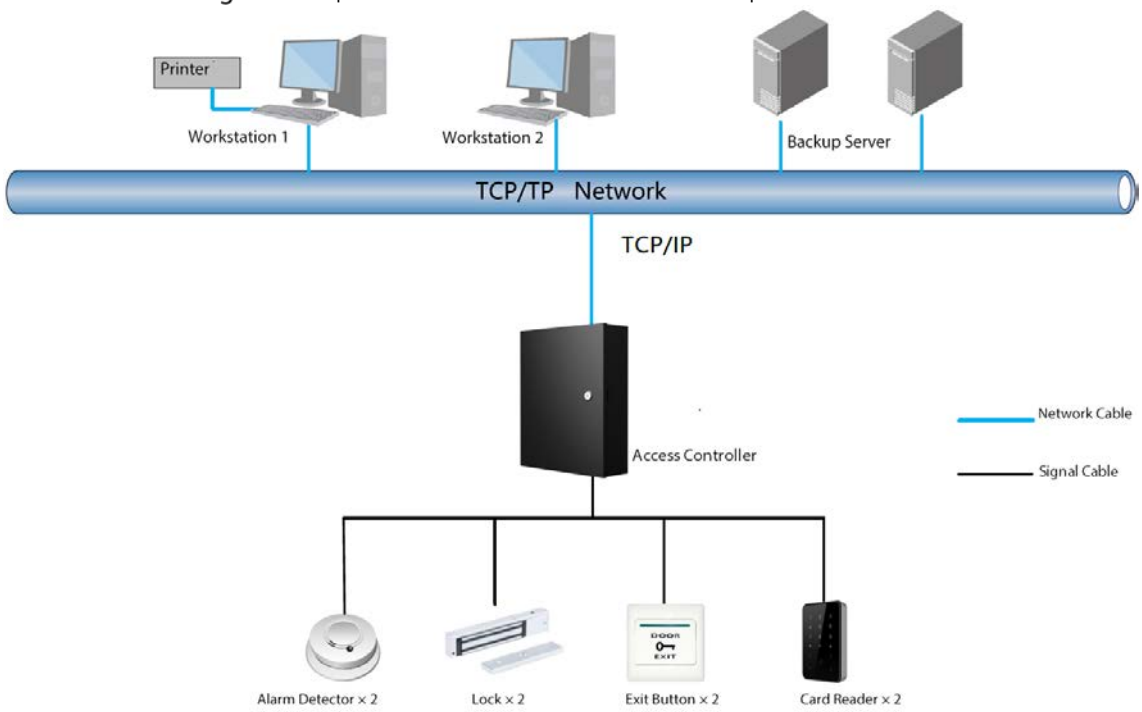
Figure 1-1 Dimensiones (mm [pulgadas])



1.3 Solicitud

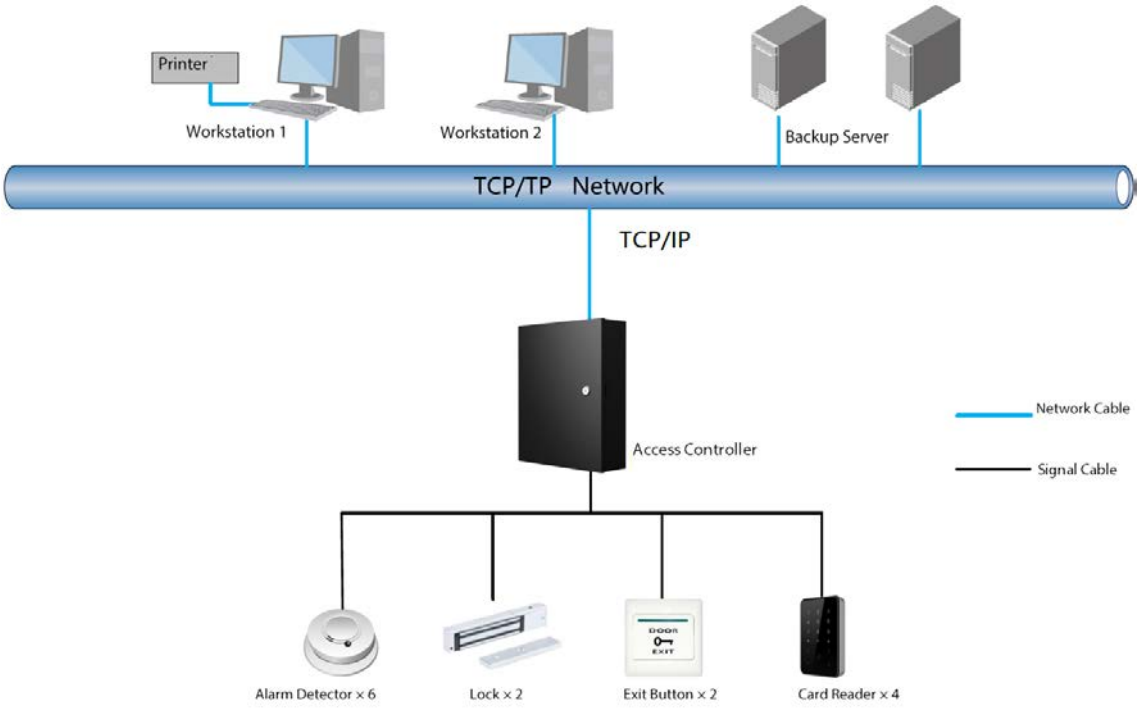
1.3.1 Unidireccional de dos puertas

Figure 1-2 Aplicación del controlador unidireccional de dos puertas



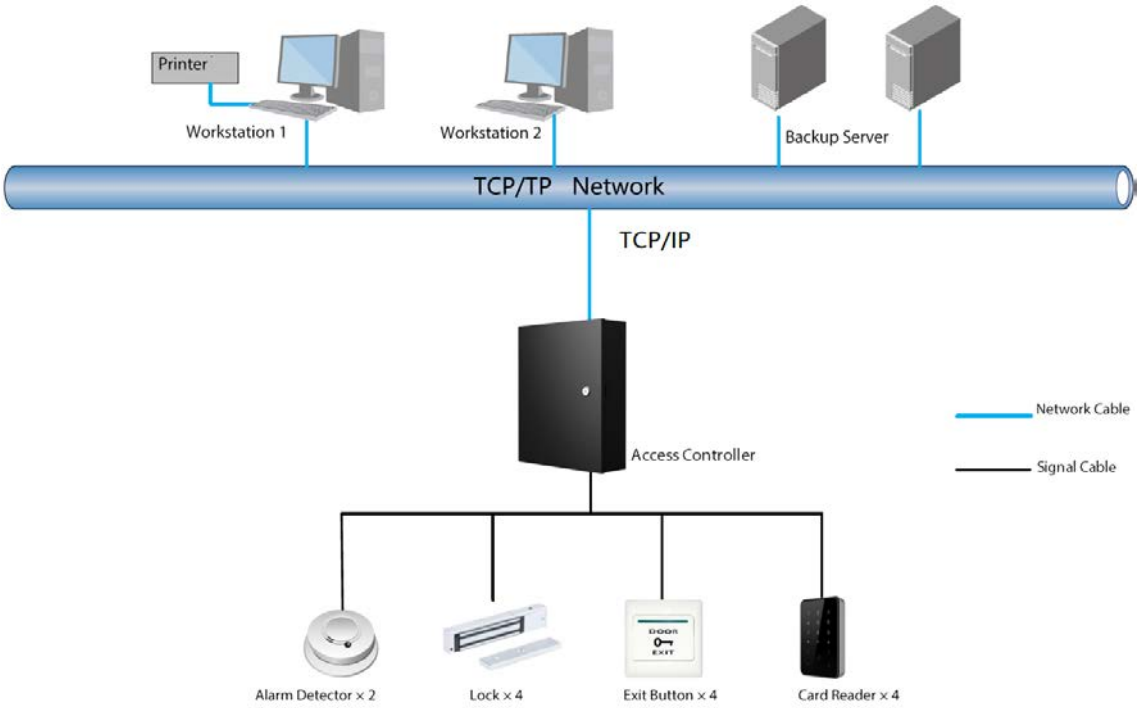
1.3.2 Dos puertas Bidireccional

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



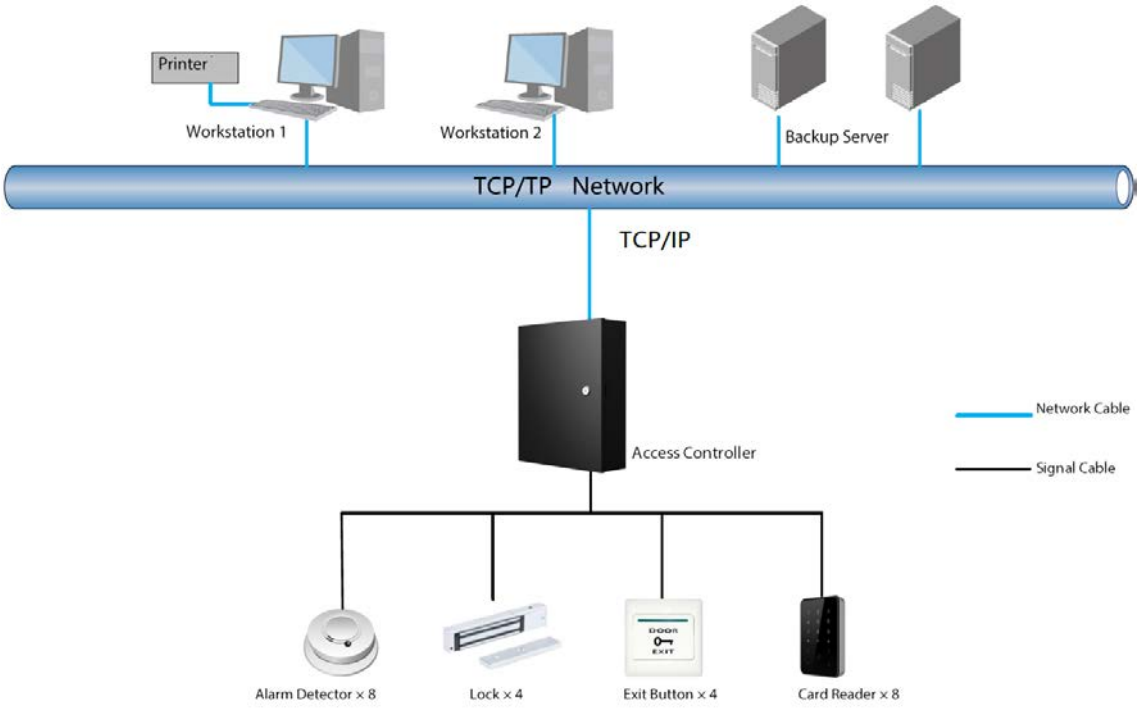
1.3.3 Unidireccional de cuatro puertas

Figure 1-4 Aplicación del controlador unidireccional de cuatro puertas



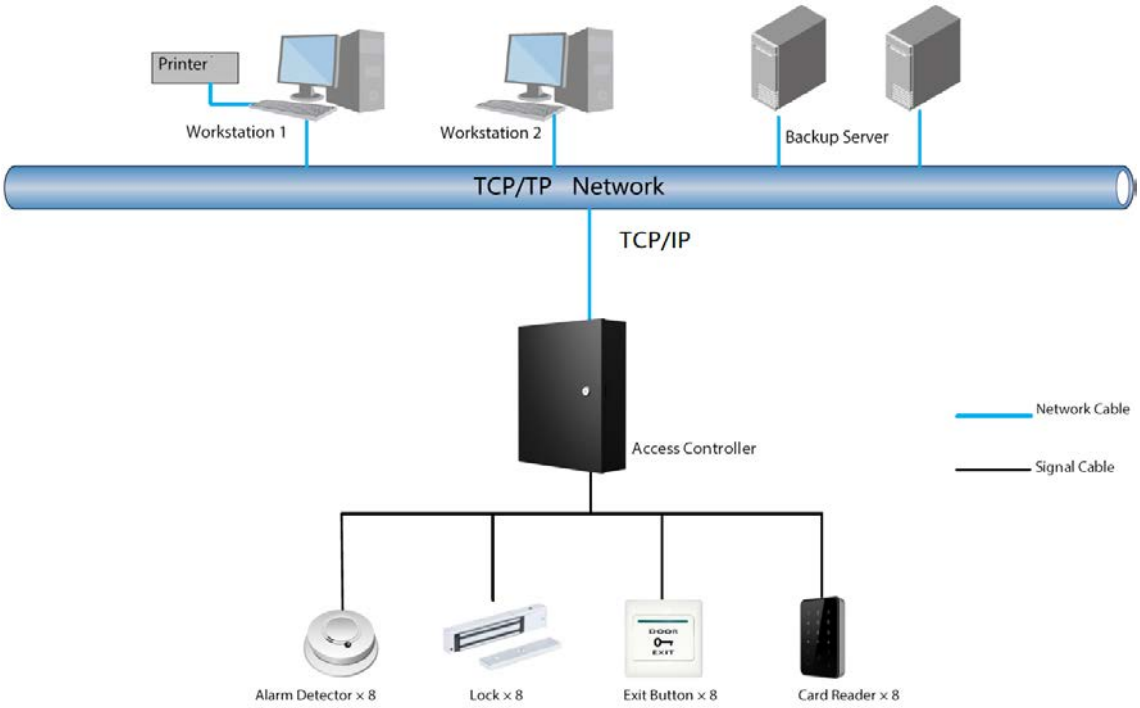
1.3.4 Bidireccional de cuatro puertas

Figure 1-5 Aplicación del controlador bidireccional de cuatro puertas



1.3.5 Unidireccional de ocho puertas

Figure 1-6 Aplicación del controlador unidireccional de ocho puertas



2 Estructura

2.1 Alambrado

⚠

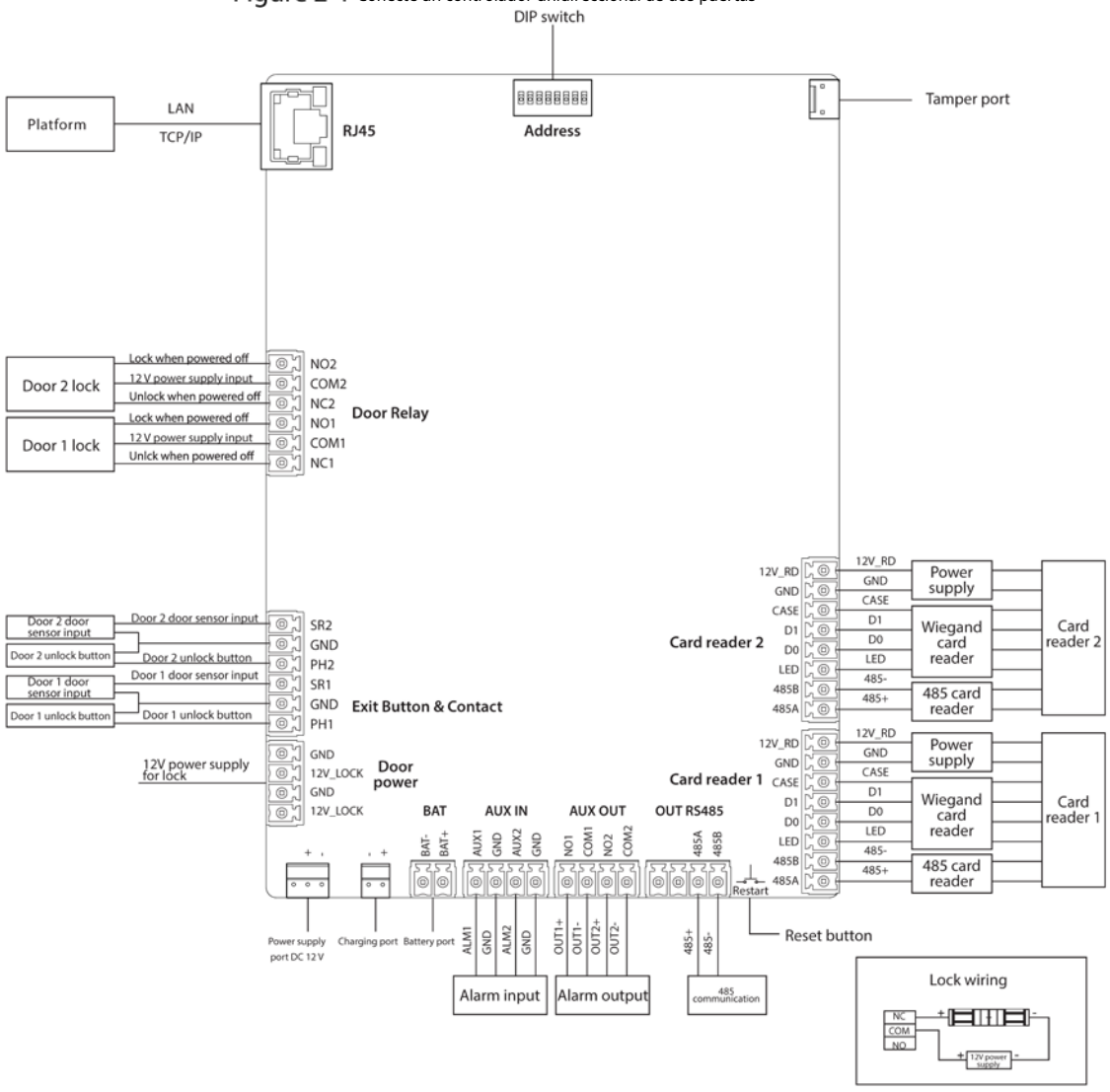
- Conecte los cables sólo cuando esté apagado.
- Asegúrese de que el enchufe de la fuente de alimentación esté conectado a
- tierra. 12 V: la corriente máxima para un módulo de extensión es 100 mA. 12
- V_RD: La corriente máxima para un lector de tarjetas es 2,5 A.
- 12 V_LOCK: La corriente máxima para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

