

Controlador de acceso (C)

Manual de usuario



Prefacio

General

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

Modelos

Unidireccional de dos puertas;

De dos puertas de dos vías;






Unidireccional de cuatro puertas;

Dos vías de cuatro puertas;

Unidireccional de ocho puertas.

Las instrucciones de seguridad

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

Palabras de advertencia	Sentido
 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 resultar en daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
 CONSEJOS	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
 NOTA	Proporciona información adicional como énfasis y complemento de el texto.

Revisión histórica

Versión	Contenido de la revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	Marzo 2021

Acerca del manual

El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.

No nos hacemos responsables de ninguna pérdida ocasionada por las operaciones que no cumplan con el manual. El manual se actualizará de acuerdo con las últimas leyes y regulaciones de los

jurisdicciones. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si existe inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.

Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar 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.

Todavía puede haber desviaciones en los datos técnicos, las funciones y la descripción de las operaciones, o errores en la impresión. Si hay alguna duda o disputa, nos reservamos el derecho a una explicación final.

Actualice el software del lector o pruebe con otro software de lectura convencional si no puede abrir el manual (en formato PDF).

Todas las marcas comerciales, marcas comerciales registradas y los nombres de empresas que aparecen en el manual son propiedad de sus respectivos propietarios.

Visite nuestro sitio web, póngase en contacto con el proveedor o el servicio de atención al cliente si surge algún problema al utilizar el dispositivo.

Si hay alguna duda o controversia, nos reservamos el derecho a una explicación final.

Salvaguardias y advertencias importantes

Este capítulo describe el contenido que cubre el manejo adecuado del controlador de acceso, la prevención de peligros y la prevención de daños a la propiedad. Lea el manual detenidamente antes de usar el controlador de acceso, cumpla con el manual cuando lo use y guárdelo para futuras consultas.

Requisitos de operación

No coloque ni instale el dispositivo en un lugar expuesto a la luz solar o cerca de una fuente de calor.

Mantenga el dispositivo alejado de la humedad, el polvo o el hollín.

Mantenga el dispositivo instalado horizontalmente en un lugar estable para evitar que se caiga.

No deje caer ni salpique líquido sobre el dispositivo, y asegúrese de que no haya ningún objeto lleno de líquido sobre el dispositivo para evitar que el líquido fluya hacia el dispositivo.

Instale el dispositivo en un lugar bien ventilado y no bloquee la ventilación del dispositivo. Opere el dispositivo dentro del rango nominal de entrada y salida de energía.

No desarme el dispositivo al azar.

Transporte, utilice y almacene el dispositivo en las condiciones de humedad y temperatura permitidas.

Seguridad ELECTRICA

El uso inadecuado de la batería puede provocar un incendio, una explosión o una inflamación.

Cuando reemplace la batería, asegúrese de que se use el mismo modelo.

Utilice los cables de alimentación recomendados en la región y cumpla con la especificación de potencia nominal.

Use el adaptador de corriente provisto con el dispositivo; de lo contrario, podrían producirse lesiones personales y daños al dispositivo.

Utilice una fuente de alimentación que cumpla con ES1 pero que no exceda los límites de PS2 definidos en IEC 62368-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas del dispositivo.

Conecte el dispositivo (estructura tipo I) a la toma de corriente con toma de tierra de protección.

El acoplador del aparato es un dispositivo de desconexión. Cuando utilice el acoplador, mantenga el ángulo para facilitar la operación.

Tabla de contenido

Prefacio.....	I
Salvaguardias y advertencias importantes
III 1 Resumen	1
1.1 Introducción.....	1
1.1 Características	1
1.2 Dimensiones.....	1
1.3 Solicitud	2
1.3.1 Dos puertas unidireccionales	2
1.3.2 Dos puertas Dos vías	3
1.3.3 Unidireccional de cuatro puertas	3
1.3.4 Cuatro puertas y dos vías	4
1.3.5 Unidireccional de ocho puertas	4
2 Estructura	5
2.1 Alambrado	5
2.1.1 Dos puertas unidireccionales	6
2.1.2 Dos puertas Dos vías	7
2.1.3 Unidireccional de cuatro puertas	8
2.1.4 Cuatro puertas y dos vías	9
2.1.5 Unidireccional de ocho puertas	10
2.1.6 Bloqueo	10
2.1.7 Entrada de alarma	11
2.1.8 Salida de alarma	11
2.1.9 Lector de tarjetas	13
2.2 Indicador de encendido.....	13
2.3 Dip switch.....	14
2.4 Fuente de alimentación.....	14
2.4.1 Puerto de alimentación de la cerradura de la puerta	14
2.4.2 Puerto de alimentación del lector de tarjetas	14
3 Configuración de CA SmartPSS	15
3.1 Acceso	15
3.2 Agregar dispositivos	15
3.2.1 Búsqueda automática	15
3.2.2 Adición manual	dieciséis
3.3 Gestión de usuarios	18
3.3.1 Configuración del tipo de tarjeta	18
3.3.2 Agregar usuario	19
3.4 Configuración de permisos	22
3.4.1 Agregar grupo de permisos	22
3.4.2 Asignación de permisos	24
3.5 Configuración del controlador de acceso	25
3.5.1 Configuración de funciones avanzadas	25
3.5.2 Configuración de Access Controller	31
3.5.3 Visualización de eventos históricos	34
3.6 Gestión de Acceso.....	36

3.6.1 Apertura y cierre de puertas de forma remota	36
3.6.2 Configuración de Siempre Abierto y Siempre Cerrado	37
3.6.3 Restablecimiento del estado de la puerta	37
3.7 Configuración de eventos	38
4 Configuración de ConfigTool	41
4.1 Agregar dispositivos	41
4.1.1 Agregar un dispositivo	41
4.1.2 Agregar varios dispositivos	42
4.2 Configuración del controlador de acceso	43
4.3 Cambio de la contraseña del dispositivo	44
Appendix 1 Recomendaciones de ciberseguridad	46

1. Información general

1.1 Introducción

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

1.1 Características

Adopta el tablero de acero SEEC para ofrecer una apariencia de alta gama.

Admite comunicación de red TCP / IP. Los datos de comunicación están encriptados 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 de múltiples usuarios, 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 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.

