Controlador de acceso

Manual de usuario

V1.0.1

Prefacio

General

Este manual presenta la instalación y las operaciones detalladas del Controlador de acceso (en lo sucesivo, "el Dispositivo").

Instrucciones de seguridad

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

Palabras de advertencia	Sentido
 **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, menor rendimiento o resultados impredecibles.
 **PUNTAS**	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
 **NOTA**	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.1	Añadido proceso de inicialización.	diciembre 2021
V1.0.0	Primer lanzamiento.	septiembre 2020

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 maneras que no están en

cumplimiento del 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, póngase en contacto con el proveedor o con el servicio de atención al cliente si se produce algún problema durante el uso del dispositivo.
- 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 Dispositivo, la prevención de riesgos y prevención de daños a la propiedad. Lea atentamente antes de usar el Dispositivo, cumpla con las pautas cuando lo utilice y guarde el manual en un lugar seguro para consultarlo en el futuro.

Requisito de transporte

Transporte el Dispositivo en condiciones de humedad y temperatura permitidas.

Requisito de almacenamiento

Guarde el dispositivo en condiciones de humedad y temperatura permitidas.

requerimientos de instalación

 **WARNING**

- No conecte el adaptador de corriente al dispositivo 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 dispositivo.
- No conecte el Dispositivo a dos o más tipos de fuentes de alimentación, para evitar daños al Dispositivo.
- 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 Dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- Instale el dispositivo en una superficie estable para evitar que se caiga.
- Instale el dispositivo 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 dispositivo.
- El dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectado a una toma de corriente con puesta a tierra de protección.

Requisitos de operación

- Compruebe si la fuente de alimentación es correcta antes de usar.
- No desconecte el cable de alimentación del lateral del dispositivo mientras el adaptador está encendido.
- Opere el dispositivo dentro del rango nominal de entrada y salida de energía.
- Utilice el dispositivo en condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquido sobre el dispositivo y asegúrese de que no haya ningún objeto lleno de líquido.

  en el dispositivo para evitar que el líquido fluya hacia él.
- No desmonte el dispositivo sin instrucción profesional.

Tabla de contenido

1.1 Introducción

El Dispositivo es un panel de control de acceso 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.

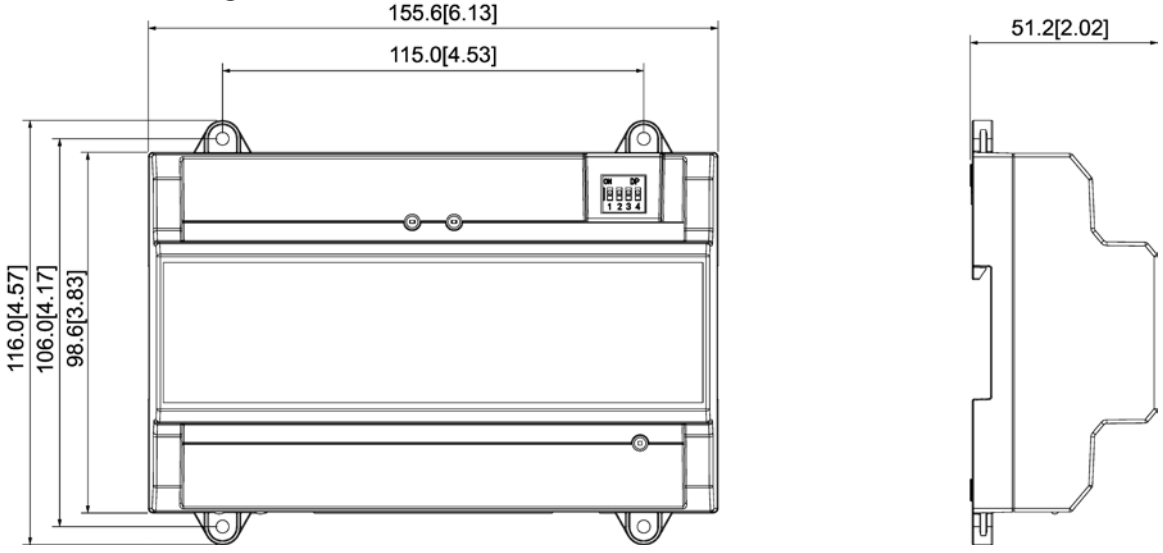
1.2 Características

- Utilizando PC+ABS como material, la apariencia es elegante y de alta gama.
- Admite comunicación de red TCP/IP, los datos de comunicación están encriptados por seguridad.
- Admite el protocolo OSDP.
- Admite la función PoE.
- 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 ilegal, 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, los datos se pueden almacenar localmente después de desconectar la red y continuar cargándose después de que se restablezca la red. 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 de soporte en períodos.
- Admite mecanismo de vigilancia para garantizar la estabilidad de la operación.

1.3 Dimensiones

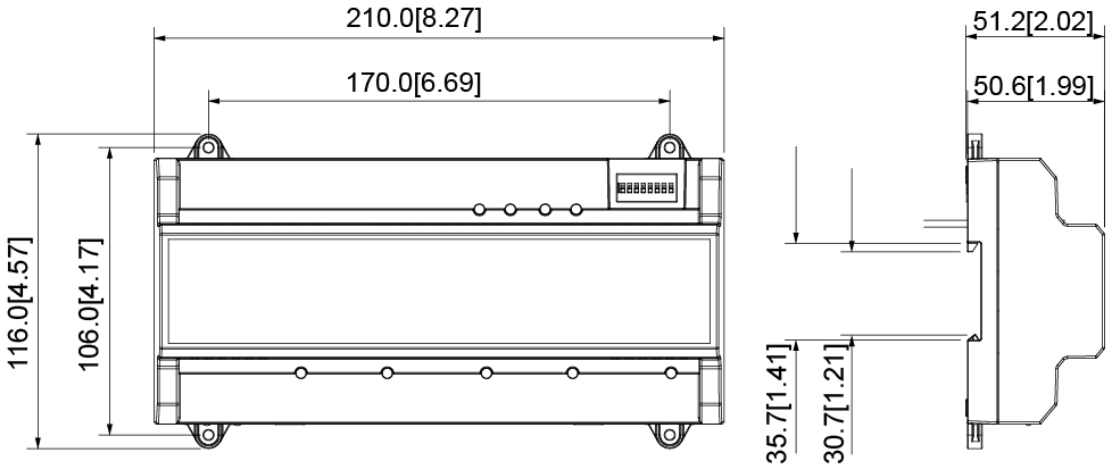
Controlador de acceso unidireccional de dos puertas

Figure 1-1 Dimensiones (dos puertas unidireccionales) (mm [pulgadas])



Controlador de acceso bidireccional de dos puertas/unidireccional de cuatro puertas

Figure 1-2 Dimensiones (dos puertas de dos vías/cuatro puertas de una vía) (mm [pulgadas])



1.4 Componentes

Controlador de acceso unidireccional de dos puertas

Figure 1-3 Componentes (dos puertas unidireccionales)

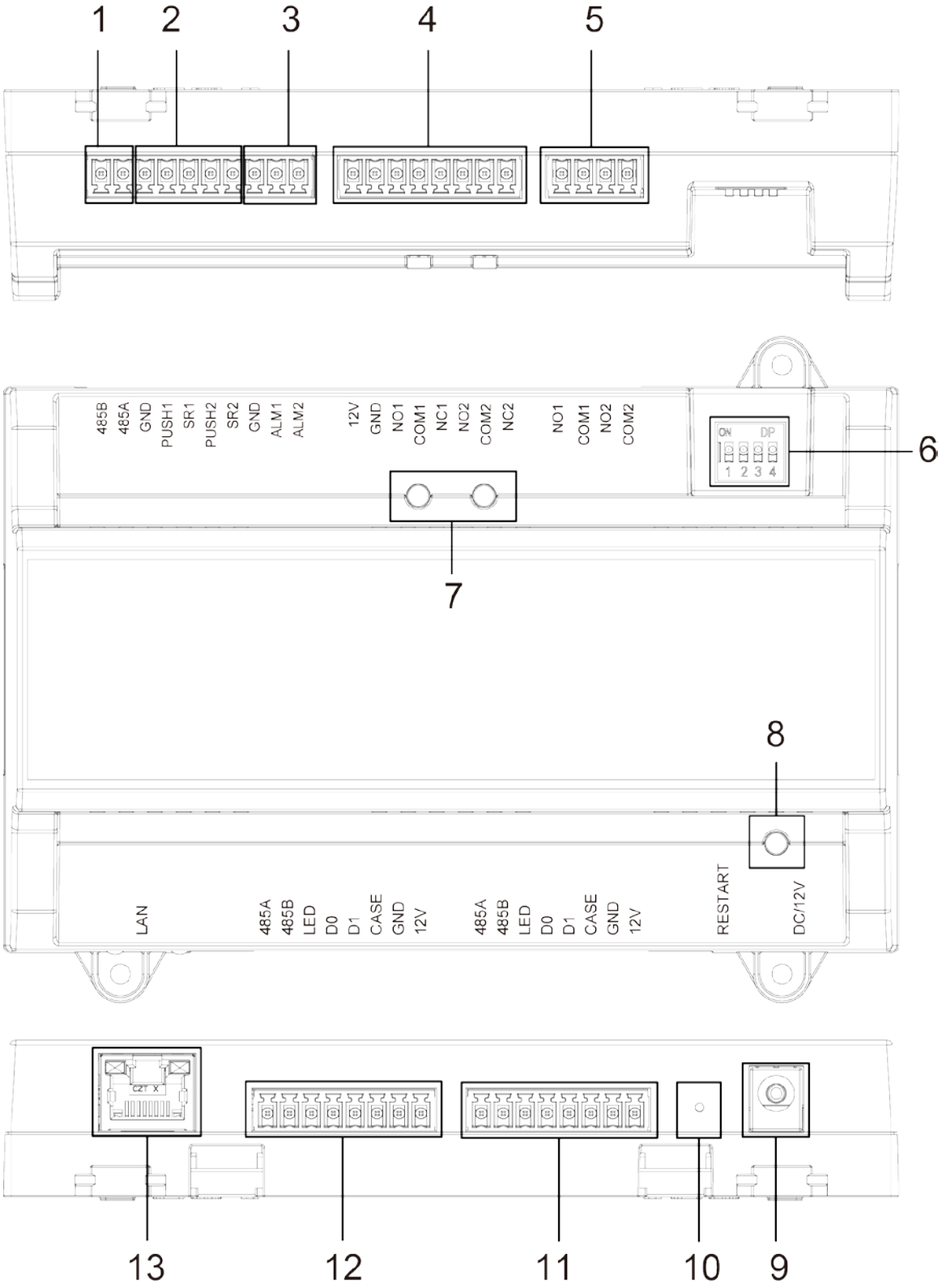


Tabla 1-1 Descripción de los componentes (dos puertas unidireccionales)

No.	Nombre	No.	Nombre
1	Puerto RS-485	8	Luz indicadora de poder
2	Botón de salida/puerto de contacto de puerta	9	Puerto de alimentación

No.	Nombre	No.	Nombre
3	Puerto de entrada de alarma	10	Botón de reinicio
4	Puerto de SALIDA de bloqueo de puerta	11	Puerto de lector de tarjetas de entrada de la puerta No.2
5	Puerto de SALIDA de alarma	12	Puerto de lector de tarjetas de entrada de la puerta No.1
6	Dip switch	13	puerto de red
7	Luz indicadora de la cerradura de la puerta	14	—

Controlador de acceso bidireccional de dos puertas

Figure 1-4 Componentes (dos puertas de dos vías)

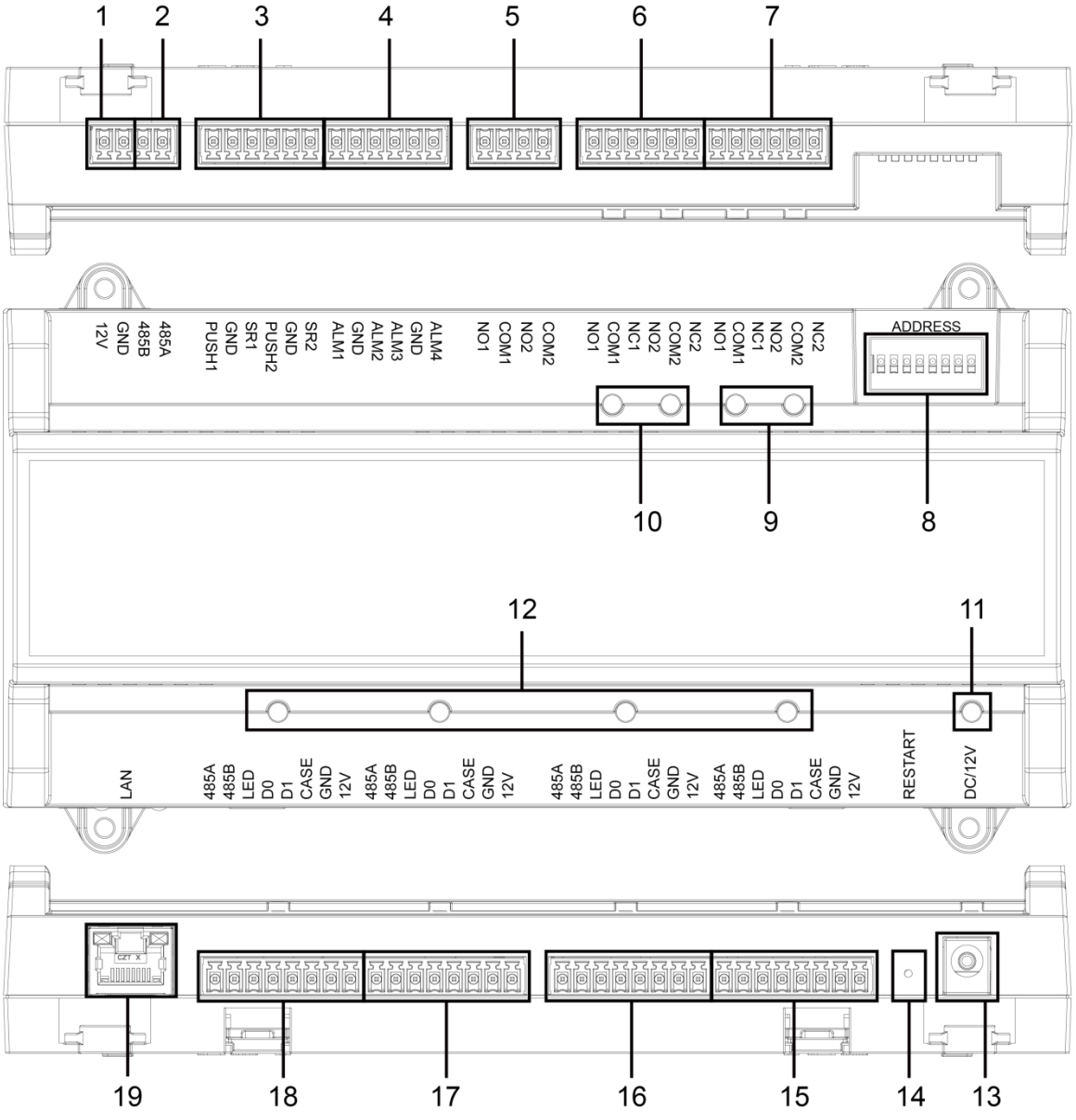


Tabla 1-2 Descripción de los componentes (dos puertas y dos vías)

No.	Nombre	No.	Nombre
1	Puerto de alimentación de bloqueo de puerta	11	Luz indicadora de poder
2	Puerto RS-485	12	Luz indicadora del lector de tarjetas
3	Botón de salida/puerto de contacto de puerta	13	Puerto de alimentación
4	Puerto de entrada de alarma externa	14	Botón de reinicio
5	Puerto de SALIDA de alarma externa	15	Salida del puerto del lector de tarjetas de la puerta No.2

No.	Nombre	No.	Nombre
6	Puerto de SALIDA de control de bloqueo de puerta	dieciséis	Puerto de lector de tarjetas de entrada de la puerta No.2
7	SALIDA de alarma interna	17	Salida del puerto del lector de tarjetas de la puerta No.1
8	Dip switch	18	Puerto de lector de tarjetas de entrada de la puerta No.1
9	Luz indicadora de alarma	19	puerto de red
10	Luz indicadora de bloqueo de puerta	—	—

Controlador de acceso unidireccional de cuatro puertas

Figure 1-5 Componentes (cuatro puertas unidireccionales)

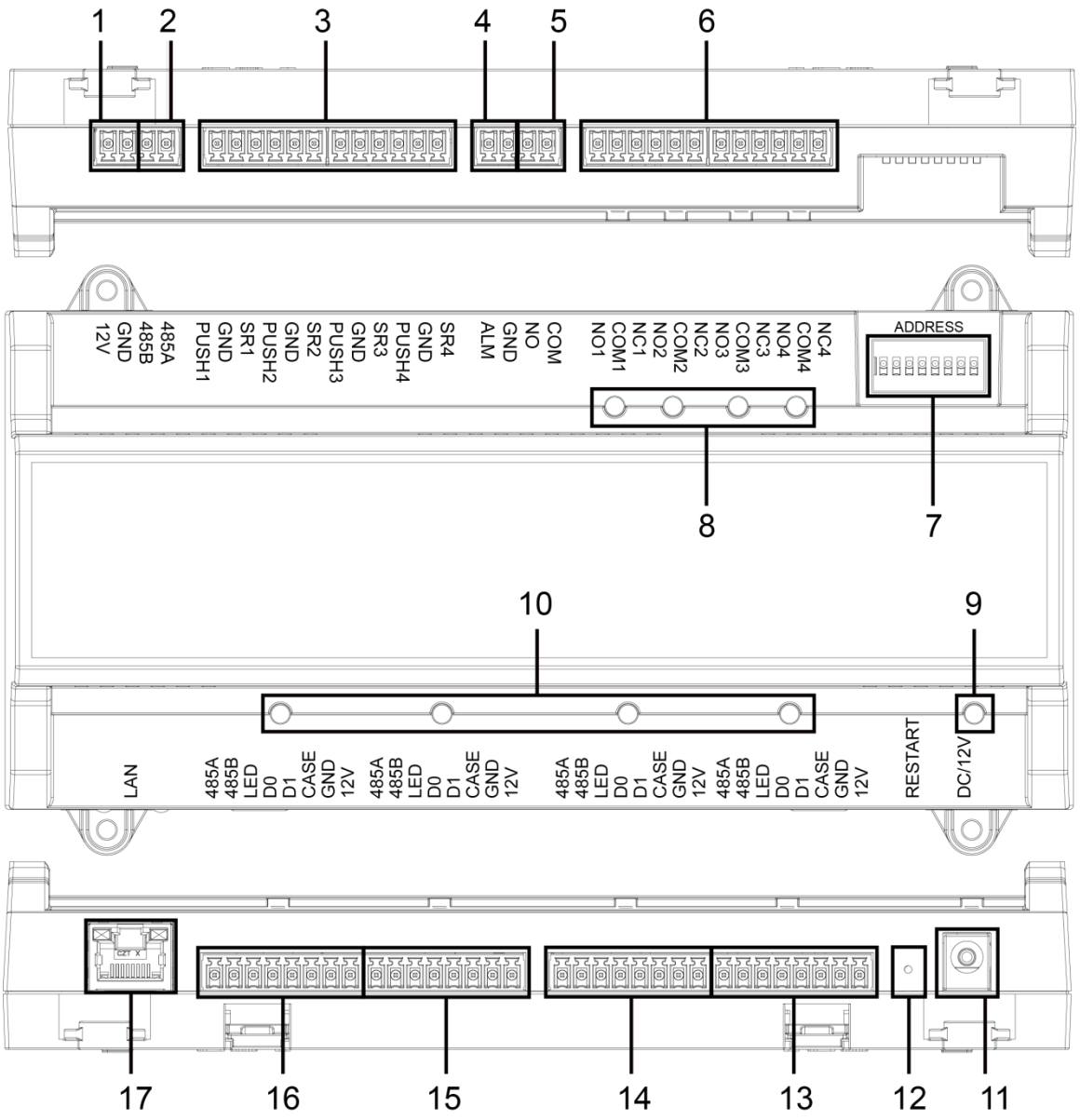


Tabla 1-3 Descripción de los componentes (cuatro puertas unidireccionales)

No.	Nombre	No.	Nombre
1	Puerto de alimentación de bloqueo de puerta	10	Luz indicadora del lector de tarjetas
2	Puerto RS-485	11	Puerto de alimentación
3	Botón de salida/puerto de contacto de puerta	12	Botón de reinicio
4	Puerto de entrada de alarma	13	Puerto de lector de tarjetas de entrada de la puerta No.4

No.	Nombre	No.	Nombre
5	Puerto de SALIDA de alarma	14	Puerto de lector de tarjetas de entrada de la puerta No.3
6	Puerto de SALIDA de control de bloqueo de puerta	15	Puerto de lector de tarjetas de entrada de la puerta No.2
7	Dip switch	dieciséis	Puerto de lector de tarjetas de entrada de la puerta No.1
8	Luz indicadora de bloqueo de puerta	17	puerto de red
9	Luz indicadora de poder	—	—

Puerto

Puerto autoadaptable de 10/100 Mbps y compatible con fuente de alimentación PoE.