Tabla 2-1 Especificación del cable

Dispositivo	Cable
Lector de tarjetas	Cat5 tw blindado de 8 núcleos
Cable de ethernet	Cat5 tw blindado de 8 núcleos
Botón	2 núcleos
Contacto de puerta	2 núcleos

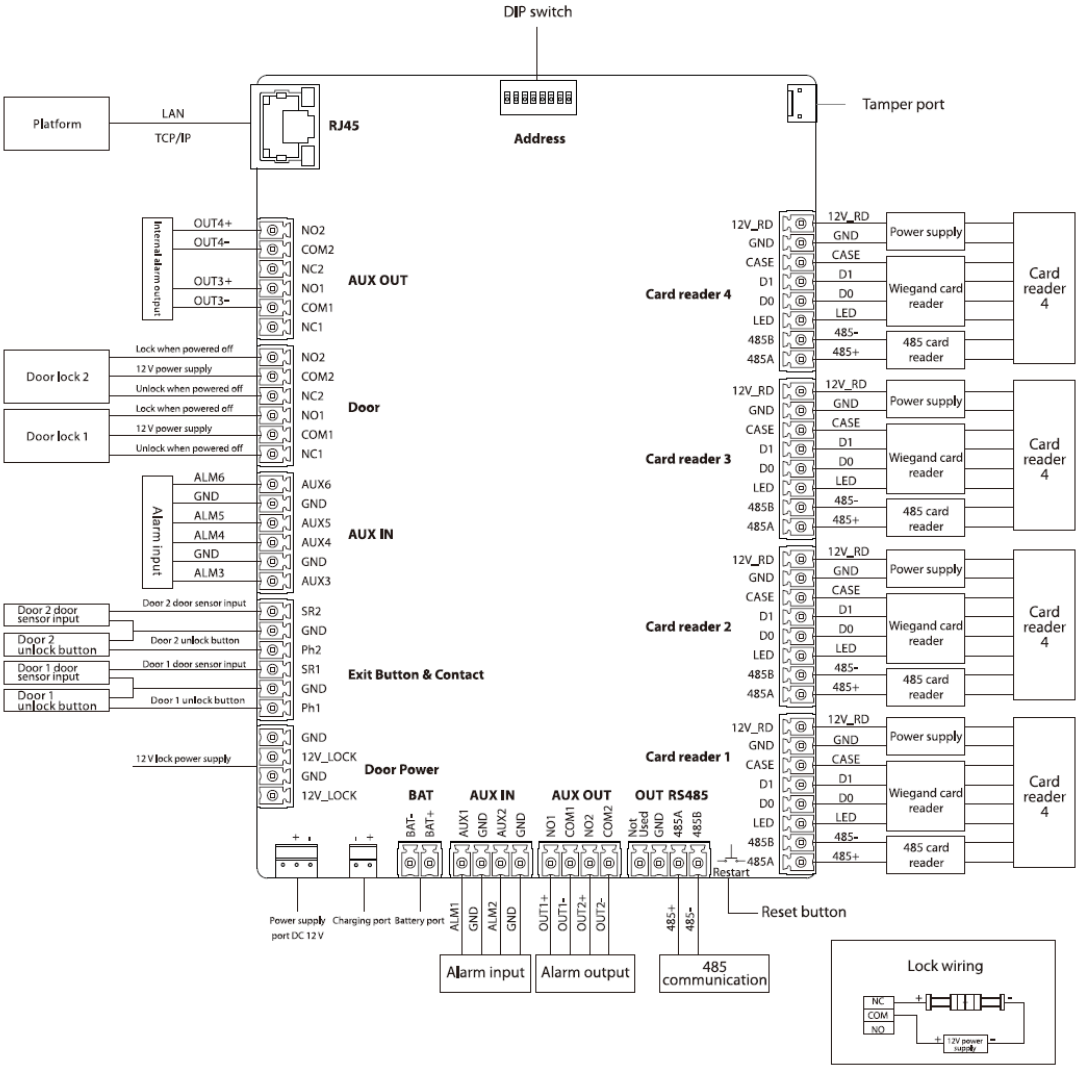
2.1.1 Unidireccional de dos puertas

Figure 2-1 Conecte un controlador unidireccional de dos puertas



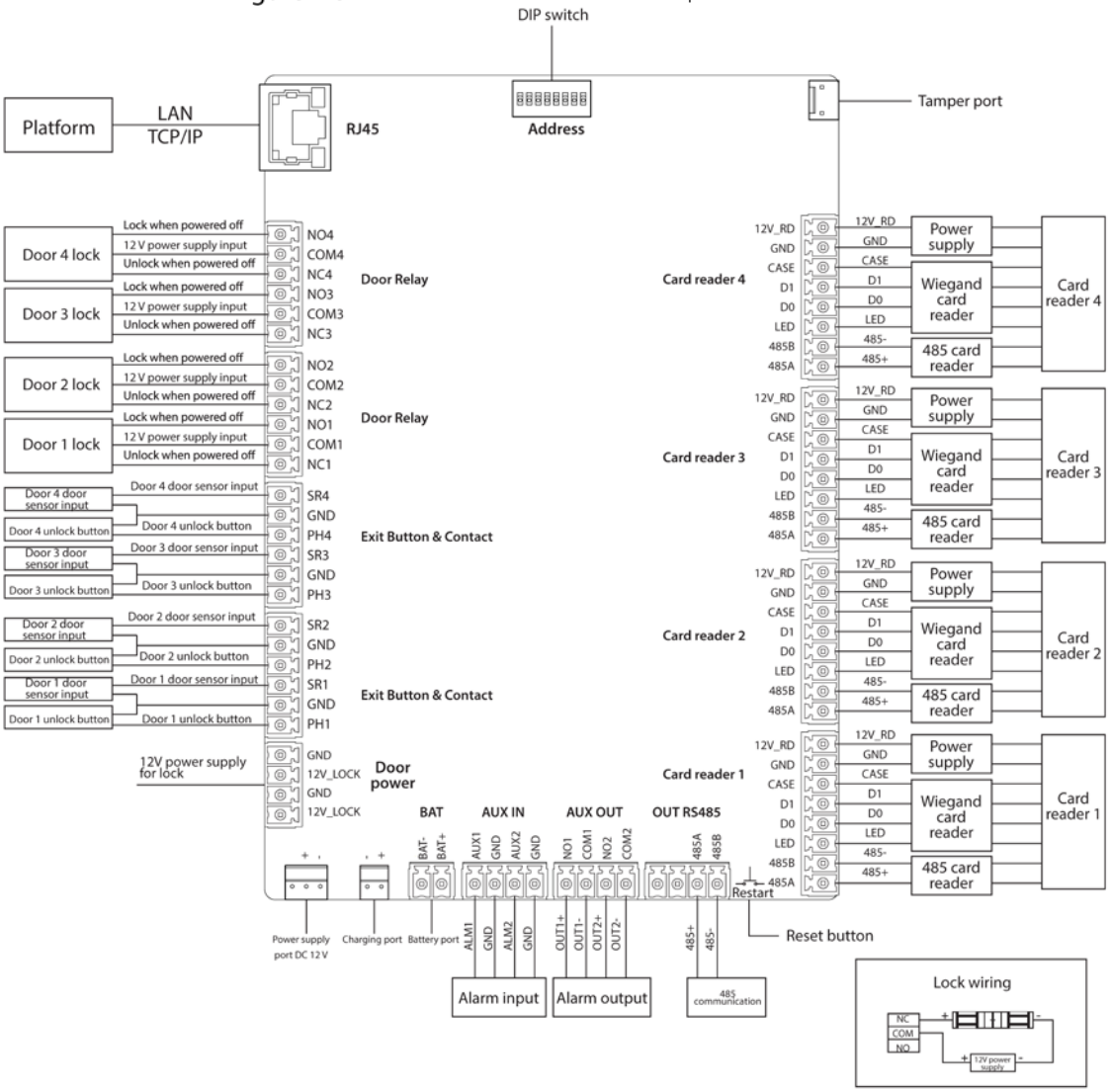
2.1.2 Dos puertas Bidireccional

Figure 2-2 Conecte un controlador bidireccional de dos puertas



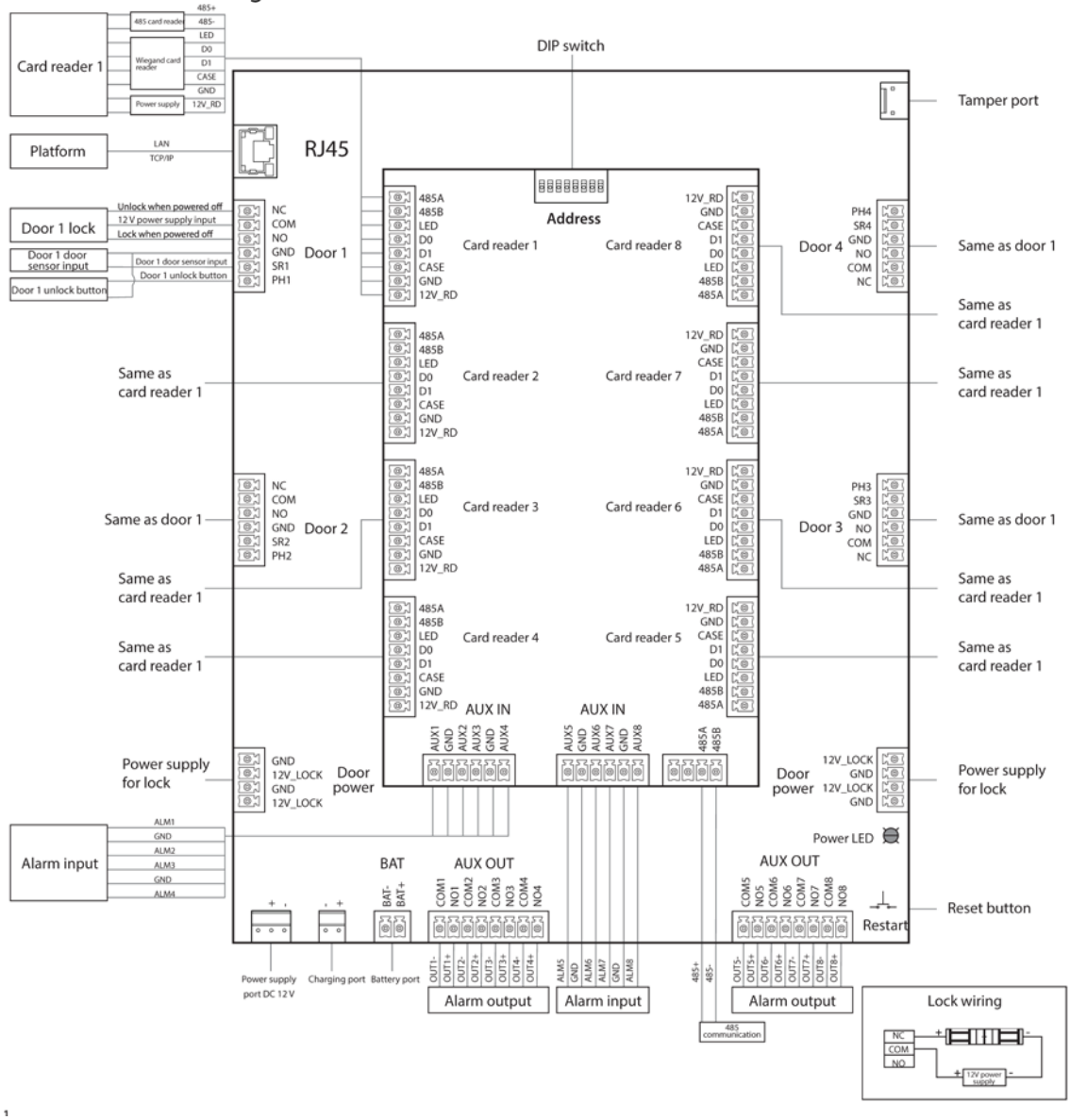
2.1.3 Unidireccional de cuatro puertas

Figure 2-3 Conecte un controlador unidireccional de cuatro puertas



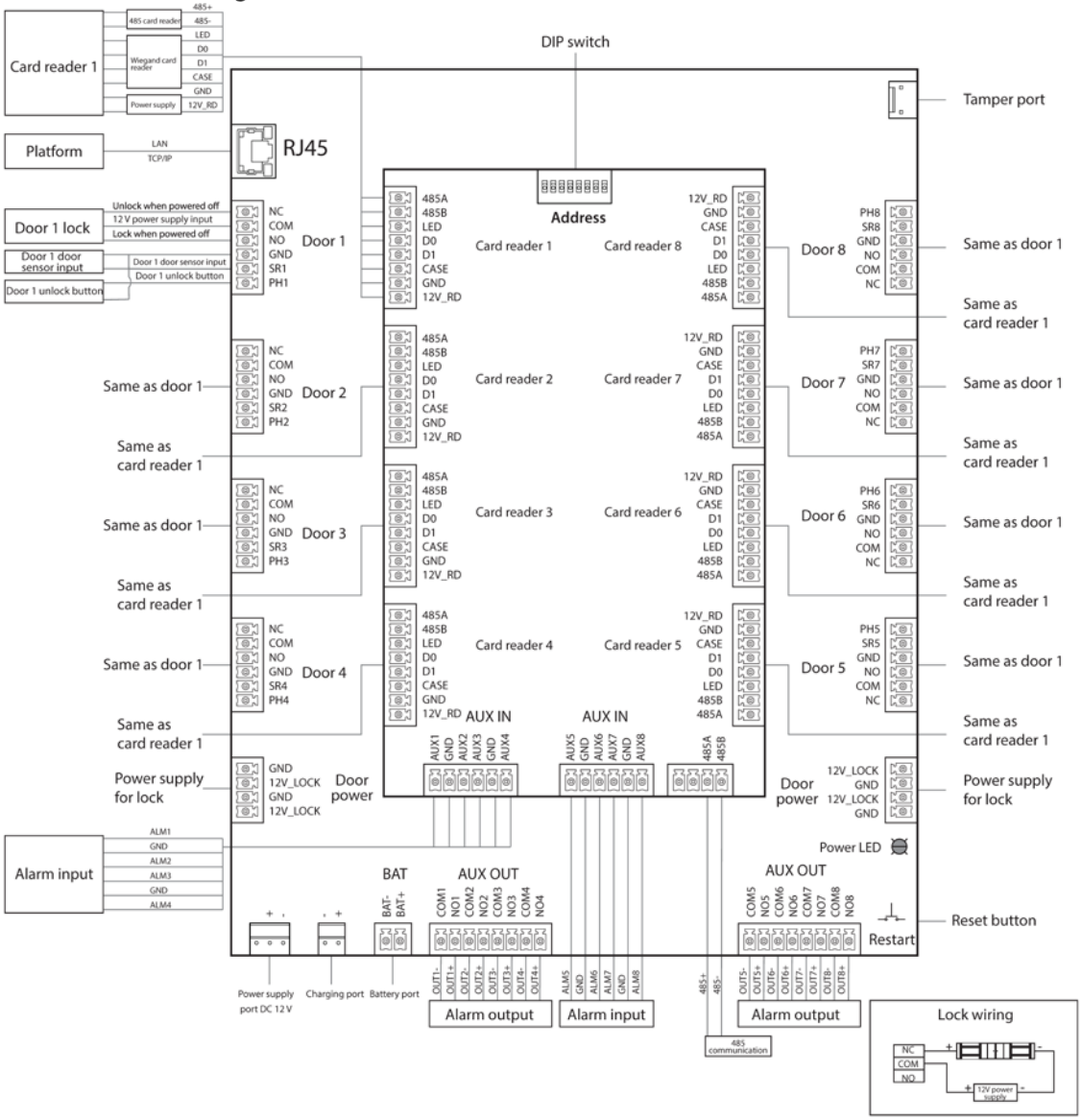
2.1.4 Bidireccional de cuatro puertas

Figure 2-4 Conecte un controlador bidireccional de cuatro puertas



2.1.5 Unidireccional de ocho puertas

Figure 2-5 Conecte un controlador unidireccional de ocho puertas



2.1.6 Bloquear

Seleccione el método de cableado según su tipo de cerradura.