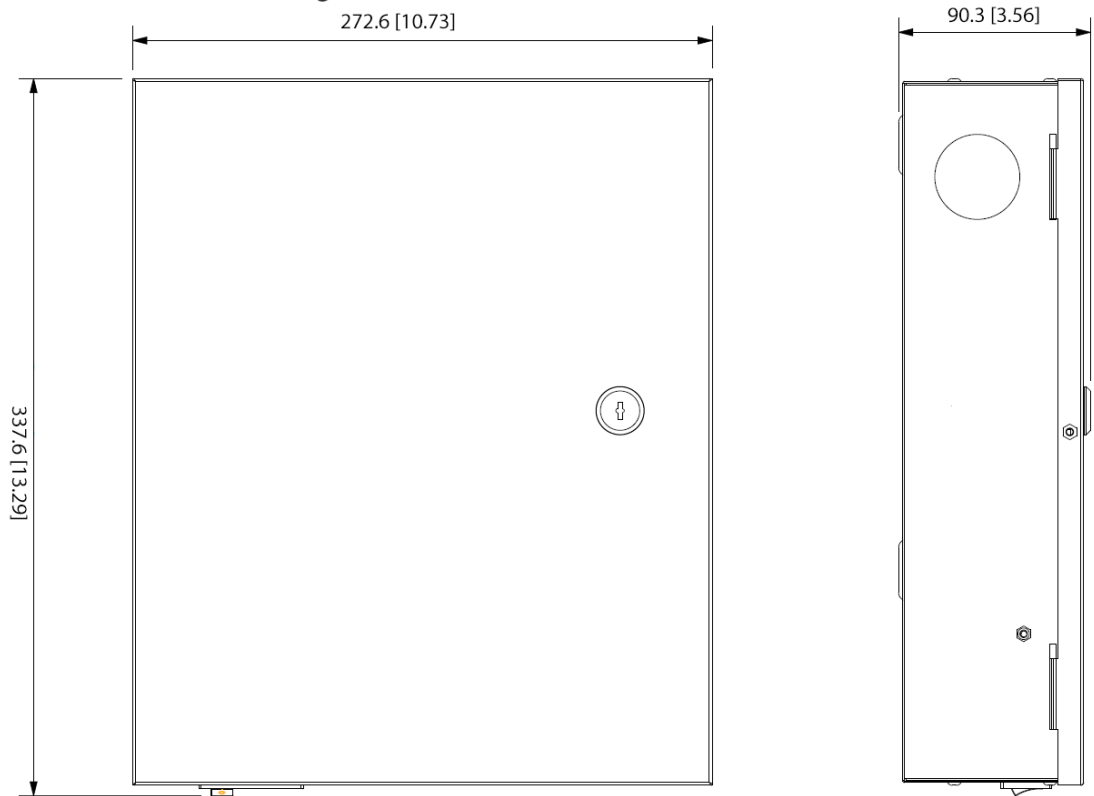
Admite el funcionamiento fuera de línea, el almacenamiento de registros de eventos y las funciones de carga, y el reabastecimiento automático de la red (ANR).

Admite 128 períodos, 128 planes de vacaciones, 128 períodos de vacaciones, períodos normalmente abiertos, períodos normalmente cerrados, períodos de desbloqueo remoto, períodos de desbloqueo de la primera tarjeta y períodos de desbloqueo. Admite el mecanismo de protección del perro guardián para garantizar la estabilidad de la operación.

1.2 Dimensiones

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

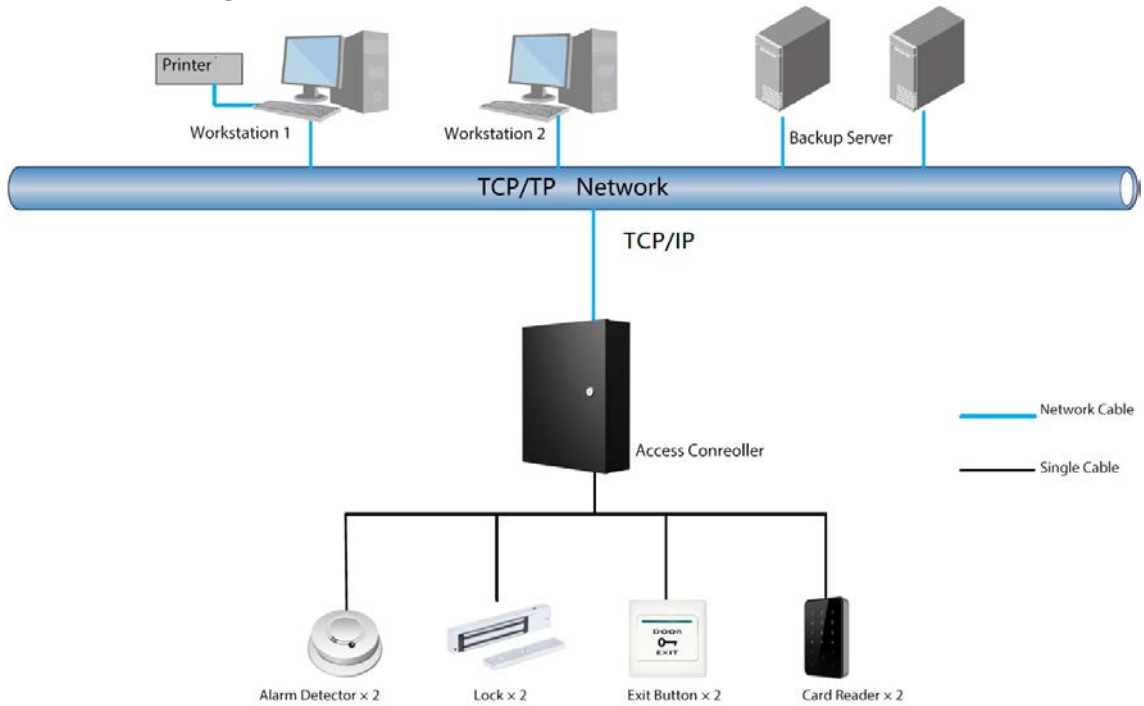
Figure 1-1 Dimensiones (mm [pulgadas])