Luz indicadora

- Luz indicadora de poder
  - ◇ Verde: Funciona normalmente.
  - ◇ Rojo: Anomalía de energía.
  - ◇ Azul: Actualización.
- Luz indicadora de alarma
  - ◇ Encendido: se activa la alarma. Apagado:
  - ◇ la alarma no se dispara. Luz indicadora
- de cerradura de puerta
  - ◇ Encendido: la cerradura de la puerta está conectada.
  - ◇ Apagado: la cerradura de la puerta no está
- conectada. Lector de tarjetas Luz indicadora
  - ◇ Encendido: El lector de tarjetas está conectado.
  - ◇ Apagado: el lector de tarjetas no está conectado.

Dip switch

Realice la operación correspondiente a través del interruptor DIP.

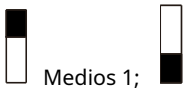
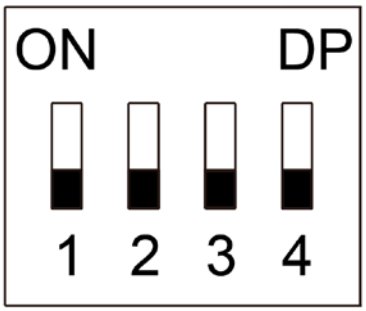
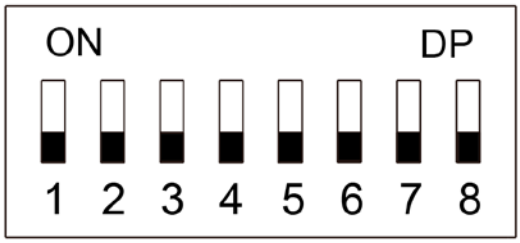
 Medios 1; significa 0.

Figure 1-6 Interruptor DIP (controlador de acceso unidireccional de dos puertas)



- 1–4 son todos 0, el dispositivo se inicia normalmente después del encendido. 1–4 son
- todos 1, el dispositivo ingresa al modo de inicio después del encendido.
- 1 y 3 son 1, 2 y 4 son 0, el dispositivo se restaura a los valores predeterminados de fábrica después de reiniciar.
- 2 y 4 son 1, 1 y 3 son 0, el dispositivo se restaura a los valores predeterminados de fábrica después de reiniciar. Pero la información del usuario se conservará.

Figure 1-7 Interruptor DIP (controlador de acceso de dos puertas de dos vías/cuatro puertas de una vía)



- 1–8 son todos 0, el dispositivo se inicia normalmente después del encendido. 1–8 son
- todos 1, el dispositivo ingresa al modo de inicio después del encendido.
- 1, 3, 5 y 7 son 1, 2, 4, 6 y 8 son 0, el dispositivo se restaura a los valores predeterminados de fábrica después de reiniciar.
- 1, 2, 4, 6 y 8 son 1, 1, 3, 5 y 7 son 0, el dispositivo se restaura a los valores predeterminados de fábrica después de reiniciar. Pero la información del usuario se conservará.

Reiniciar

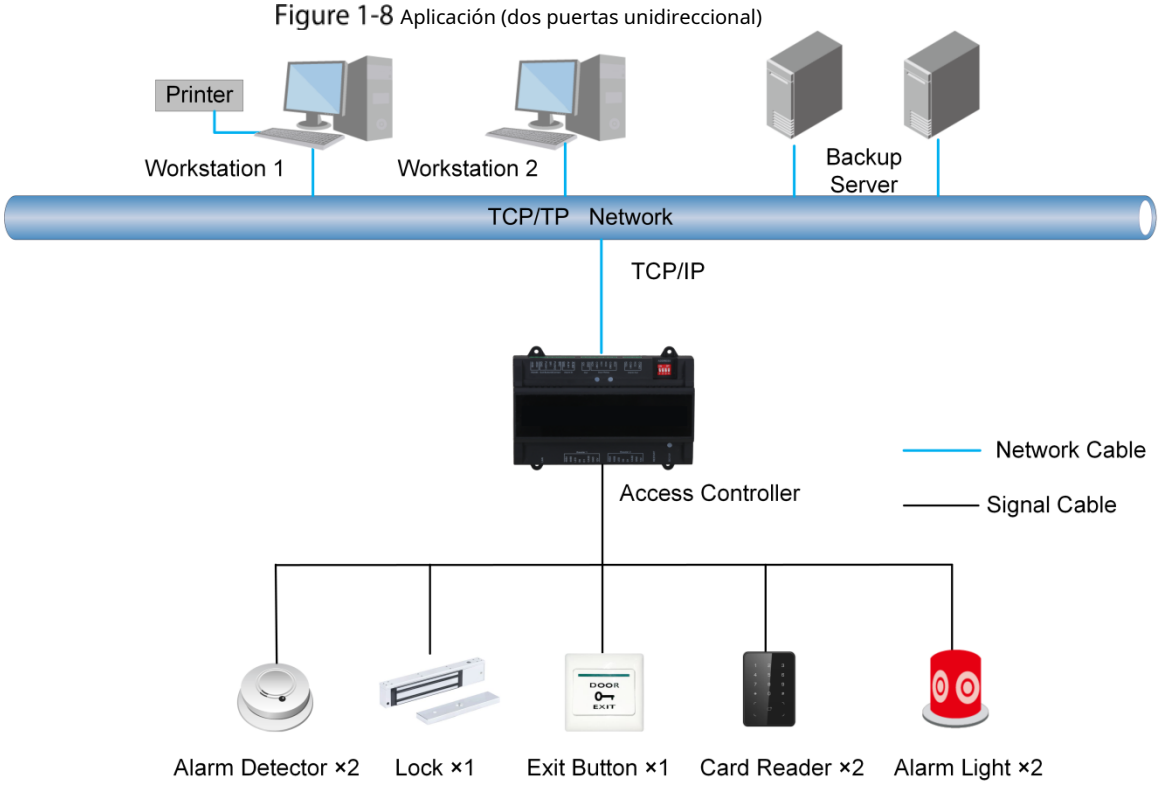
Inserte una aguja en el orificio de REINICIO y presiónela para reiniciar el dispositivo.

El botón de reinicio es para reiniciar el dispositivo, en lugar de modificar la configuración.

1.5 Solicitud

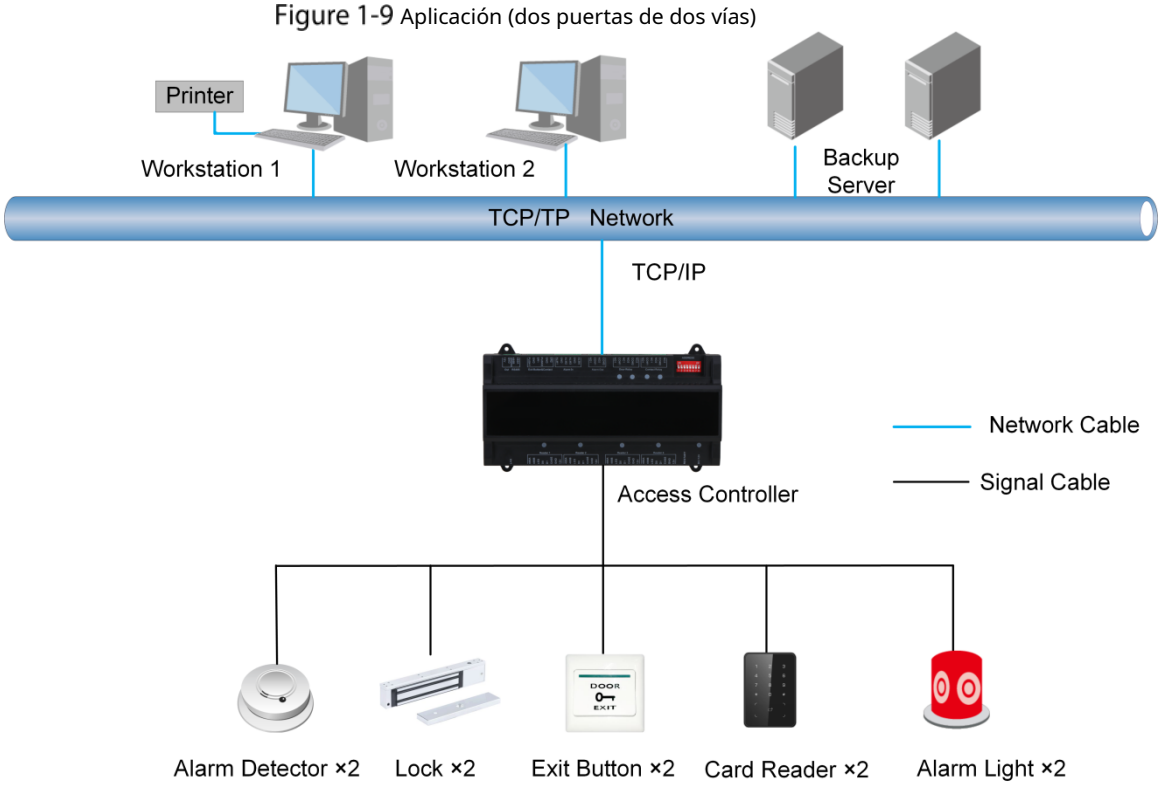
Controlador de acceso unidireccional de dos puertas

Figure 1-8 Aplicación (dos puertas unidireccional)



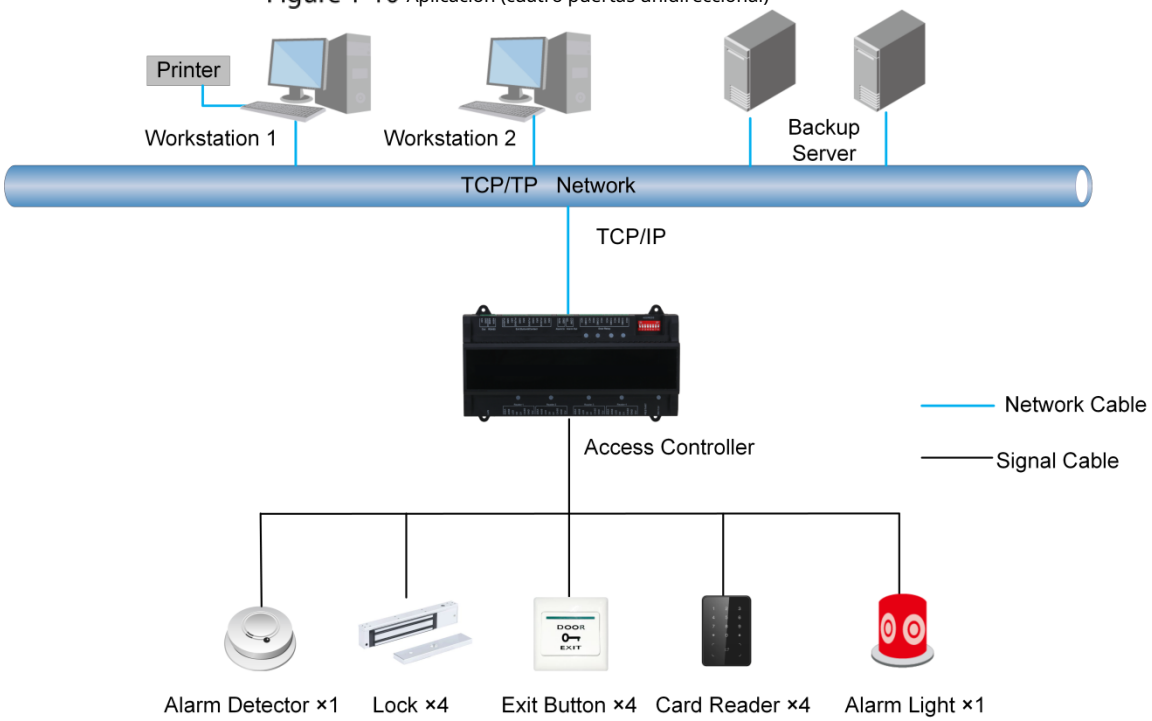
Controlador de acceso bidireccional de dos puertas

Figure 1-9 Aplicación (dos puertas de dos vías)



Controlador de acceso unidireccional de cuatro puertas

Figure 1-10 Aplicación (cuatro puertas unidireccional)

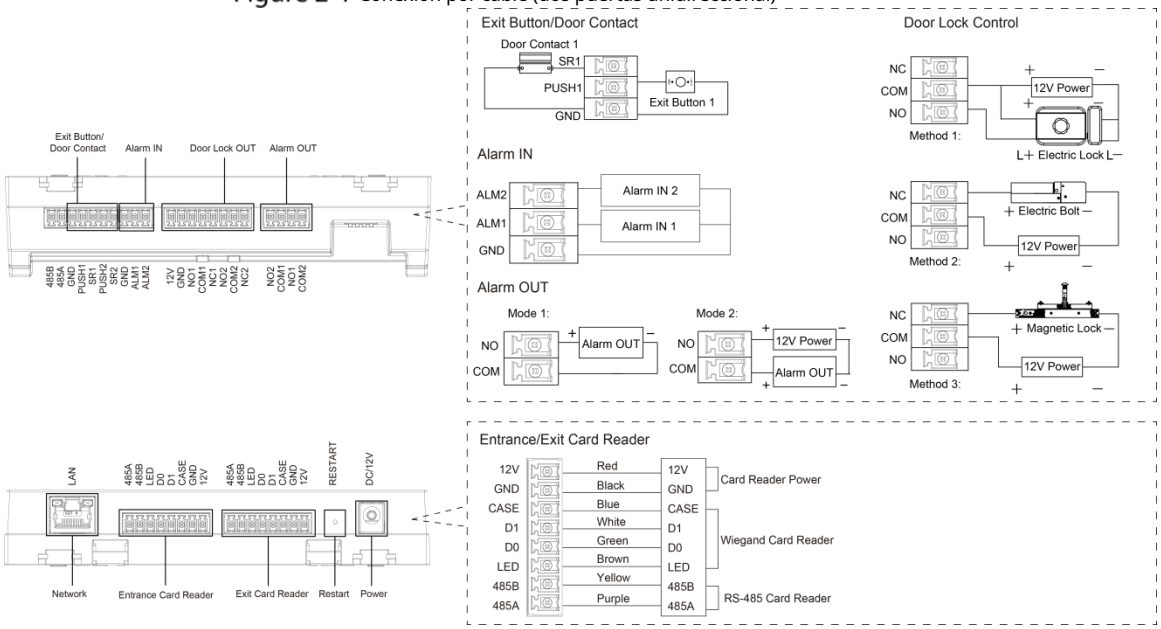


2 Instalación

2.1 Conexión de cable

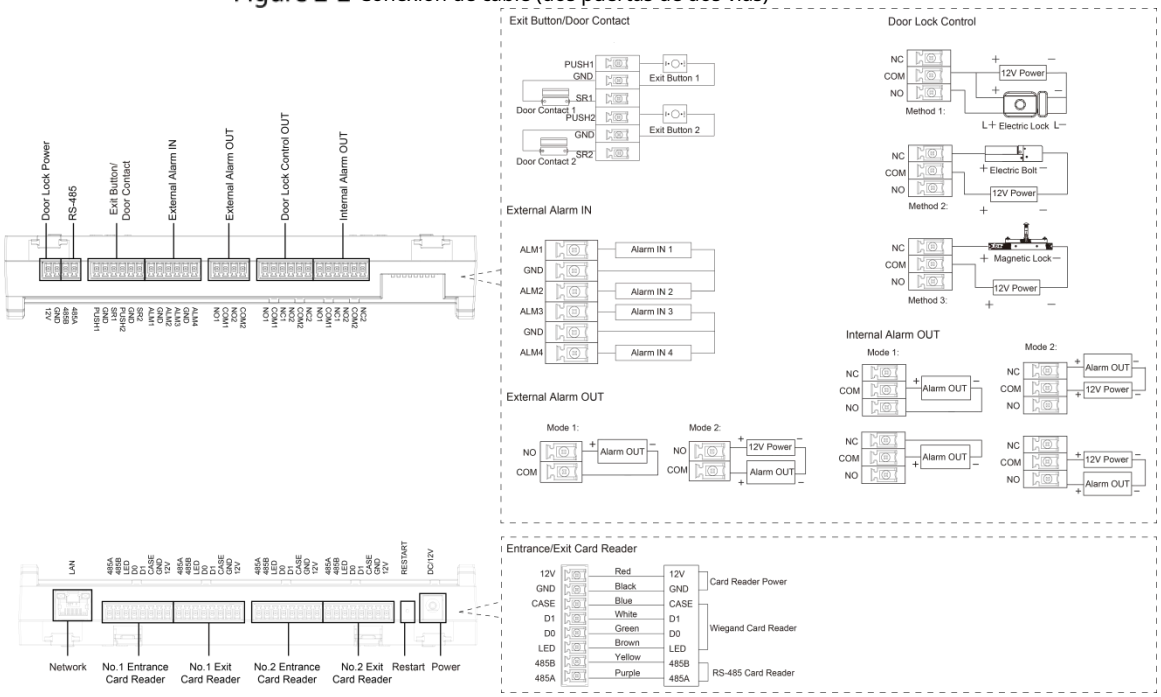
Controlador de acceso unidireccional de dos puertas