Figure 2-6 cerradura electrica

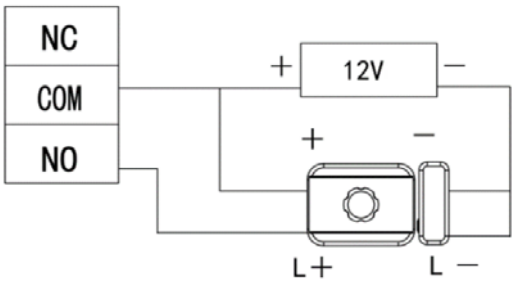


Figure 2-7 Cerradura magnética

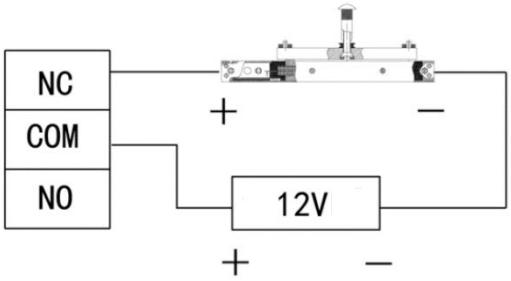
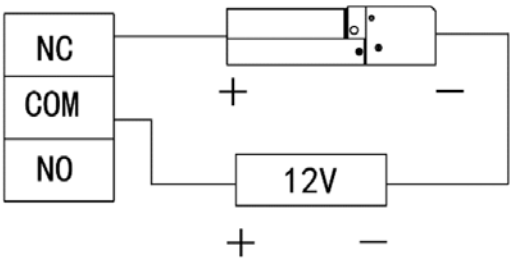


Figure 2-8 cerrojo electrico



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 externos AUX2 Normalmente cerrados para todas las puertas.
Dos puertas bidireccional	6	Estado de la puerta enlazable: ● Enlaces de alarma externa AUX1–AUX2 Normalmente abiertos para todas las puertas. ● Enlaces de alarma externos 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 externos AUX2 Normalmente cerrados para todas las puertas.
cuatro puertas bidireccional	8	Estado de la puerta enlazable: ● Enlaces de alarma externa AUX1–AUX2 Normalmente abiertos para todas las puertas. ● Enlaces de alarma externos 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 externos 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 de dos vías 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 de espera de puerta y salida de alarma de intrusión para la puerta 1. ● Lector de Tarjetas 1 salida de alarma de manipulación.
		COM1	
		NO2	● AUX2 activa la salida de alarma. ● Tiempo de espera de puerta y salida de alarma de intrusión para la puerta 2. ● Lector de tarjetas 2 salidas de alarma de manipulación.
		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 puerta 1 y salida de alarma de intrusión.
		COM1	
		NO1	
		NC2	● Lector de Tarjetas Salida de alarma antisabotaje 3/4. Tiempo de ● espera de 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 de espera 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 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 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 de manipulación. Tiempo ● de espera de puerta 3 y salida de alarma de intrusión.
		COM3	
		NO. 4	● AUX4 activa la salida de alarma. ● Lector de Tarjetas Salida de alarma antisabotaje 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 ● de manipulación. Tiempo de espera de 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 salidas de ● alarma de manipulación. Tiempo de espera de puerta 2 y salida ● de alarma de intrusión.
		NUMERO 3 COM3	● AUX3 activa la salida de alarma. Lector de tarjetas 3 salidas de ● alarma de manipulación. Tiempo de espera de puerta 3 y salida ● de alarma de intrusión.
		NO. 4 COM4	● AUX4 activa la salida de alarma. Lector de tarjetas 4 salidas de ● alarma de manipulación. 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 salidas de ● alarma de manipulación. 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 salidas de ● alarma de manipulación. 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 salidas de ● alarma de manipulación. 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 salidas de ● alarma de manipulación. Tiempo de espera de la puerta 8 y ● salida de alarma de intrusión.

2.1.9 Lector de tarjetas

En una puerta sólo se pueden conectar lectores de tarjetas del mismo tipo, ya sea RS-485 o Wiegand.

Tabla 2-4 Descripción de las especificaciones del cable del lector de tarjetas

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

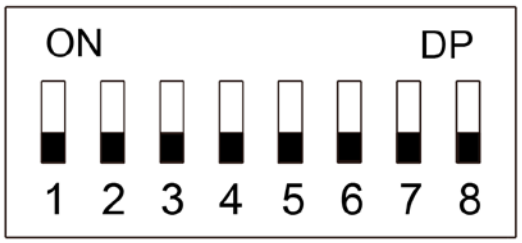
2.2 Indicador de encendido

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

2.3 Dip switch

 (ENCENDIDO) indica 1;  indica 0.

Figure 2-9 Dip switch



- Cuando 1–8 cambian a 0, el controlador se inicia normalmente después del encendido. Cuando
- 1–8 cambian a 1, el controlador ingresa al modo BOOT después de iniciarse.
- Cuando 1, 3, 5 y 7 cambian a 1 y los demás a 0, el controlador restaura 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 restaura los valores predeterminados de fábrica pero conserva la información del usuario después de reiniciarse.

2.4 Fuente de alimentación

2.4.1 Puerto de alimentación de la cerradura de la 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 alimentación 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, dos puertas, dos vías y 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 SmartPSS

Puede gestionar 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 de referencia y pueden diferir de las el producto real.

3.1 Acceso

Step 1 Instale el SmartPSS AC.

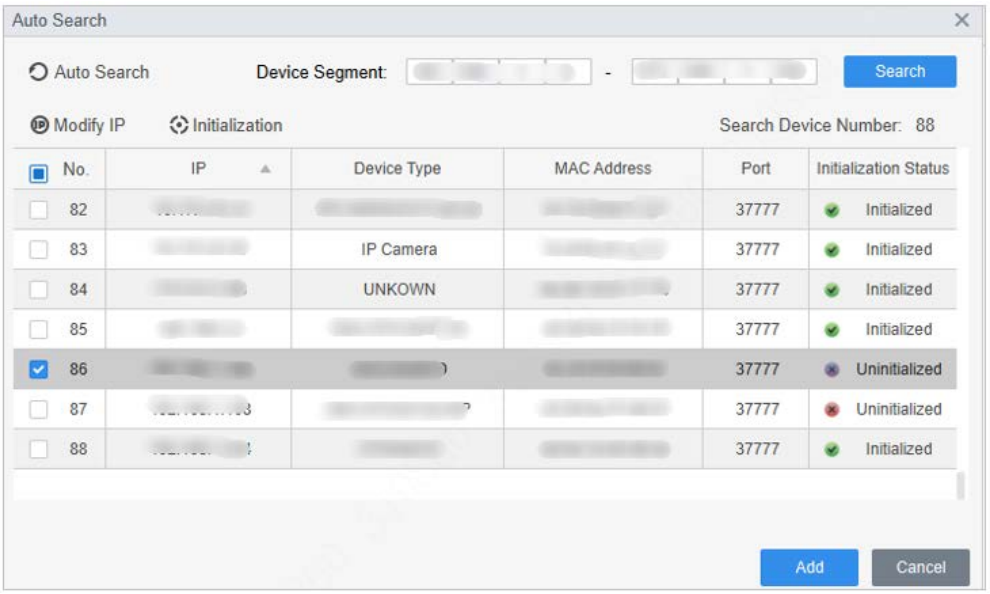
Step 2 Haga doble clic y luego siga las instrucciones para finalizar la inicialización e iniciar sesión.

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



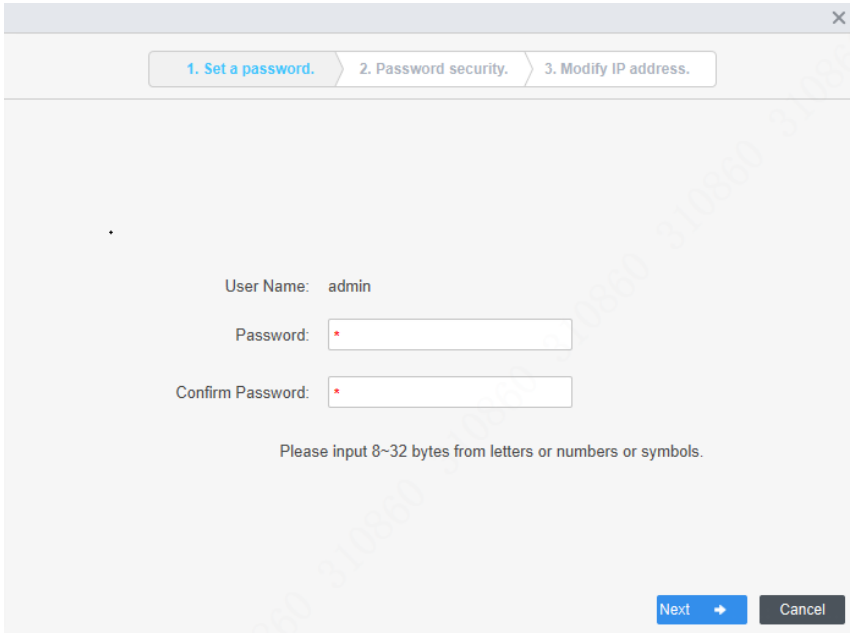
Step 2 Introduzca un rango de segmento de red y luego haga clic en**Buscar**.

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, utilice el interruptor DIP para restaurar los valores predeterminados de fábrica.

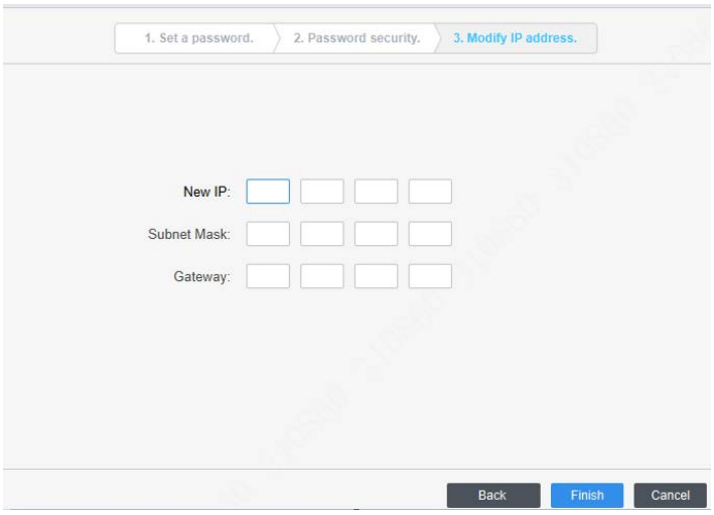
Figure 3-2 Configurar la clave



Step 5 Asocie el número de teléfono y luego haga clic en**Próximo**. Ingrese una

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

Figure 3-3 Modificar dirección IP



Step 7 Hacer clic**Finalizar**.

3.3 Agregar dispositivos

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

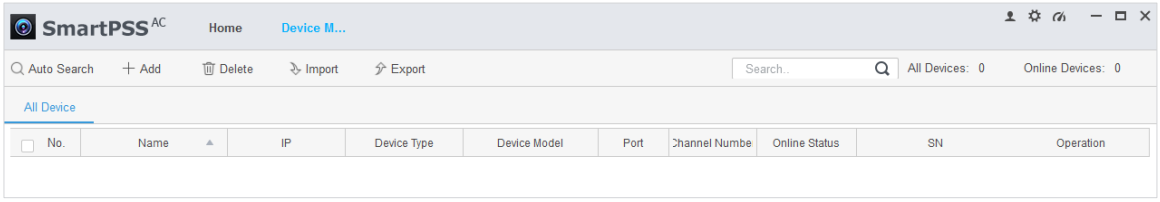
3.3.1 Búsqueda automática

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

Step 1 Inicie sesión en SmartPSS AC.

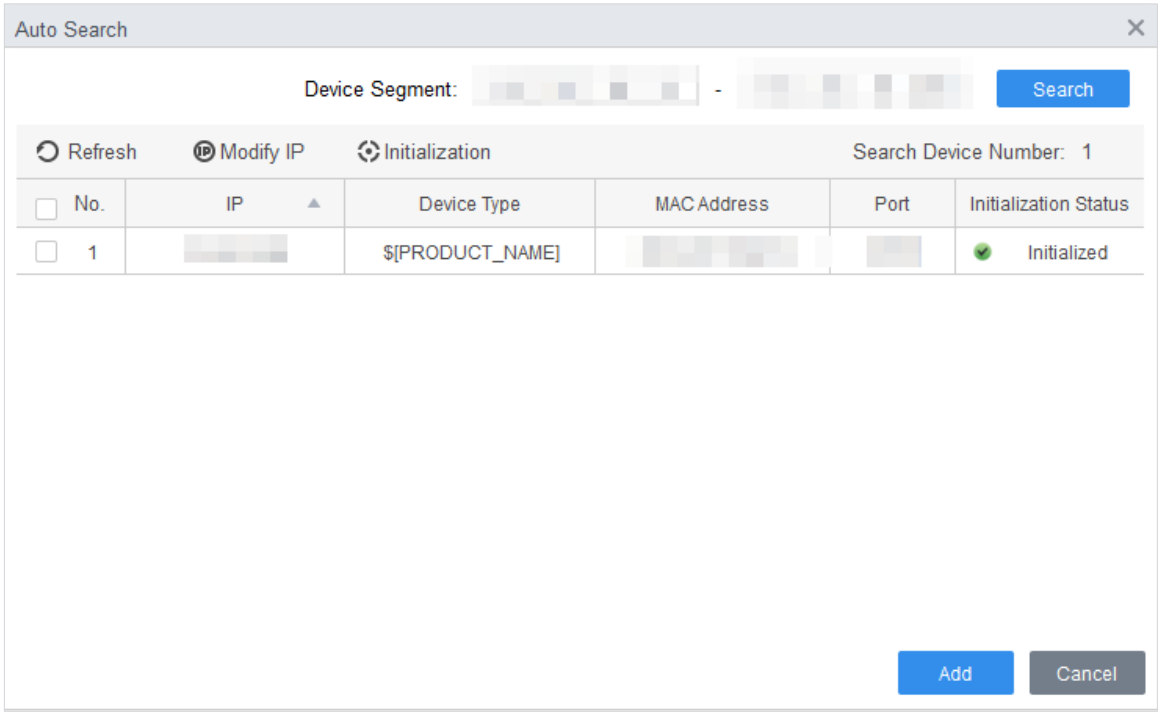
Step 2 Hacer clic**Administrador de dispositivos**en la esquina inferior izquierda.

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**Buscar**. Se mostrará una lista de resultados de búsqueda.

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

Step 5 Seleccione los dispositivos que desea agregar al 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 el**Dispositivos**página.