1.3 Solicitud

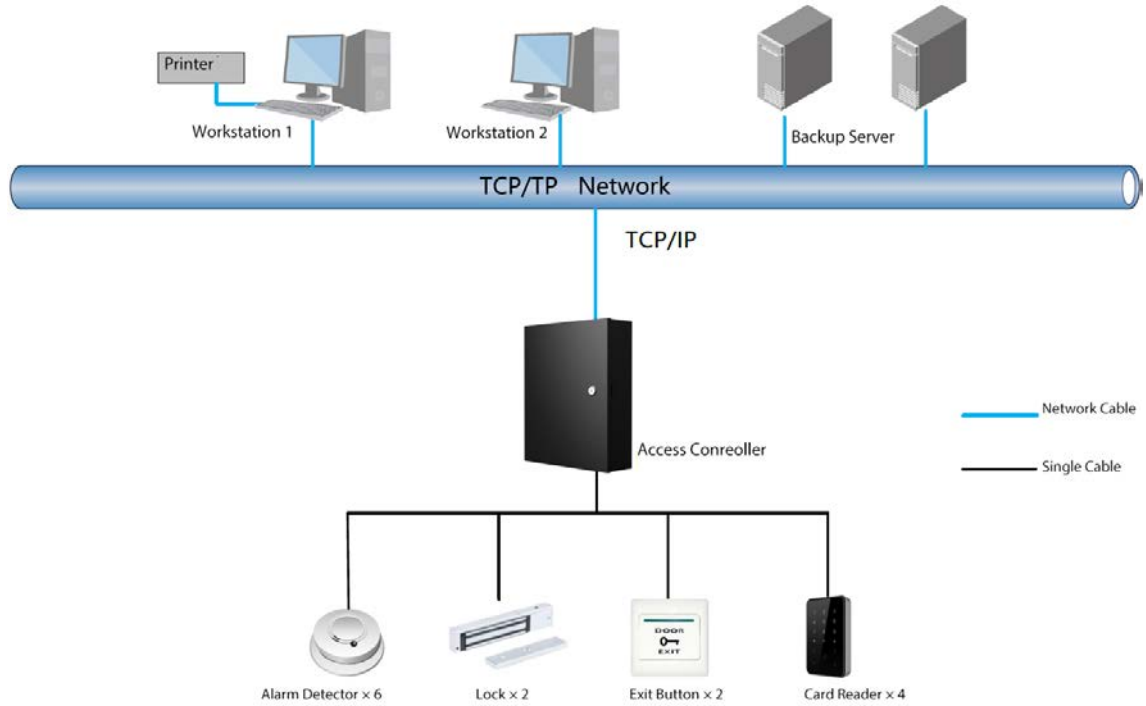
1.3.1 Dos puertas unidireccionales

Figure 1-2 Aplicación del controlador unidireccional de dos puertas



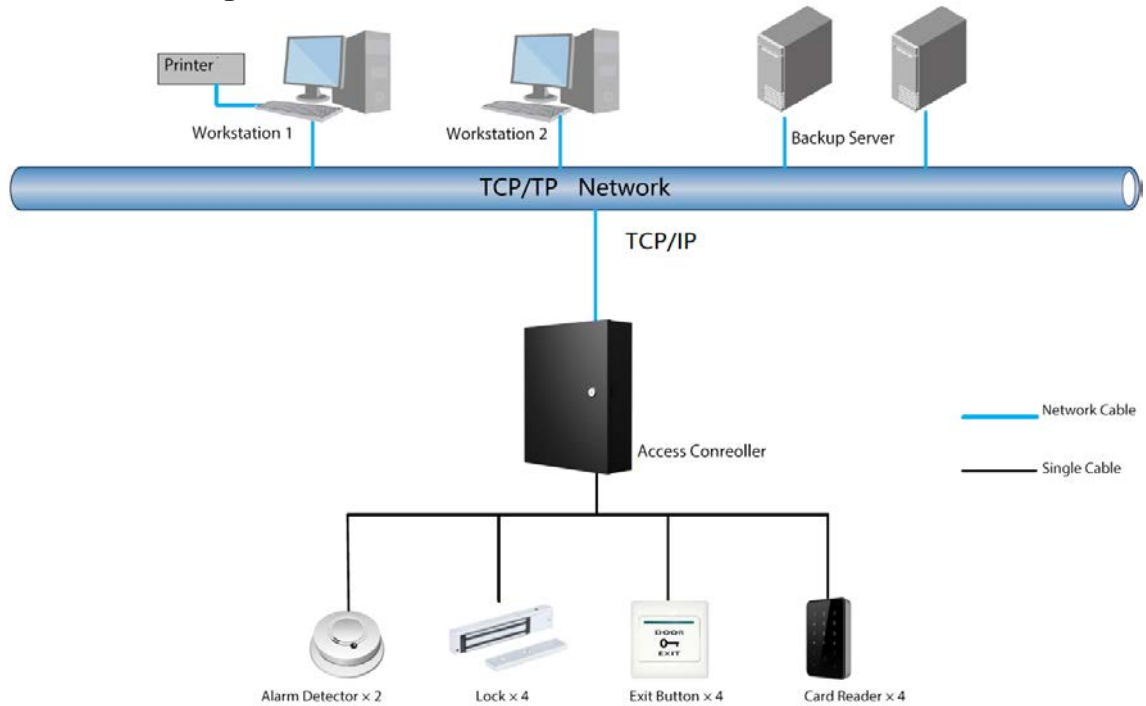
1.3.2 Dos puertas Dos vías

Figure 1-3 Aplicación del controlador bidireccional de dos puertas



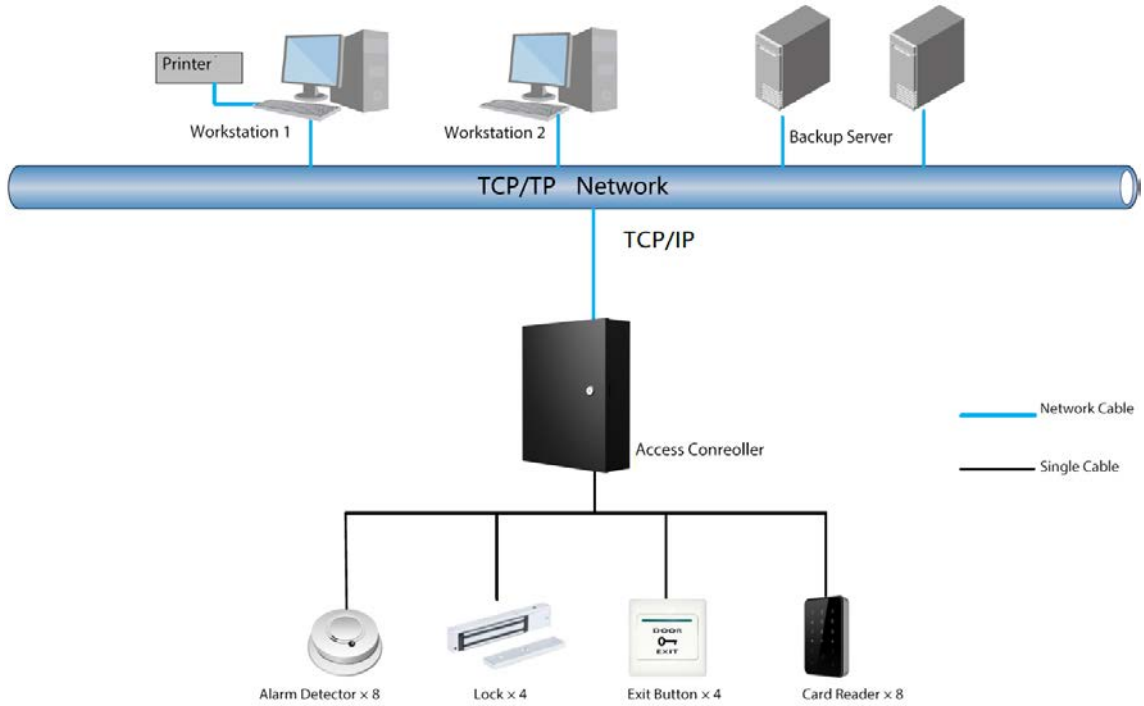
1.3.3 Unidireccional de cuatro puertas

Figure 1-4 Aplicación del controlador unidireccional de cuatro puertas



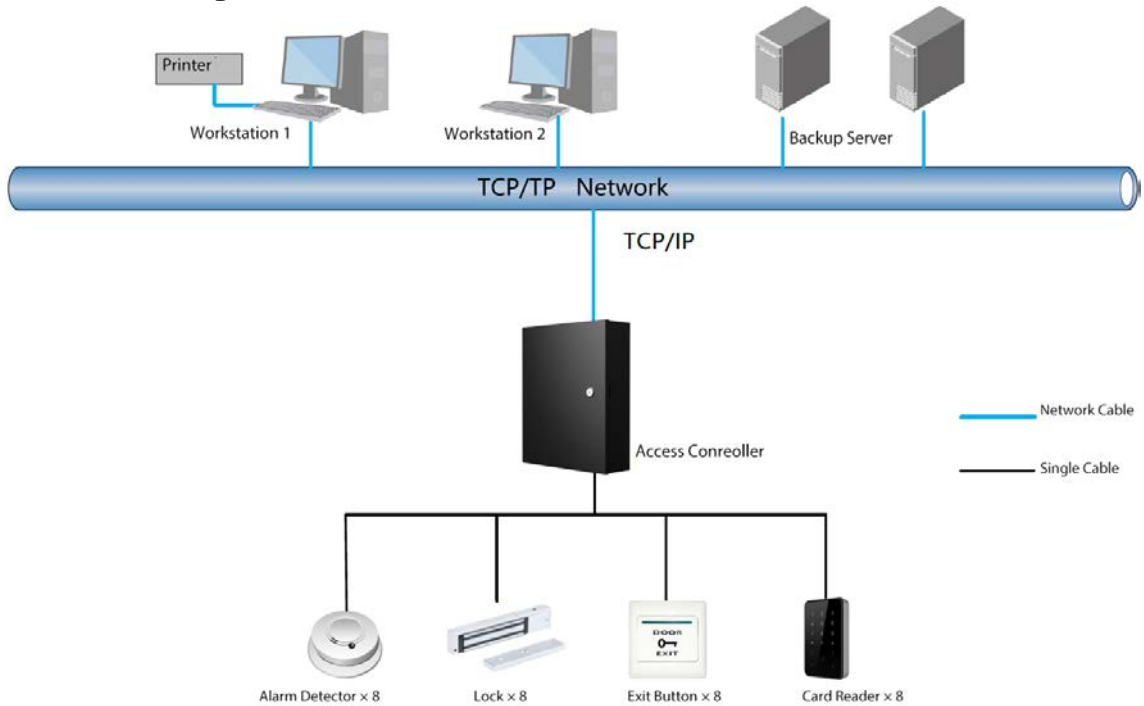
1.3.4 Cuatro puertas y dos vías

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



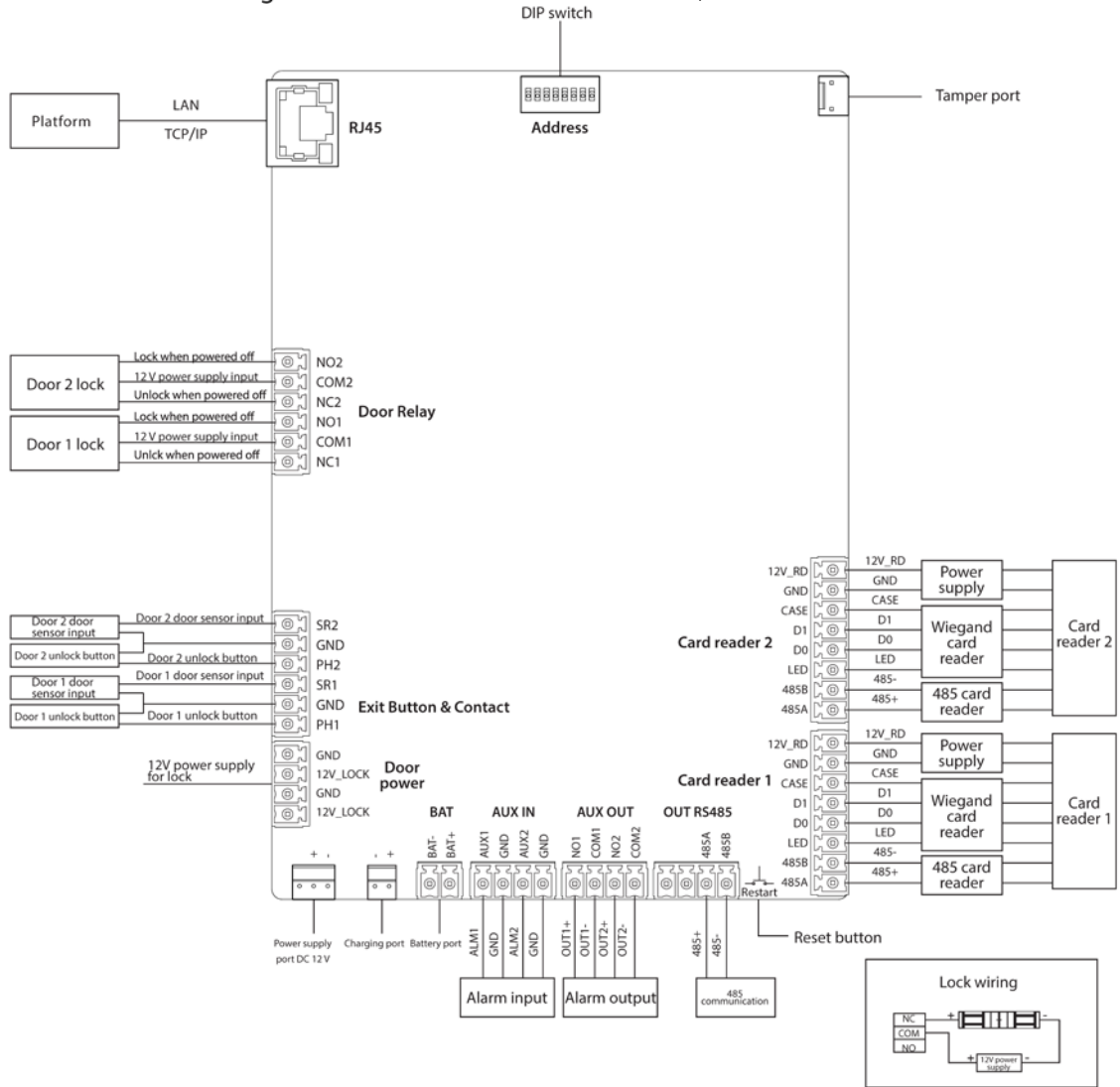
Conecte los cables solo cuando esté apagado.
Asegúrese de que el enchufe de la fuente de alimentación esté conectado a tierra. 12 V: la corriente máxima para un módulo de extensión es 100 mA. 12 V_RD: la corriente máxima para un lector de tarjetas es de 2,5 A. 12 V_LOCK: la corriente máxima para una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

Tabla 2-1 Especificaciones del cable

Dispositivo	Cable	Área de sección transversal de Cada núcleo	Observaciones
Lector de tarjetas	Cat5 de 8 núcleos blindado par trenzado	$\geq 0,22 \text{ mm}^2$	Sugerido $\leq 100 \text{ m}$
Cable de ethernet	Cat5 de 8 núcleos blindado par trenzado	$\geq 0,22 \text{ mm}^2$	Sugerido $\leq 100 \text{ m}$
Botón	2 núcleos	$\geq 0,22 \text{ mm}^2$	-
Contacto de puerta	2 núcleos	$\geq 0,22 \text{ mm}^2$	-