Figure 2-1 Conexión por cable (dos puertas unidireccional)



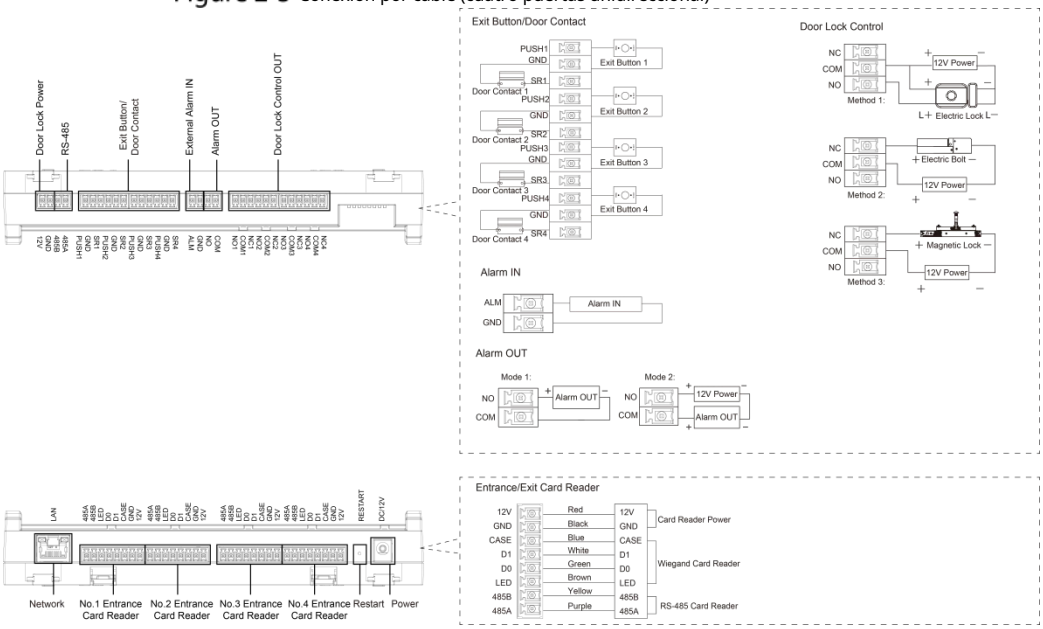
Controlador de acceso bidireccional de dos puertas

Figure 2-2 Conexión de cable (dos puertas de dos vías)



Controlador de acceso unidireccional de cuatro puertas

Figure 2-3 Conexión por cable (cuatro puertas unidireccional)



2.1.1 Conexión de cable de entrada de alarma

El puerto de entrada de alarma externa se puede conectar a detectores de humo, detectores de infrarrojos y más.

Tabla 2-1 Conexión de cable de entrada de alarma

Modelo	Canal de entrada de alarma	Descripción
Dos puertas de una sola mano	Entrada de alarma de 2 canales.	La alarma externa se puede vincular al estado de bloqueo/desbloqueo de la puerta. La alarma externa ALM1 vincula todas las puertas para que estén normalmente abiertas. La alarma externa ALM2 vincula todas las puertas para que estén normalmente cerradas.
Dos puertas bidireccional	Entrada de alarma de 4 canales.	La alarma externa se puede vincular al estado de bloqueo/desbloqueo de la puerta. La alarma externa ALM1–ALM2 vincula todas las puertas para que estén normalmente abiertas. La alarma externa ALM3–ALM4 vincula todas las puertas para que estén normalmente cerradas.
cuatro puertas de una sola mano	Entrada de alarma de 1 canal.	Cuando se dispara la alarma externa, todas las puertas están normalmente abiertas.

2.1.2 Conexión de cable de salida de alarma

La entrada de alarma interna o externa activa una alarma, y el dispositivo de salida de alarma emite una alarma durante 15 s.

Hay dos modos de conexión de salida de alarma. Seleccione el modo de conexión según el dispositivo de alarma. Por ejemplo, IPC puede usar el modo 1, y el dispositivo de luz y sonido puede usar el modo 2.

Cuando los controladores de acceso bidireccional de dos puertas están conectados al dispositivo de salida de alarma interna, seleccione NC/NO según el estado normalmente abierto o normalmente cerrado.

Tabla 2-2 Conexión de cable de salida de alarma

Modelo	Canal de salida de alarma	Puerto	Descripción
	Salida de alarma de 2 canales.	NO1	ALM1 activa la salida de alarma.

Modelo	Canal de salida de alarma	Puerto	Descripción
Dos puertas de una sola mano		COM1	Alarma de tiempo de espera de contacto de puerta y alarma de intrusión. Salida de alarma de sabotaje del lector de tarjetas de entrada de la puerta No.1.
		NO2	ALM2 activa la salida de alarma.
		COM2	Salida de alarma de sabotaje del lector de tarjetas de entrada de la puerta No.2.
Dos puertas bidireccional	2 canales externo salida de alarma	NO1	Salida de alarma de activación ALM1/ALM2.
		COM1	
		NO2	Salida de alarma de activación ALM3/ALM4.
		COM2	
	2 canales interno salida de alarma	NC1	Salida de alarma antisabotaje de los lectores de tarjetas de entrada y salida de la puerta n.º 1.
		COM1	
		NO1	Alarma de tiempo de espera de contacto de puerta y alarma de intrusión de la puerta n.º 1.
		NC2	Salida de alarma de sabotaje de los lectores de tarjetas de entrada y salida de la puerta No.2.
		COM2	
		NO2	Alarma de tiempo de espera de contacto de puerta y alarma de intrusión de la puerta No.2.
cuatro puertas de una sola mano	Salida de alarma de 1 canal.	NO	ALM activa la salida de alarma.
		COM	Alarma de tiempo de espera de contacto de puerta y alarma de intrusión. Salida de alarma de manipulación del lector de tarjetas.

2.1.3 Conexión del cable del lector de tarjetas

Una puerta solo admite un tipo de lector de tarjetas: RS-485 o Wiegand.

Tabla 2-3 Especificación del cable y longitud del lector de tarjetas

Tipo de lector de tarjetas	Modo de conexión	Longitud
Lector de tarjetas RS-485	Cable de red CAT5e, conexión RS-485	100 metros
Lector de tarjetas Wiegand	Cable de red CAT5e, conexión Wiegand	30 metros

2.2 Instalación del dispositivo

Hay dos métodos de instalación.

- Fije el dispositivo en la pared con tornillos.
- Instale el riel guía en forma de U (no incluido) en la pared y luego cuelgue el dispositivo en el riel guía.

Figure 2-4 Instalación (1)

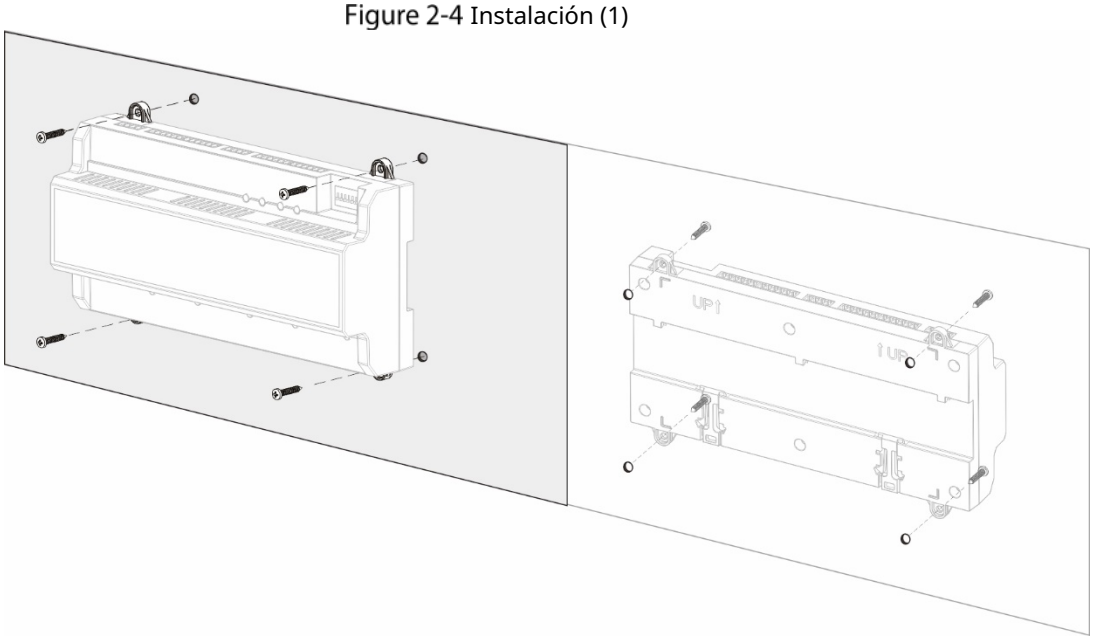
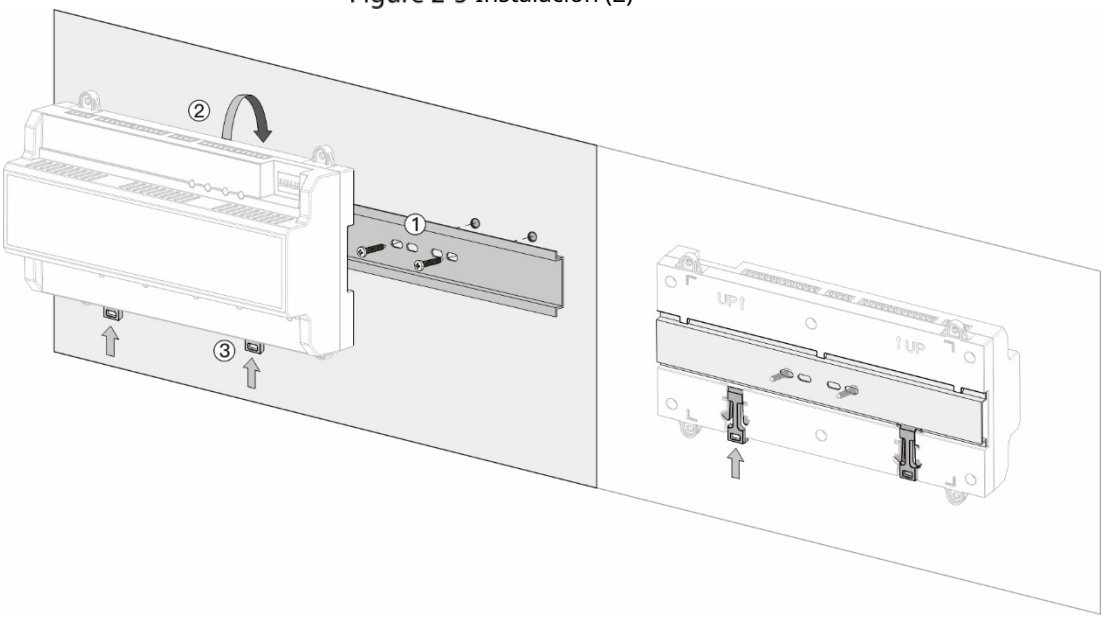


Figure 2-5 Instalación (2)



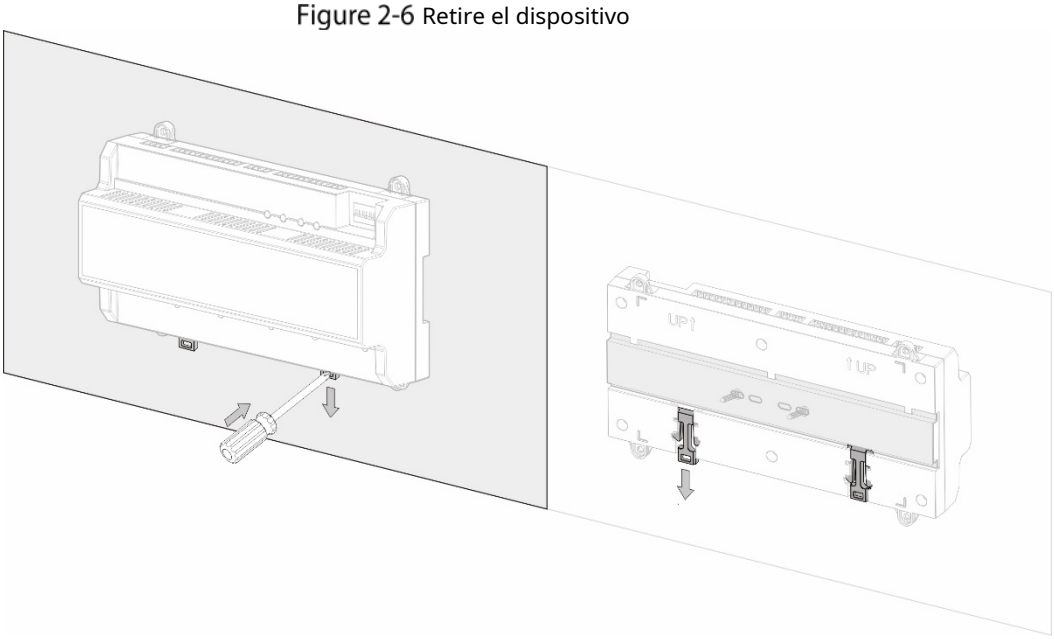
Step 1 Fije el riel guía en forma de U en la pared con tornillos.
Step 2 Abroche la parte trasera superior del dispositivo en el riel guía en forma de U. Empuje hacia
Step 3 arriba la hebilla en la parte inferior del dispositivo hasta que escuche un clic.

2.3 Quitar el dispositivo

Si el dispositivo se instala con el segundo método de instalación, consulte la Figura 2-6 cuando desee retirar el dispositivo.

Use un destornillador para presionar firmemente la hebilla y luego haga rebotar la hebilla para quitar el dispositivo.

Figure 2-6 Retire el dispositivo



3 Configuración de CA de SmartPSS

Puede administrar el dispositivo a través de SmartPSS AC. Esta sección presenta principalmente la configuración rápida de dispositivos. 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.

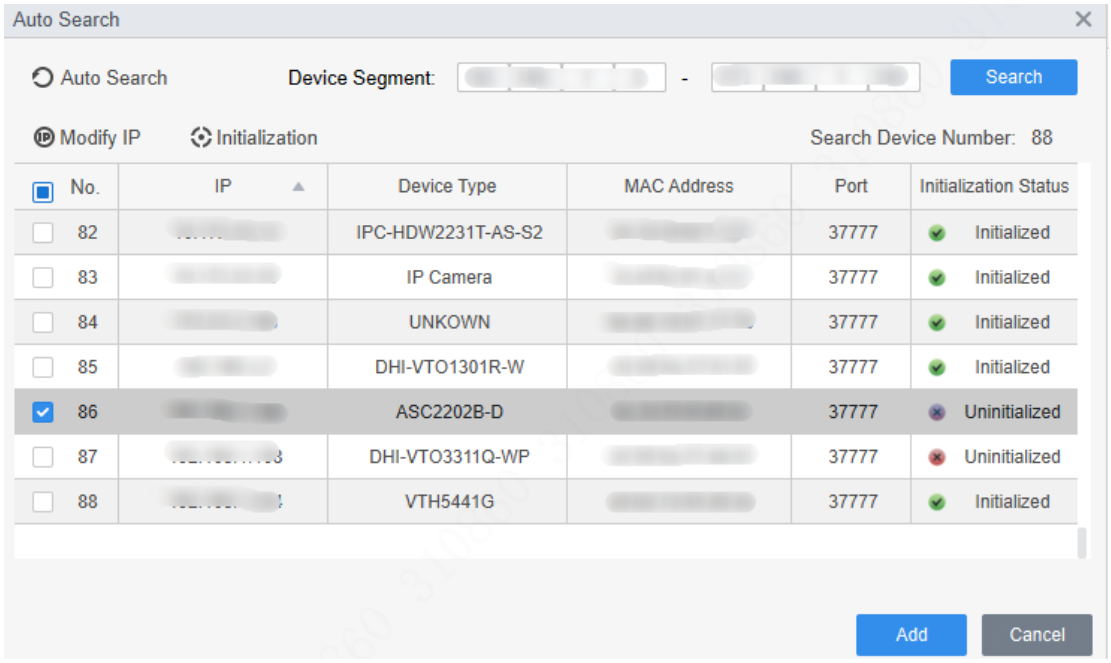
Step 2 Haga doble clic y luego siga las instrucciones para finalizar la inicialización e iniciar sesión.

3.2 Inicialización

Antes de la inicialización, asegúrese de que el dispositivo 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



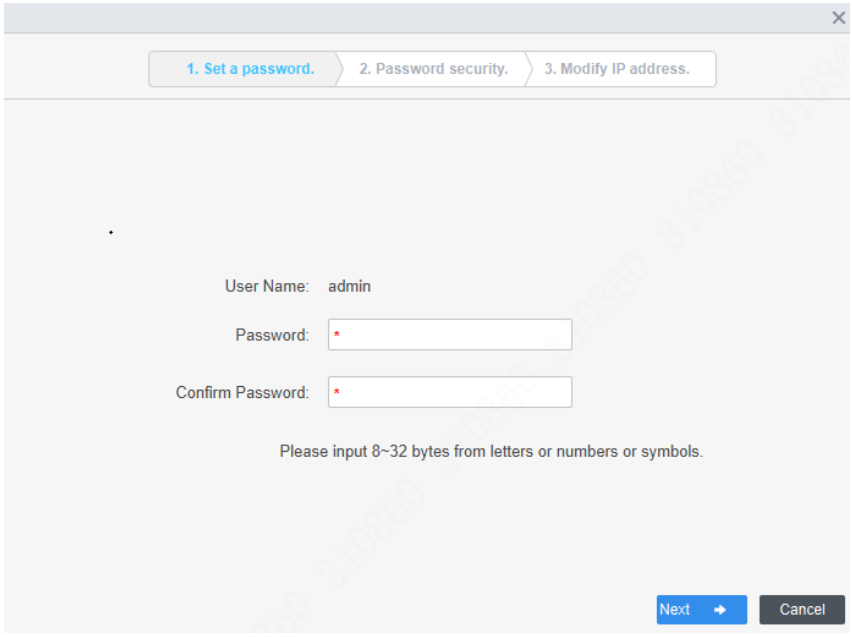
Step 2 Ingrese un rango de segmento de red y luego haga clic en**Búsqueda**.