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

3.3.2 Agregar manualmente

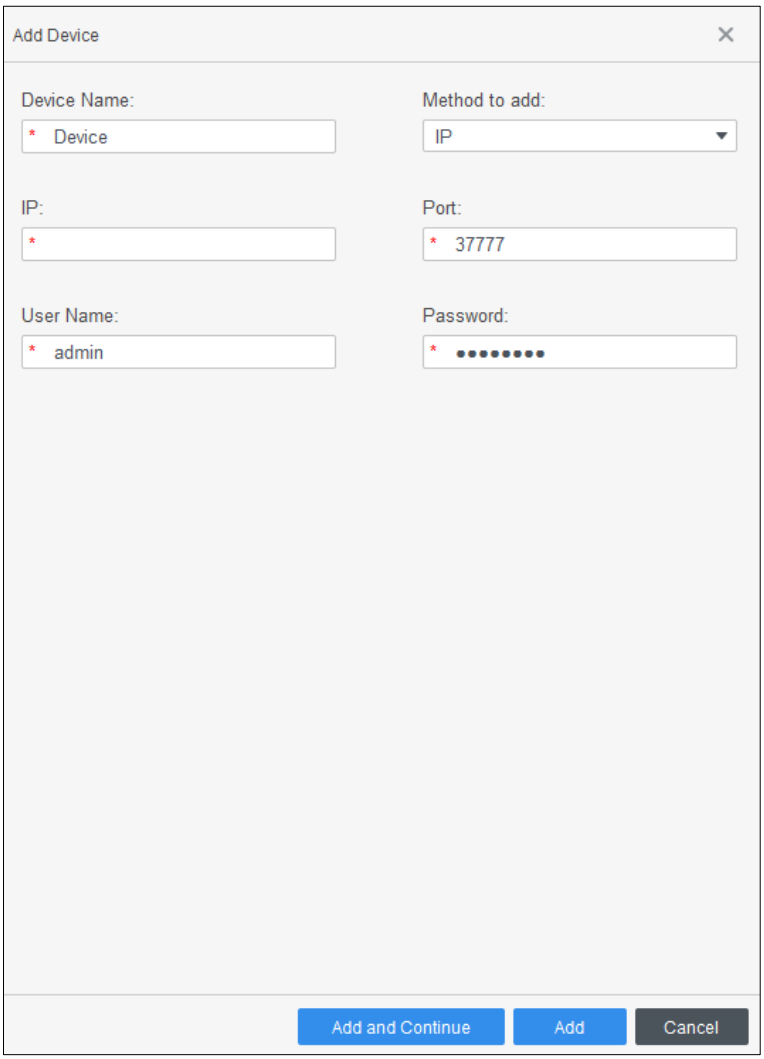
Puede agregar dispositivos manualmente. Necesita conocer las direcciones IP y los nombres de dominio de los controladores de acceso que desea agregar.

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 Agregar manualmente



Step 4 Ingrese información detallada del Responsable.

Tabla 3-1 Parámetros

Parámetro	Descripción
Nombre del dispositivo	Introduzca un nombre del controlador. Le recomendamos que nombre el controlador según su área de instalación para una fácil identificación.
Método para agregar	Seleccionar**IP**para agregar el controlador a través de la dirección IP.
IP	Ingrese la dirección IP del controlador. Es 192.168.1.108 por defecto.
Puerto	Ingrese el número de puerto del dispositivo. El número de puerto es 37777 de forma predeterminada.
Nombre de usuario, Contraseña	Ingrese el nombre de usuario y contraseña del Controlador. El nombre de usuario es admin y la contraseña es admin123 de forma predeterminada. 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 iniciar sesión exitosamente, el pantallas de estado**En línea**. De lo contrario, se 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

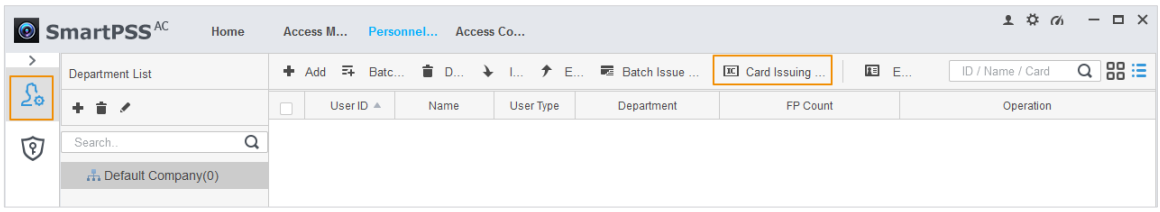
Antes de asignar una tarjeta, configure primero el tipo de tarjeta. Por ejemplo, si la tarjeta asignada es DNI, seleccione el tipo como DNI.

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

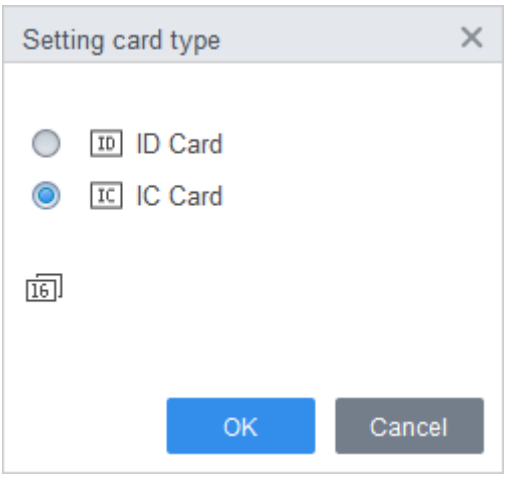


Step 3 Sobre el**Gerente de Personal**página, haga clic , luego haga clic .

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 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 Añade información básica del usuario.

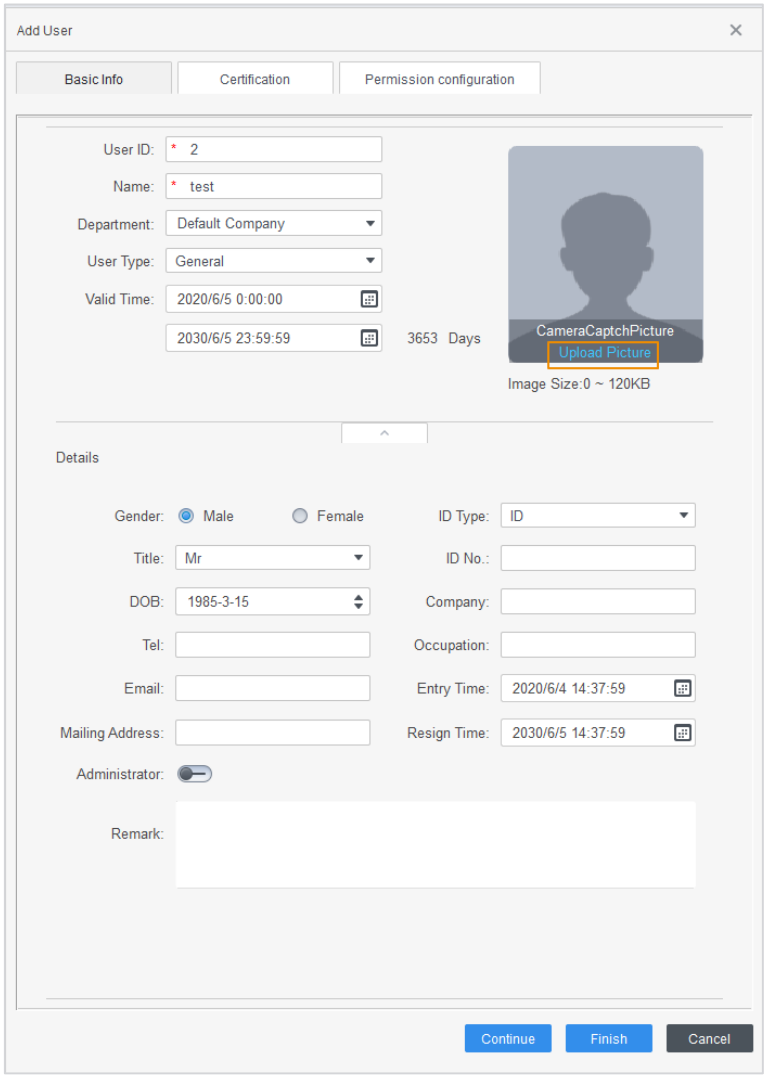
1) Haga clic en**Información básica**pestaña en el**Agregar usuario**página y luego agregar información básica del usuario.

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

La imagen del rostro cargada se mostrará en el marco 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 del personal; para otros dispositivos, configure la contraseña de la tarjeta. La nueva contraseña debe constar de 6 dígitos.

- Configurar tarjeta.

El número de tarjeta se puede leer automáticamente o ingresar 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.

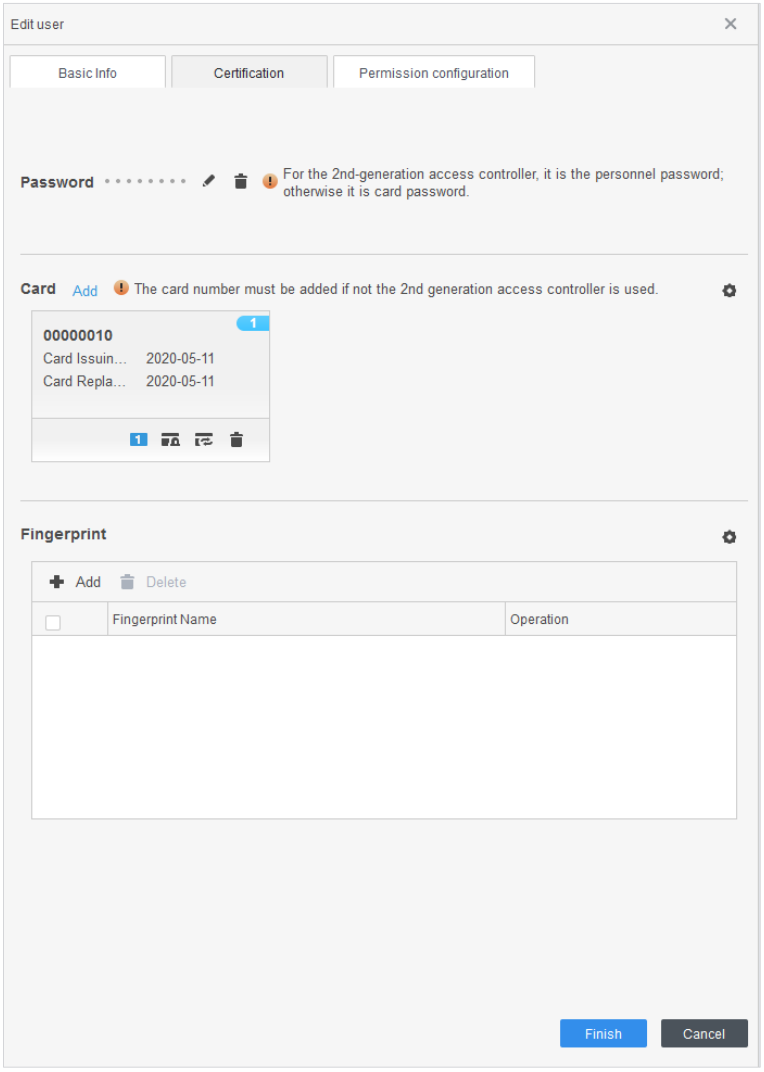
3) Después de agregarla, puede configurar la tarjeta como tarjeta principal o tarjeta de coacción, reemplazar la tarjeta por una nueva o eliminarla.

- Configurar huella digital.

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

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

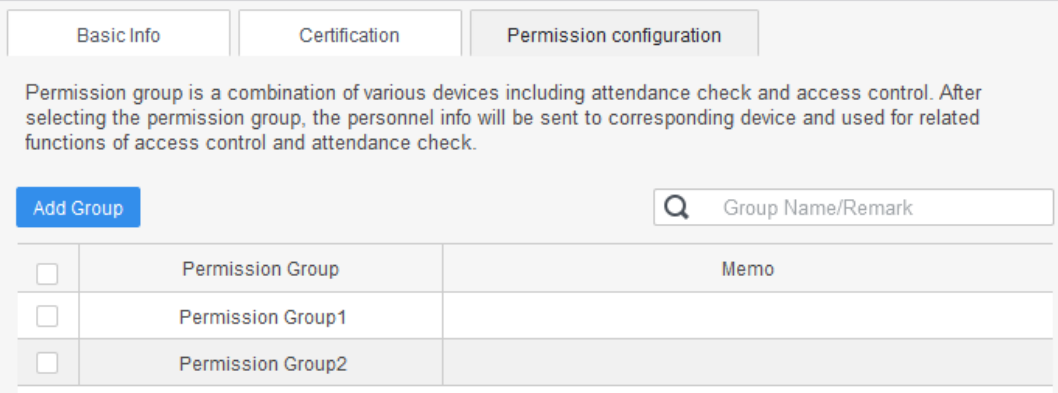
Figure 3-10 Configurar la certificación



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**Finalizar**.

3.4.2.2 Agregar en lotes

Puede agregar usuarios en lotes.

Step 1 Inicie sesión en SmartPSS AC.

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

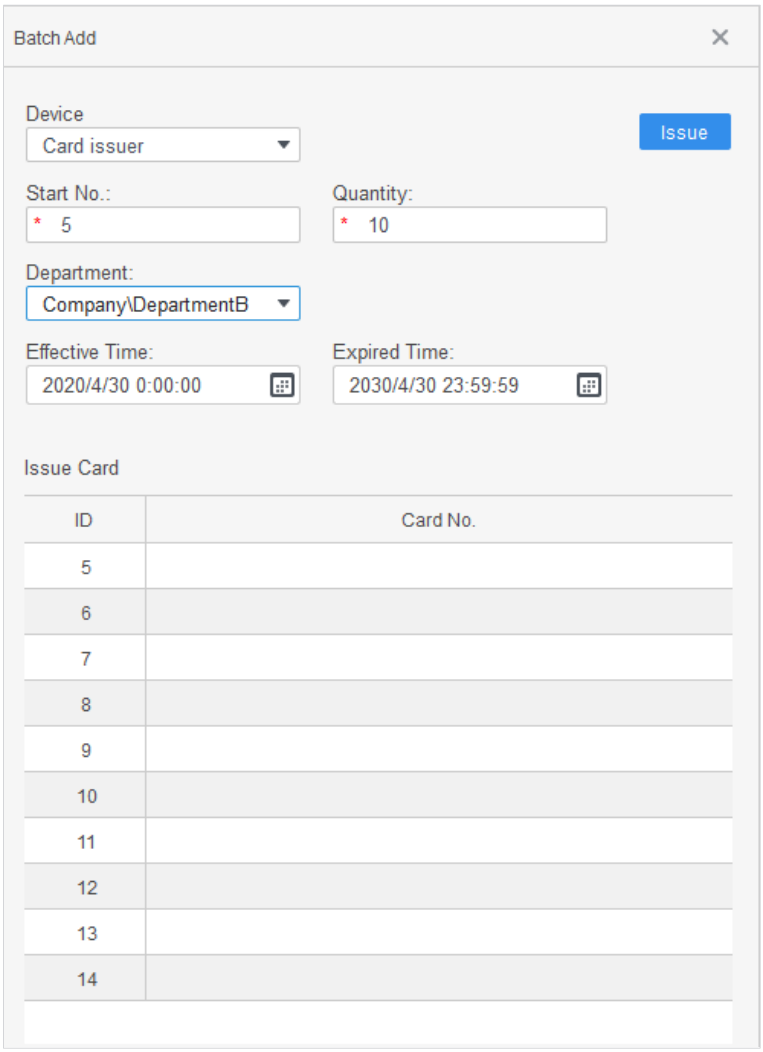
Step 3 Seleccione el lector de tarjetas y el departamento de usuario. Establezca el número de inicio, la cantidad de tarjeta, el tiempo de vigencia y el tiempo de vencimiento de la tarjeta.

Step 4 Hacer clic**Asunto**para asignar tarjetas.

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

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

Figure 3-12 Agregar usuarios en lotes



3.5 Configurar permiso

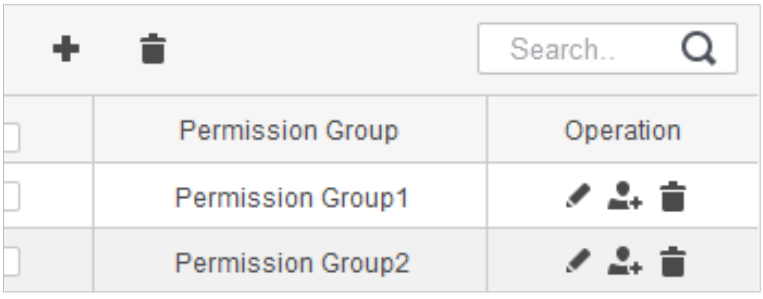
3.5.1 Agregar grupo de permisos

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.