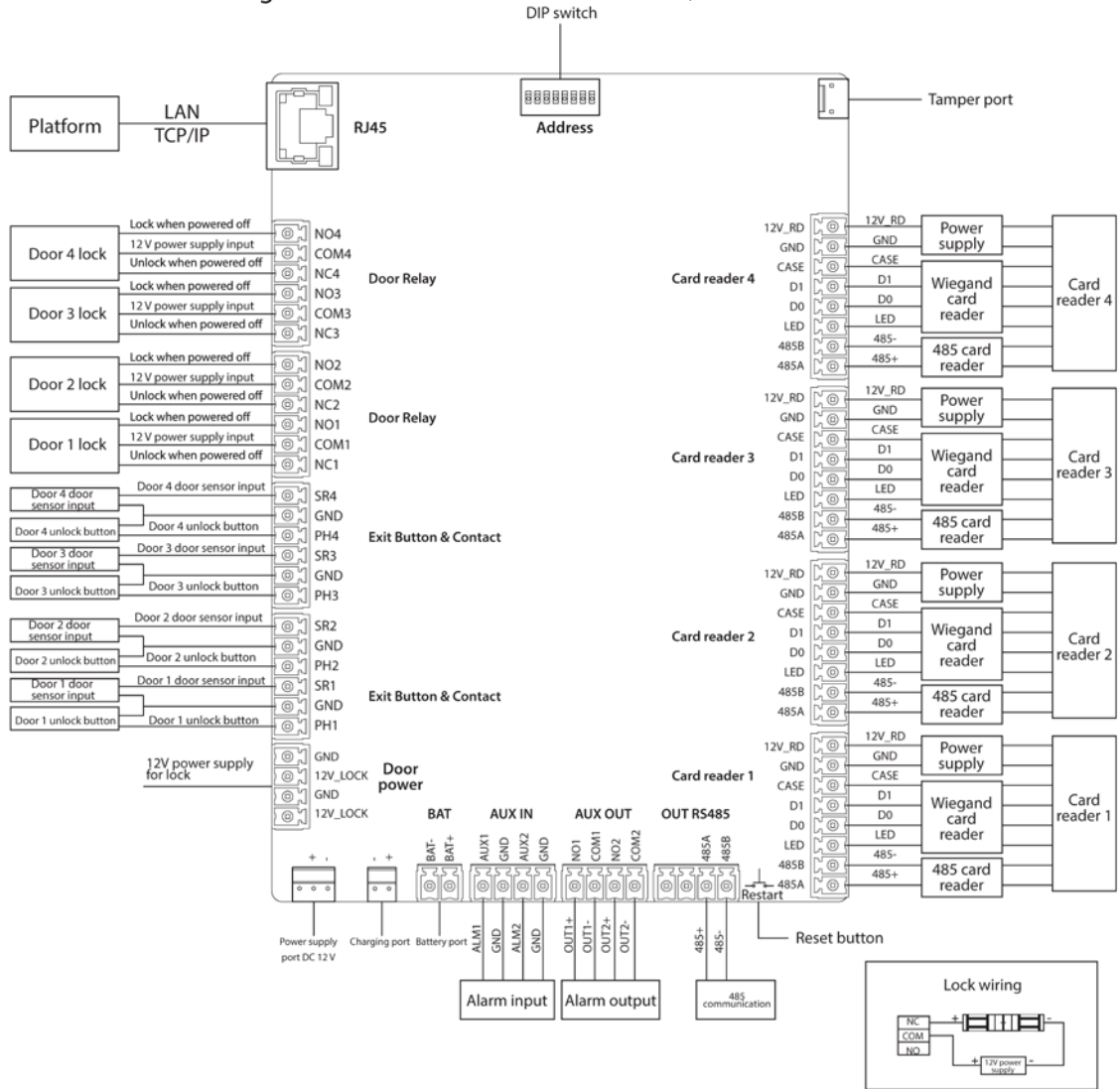
2.1.1 Dos puertas unidireccionales

Figure 2-1 Cable un controlador unidireccional de dos puertas



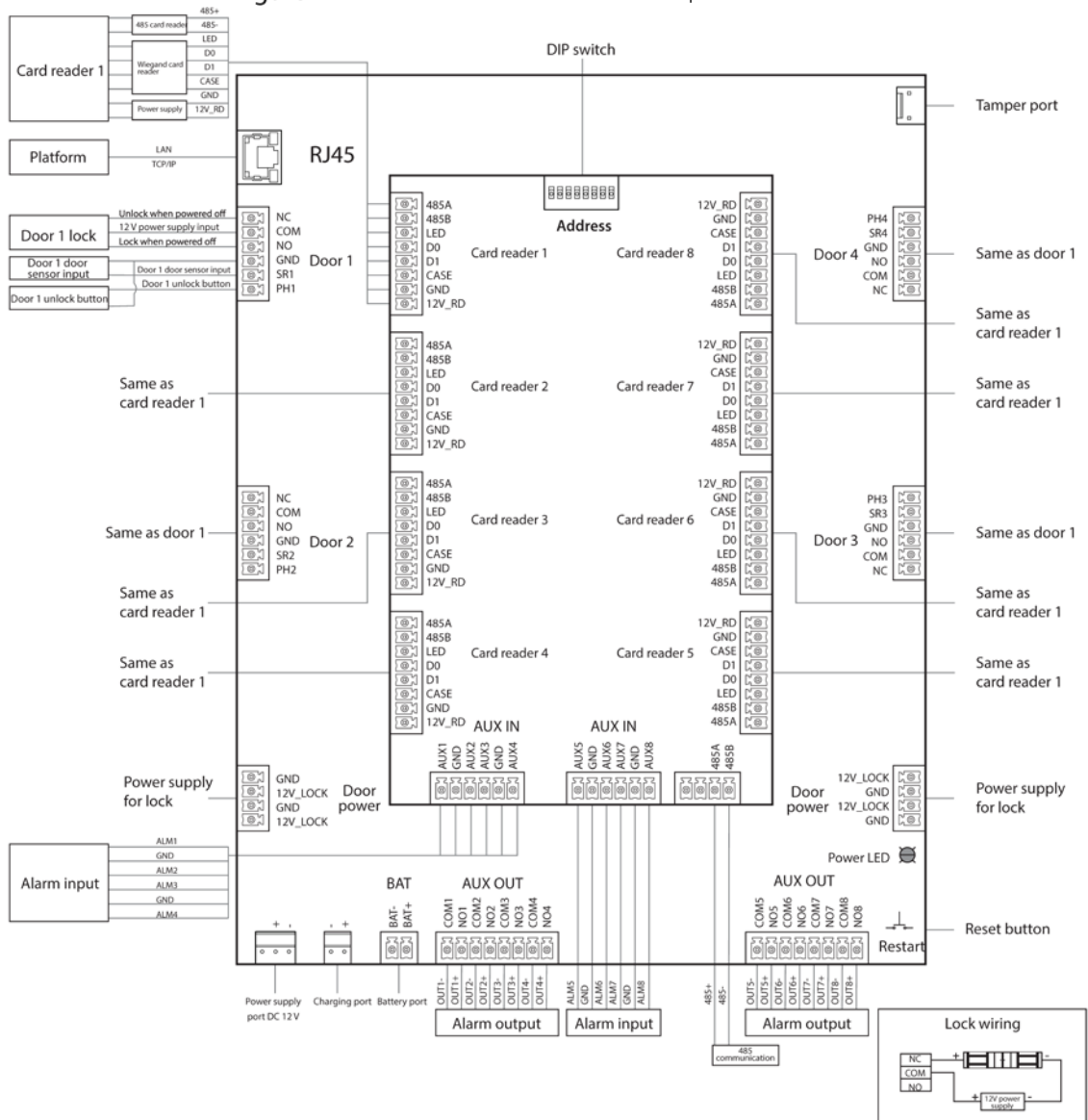
2.1.3 Unidireccional de cuatro puertas

Figure 2-3 Cablee un controlador unidireccional de cuatro puertas



2.1.4 Cuatro puertas y dos vías

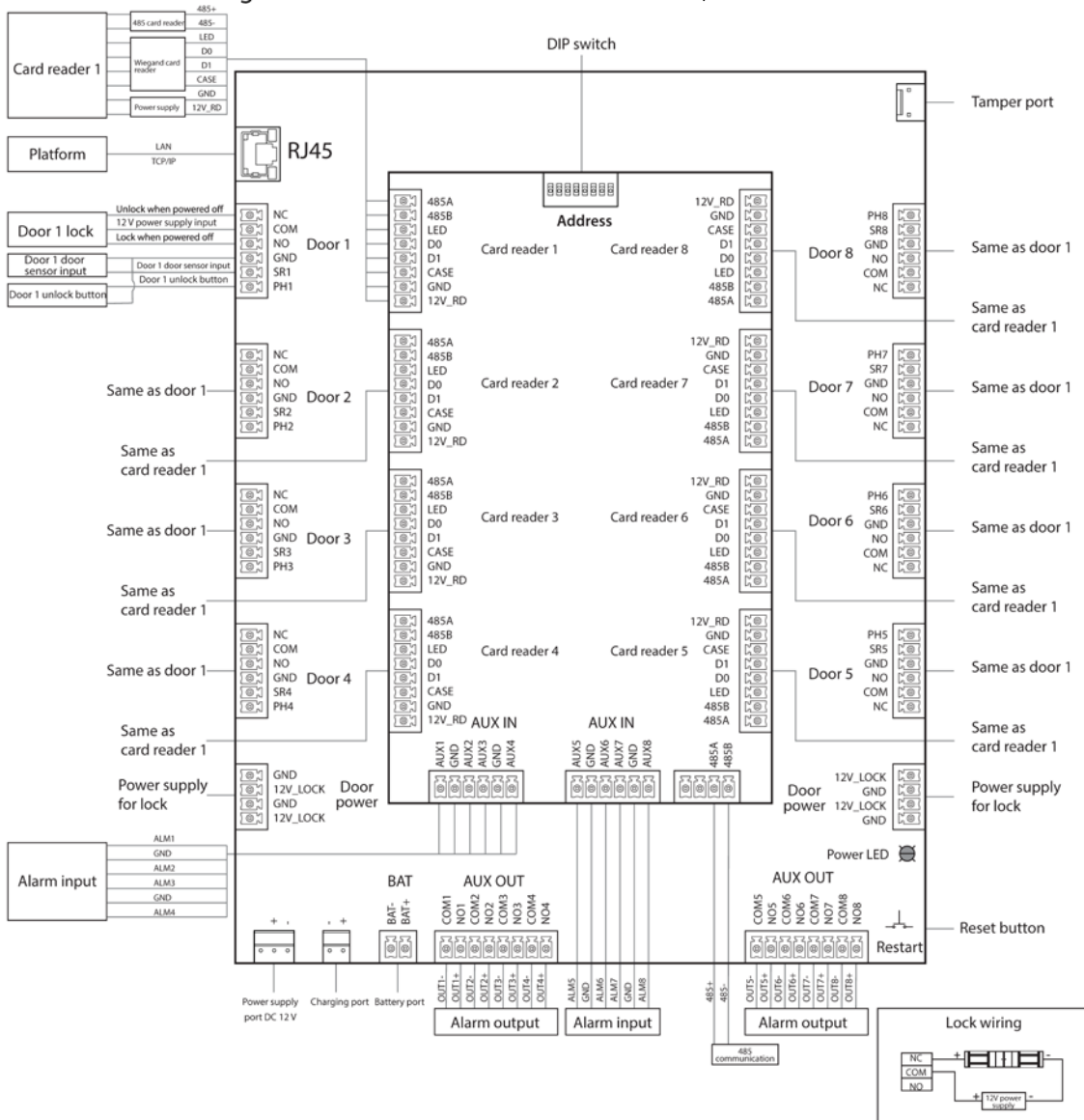
Figure 2-4 Cablea un controlador bidireccional de cuatro puertas



1

2.1.5 Unidireccional de ocho puertas

Figure 2-5 Cablee un controlador unidireccional de ocho puertas



2.1.6 Bloqueo

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

Figure 2-6 Cerradura electrica

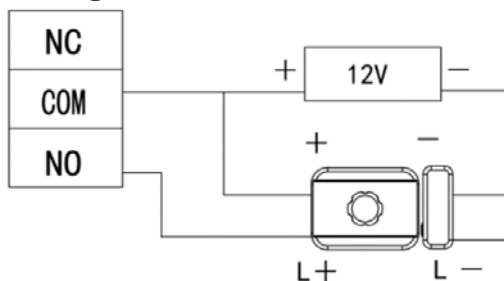


Figure 2-7 Cerradura magnética

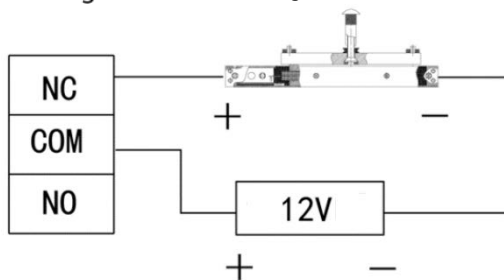
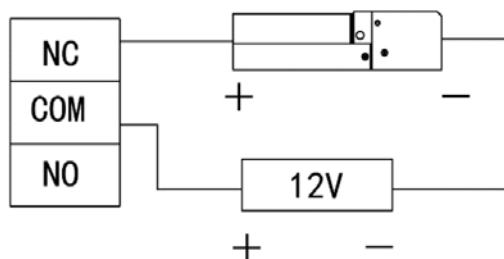


Figure 2-8 Cerrojo eléctrico



2.1.7 Entrada de alarma

El puerto de entrada de alarma se conecta a dispositivos de alarma externos, como el detector de humo y el detector de infrarrojos. Algunas alarmas en los puertos pueden vincular el estado de puerta abierta / cerrada.

Tabla 2-2 Entrada de alarma de cableado

Escribe	Número de Entrada de alarma Canales	Descripción