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. Para obtener más información, consulte "1.4 Componentes".

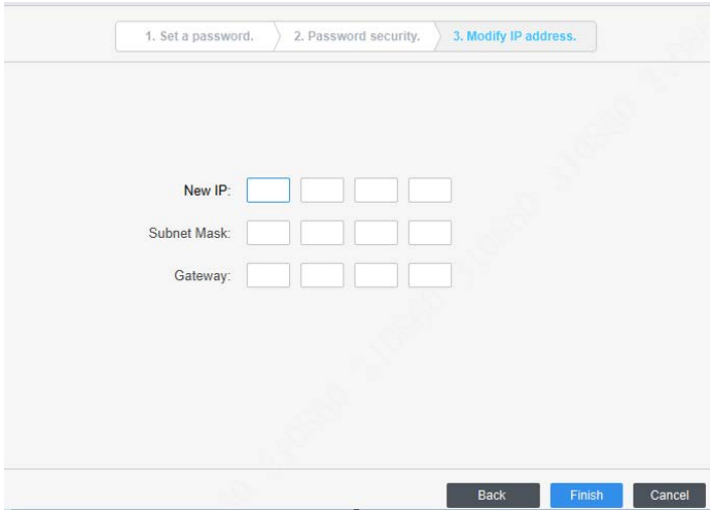
Figure 3-2 Configurar la clave



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**Finalizar**.

3.3 Adición de dispositivos

Debe agregar el dispositivo a SmartPSS AC. Puede agregar dispositivos en lotes mediante la búsqueda automática o agregar dispositivos individualmente.

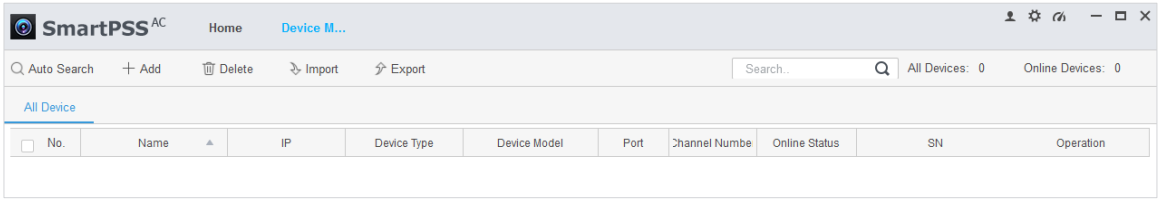
3.3.1 Búsqueda automática

Le recomendamos que agregue dispositivos mediante la búsqueda automática cuando necesite agregar dispositivos en lotes en el mismo segmento de red, o cuando conozca el rango del segmento de red en lugar de la dirección IP exacta.

Step 1 Inicie sesión en SmartPSS AC.

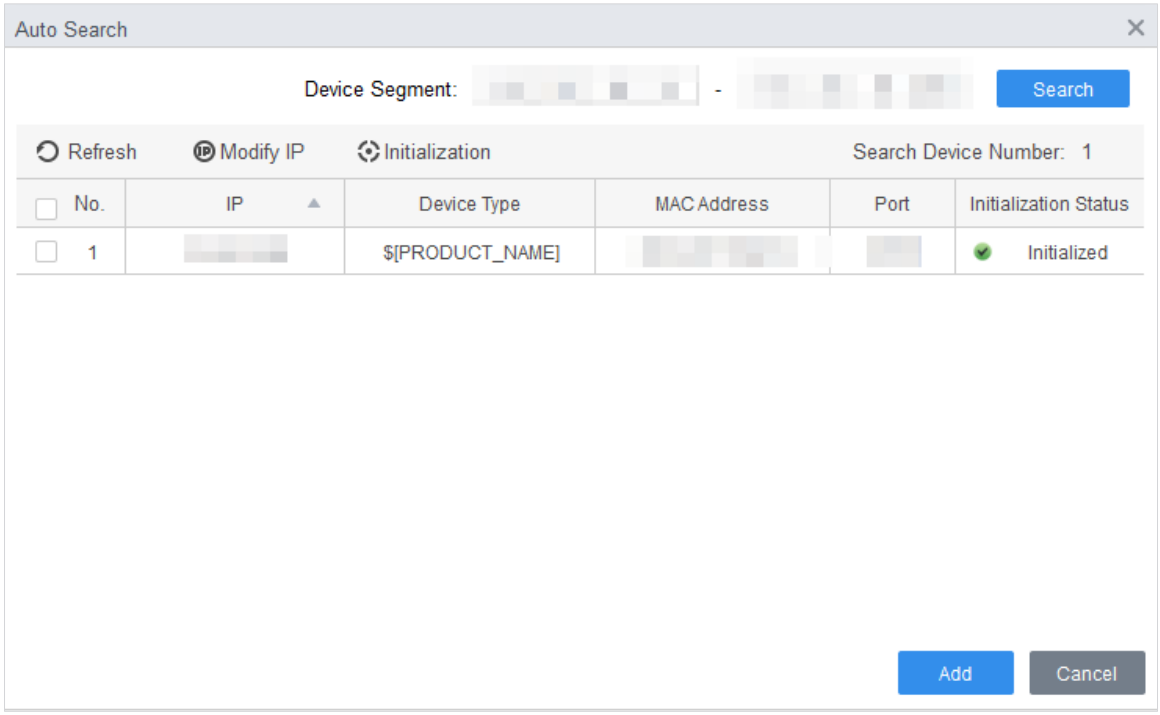
Step 2 Hacer clic**Administrador de dispositivos**en la esquina inferior izquierda.

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**.

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

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.

- El nombre de usuario es admin y la contraseña es admin123 por defecto. Te recomendamos modificar la contraseña después de iniciar sesión.
- Después de un inicio de sesión exitoso, se muestra el estado del dispositivo**En línea**. De lo contrario, muestra**Desconectado**.

3.3.2 Adición manual

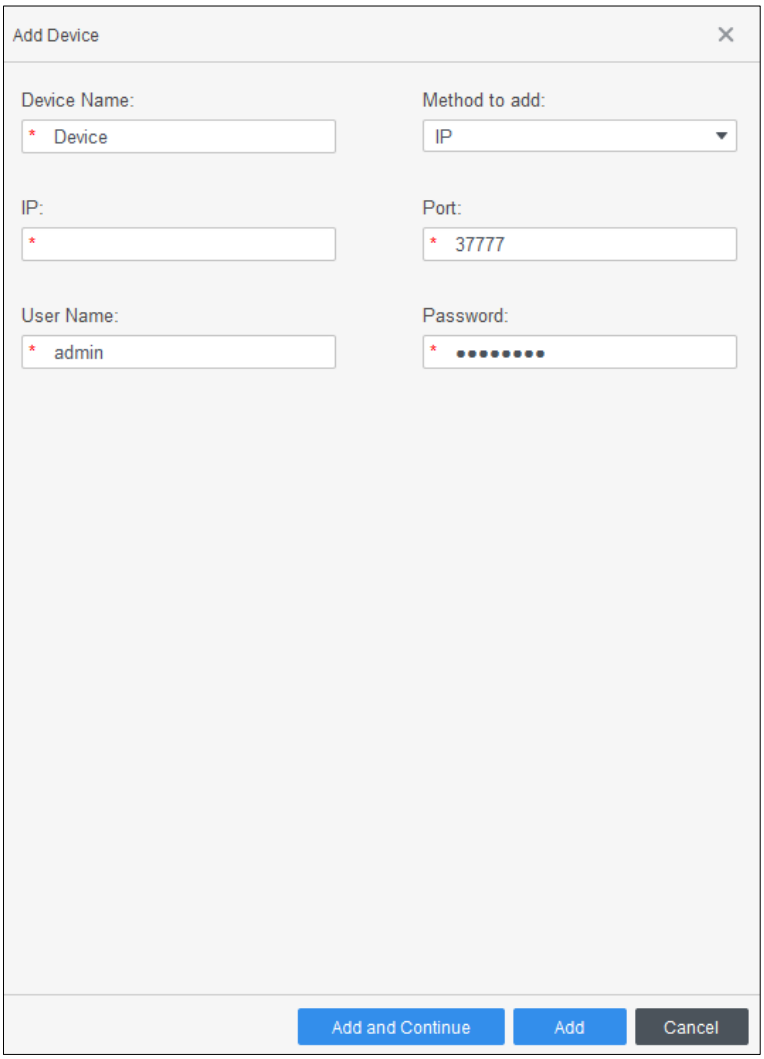
Puede agregar dispositivos manualmente. Debe conocer las direcciones IP y los nombres de dominio del controlador de acceso que desea agregar.

Step 1 Inicie sesión en SmartPSS AC.

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

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

Figure 3-6 Adición manual



Step 4 Ingrese la información del dispositivo.

Tabla 3-1 Parámetros

Parámetro	Descripción
Nombre del dispositivo	Ingrese un nombre del dispositivo. Le recomendamos que asigne al Dispositivo el nombre de su ubicación de instalación para facilitar su identificación.
Método para agregar	Seleccione**IP**para agregar el Dispositivo a través de su dirección IP.
IP	Ingrese la dirección IP del dispositivo. Es 192.168.1.108 por defecto.
Puerto	Introduzca el número de puerto del dispositivo. El número de puerto predeterminado es 37777.
Nombre de usuario, Clave	Ingrese el nombre de usuario y la contraseña del Dispositivo. El nombre de usuario es admin y la contraseña es admin123 por defecto. Se recomienda modificar la contraseña después de iniciar sesión.

Step 5 Hacer clic**Agregar**, y luego puede ver el dispositivo en la**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

3.4.1 Configuración del tipo de tarjeta

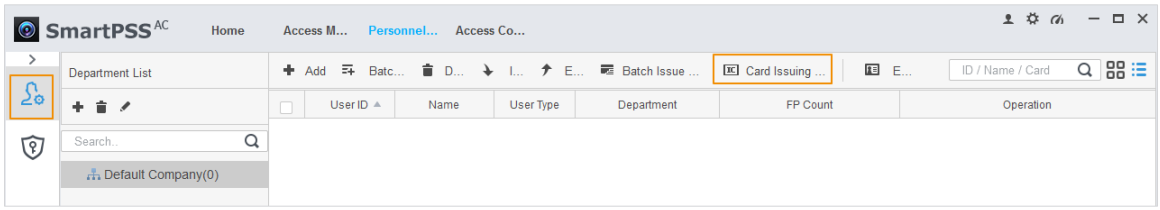
Antes de asignar una tarjeta, establezca primero el tipo de tarjeta. Por ejemplo, si la tarjeta asignada es una tarjeta de identificación, seleccione el tipo como tarjeta de identificación.

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

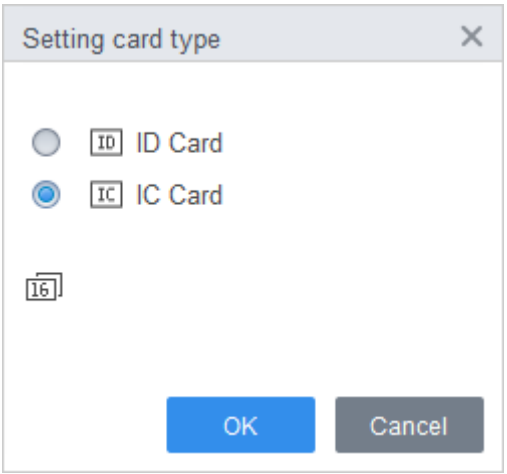


Step 3 Sobre el**Gerente de Personal**página, haga clic y luego haga clic en .

Step 4 Sobre el**Configuración del tipo de tarjeta**página, 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**OK**.

3.4.2 Agregar usuario

3.4.2.1 Añadir manualmente

Puede agregar usuarios individualesidualmente o manualmente.

Step 1 Inicie sesión en SmartPSS AC.

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

Step 3 Añadir información básica del usuario.

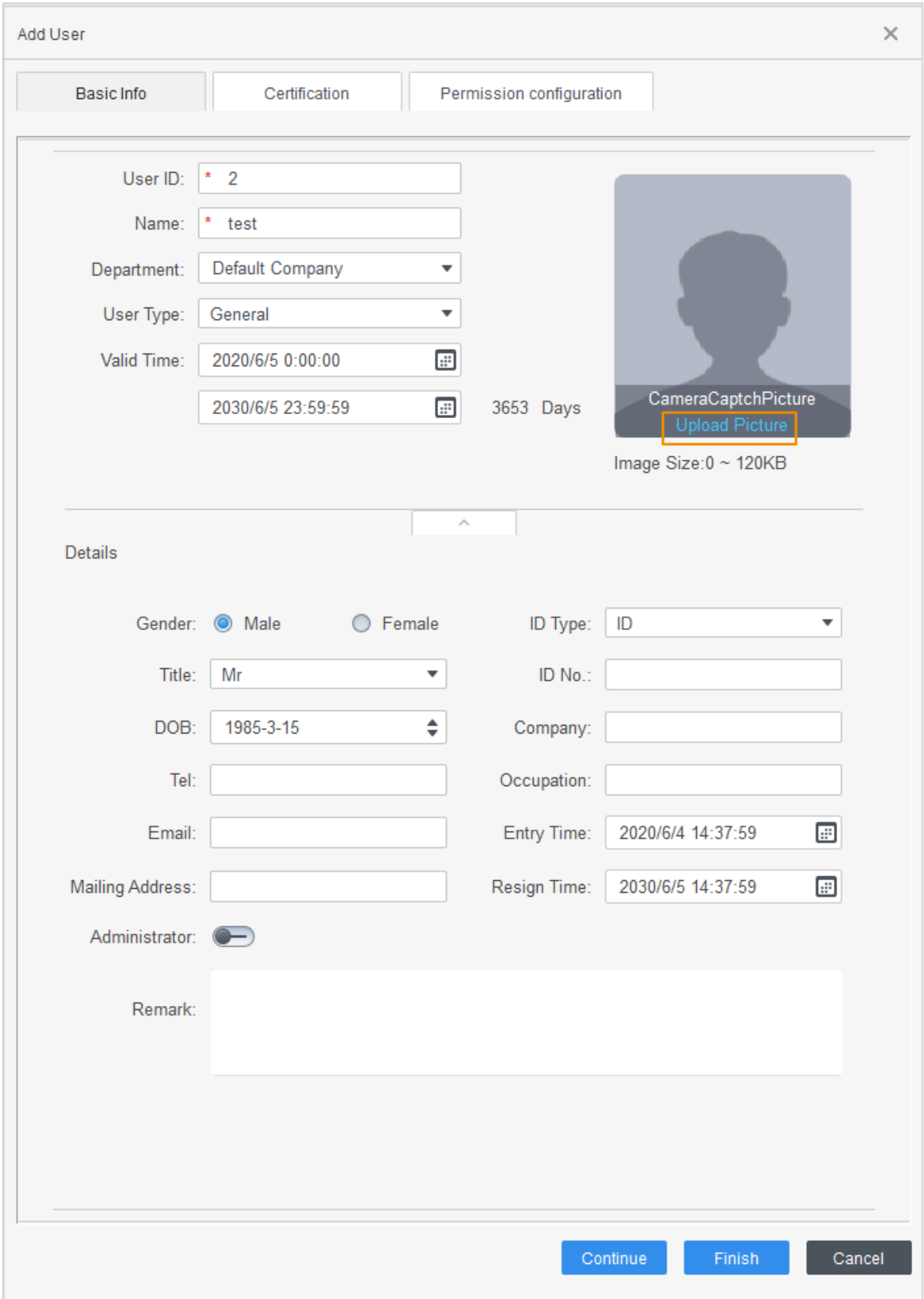
1) Haga clic en el**Información básica**pestaña en el**Agregar usuario**página, y luego agregue información básica del usuario.

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, configure 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 puede leerse automáticamente o rellenarse manualmente. Para leer automáticamente, seleccione un lector de tarjetas y luego coloque la tarjeta en el lector de tarjetas. Se lee el número de tarjeta automáticamente después de eso.

1) Haga clic para seleccionar**Dispositivo**o**Emisor de la tarjeta**como lector de tarjetas.

2) Añadir tarjeta. El número de tarjeta debe agregarse si se utiliza el controlador de acceso que no es de segunda generación.