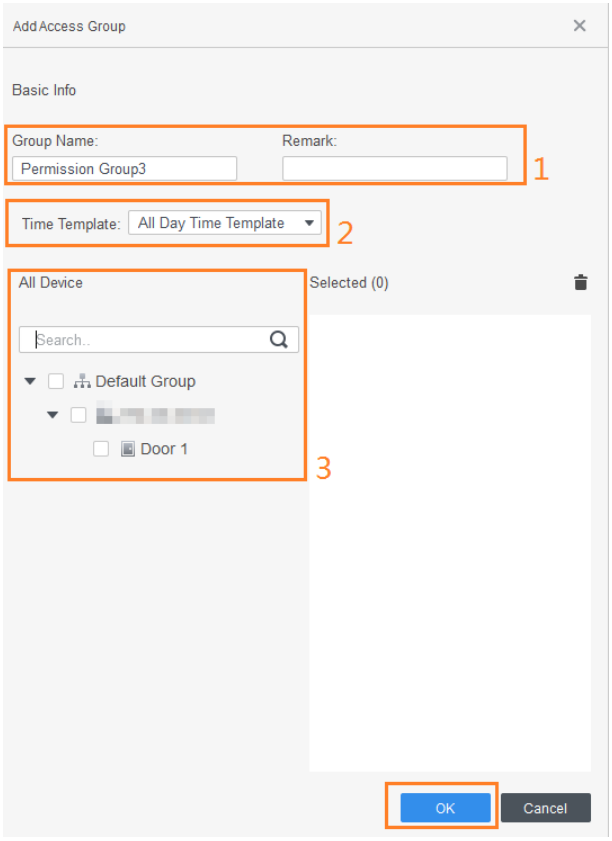
1) Ingrese el nombre del grupo y el comentario.

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 por ejemplo 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, puedes:

- 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

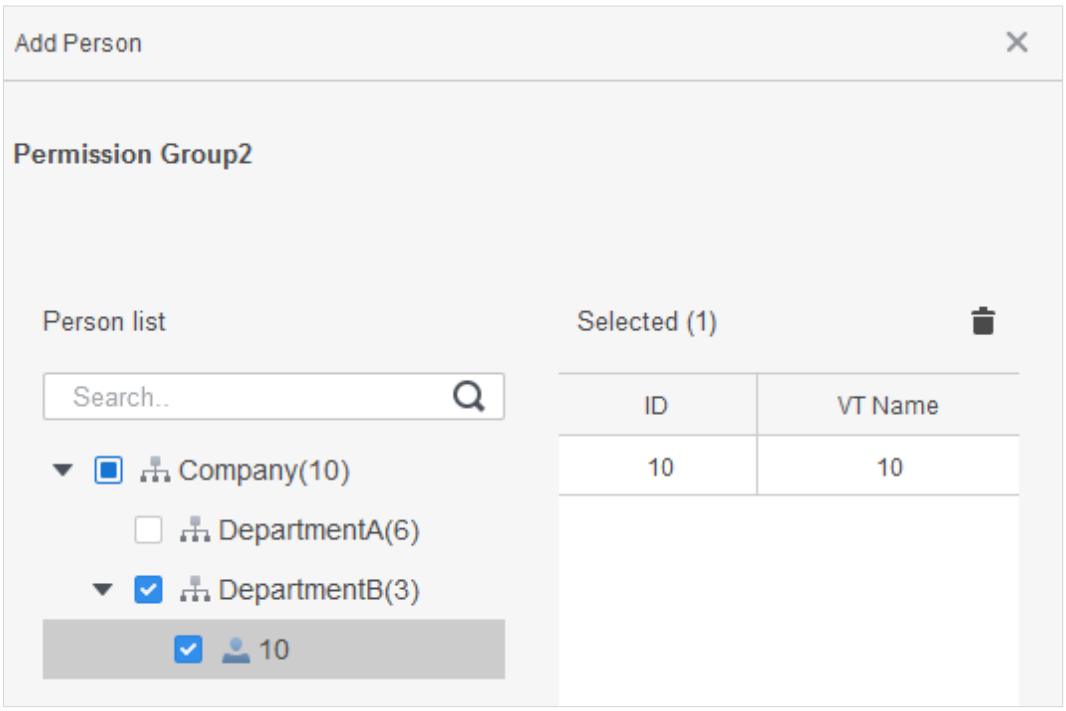
Asocie usuarios con los grupos de permisos deseados y luego a los usuarios se les asignarán permisos de acceso a puertas definidas.

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 el dedo para desbloquear la puerta solo después de que el primer titular de la tarjeta especificado deslice la tarjeta. Puede configurar varias primeras cartas. Otros usuarios sin la primera tarjeta 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 debe ser de la**General**usuario escriba y tenga permisos de determinadas puertas. Establezca el tipo al agregar usuarios. Para más detalles, consulte "3.3.2 Agregar usuario".
- Para obtener detalles sobre la asignación de permisos, consulte "3.5 Configuración de permisos".

Step 1 Seleccionar**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 luego haga clic en**Ahorrar**.

Figure 3-16 Configuración de desbloqueo de la primera tarjeta

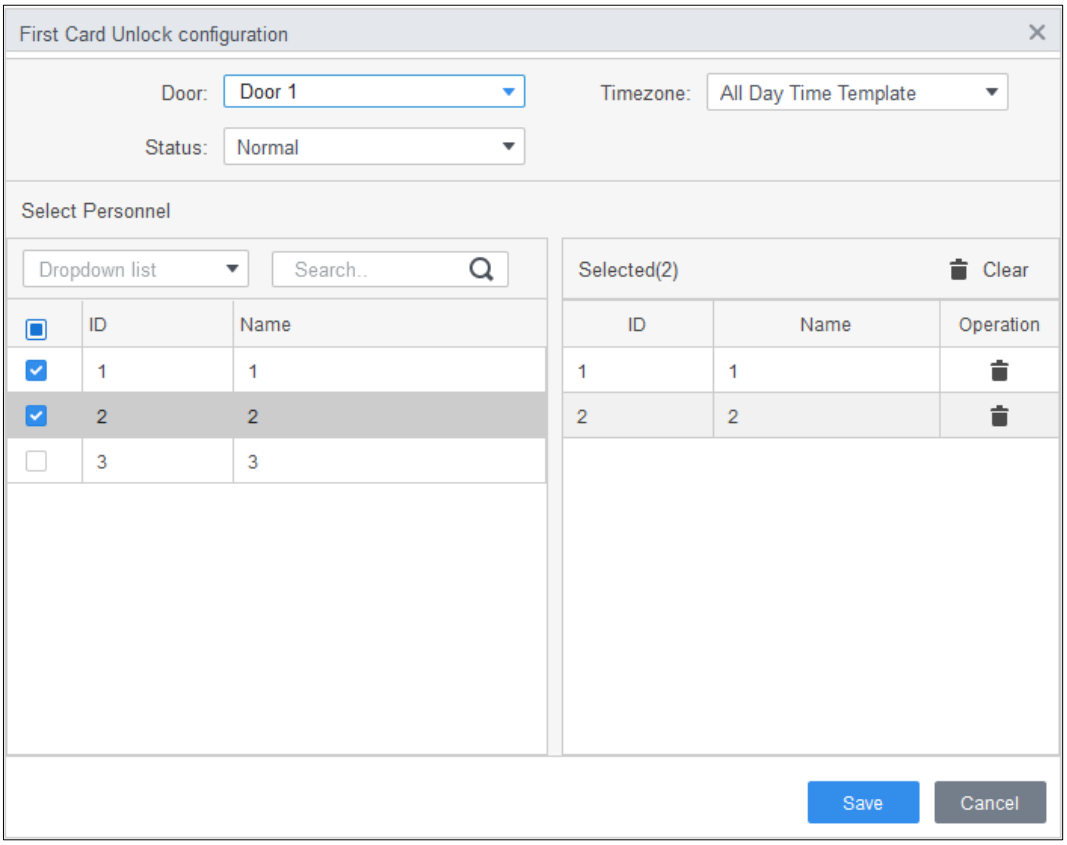


Tabla 3-2 Parámetros del desbloqueo de la primera tarjeta

Parámetro	Descripción
Puerta	Seleccione el canal de control de acceso de destino para configurar el primer desbloqueo de 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 la posición**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 . El icono cambia 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 de múltiples tarjetas

Los usuarios solo pueden desbloquear la puerta después de que 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 de múltiples tarjetas 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 varias tarjetas, lo que significa que si las dos reglas son ambas habilitado, el primer desbloqueo de tarjeta es lo primero. Te recomendamos no asignar desbloqueo multitarjeta permiso a los primeros titulares de la 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".

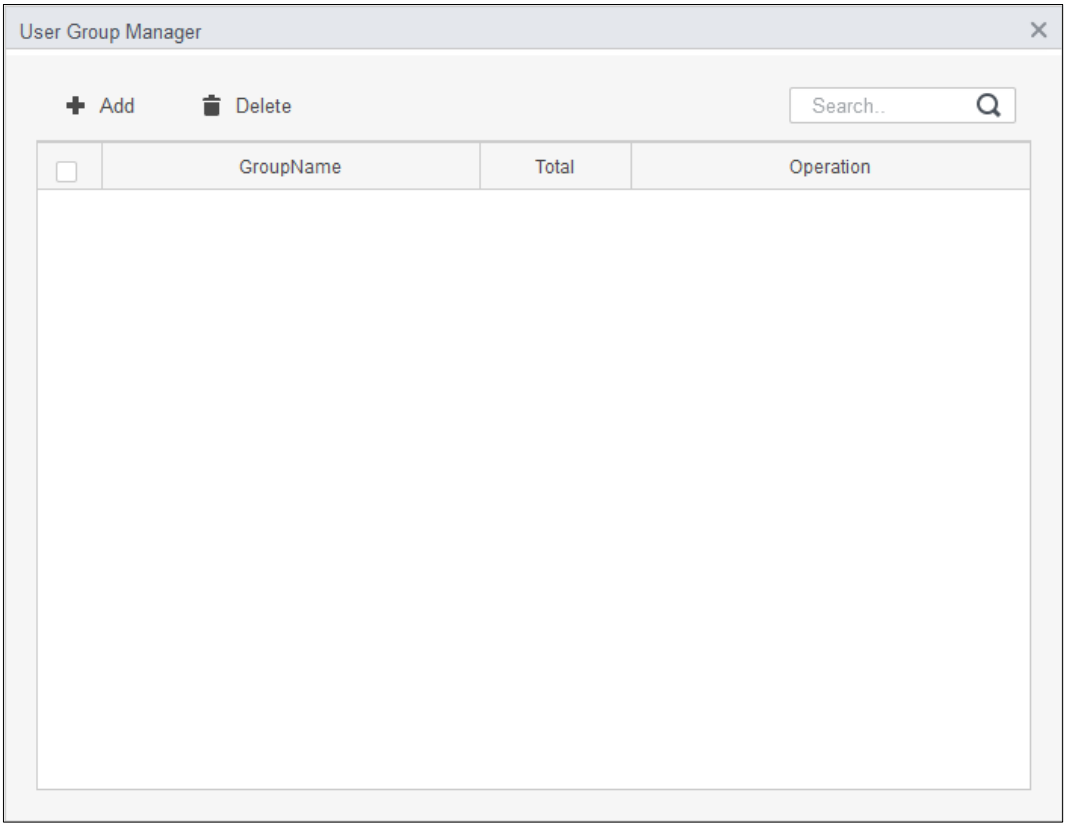
Step 1 Seleccionar**Configuración de acceso**>**Configuración avanzada**. Haga clic en

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

Step 3

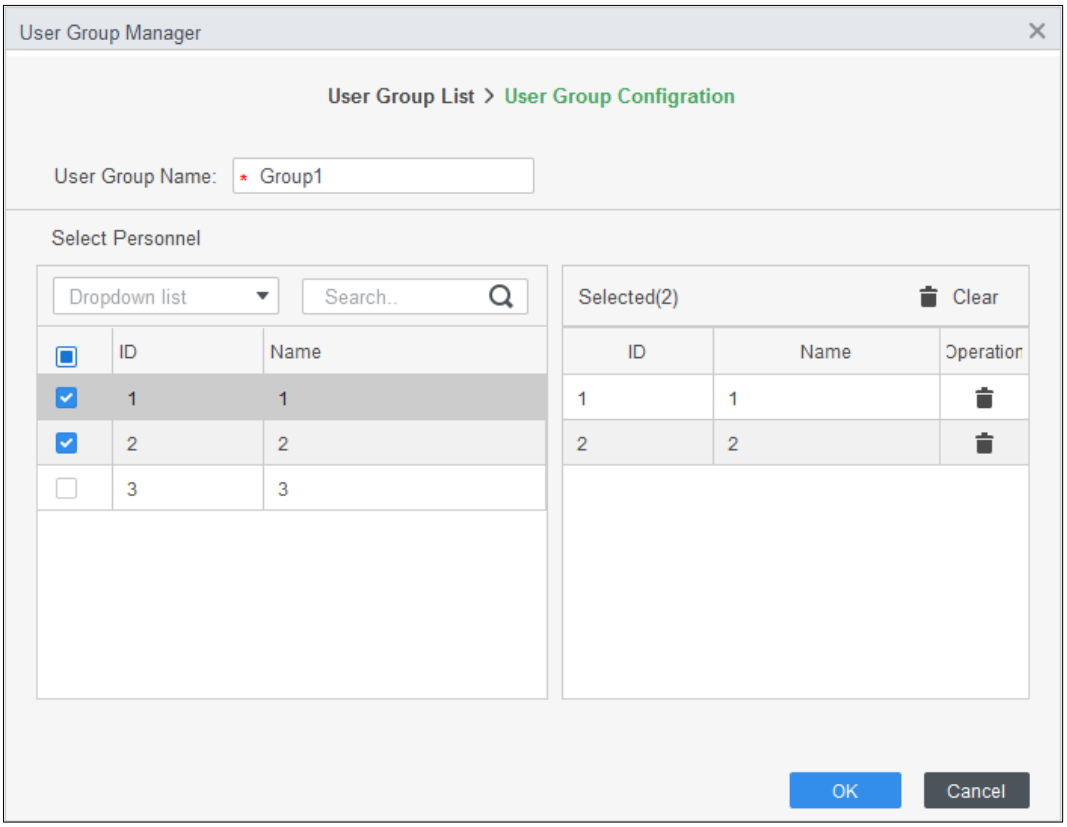
1) Haga clic**Grupo de usuario**.

Figure 3-17 Administrador de grupo de usuarios



2) Haga clic**Agregar**.