Dos puertas De una sola mano	2	Estado de la puerta enlazable: <ul style="list-style-type: none"> ● Enlaces de alarma externa AUX1 Normalmente abiertos para todas las puertas. ● Enlaces de alarma externa AUX2 Normalmente cerrados para todas las puertas.
Dos puertas Bidireccional	6	Estado de la puerta enlazable: <ul style="list-style-type: none"> ● Enlaces de alarma externa AUX1 - AUX2 Normalmente abiertos para todas las puertas. ● Enlaces de alarma externa AUX3 - A UX4 Normalmente cerrados para todas las puertas.
Cuatro puertas De una sola mano	2	Estado de la puerta enlazable: <ul style="list-style-type: none"> ● Enlaces de alarma externa AUX1 Normalmente abiertos para todas las puertas. ● Enlaces de alarma externa AUX2 Normalmente cerrados para todas las puertas.
Cuatro puertas Bidireccional	8	Estado de la puerta enlazable: <ul style="list-style-type: none"> ● Enlaces de alarma externa AUX1 - AUX2 Normalmente abiertos para todas las puertas. ● Enlaces de alarma externa AUX3 - A UX4 Normalmente cerrados para todas las puertas.
Ocho puertas De una sola mano	8	Estado de la puerta enlazable: <ul style="list-style-type: none"> ● Enlaces de alarma externa AUX1 - AUX2 Normalmente abiertos para todas las puertas. ● Enlaces de alarma externa AUX3 - A UX4 Normalmente cerrados para todas las puertas.