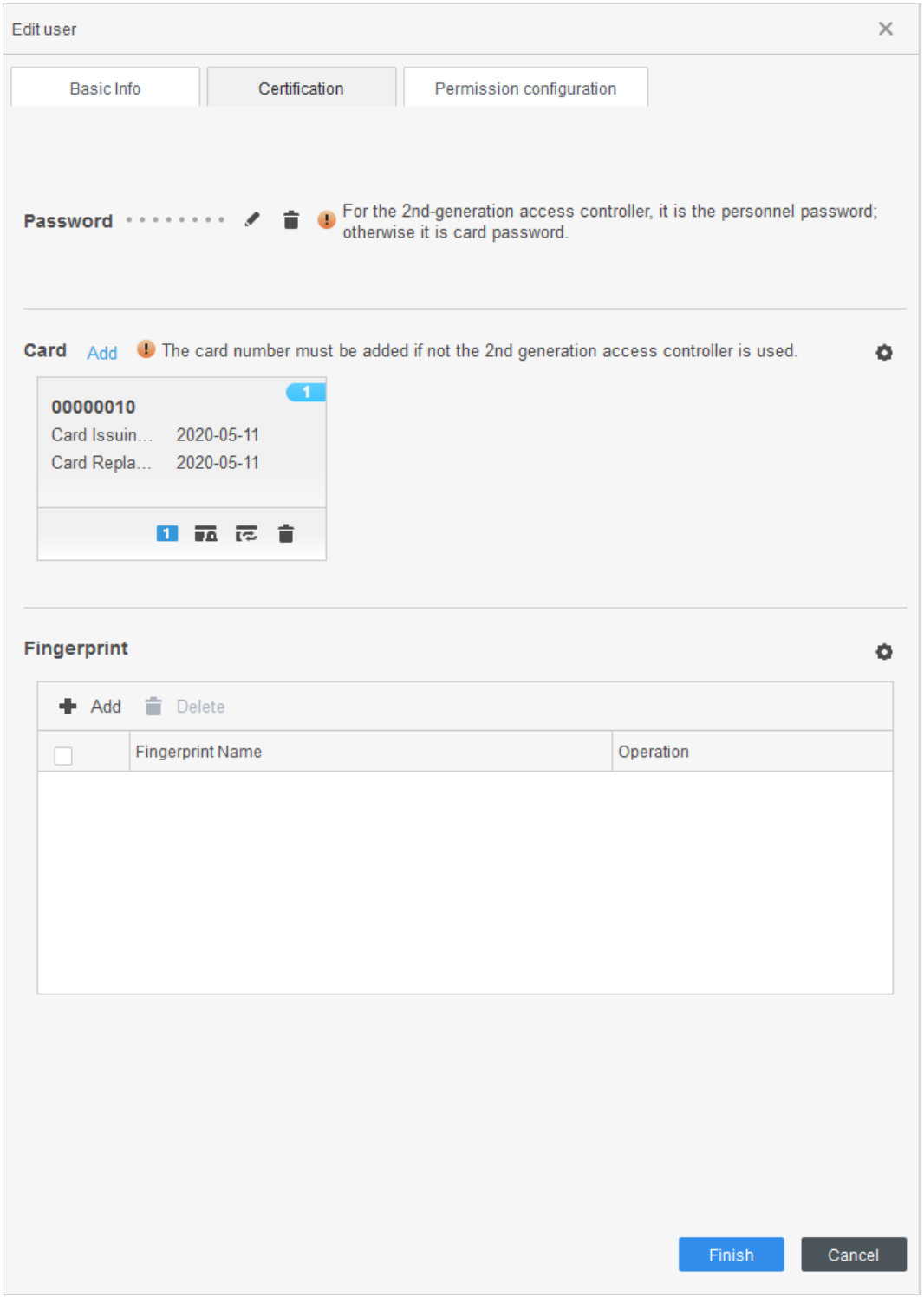
3) Después de agregar, puede seleccionar la tarjeta como tarjeta principal o tarjeta de coacción, o reemplazar la tarjeta por una nueva, o eliminar la tarjeta.

- Configurar huella dactilar.

1) Haga clic para seleccionar**Dispositivo**o**Escáner de huellas dactilares**como recolector de huellas dactilares.

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

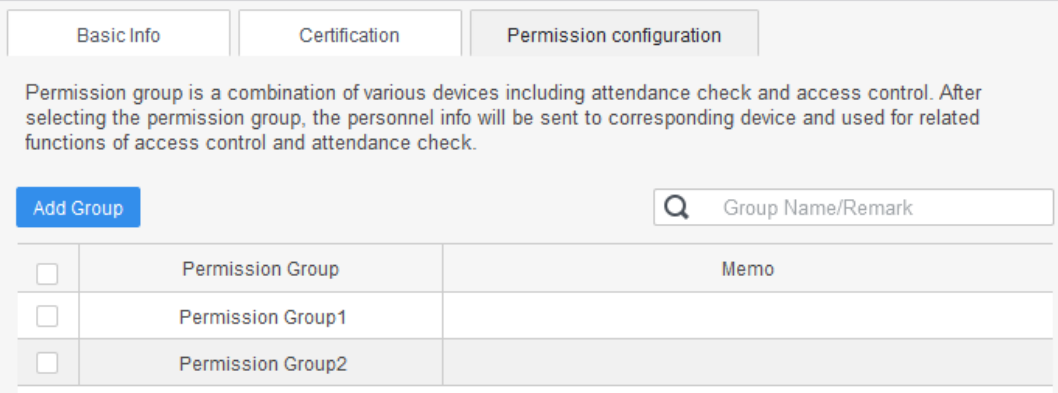
Figure 3-10 Configurar certificación



Step 5 Configure el permiso para el usuario.

Para más detalles, consulte "3.5 Configuración de permisos".

Figure 3-11 Configuración de permisos



Step 6 Hacer clic**Finalizar**.

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**.

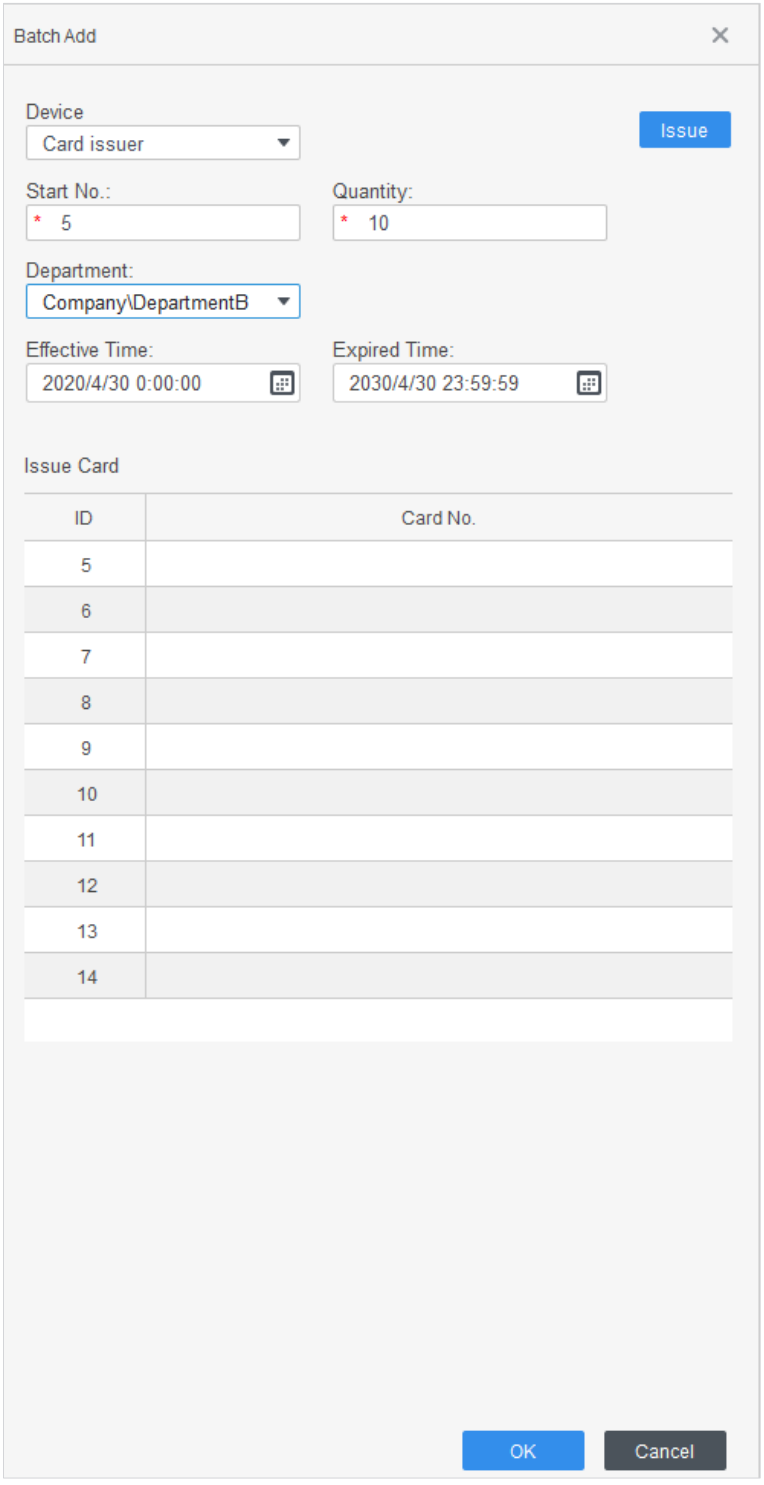
Step 3 Seleccione el lector de tarjetas y el departamento de usuario.

Step 4 Establezca el número de inicio, la cantidad de tarjetas, el tiempo efectivo y el tiempo de vencimiento de la tarjeta.

Step 5 Hacer clic**Tema**para asignar tarjetas de acceso a los usuarios. El número de tarjeta se leerá automáticamente. Hacer clic**Deténgase**después de asignar la tarjeta, y luego haga clic en**OK**.

Step 6

Figure 3-12 Agregar usuario en lotes



Step 7 En la lista de usuarios, haga clic en para modificar información o añadir detalles de usuarios.

3.5 Configuración de permisos

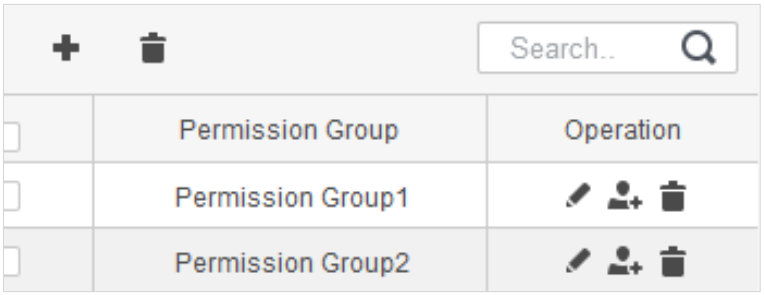
3.5.1 Agregar grupo de permisos

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.

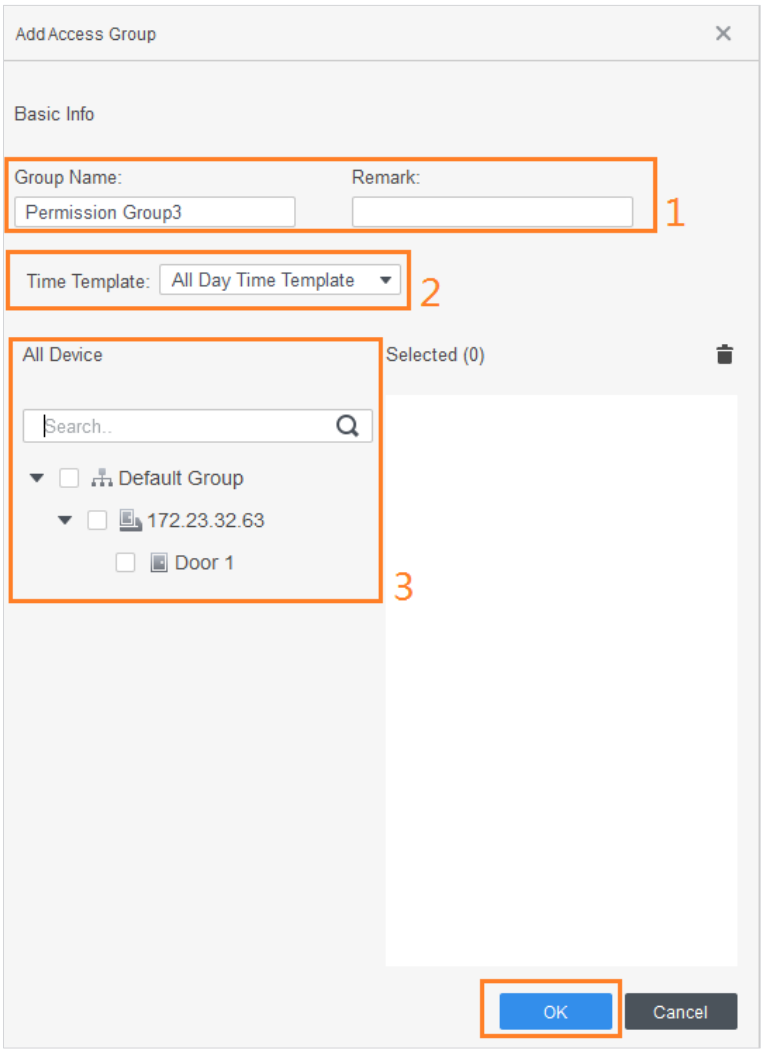
1) Introduzca el nombre del grupo y el comentario.

2) Seleccione una plantilla de tiempo.

Para obtener más información, 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**OK**.

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

- Hacer 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 permisos de acceso

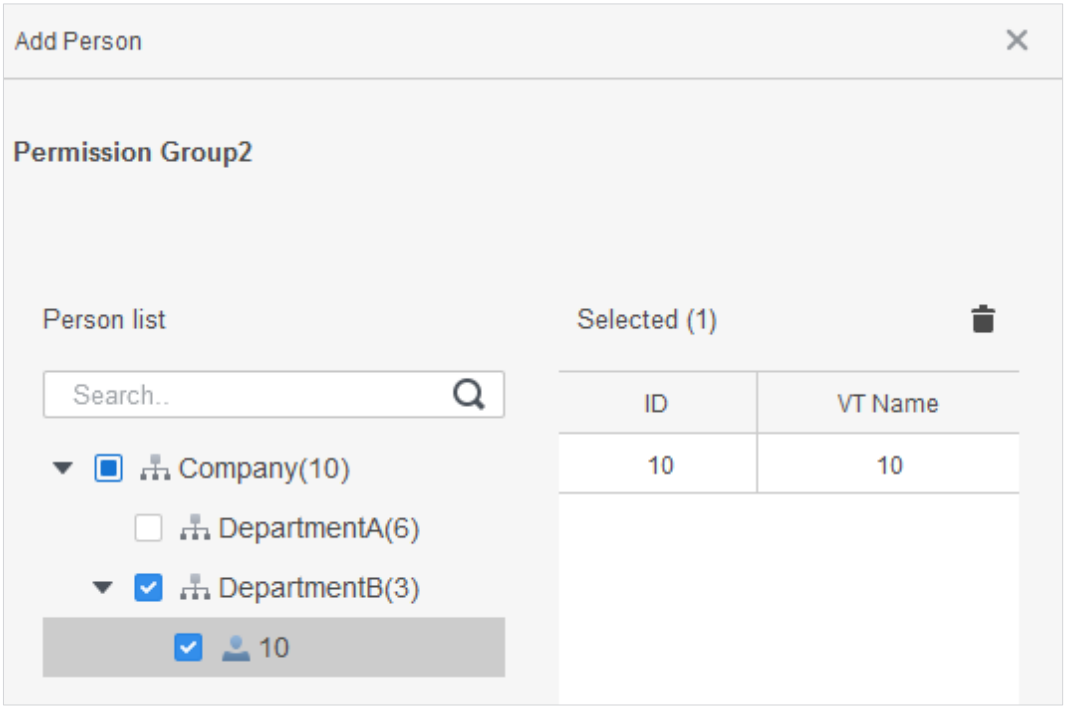
Asocie a los usuarios con los grupos de permisos deseados y luego a los usuarios se les asignarán permisos de acceso a las puertas definidas.

Step 1 Inicie sesión en SmartPSS AC.

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

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

Figure 3-15 Configurar permiso



Step 4 Seleccione usuarios para asociarlos con el grupo seleccionado.

Step 5 Hacer clic**OK**.

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 otorgará el permiso de primera tarjeta debe ser el**General**tipo de usuario y tienen acceso a ciertas puertas. Para obtener más información, consulte "3.4.2 Agregar 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 haga clic**Ahorrar**.

Figure 3-16 Configuración de desbloqueo de la primera tarjeta

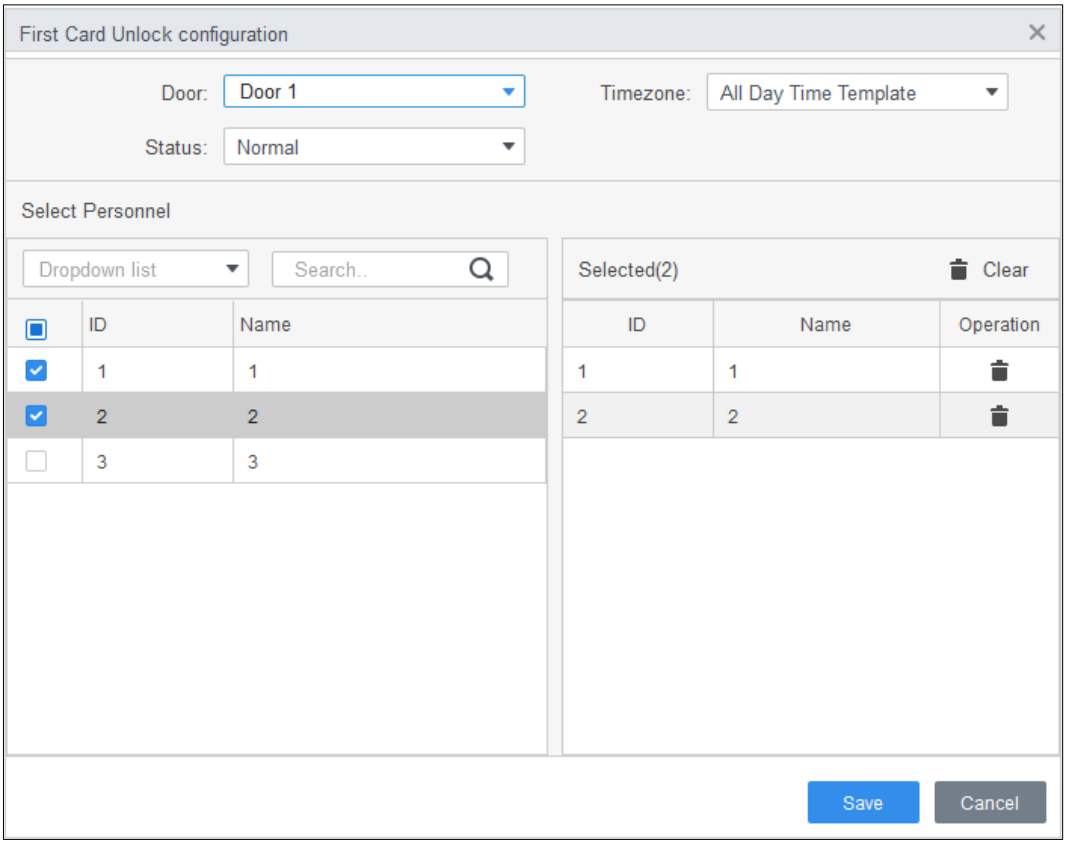


Tabla 3-2 Parámetros de desbloqueo de la primera tarjeta

Parámetro	Descripción
Puerta	Seleccione la puerta para el permiso de la primera tarjeta.