Figure 3-18 Configuración del grupo de usuarios



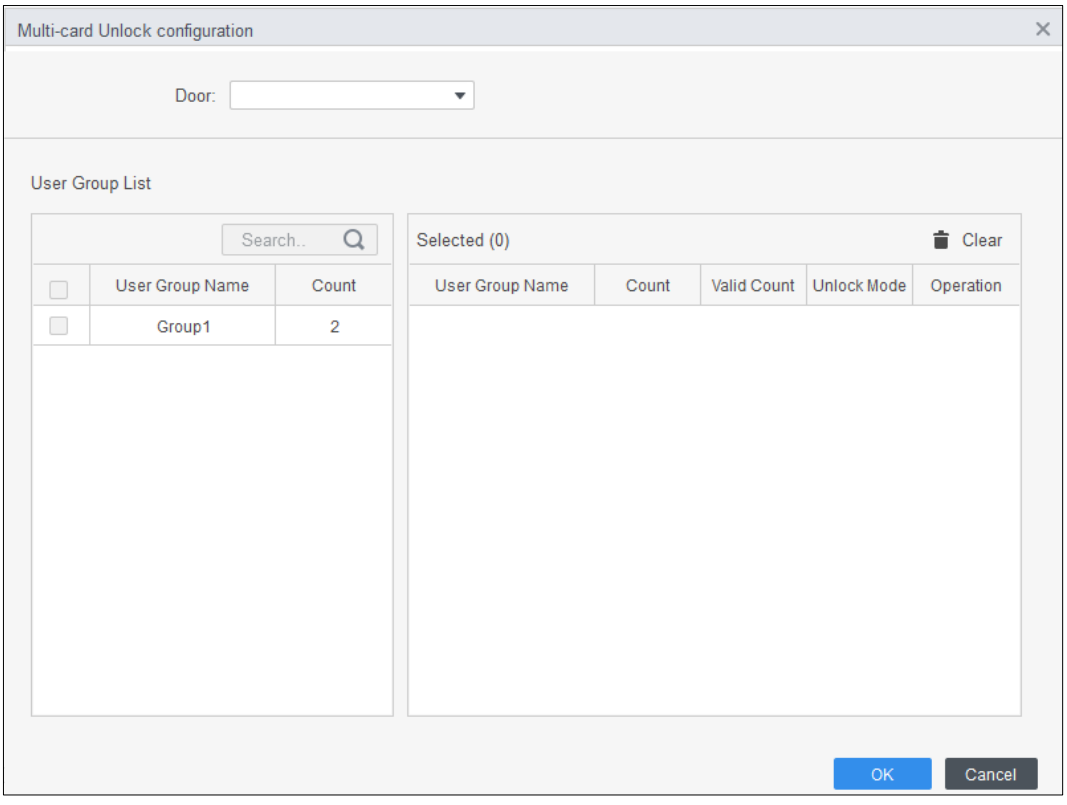
3) configurar**Nombre del grupo de usuarios**. Seleccionar usuarios de**Lista de usuarios**y haga clic**DE ACUERDO**. Puede seleccionar hasta 50 usuarios.

4) Haga clic en en la esquina superior derecha del**Administrador de grupo de usuarios**página. Configure

Step 4 los parámetros de desbloqueo de múltiples tarjetas.

1) Haga clic**Agregar**.

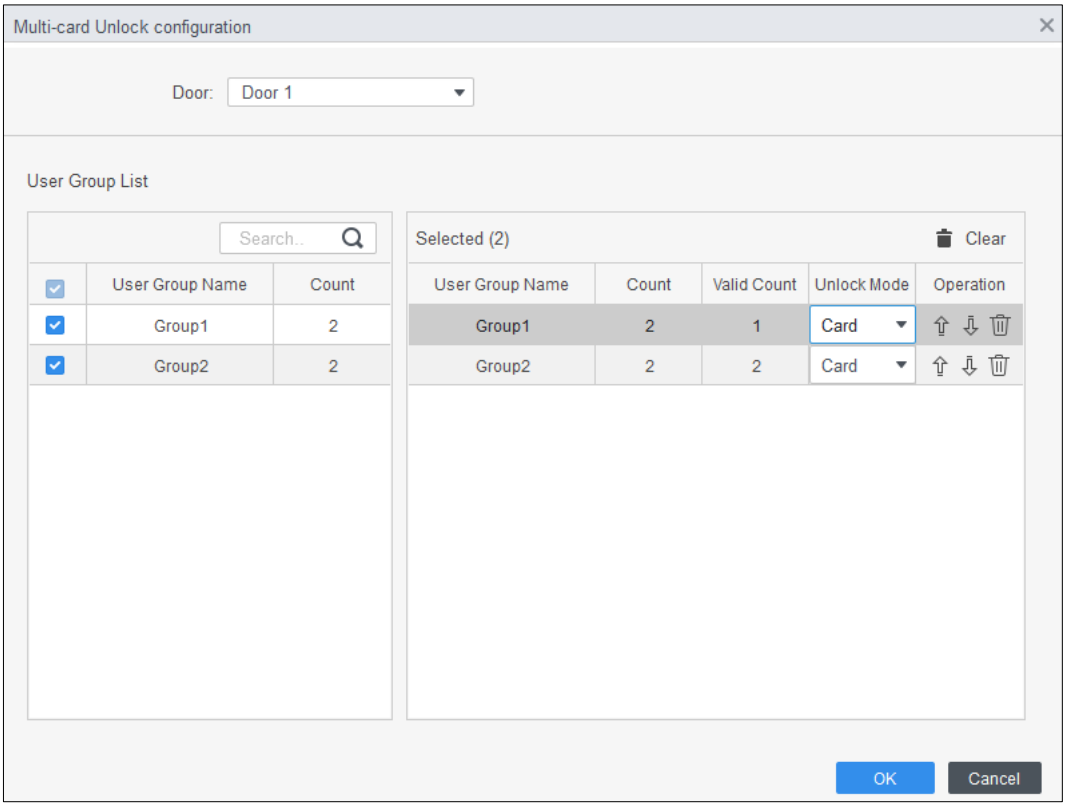
Figure 3-19 Configuración de desbloqueo multitarjeta (1)



2) Seleccione la puerta.

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

Figure 3-20 Configuración de desbloqueo multitarjeta (2)



4) Ingrese 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 recuento válido se refiere al número de usuarios de cada grupo que deben estar en el sitio para deslizar sus tarjetas. Tome la Figura 3-17 como ejemplo. La puerta sólo 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 . El icono cambia a indica**Desbloqueo de múltiples tarjetas**está habilitado.

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

3.6.1.3 Anti-passback

Los usuarios deberán verificar su identidad tanto para el ingreso 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 al mismo tiempo se le negará el acceso. Si una persona entra sin verificación de identidad y sale con verificación, se le niega la salida cuando intenta salir.

Step 1 Seleccionar**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) Establezca el tiempo de descanso y la unidad sea minuto.

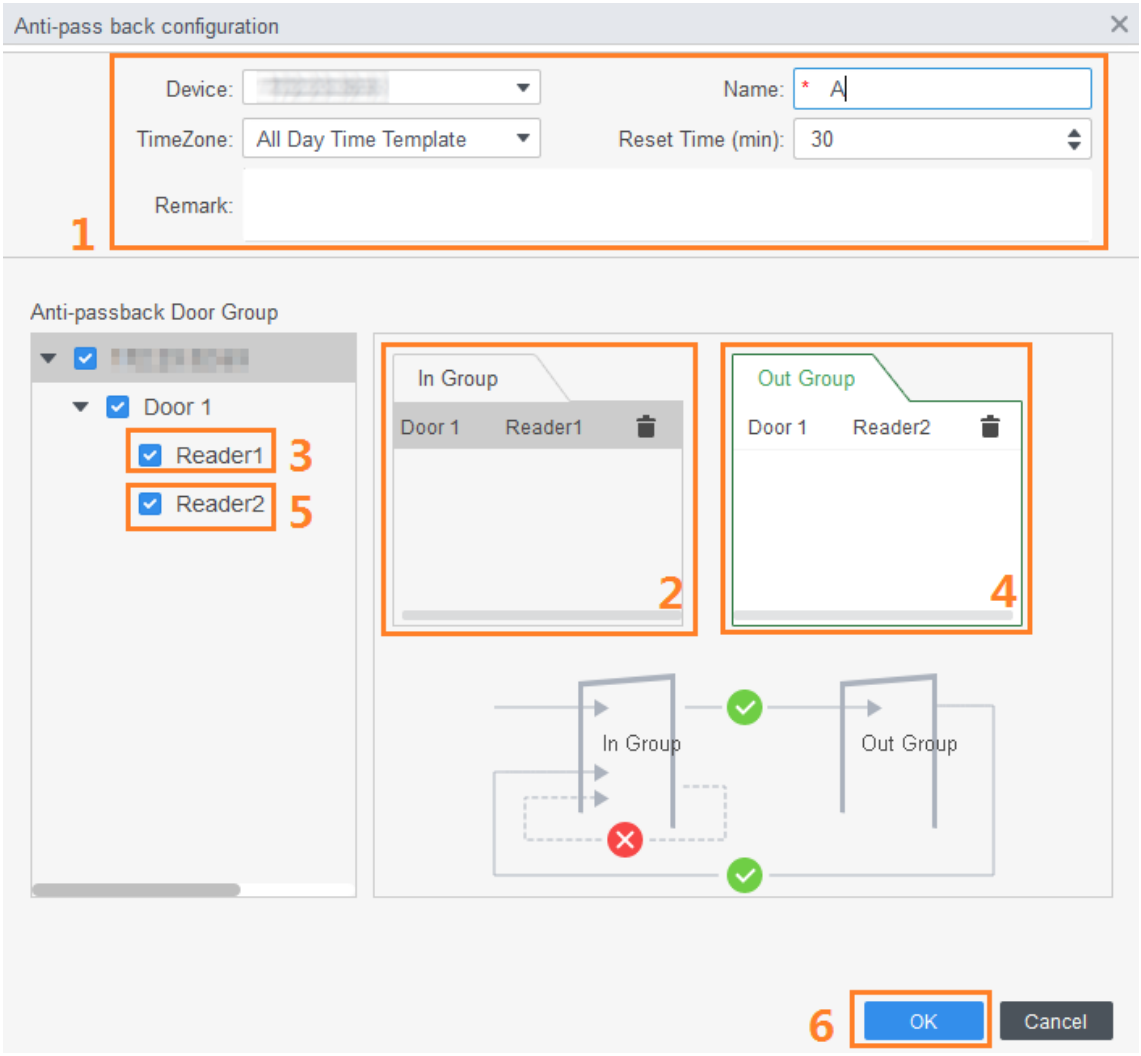
Por ejemplo, establezca el tiempo de reinicio en 30 minutos. Si un miembro del personal ha ingresado pero no ha salido, la alarma anti-regreso se activará cuando este personal tienda a ingresar nuevamente dentro de los 30 minutos. El segundo pase de este personal solo es válido después de 30 minutos.

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 enviará al dispositivo y entrará en vigor.

Figure 3-21 Configuración anti-retorno



Step 4 (Opcional) Haga clic . El icono cambia 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 entrelazadas, puede acceder a través de una puerta solo cuando la otra está cerrada. Un dispositivo admite dos grupos de puertas con hasta 4 puertas en cada grupo.

Step 1 Seleccionar**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**DE ACUERDO**. 1) Seleccione el dispositivo e ingrese el nombre del dispositivo.

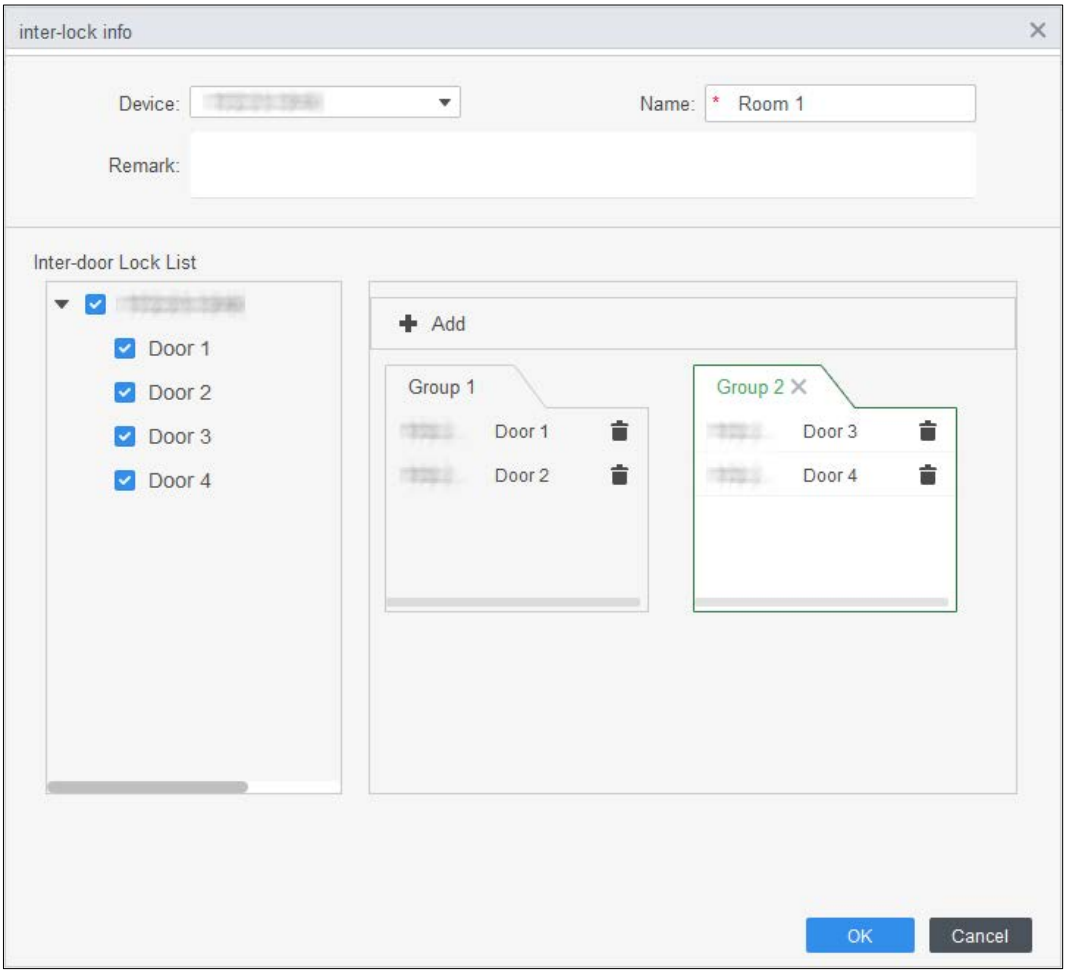
2) Introduzca el comentario.

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 . El icono cambia 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 Seleccionar**Configuración de acceso**>**Acceder a la**

Step 2 **configuración**. Haga clic en la puerta que necesita

Step 3 configurarse. Configurar parámetros.