2.1.8 Salida de alarma

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



Cuando conecte el dispositivo de doble puerta bidireccional al dispositivo de salida de alarma interno, seleccione NC / NO de acuerdo con el estado Siempre abierto o Siempre cerrado.

NC: normalmente cerrado.

NO: Normalmente abierto.

Tabla 2-3 Salida de alarma de cableado

Escribe	Número de Salida de alarma Canales	Descripción
Dos puertas	2 NO1	<ul style="list-style-type: none"> ● AUX1 activa la salida de alarma.

Escribe	Número de Salida de alarma Canales	Descripción	
De una sola mano		COM1	<ul style="list-style-type: none"> ● Salida de alarma de intrusión y tiempo de espera de puerta para la puerta 1. ● Lector de tarjetas 1 salida de alarma de
		NO2	<ul style="list-style-type: none"> ● manipulación. AUX2 activa la salida de alarma.
		COM2	<ul style="list-style-type: none"> ● Salida de alarma de intrusión y tiempo de espera de puerta para puerta 2. ● Salida de alarma de manipulación del lector de tarjetas 2.
Dos puertas Bidireccional	2	NO1	AUX1 / AUX2 activa la salida de alarma.
		COM1	
		NO2	
		COM2	
	2	NC1	<ul style="list-style-type: none"> ● Lector de tarjetas 1/2 salida de alarma de sabotaje. Salida de alarma de intrusión y tiempo de espera de puerta 1.
		COM1	
NO1			
NC2			
COM2			
NO2			
Cuatro puertas De una sola mano	2	NO1	<ul style="list-style-type: none"> ● AUX1 activa la salida de alarma.
		COM1	<ul style="list-style-type: none"> ● Salida de alarma de intrusión y tiempo de espera de puerta. Salida de alarma de manipulación del lector de tarjetas.
		NO2	AUX2 activa la salida de alarma.
		COM2	
Cuatro puertas Bidireccional	8	NO1	<ul style="list-style-type: none"> ● AUX1 activa la salida de alarma.
		COM1	<ul style="list-style-type: none"> ● Lector de tarjetas 1/2 salida de alarma de sabotaje. Salida de alarma de intrusión y tiempo de espera de puerta 1. ● Salida de alarma de manipulación del
		NO2	<ul style="list-style-type: none"> ● dispositivo. AUX2 activa la salida de alarma.
		COM2	<ul style="list-style-type: none"> ● Lector de tarjetas 1/2 salida de alarma de sabotaje. Salida de alarma de intrusión y tiempo de espera de puerta 2.
		NUMERO 3	<ul style="list-style-type: none"> ● AUX3 activa la salida de alarma.
		COM3	<ul style="list-style-type: none"> ● Lector de tarjetas 5/6 salida de alarma de manipulación. ● Salida de alarma de intrusión y tiempo de espera de puerta 3.
		NO. 4	<ul style="list-style-type: none"> ● AUX4 activa la salida de alarma.
		COM4	<ul style="list-style-type: none"> ● Lector de tarjetas con salida de alarma de sabotaje 7/8. ● Salida de alarma de intrusión y tiempo de espera de puerta 4.
		NUMERO 5	AUX5 activa la salida de alarma.
		COM5	AUX6 activa la salida de alarma.
		NO6	
		COM6	AUX7 activa la salida de alarma.
		NO7	
		COM7	AUX8 activa la salida de alarma.
		NO8	
		COM8	

Escribe	Número de Salida de alarma Canales	Descripción	
Ocho puertas De una sola mano	8	NO1	<ul style="list-style-type: none"> ● AUX1 activa la salida de alarma. ● Lector de tarjetas 1 salida de alarma de manipulación. ● Salida de alarma de intrusión y tiempo de espera de puerta 1. ● Salida de alarma de manipulación del
		COM1	
		NO2	<ul style="list-style-type: none"> ● dispositivo. AUX2 activa la salida de alarma. ● Salida de alarma de manipulación del lector de tarjetas 2. ● Salida de alarma de intrusión y tiempo de espera de puerta 2.
		COM2	
		NUMERO 3	<ul style="list-style-type: none"> ● AUX3 activa la salida de alarma. ● Lector de tarjetas 3 salida de alarma de manipulación. ● Salida de alarma de intrusión y tiempo de espera de puerta 3.
		COM3	
		NO. 4	<ul style="list-style-type: none"> ● AUX4 activa la salida de alarma. ● Lector de tarjetas 4 salida de alarma de manipulación. ● Salida de alarma de intrusión y tiempo de espera de puerta 4.
		COM4	
		NUMERO 5	<ul style="list-style-type: none"> ● AUX5 activa la salida de alarma. ● Lector de tarjetas 5 salida de alarma de manipulación. ● Salida de alarma de intrusión y tiempo de espera de puerta 5.
		COM5	
		NO6	<ul style="list-style-type: none"> ● AUX6 activa la salida de alarma. ● Lector de tarjetas 6 salida de alarma de manipulación. ● Salida de alarma de intrusión y tiempo de espera de puerta 6.
		COM6	
		NO7	<ul style="list-style-type: none"> ● AUX7 activa la salida de alarma. ● Lector de tarjetas 7 salida de alarma de manipulación. ● Salida de alarma de intrusión y tiempo de espera de puerta 7.
		COM7	
		NO8	<ul style="list-style-type: none"> ● AUX8 activa la salida de alarma. ● Lector de tarjetas 8 salida de alarma de manipulación. ● Salida de alarma de intrusión y tiempo de espera de puerta 8.
		COM8	

2.1.9 Lector de tarjetas



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

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

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

2.2 Indicador de encendido

Verde fijo: Normal.

Rojo: anormal.

Parpadea en verde: cargando.

Azul: el dispositivo está en modo de arranque.

2.3 Dip switch

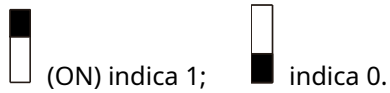
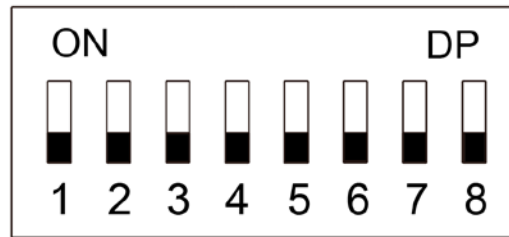


Figure 2-9 Dip switch



Cuando 1-8 se cambian todos a 0, el dispositivo se inicia normalmente después del encendido. Cuando 1-8 se cambian todos a 1, el dispositivo ingresa al modo BOOT después de iniciarse.

Cuando 1, 3, 5 y 7 se cambian a 1 y los demás a 0, el dispositivo se restablece a los valores predeterminados de fábrica después de reiniciarse.

Cuando 2, 4, 6 y 8 se cambian a 1 y los demás a 0, el dispositivo se restablece a 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 energía excede la corriente nominal máxima, proporcione una fuente de alimentación adicional.

2.4.2 Puerto de alimentación del lector de tarjetas

Controladores unidireccionales de dos puertas, 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 de cuatro puertas, bidireccionales y de ocho puertas unidireccionales: 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 administrar de forma remota el dispositivo a través de SmartPSS AC. Este capítulo presenta principalmente la configuración rápida. Para obtener información detallada sobre las operaciones, consulte el manual del usuario de SmartPSS AC.