Parámetro	Descripción
Zona horaria	El permiso de la primera tarjeta solo es válido durante la plantilla de tiempo seleccionada.
Estado	Después de habilitar el desbloqueo de la primera tarjeta, seleccione el estado de la puerta:**Modo normal**o **Modo siempre abierto**.
Usuario	Puede seleccionar uno o varios titulares 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 de varias tarjetas

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 configure el tipo VIP o Patrulla para personas en el grupo de usuarios. Para obtener más información, consulte “3.4.2 Agregar usuario”.
- Para obtener detalles sobre la asignación de permisos, consulte "3.5 Configuración de permisos".

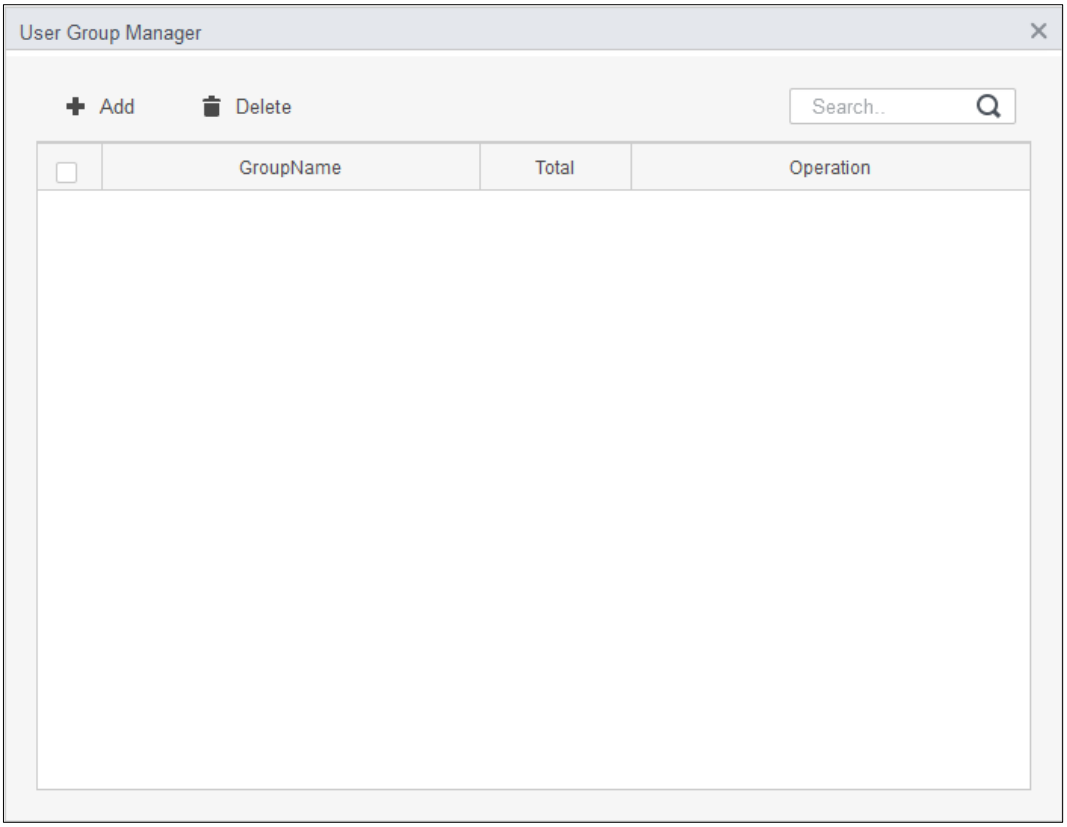
Step 1 Seleccione**Configuración de acceso**>**Configuración avanzada**. Haga clic en

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

Step 3

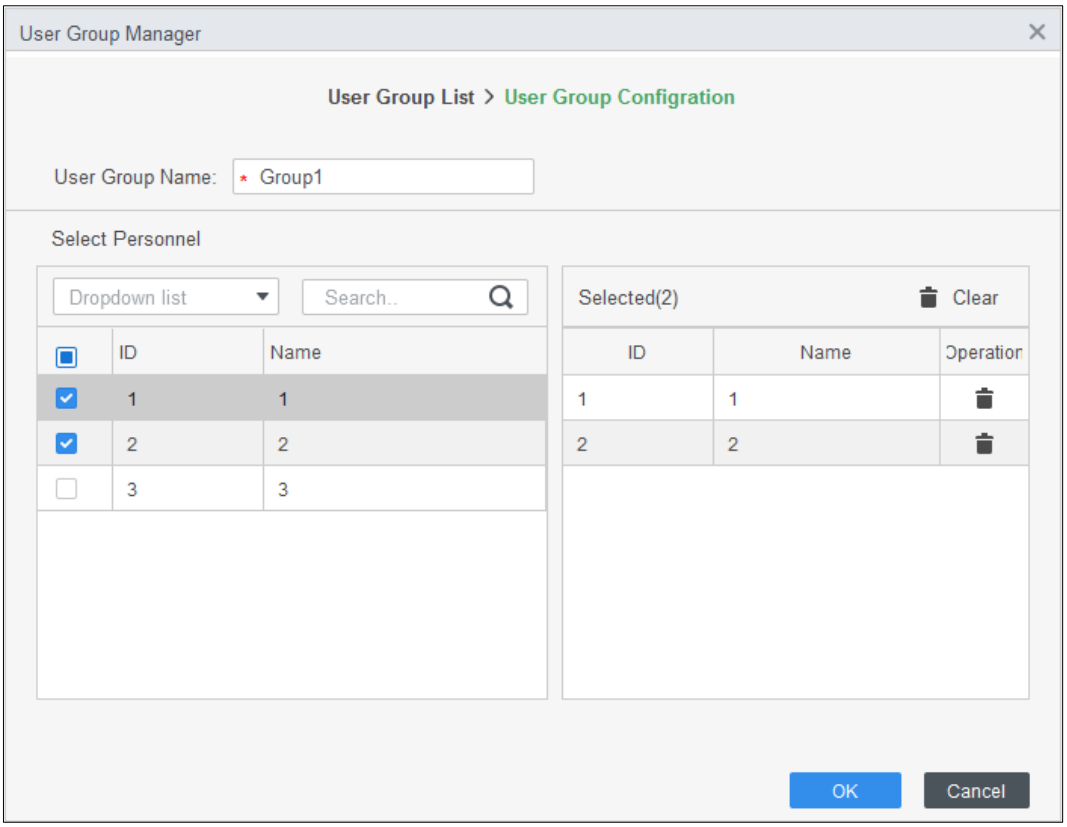
1) Haga clic**Grupo de usuario**.

Figure 3-17 Administrador de grupos de usuarios



2) Haga clic**Agregar**.

Figure 3-18 Configuración del grupo de usuarios



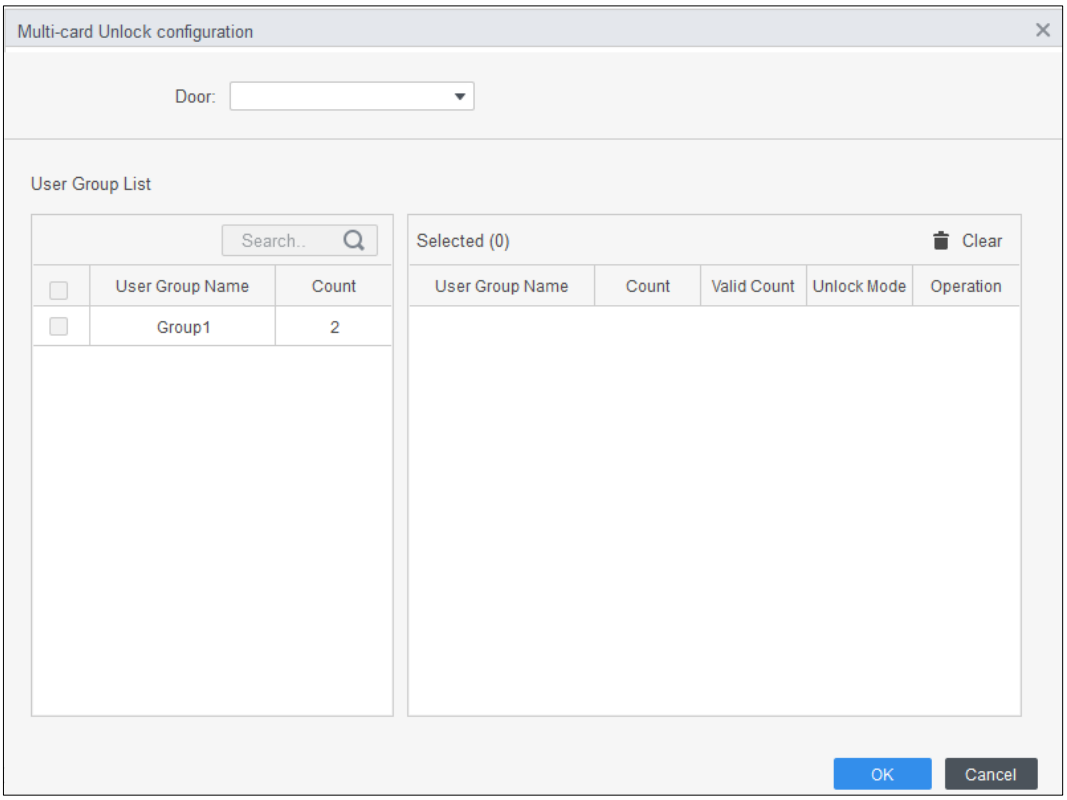
3) Introduzca el nombre del grupo de usuarios. Seleccione usuarios de la lista de usuarios y haga clic en**OK**. Puede seleccionar hasta 50 usuarios en un grupo.

4) Haga clic en

Step 4 Configure el parámetro de desbloqueo de múltiples tarjetas. 1)

Haga clic**Agregar**.

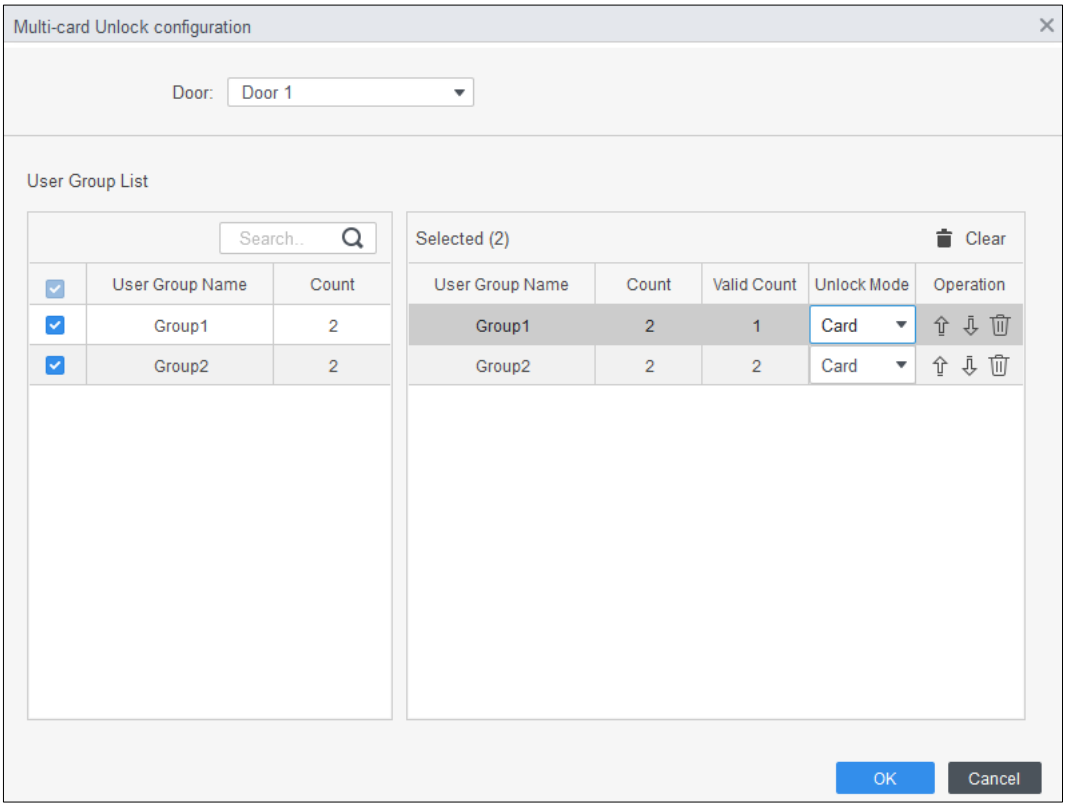
Figure 3-19 Configuración de desbloqueo multitarjeta (1)



2) Seleccione la puerta.

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

Figure 3-20 Configuración de desbloqueo de tarjetas múltiples (2)



4) Introduzca el**Recuento válido**en cada grupo. Haga clic en o para ajustar la secuencia del grupo a verificar identidad.

- El conteo válido se refiere al número de usuarios en cada grupo que debe estar presente para verificar sus identidades para desbloquear la puerta. Tome la figura 3-20 como ejemplo. La puerta se puede desbloquear solo después de que un usuario en el grupo 1 deslice la tarjeta primero y dos usuarios en grupo deslizan sus tarjetas.
- Se permiten hasta cinco usuarios válidos en total.

5) Haga clic**OK**.

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

los**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.

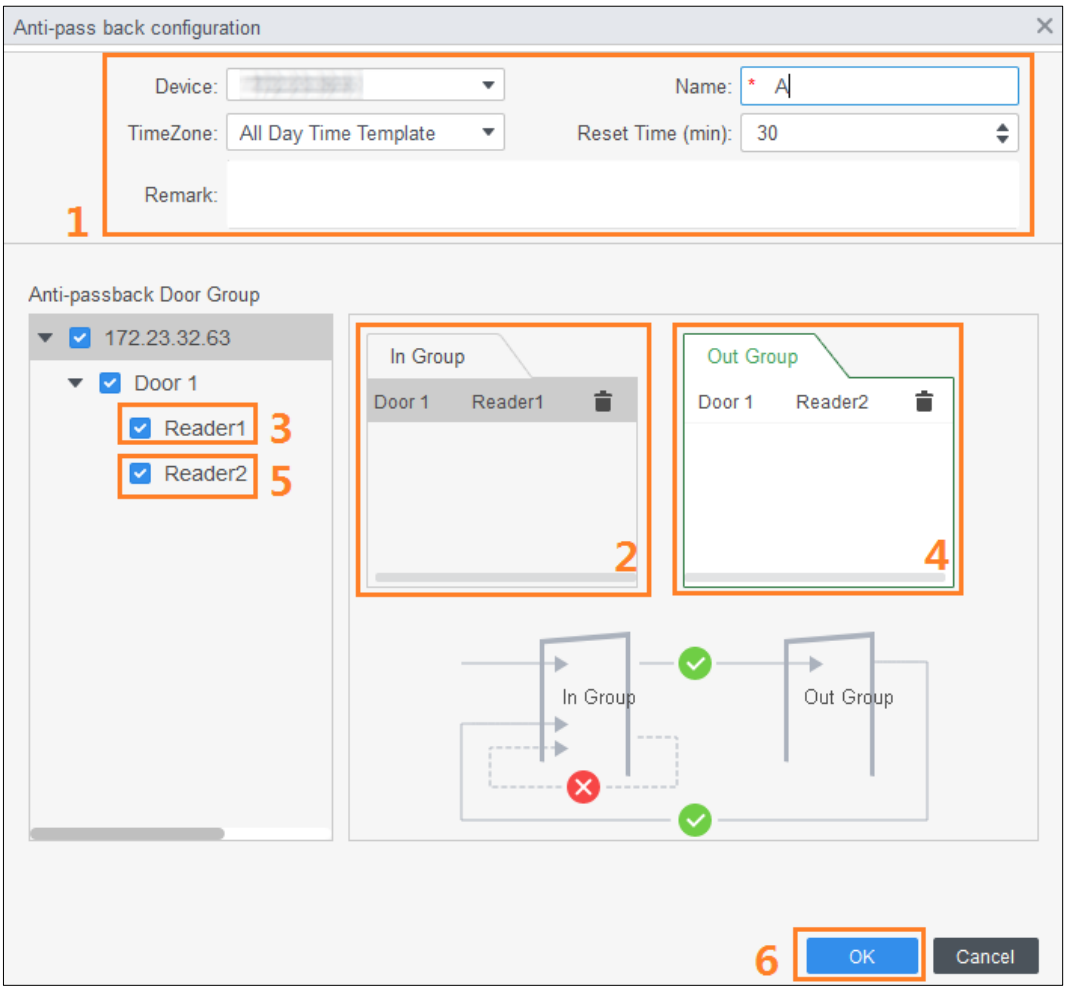
3) Establecer el tiempo de descanso.

Por ejemplo, establezca el tiempo de reinicio en 30 minutos. Si una persona desliza el dedo pero no sale, la alarma anti-retroceso se activará cuando la persona intente deslizar el dedo nuevamente dentro de los 30 minutos. Pueden ingresar al área controlada hasta que haya transcurrido el período de tiempo definido.

4) Haga clic**En grupo**y seleccione el lector de entrada, y luego haga clic en**fuera del grupo**y seleccione el lector de salida.

5) Haga clic**OK**.

Figure 3-21 Configuración anti-pass back



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

los**Anti-passback**está habilitado de forma predeterminada.

3.6.1.4 Enclavamiento de puerta

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**OK**.