Figure 3-23 Configurar puerta de acceso

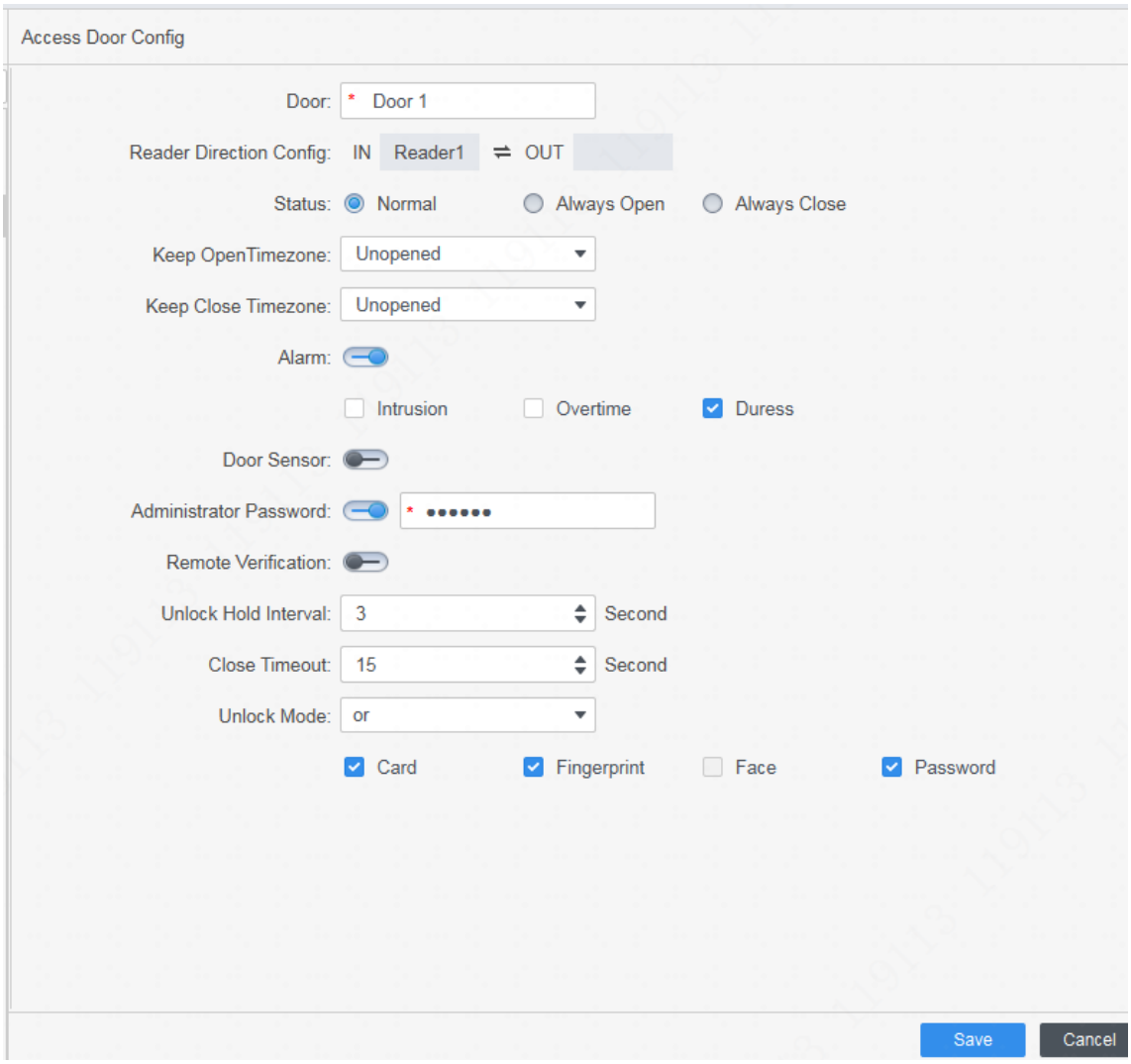


Figure 3-24 Desbloquear por período de tiempo

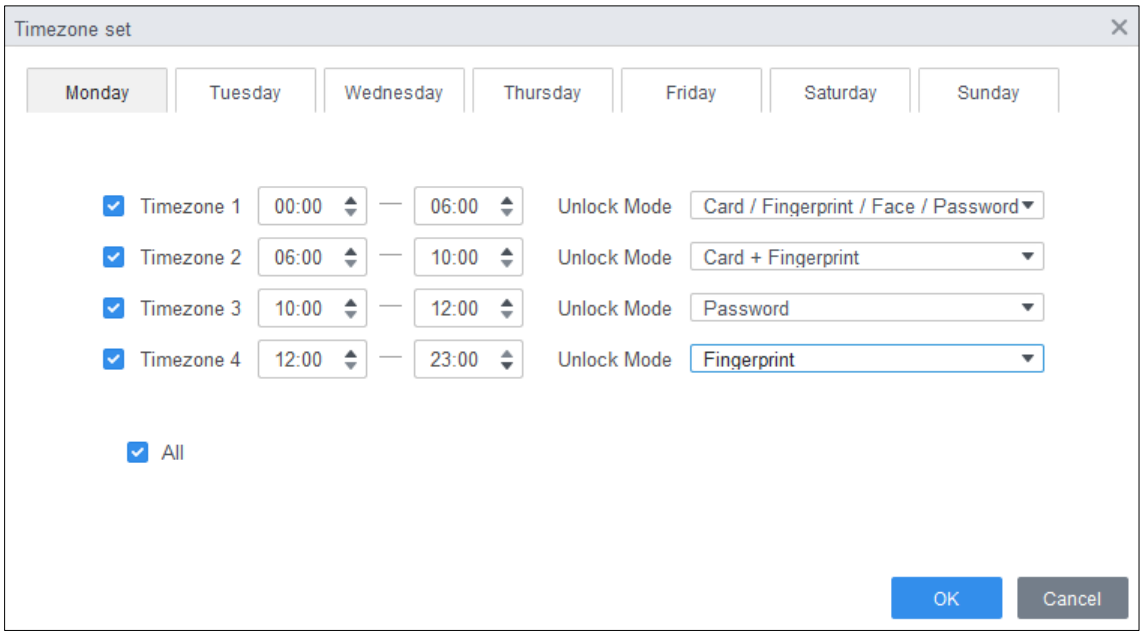


Tabla 3-3 Parámetros de la puerta de acceso

Parámetro	Descripción
Puerta	Introduzca el nombre de la puerta.
Dirección del lector configuración	Hacer clic ⇌ para establecer la dirección del lector de acuerdo con situaciones reales.
Estado	Establecer el estado de la puerta, incluido**Normal**,**Siempre abierto**y**Siempre cerca**. 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 abierta la zona horaria	Seleccione la plantilla de tiempo cuando la puerta esté siempre abierta.
Mantener zona horaria cercana	Seleccione la plantilla de tiempo cuando la puerta esté siempre cerrada.
Alarma	Habilite la función de alarma y establezca el tipo de alarma, incluidas intrusión, horas extras 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 Contraseña	Habilite y establezca la contraseña de administrador. Podrás 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 retención de desbloqueo	Establezca el intervalo de retención de desbloqueo. La puerta se cerrará automáticamente cuando se acabe el tiempo.
Cerrar tiempo de espera	Establezca 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. ● Seleccionar**Y**y seleccione métodos de desbloqueo. Puede abrir la puerta combinando los métodos de desbloqueo seleccionados. ● Seleccionar**O**y seleccione métodos de desbloqueo. Puede abrir la puerta de una de las formas que haya configurado. ● Seleccionar**Desbloquear por período de tiempo**y seleccione el modo de desbloqueo para cada período de tiempo. La puerta solo se puede abrir mediante el método seleccionado dentro del período definido.

Step 4 Hacer clic**Ahorrar**.

3.6.3 Visualización de eventos históricos

Los eventos de puerta del historial incluyen eventos tanto en SmartPSS-AC como en dispositivos. Extraiga el historial de eventos de los dispositivos para asegurarse de que todos los registros de eventos estén disponibles para ser buscados.

Step 1 Agregue el personal necesario al SmartPSS-AC.

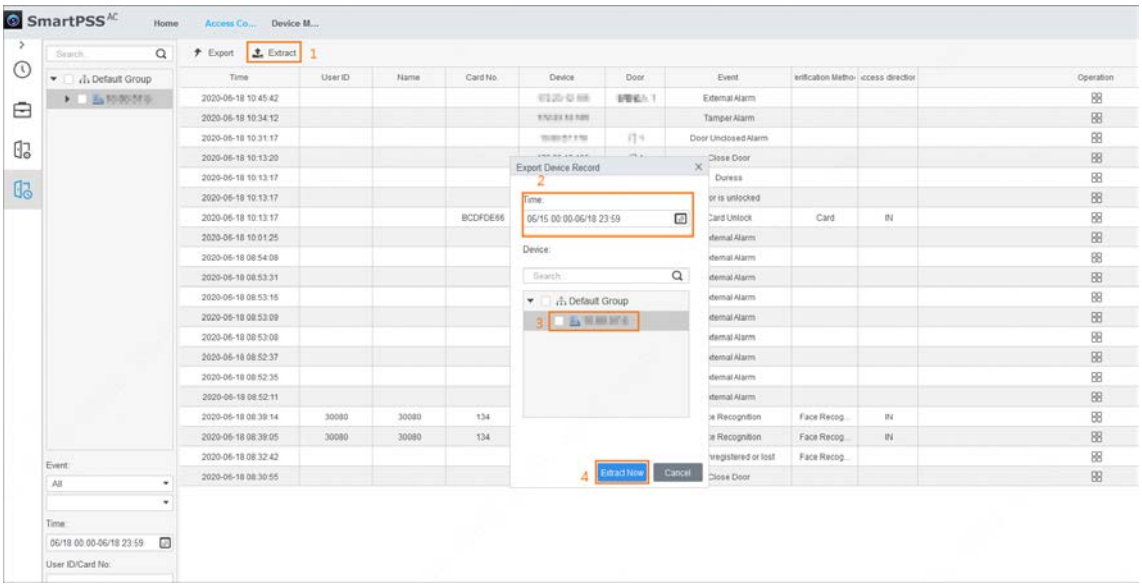
Step 2 Hacer clic**Configuración de acceso**>**Evento histórico**en la página de inicio. Clickea

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

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

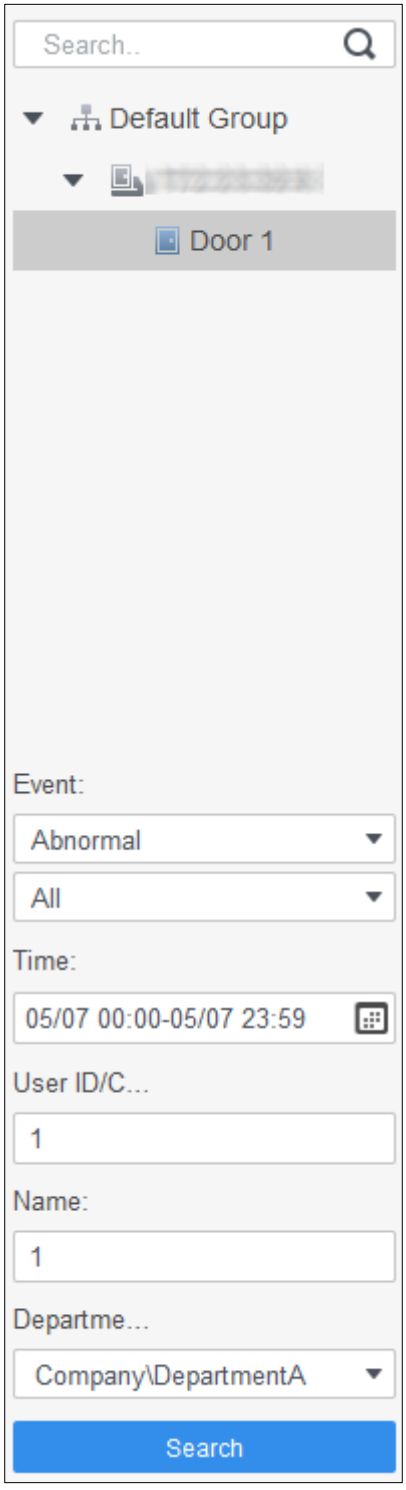
Puede seleccionar varios dispositivos a la vez para extraer eventos.

Figure 3-25 Extraer eventos



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

Figure 3-26 Buscar eventos filtrando condiciones



3.7 Gestión de Acceso

3.7.1 Apertura y cierre de puertas de forma remota

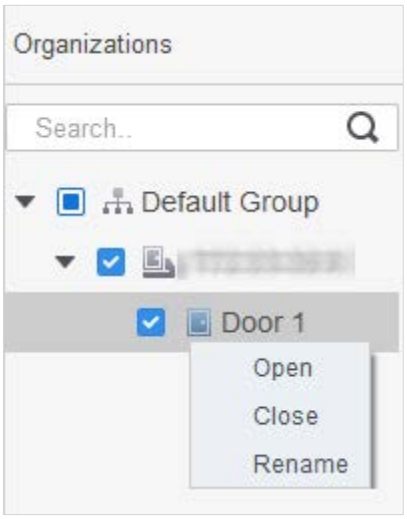
Puede controlar la puerta de forma remota a través de SmartPSS AC.

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

Step 2 Controla 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 los eventos de los tipos seleccionados. Por ejemplo, seleccione**Alarma**y la lista de eventos solo muestra 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 junto a**Información del evento**para borrar todos los eventos en la lista de eventos.

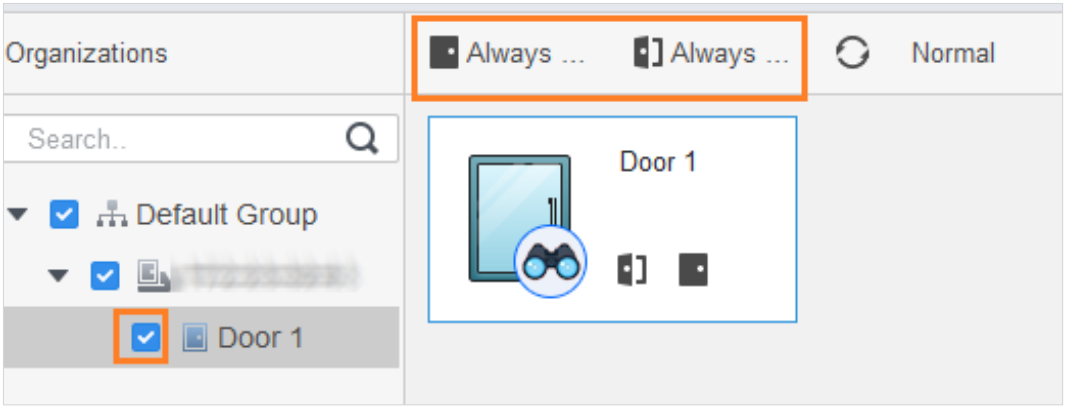
3.7.2 Configuración del estado de la puerta

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 desbloquearla después de la verificación de identidad.

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

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

Figure 3-29 Establecer siempre abierto o siempre cerrado



3.7.3 Configuración del enlace de alarma

Después de configurar el enlace de alarma, 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.
- Configurar enlaces de 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 acciones de vinculación de alarmas de intrusión según sea necesario.

- Habilitar sonido de alarma.

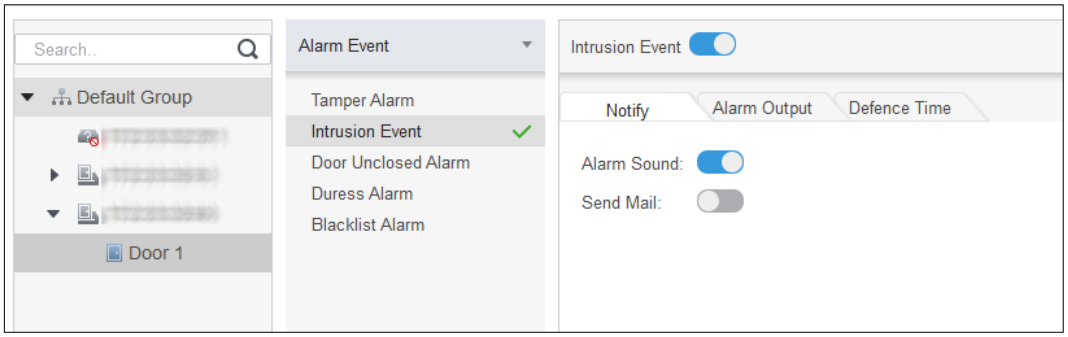
  Haga clic en el**Notificar**pestaña y haga clic en junto a**Sonido de alarma**. Cuando el evento de intrusión Esto sucede, el controlador de acceso avisa con un sonido de alarma. Enviar

- correo de alarma.

  1) Habilitar**Enviar correo**y confirme para configurar SMTP. El**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**Salida de alarma**pestaña.

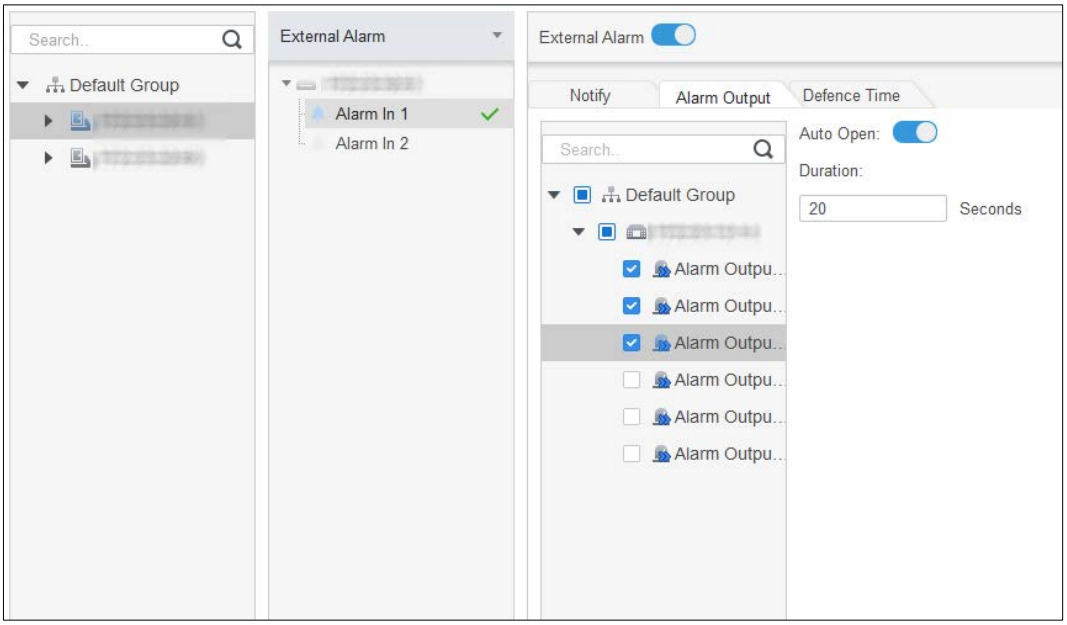
2) Seleccione el dispositivo que admita la entrada de alarma, seleccione la interfaz de entrada de alarma y luego habilite **Alarma externa**.