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

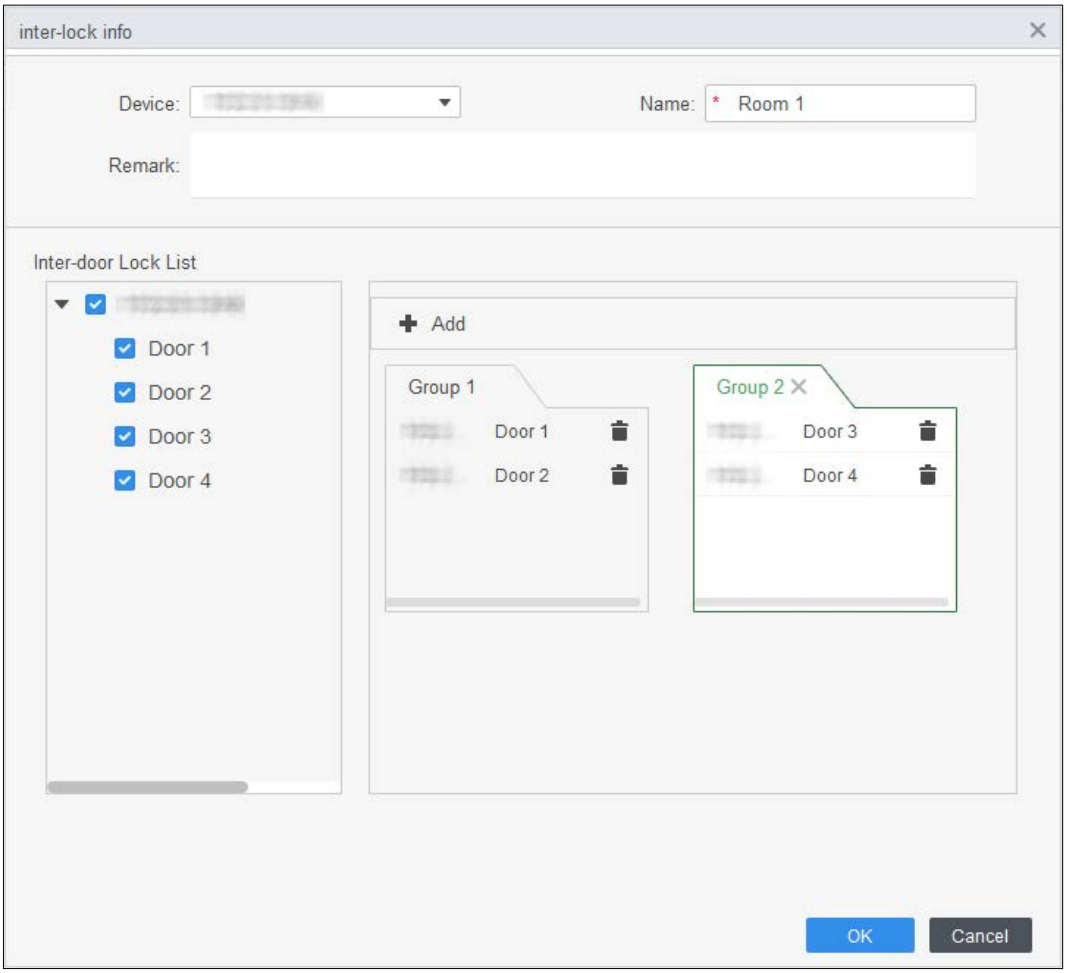
2) Introducir comentario.

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

4) Agregar puertas a grupos de puertas.

5) Haga clic**OK**.

Figure 3-22 Configuración de cerradura entre puertas



Step 5 (Opcional) Haga clic en . El ícono cambiando a indica**Cerradura entre puertas**está habilitado.

los**Cerradura entre puertas**está habilitado de forma predeterminada.

3.6.2 Configuración del controlador de acceso

Puede configurar la puerta de acceso, como el lector de entrada y el lector de salida, y el estado de la puerta.

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

Step 2 Haz clic en la puerta.

Step 3 Configurar parámetros.

Figure 3-23 Configurar puerta de acceso

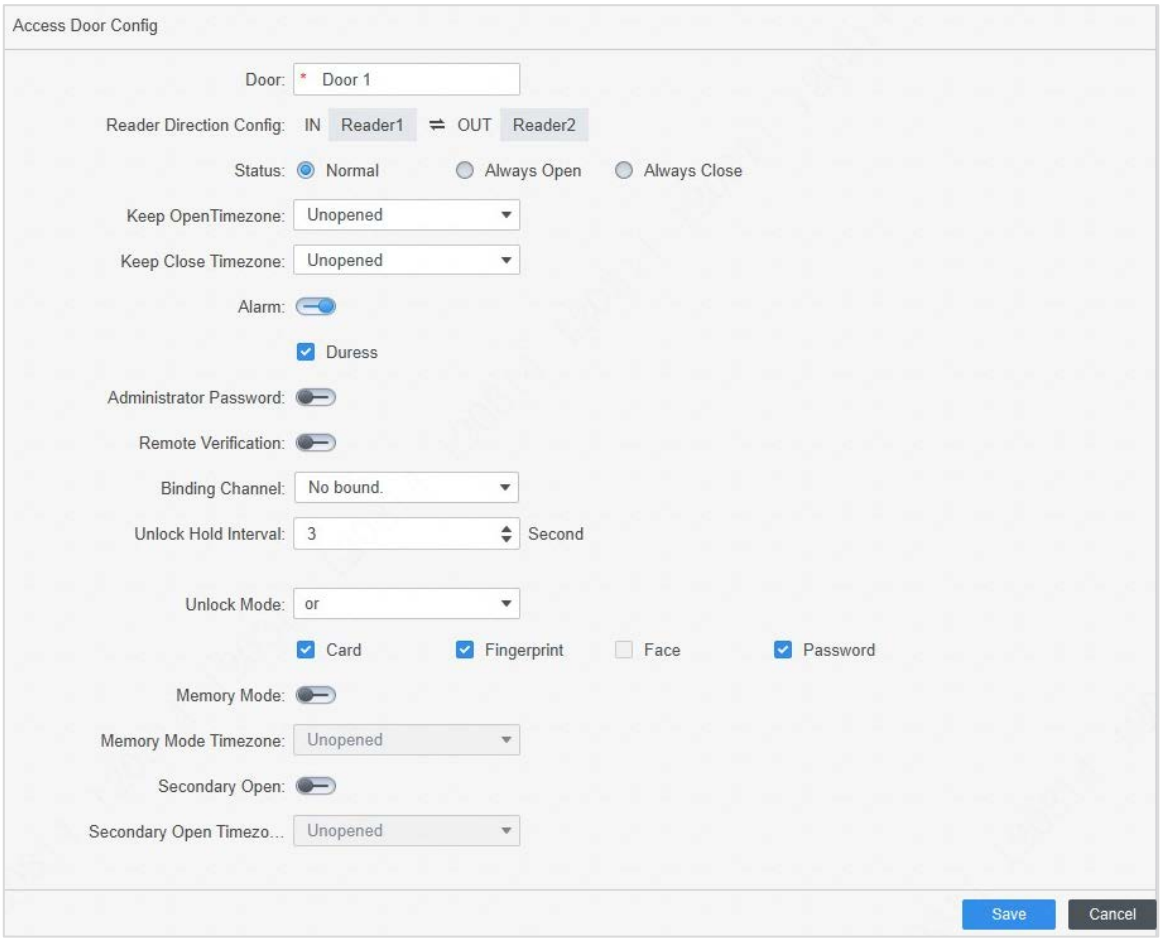


Figure 3-24 Desbloqueo por período de tiempo

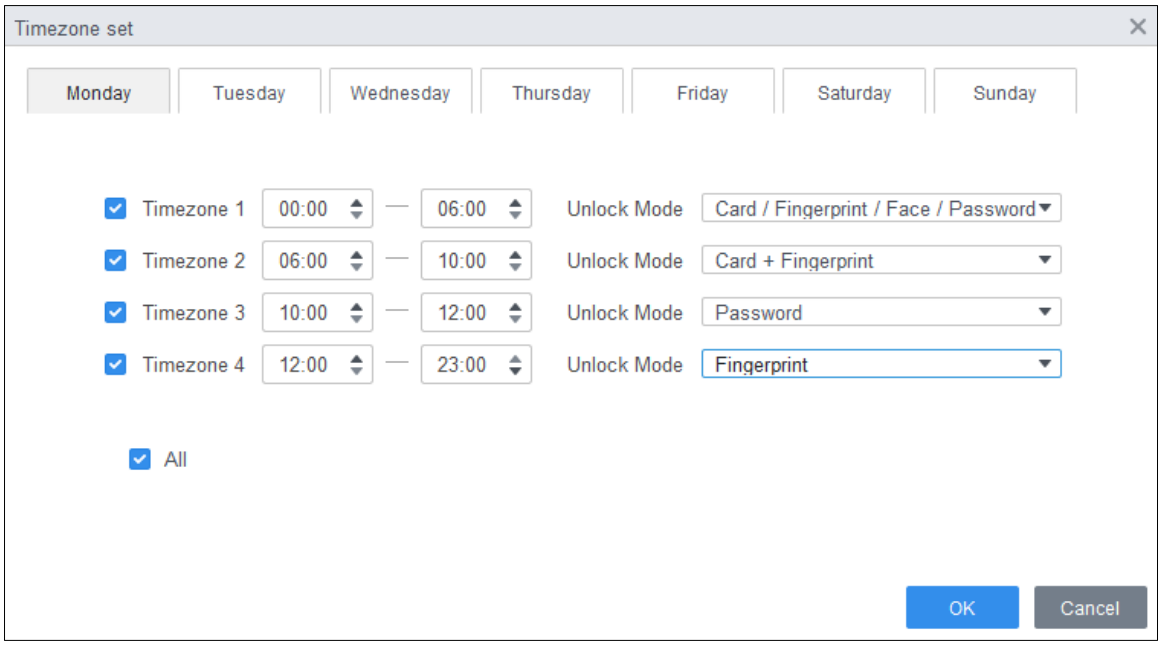


Tabla 3-3 Parámetros de la puerta de acceso

Parámetro	Descripción
Puerta	Introduzca el nombre de la puerta.
Dirección del lector	Hacer clic ⇌ para configurar el lector de entrada y salida.
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 y la puerta permanecerá abierta durante el período definido.
Mantener cerrada la zona horaria	Seleccione la plantilla de tiempo y la puerta permanecerá cerrada durante el período definido.
Alarma	Habilite la función de alarma y configure el tipo de alarma, incluidas intrusión, horas extra y coacción. Cuando la función de alarma está habilitada, el SmartPSS-AC recibirá mensajes de alarma cuando se active la alarma.
sensor de puerta	Habilite el sensor de puerta para que pueda conocer el estado real de la puerta. Le recomendamos que habilite la función.
Contraseña de administrador	Habilite y establezca la contraseña de administrador. Puede acceder introduciendo la contraseña.
Verificación remota	Habilite la función y configure la plantilla de tiempo. El acceso debe otorgarse desde SmartPSS-AC cuando un usuario intenta desbloquear la puerta después de una verificación de identidad válida.

Parámetro	Descripción
Canal remoto	Vincular canal de vídeo con canal de acceso. Puede ver el video en tiempo real del canal de acceso.
Intervalo de espera de desbloqueo	El tiempo durante el cual la puerta permanece abierta después de desbloquearla. La puerta se cerrará automáticamente cuando termine el tiempo predefinido.
Cerrar tiempo de espera	Se dispara una alarma cuando la puerta permanece abierta más allá del período definido. Por ejemplo, establezca el tiempo de espera de cierre en 60 segundos. Si la puerta permanece abierta durante más de 60 segundos, se dispara la alarma.
Modo de desbloqueo	Seleccione el modo de desbloqueo. **Y:**Verifique todos los métodos de desbloqueo seleccionados para abrir la puerta. **O**: Verifique uno de los métodos de desbloqueo seleccionados para abrir la puerta. **Desbloqueo por período de tiempo**: Los usuarios solo pueden desbloquear la puerta a través de métodos de desbloqueo predefinidos y según los horarios.
Modo de memoria	Después de deslizar la tarjeta una vez, más de una persona puede pasar el torniquete. Hay dos modos: Desactivado (predeterminado) y Activado. Si a varias personas se les permite el acceso a través del torniquete, y una de ellas no comenzó a pasar el torniquete en 5 segundos, o una de ellas no pasó el torniquete dentro de la duración definida y permaneció más tiempo entre los torniquetes, las barreras giratorias se bloquearán. . En este momento, debe deslizar las tarjetas varias veces para permitir que varias personas pasen el torniquete continuamente. En el modo de memoria, si el intervalo de pasar la tarjeta excede la duración del paso de una sola persona, la función de memoria no se activará. El intervalo entre dos verificaciones de identidad debe ser más largo que la duración de desbloqueo del controlador de acceso o el controlador de acceso de reconocimiento facial; de lo contrario, solo se contará una verificación de identidad. El intervalo de verificación de identidad recomendado es de 2 sa 5 s. En el modo de memoria, como máximo 255 personas pueden pasar el torniquete continuamente.
Segundo desbloqueo	Después de que las personas ingresaron al torniquete y activaron las alarmas, no necesitan retroceder y pueden verificar sus identidades. Solo los torniquetes admiten el modo de memoria y las funciones de segundo desbloqueo.

Step 4 Hacer clic**Ahorrar**.

3.6.3 Ver historial de eventos

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.

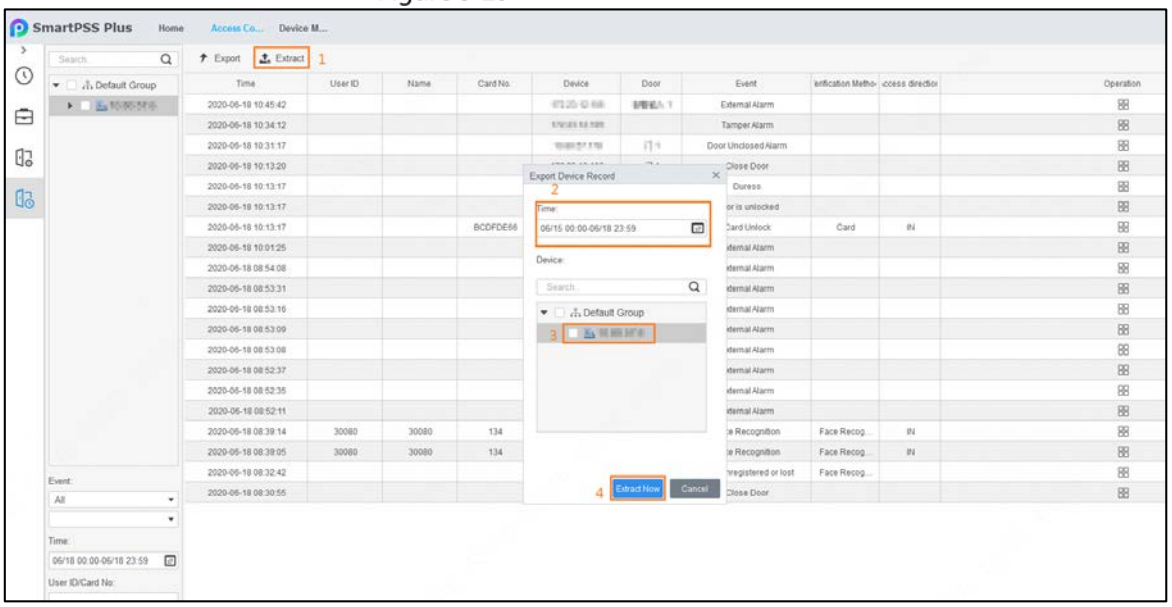
Step 1 Hacer clic**Configuración de acceso**>**Evento de historia**en la página de inicio. Hacer clic

Step 2 **Administrador de acceso**.

Step 3 Extraiga eventos del dispositivo de puerta al local. Hacer clic**Extracto**, configure la hora, seleccione el dispositivo y luego haga clic en**Extraer ahora**.

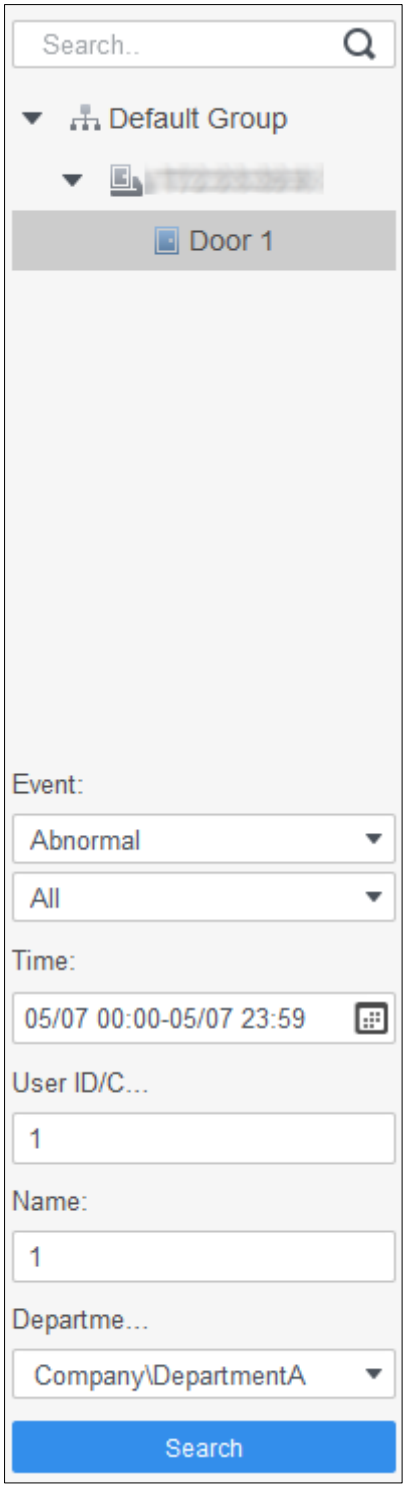
Puede seleccionar varios dispositivos al mismo tiempo.

Figure 3-25 Extraer eventos



Step 4 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 Acceso a la puerta de control remoto

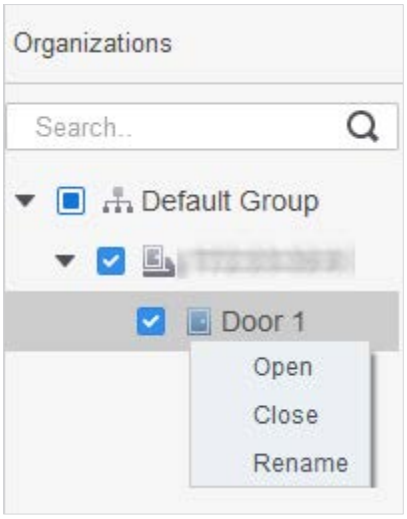
Puede controlar la puerta de forma remota a través de SmartPSS AC.

Step 1 Hacer clic**Administrador de acceso**en la página de inicio o haga clic en**Guía de acceso**.

Step 2 **>** Controle remotamente el acceso a 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)

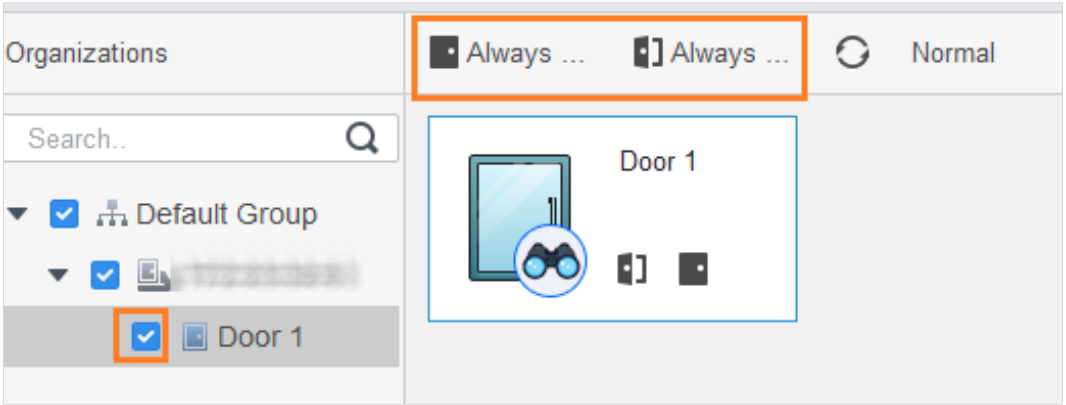
3.7.2 Configuración del estado de la puerta

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



3.8 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

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**.

Step 3 Encender**Evento de intrusión**. Configure el enlace de la alarma de intrusión.

Step 4

- Encienda la alarma de sonido.

  Haga clic en el**Notificar**pestaña y encienda**Sonido de alarma**. Cuando ocurren eventos de intrusión, se activan alarmas sonoras.

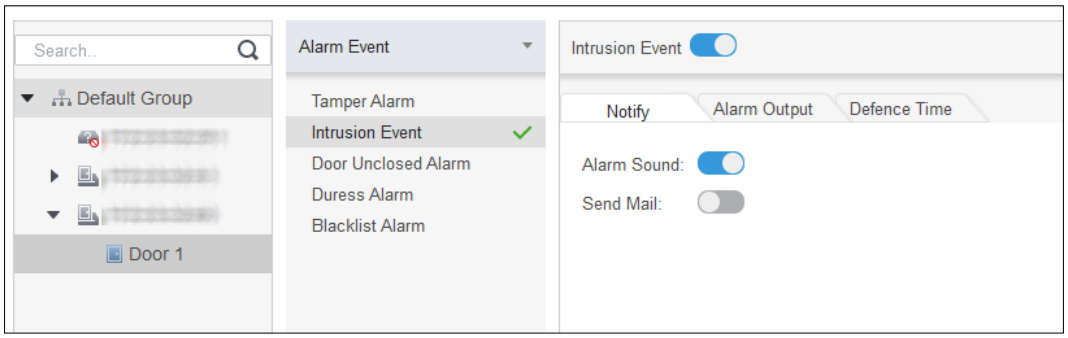
- Enviar correo.

1) Encender**Enviar correo**y confirme para establecer SMTP.

2) Configure 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 salida de alarma.

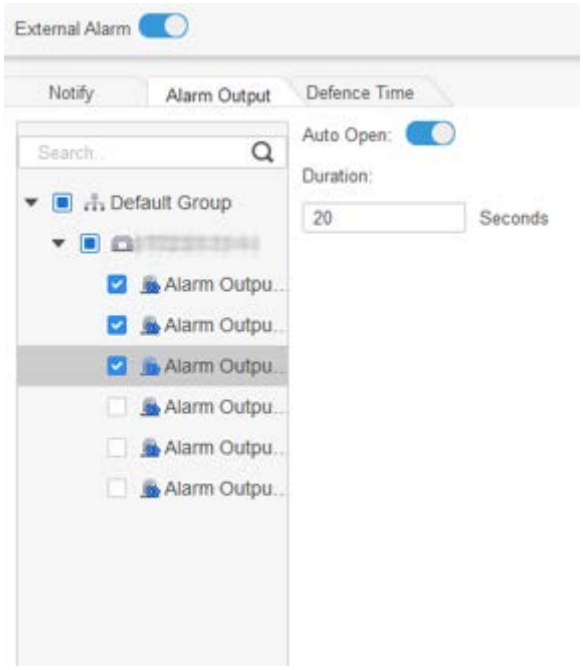
1) Haga clic**Salida de alarma**pestaña.

2) Seleccione el dispositivo que admita salida de alarma y, a continuación, seleccione el puerto de salida de alarma.

3) Encender**Apertura automática**para el enlace de alarma.

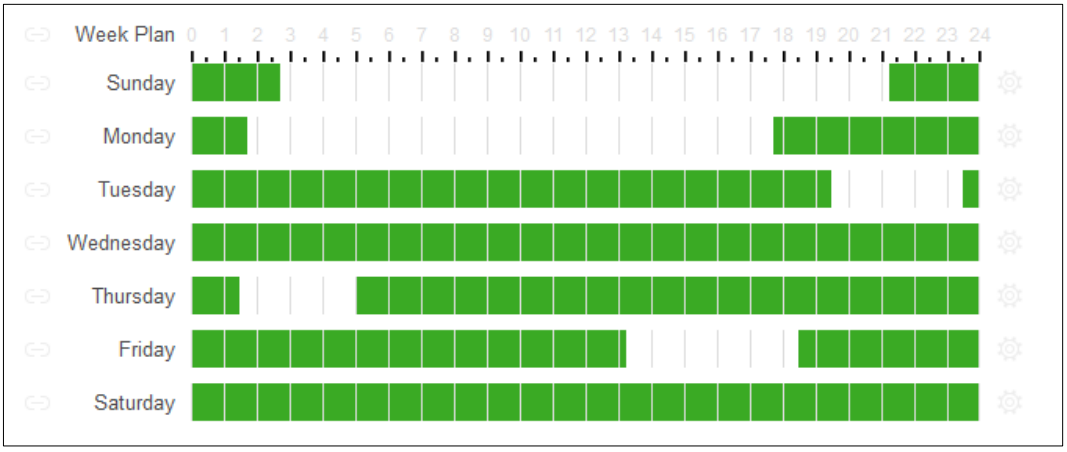
4) Configure la duración de la alarma.

Figure 3-31 Configurar enlace de alarma



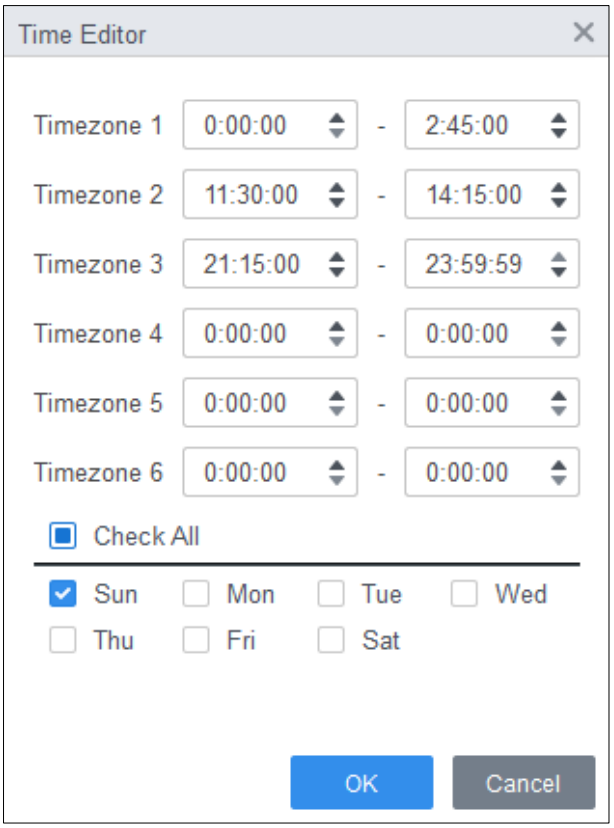
- Establecer periodos de armado. Hay dos métodos.
  - Método 1: Mueva el cursor para establecer períodos. Cuando el cursor es un lápiz, haga clic para agregar puntos; cuando el cursor es borrador, haga clic para eliminar puntos. El área verde son los períodos de armado

Figure 3-32 Establecer defensase tiempo (método 1)



-Método 2: haga clic  para configurar los períodos de armado y luego haga clic en**OK**.

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**OK**. Hacer clic**Ahorrar**.

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 dispositivo y la computadora estén en la misma red.

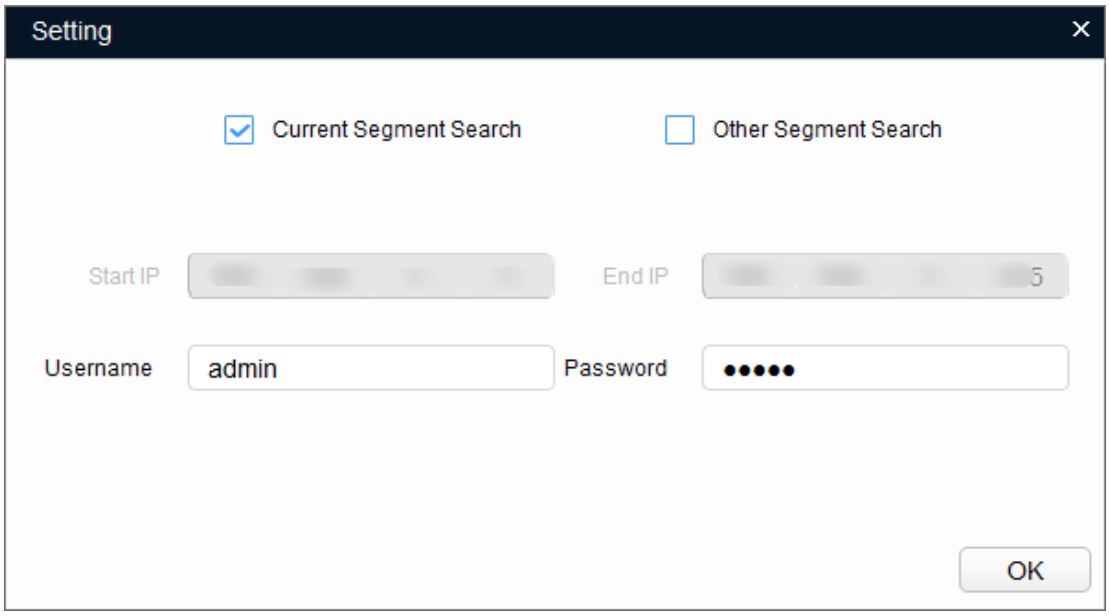
Step 1 Busque el dispositivo a través de ConfigTool. 1)

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**OK**.

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

Figure 4-1 Buscar el dispositivo



Step 2 Seleccione dispositivos no inicializados y luego haga clic en**Inicializar.**

Step 3 Hacer clic**OK**.

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

Step 4 Hacer clic**Finalizar**.

4.2 Adición de dispositivos

Puede agregar uno o varios dispositivos.

Asegúrese de que el Dispositivo y la computadora donde está instalado ConfigTool estén conectados; de lo contrario, ConfigTool no puede encontrar el dispositivo.

4.2.1 Agregar dispositivo individualmente

Step 1 Hacer clic .

Step 2 Hacer clic**Adición manual**.

Step 3 Seleccionar**Dirección IP**o**Número de serie del dispositivo**de**Añadir tipo**lista.

Figure 4-2 Añadir manualmente (dirección IP)

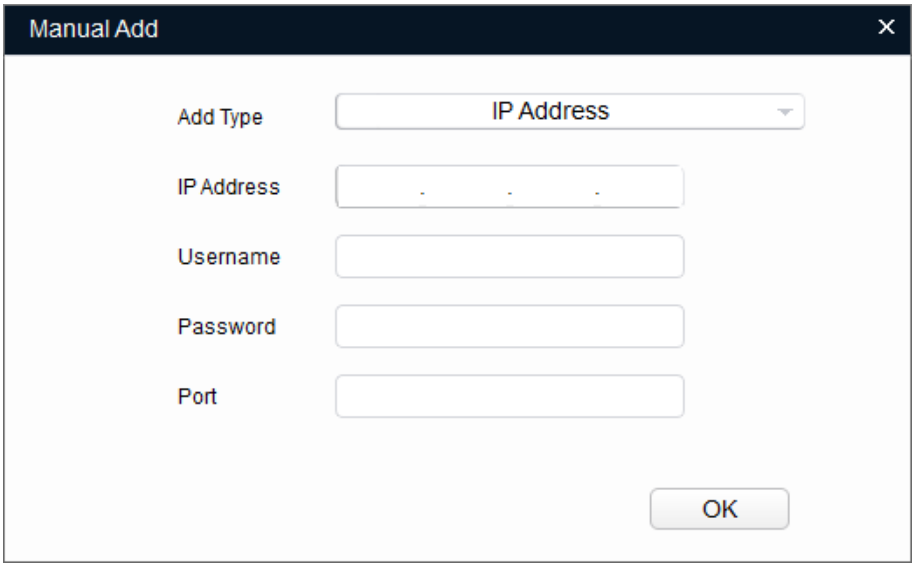


Figure 4-3 Agregar manualmente (SN del dispositivo)

Step 4 Configure los parámetros del dispositivo.

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.

Agregar método	Parámetro	Descripción
	Nombre de usuario	El nombre de usuario y la contraseña para iniciar sesión en el dispositivo.
	Clave	
	Puerto	El número de puerto del dispositivo.
SN del dispositivo (Dispositivo admite solo P2P)	número de serie	El número de serie del dispositivo.
	Nombre de usuario	El nombre de usuario y la contraseña para iniciar sesión en el dispositivo.
	Clave	

Step 5 Hacer clic**OK**.

El dispositivo 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.

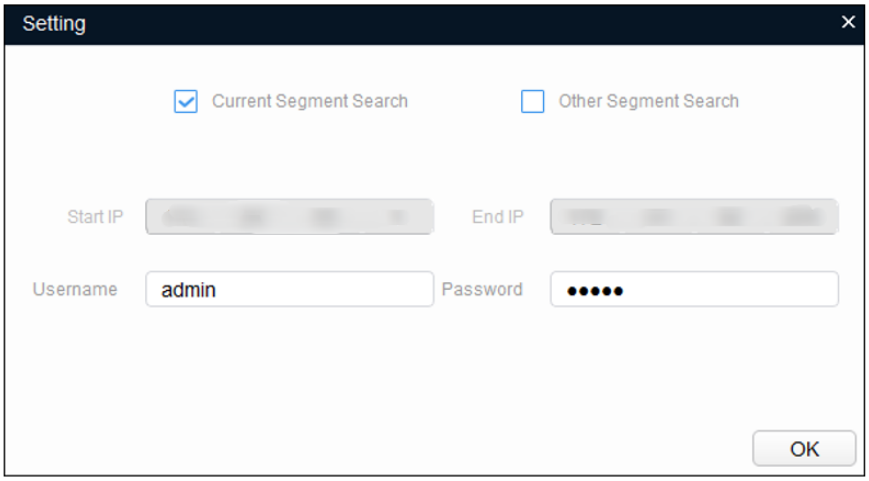
4.2.2.1 Adición mediante búsqueda

Puede agregar varios dispositivos buscando el segmento de red actual u otro segmento de red.

Puede establecer las condiciones de filtrado para buscar dispositivos.

Step 1 Hacer clic Search setting .

Figure 4-4 Ajuste



Step 2 Seleccione los métodos de búsqueda.

- Búsqueda de segmento actual

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

- Búsqueda de 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**OK**para 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 cuando sale 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**OK**.

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**OK**. Establecer los

Step 4 parámetros del controlador de acceso.

Figure 4-5 Configurar controlador de acceso

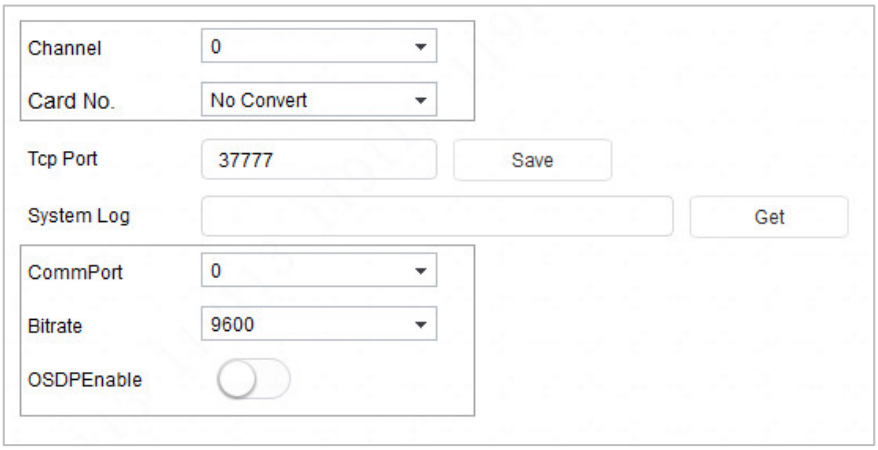


Tabla 4-2 Parámetros del controlador de acceso

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**. **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**Obtener**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 a los que necesita aplicar los parámetros configurados y luego haga clic en**Configuración**.

✓ indica el éxito de la aplicación; ⚠ indica que la aplicación falló. Puede hacer clic en ellos para ver detalles.

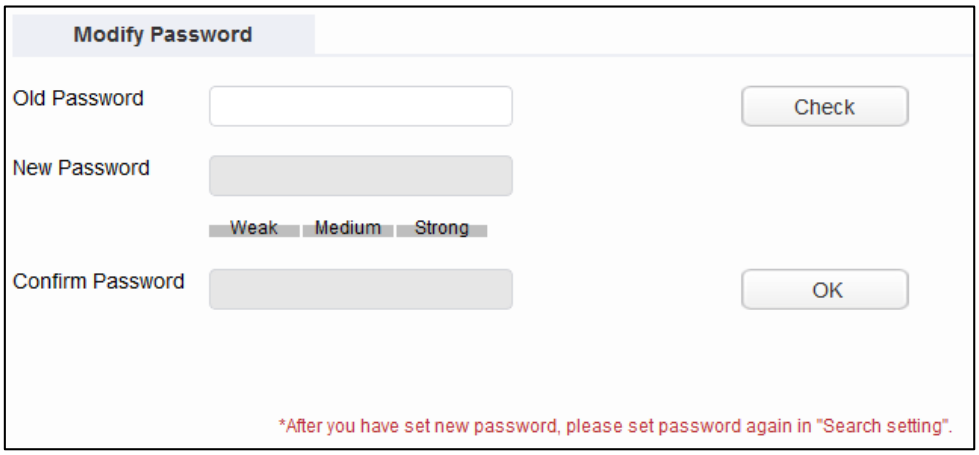
4.4 Modificación de la contraseña del dispositivo

Puede modificar la contraseña de inicio de sesión del dispositivo.

Step 1 Hacer clic  .

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

Figure 4-6 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**Controlar**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**OK**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. Use 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 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 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 la red de su dispositivo: 1. Protección física

Le sugerimos que realice una protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala y gabinete de computadoras especiales, e implemente un permiso de control de acceso y una administración de claves bien hechos para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de un dispositivo extraíble (como un disco flash USB). , puerto serie), 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 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 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 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 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 dispositivo: 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 capacidad de almacenamiento limitada del dispositivo, 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 del dispositivo 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.