3) Seleccione el dispositivo que admite salida de alarma y luego seleccione la interfaz de salida de alarma.

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

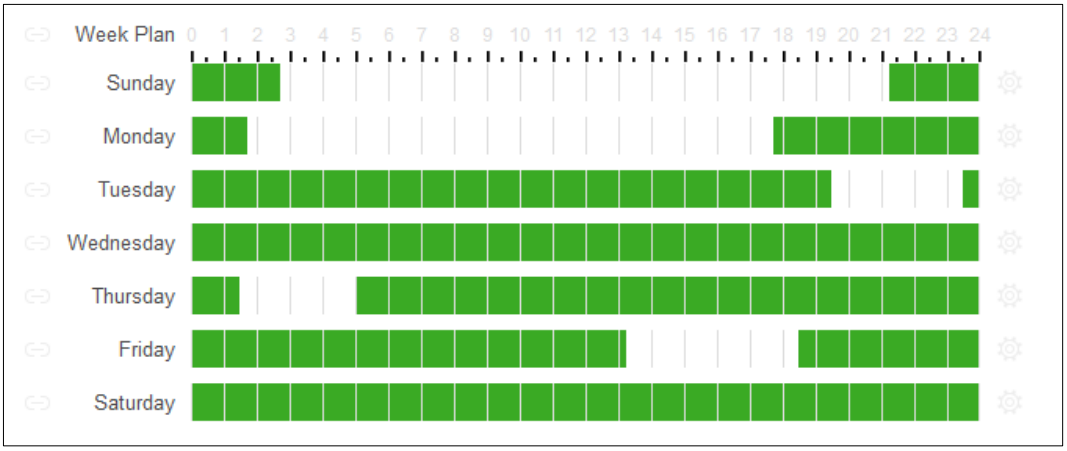
5) Establezca la duración.

Figure 3-31 Configurar el enlace de alarma



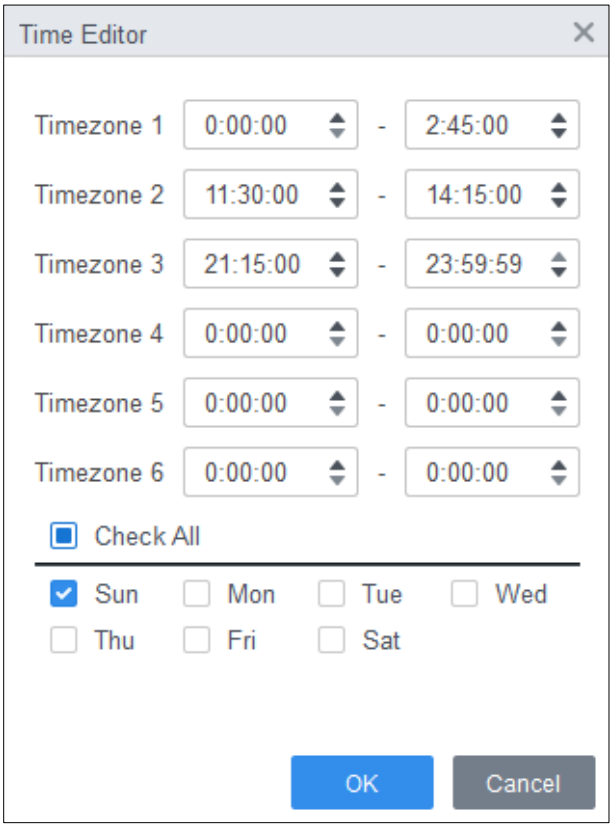
- Establezca el tiempo de armado. Hay dos métodos.
  - Método 1: Mueva el cursor para establecer períodos. Cuando el cursor esté en forma de lápiz, haga clic para agregar puntos; cuando el cursor sea borrador, haga clic para eliminar puntos. El área verde son los períodos de armado.

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



-Método 2: haga clic para establecer períodos y luego 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**Ahorrar**.

Step 6

4 Configuración de la herramienta de configuración

ConfigTool se utiliza principalmente para configurar y mantener el dispositivo.

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

4.1 Inicialización

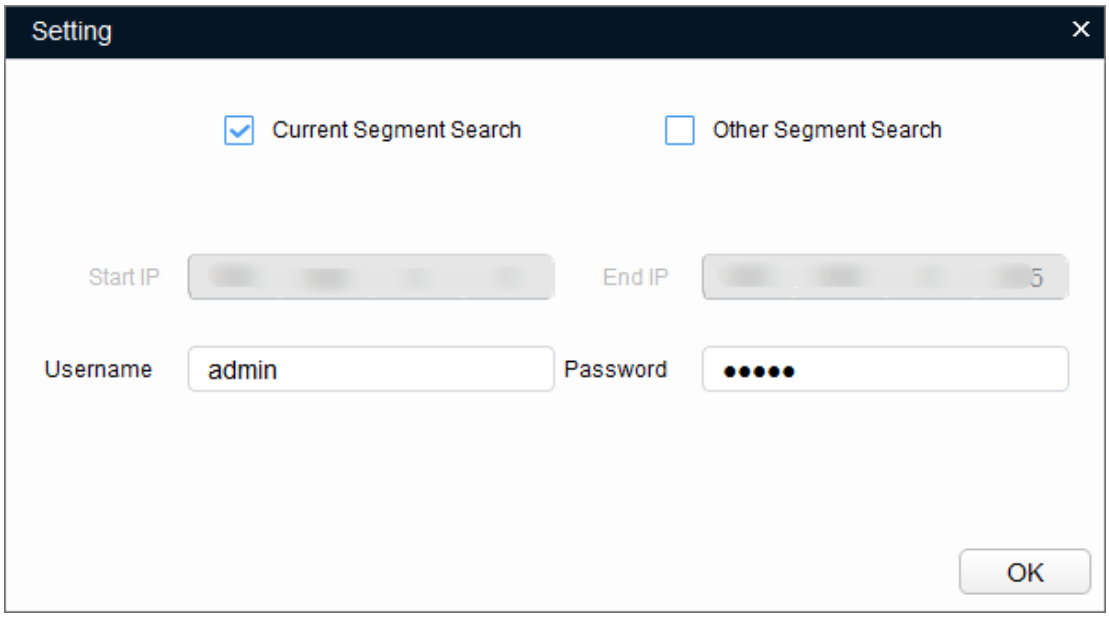
Antes de la inicialización, asegúrese de que el controlador y la computadora estén en la misma red.

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**Finalizar**.

4.2 Agregar 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.

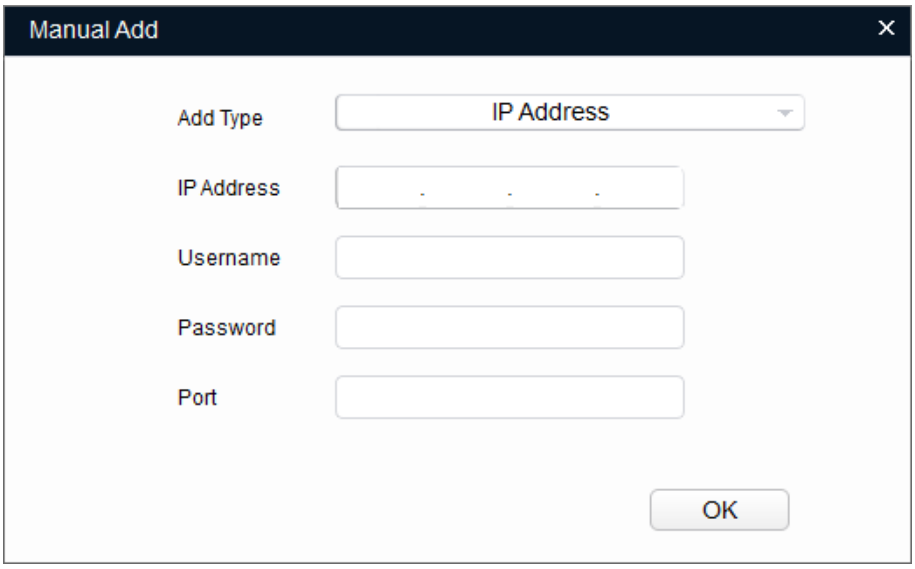
4.2.1 Agregar dispositivo individualmente

Step 1 Hacer clic .

Step 2 Hacer clic**Agregar manualmente**.

Step 3 Seleccionar**Dirección IP**de**Agregar tipo**.

Figure 4-2 Agregar manualmente (dirección IP)



Step 4 Configure los parámetros del controlador.

Tabla 4-1 Parámetros de adición manual

Agregar 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.
	Contraseña	
	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 Agregar dispositivos en lotes

Puede agregar varios dispositivos buscando dispositivos o importando la plantilla.

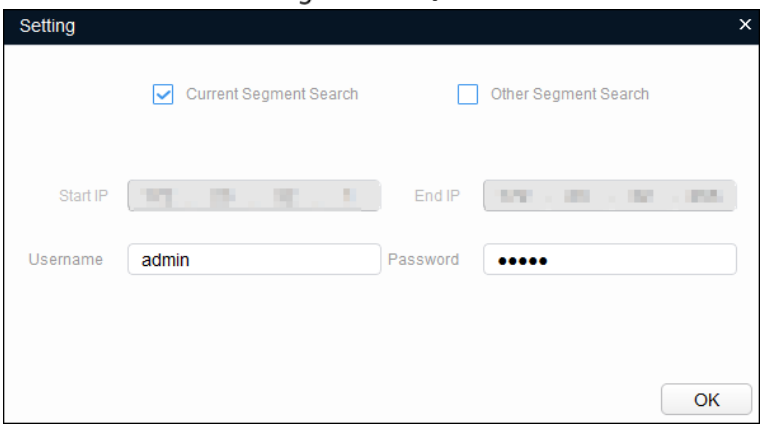
4.2.2.1 Agregar mediante búsqueda

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

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

Step 1 Hacer clic Search setting.

Figure 4-3 Configuración



Step 2 Seleccione la forma de búsqueda. Las dos formas siguientes están seleccionadas de forma predeterminada.

- Buscar segmento actual

  Seleccionar**Búsqueda de segmento actual**. Ingrese el nombre de usuario y la contraseña. El sistema buscará dispositivos en consecuencia.

- Buscar otro segmento

  Seleccionar**Búsqueda de otros segmentos**. Ingrese la dirección IP inicial y la dirección IP final. Ingrese el nombre de usuario y la contraseña. El sistema buscará dispositivos en consecuencia.

- Si seleccionas ambos**Búsqueda de segmento actual**y**Búsqueda de otros segmentos**, el sistema busca dispositivos en ambos segmentos.
- El usuario y la contraseña son los que se utilizan para iniciar sesión cuando se desea modificar IP, configurar el sistema, actualizar el dispositivo, reiniciar 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 la próxima vez que se inicie el software.

4.2.2.2 Agregar 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 que aparecen en pantalla para guardar el archivo de plantilla localmente.

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

Step 4 Importa la plantilla. Hacer clic**Importar**, seleccione la plantilla y haga clic**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 Configurar el 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 Establezca los parámetros del controlador de acceso.

Figure 4-4 Configurar el controlador de acceso

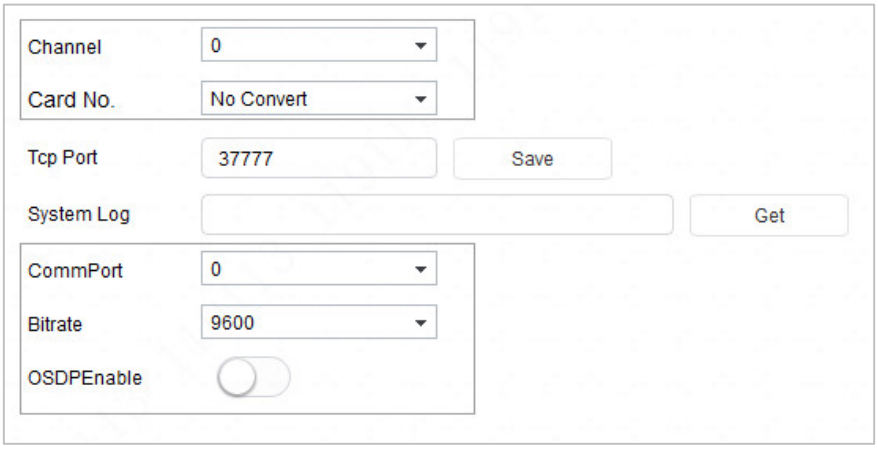


Tabla 4-2 Parámetros del controlador de acceso

Parámetro
Canal
Número de tarjeta
Puerto TCP

Parámetro
Registro del sistema
Puerto de comunicaciones
tasa de bits
OSDPHabilitar

Step 5 (Opcional) Haga clic**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 clic en el icono para ver información detallada. se visualiza. Tú

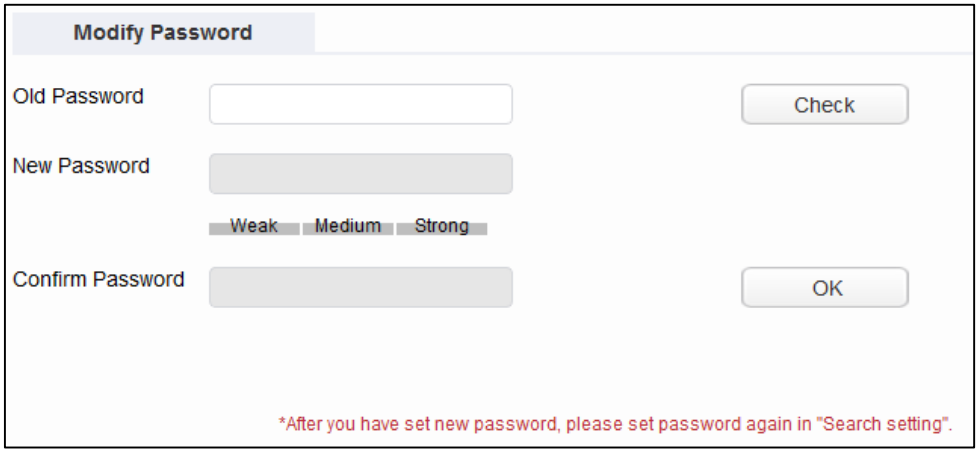
4.4 Cambiar la contraseña del dispositivo

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 Establece 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	Ingrese la contraseña anterior del dispositivo. Para asegurarse de que la contraseña anterior se haya ingresado correctamente, puede hacer clic en**Controlar**para verificar.
Nueva contraseña	Ingrese 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 (excluyendo ' " ; : &).
confirmar Contraseña	Confirme la nueva contraseña.

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

Appendix 1 Recomendaciones de ciberseguridad

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 ni 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 a tiempo

- 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. Cuando el dispositivo está conectado a la red pública, se recomienda habilitar la función "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 "es bueno tener" para mejorar la seguridad de la red de su dispositivo: 1. Protección física

Le sugerimos que realice protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras y un gabinete especiales, e implemente permisos de control de acceso y administración de claves bien hechos para evitar que 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 que las adivinen o las descifren.

3. Establecer y actualizar contraseñas Restablecer información oportuna

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 preguntas de protección con contraseña, se sugiere no utilizar aquellas que puedan adivinarse fácilmente.

4. Habilite el bloqueo de cuenta

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

5. Cambie HTTP predeterminado y otros puertos de servicio

Le sugerimos que cambie 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. Habilite HTTPS

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

7. Vinculación de direcciones MAC

Le recomendamos vincular la dirección IP y MAC de la puerta de enlace al dispositivo, reduciendo así el riesgo de suplantación de ARP.

8. Asigne cuentas y privilegios de manera 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 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 cifrado WPA2-PSK y configure contraseñas seguras.

10. Transmisión cifrada de audio y vídeo

Si el contenido de sus datos de audio y video es muy importante o confidencial, le recomendamos que utilice la función de transmisión cifrada para reducir el riesgo de que los datos de audio y video sean robados durante la transmisión.

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

11. Auditoría segura

- Verifique los usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo inició sesión sin autorización.
- Verifique 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 un período prolongado, se recomienda habilitar la función de registro de red para garantizar 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:

- Deshabilite la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa.
- La red debe dividirse y aislarse según 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.