El cliente Smart PSS AC ofrece diferentes interfaces para diferentes versiones.

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 Agregar dispositivos

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

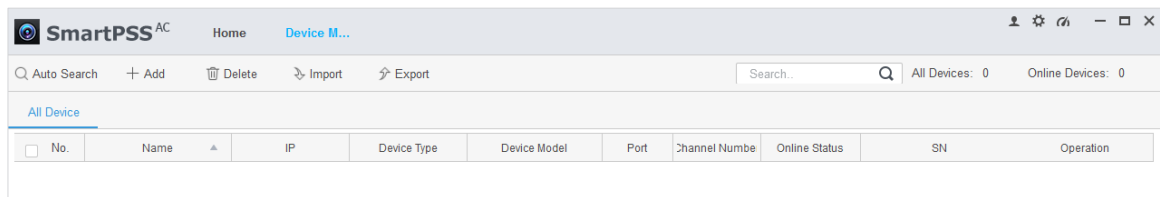
3.2.1 Búsqueda automática

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 libre 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 3-1 Dispositivos



Step 3 Hacer clic **Auto búsqueda**.

Figure 3-2 Auto búsqueda

No.	IP	Device Type	MAC Address	Port	Initialization Status
<input type="checkbox"/> 1	[redacted]	[\$PRODUCT_NAME]	[redacted]	[redacted]	<input checked="" type="checkbox"/> Initialized

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 en **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**.

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

sesión. Puede ver los dispositivos agregados en el **Dispositivos** interfaz.



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. En caso de iniciar sesión correctamente, se muestra el estado **En línea**. De lo contrario, muestra **Desconectado**.

3.2.2 Adición manual

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

Step 1 Inicie sesión en SmartPSS AC. Hacer clic **Administrador de dispositivos**


Step 2 en la esquina inferior izquierda. Hacer clic **Agregar** sobre el

Step 3 **Administrador de dispositivos** interfaz.

Figure 3-3 Agregar manual

Step 4 Ingrese información detallada del dispositivo.

Tabla 3-1 Parámetros

Parámetro	Descripción
Nombre del dispositivo	Ingrese un nombre del dispositivo. Recomendamos nombrar el dispositivo con el área de instalación para una fácil identificación.
Método para agregar	Seleccione IP para agregar el dispositivo a través de la dirección IP.
IP	Ingrese la dirección IP del dispositivo. 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 la contraseña del dispositivo agregado.  El nombre de usuario es admin y la contraseña es admin123 de forma predeterminada. Recomendamos cambiar la contraseña después de iniciar sesión.

Step 5 Hacer clic **Agregar**, y luego puede ver el dispositivo agregado en el **Dispositivos** interfaz.



Después de agregar, SmartPSS AC inicia sesión en el dispositivo automáticamente. En caso de iniciar sesión correctamente, se muestra el estado **En línea**. De lo contrario, muestra **Desconectado**.

3.3 Gestión de usuarios

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

3.3.1 Configuración del tipo de tarjeta

Antes de emitir la tarjeta, configure primero el tipo de tarjeta. Por ejemplo, si la tarjeta emitida es una tarjeta de identificación, configure el tipo como tarjeta de identificación.

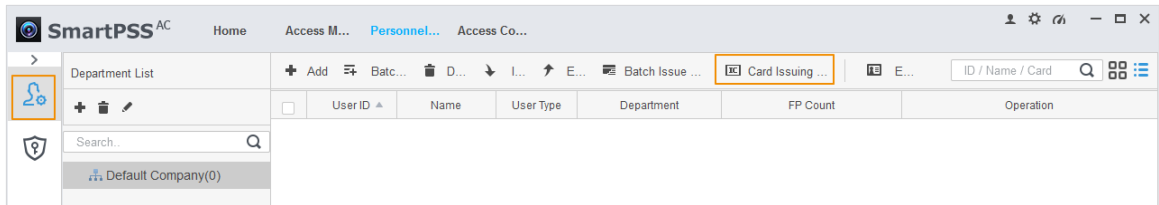




Los tipos de tarjetas deben ser los mismos que los tipos de emisores de tarjetas; de lo contrario, los números de las tarjetas no se pueden leer.

Step 1 Inicie sesión en SmartPSS AC. Hacer

Step 2 clic **Responsable de personal**.

Figure 3-4 Gerente de personal



Step 3 Sobre el **Gerente de personal** interfaz, haga clic en el **Configuración**  haga clic en .

Step 4 de **CardType** interfaz, seleccione un tipo de tarjeta.


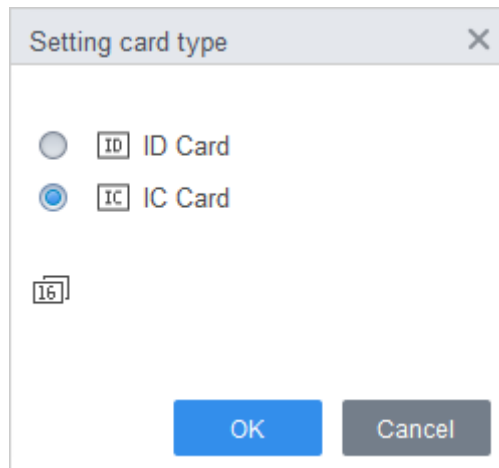
Step 5 Hacer clic  para seleccionar el método de visualización del número de tarjeta en decimal o en hexadecimal.

Figure 3-5 Configuración del tipo de tarjeta



Step 6 Hacer clic **está bien**.

3.3.2 Agregar usuario

3.3.2.1 Adición manual

Puede agregar usuarios uno por uno manualmente.

Step 1 Inicie sesión en SmartPSS AC. Hacer clic **Administrador de**

Step 2 **personal**> **Usuario**> **Agregar**.

Step 3 Agrega información básica del usuario.

1) Haga clic en el **Información básica** pestaña en el **Agregar usuario** interfaz, 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 cara.

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



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

Figure 3-6 Agregar información básica

The screenshot shows the 'Add User' window with the following details:

- Basic Info:**
 - User ID: 2
 - Name: test
 - Department: Default Company
 - User Type: General
 - Valid Time: 2020/6/5 0:00:00 to 2030/6/5 23:59:59 (3653 Days)
 - Image: CameraCaptchPicture (Upload Picture button, Image Size: 0 ~ 120KB)
- Details:**
 - Gender: Male (selected)
 - Title: Mr
 - DOB: 1985-3-15
 - Mailing Address: (empty)
 - Administrator: (toggle off)
 - Remark: (empty text area)
 - ID Type: ID
 - ID No.: (empty)
 - Company: (empty)
 - Occupation: (empty)
 - Entry Time: 2020/6/4 14:37:59
 - Resign Time: 2030/6/5 14:37:59

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

- 1) Haga clic  para establecer **Dispositivo** o **Emisor de la tarjeta** al lector de tarjetas.
- 2) El número de tarjeta debe agregarse si se utiliza un controlador de acceso que no sea de segunda generación.
- 3) Después de agregar, puede configurar la tarjeta como tarjeta principal o tarjeta de coacción, o reemplazar la tarjeta por una nueva o eliminar la tarjeta.

Configurar huella digital.


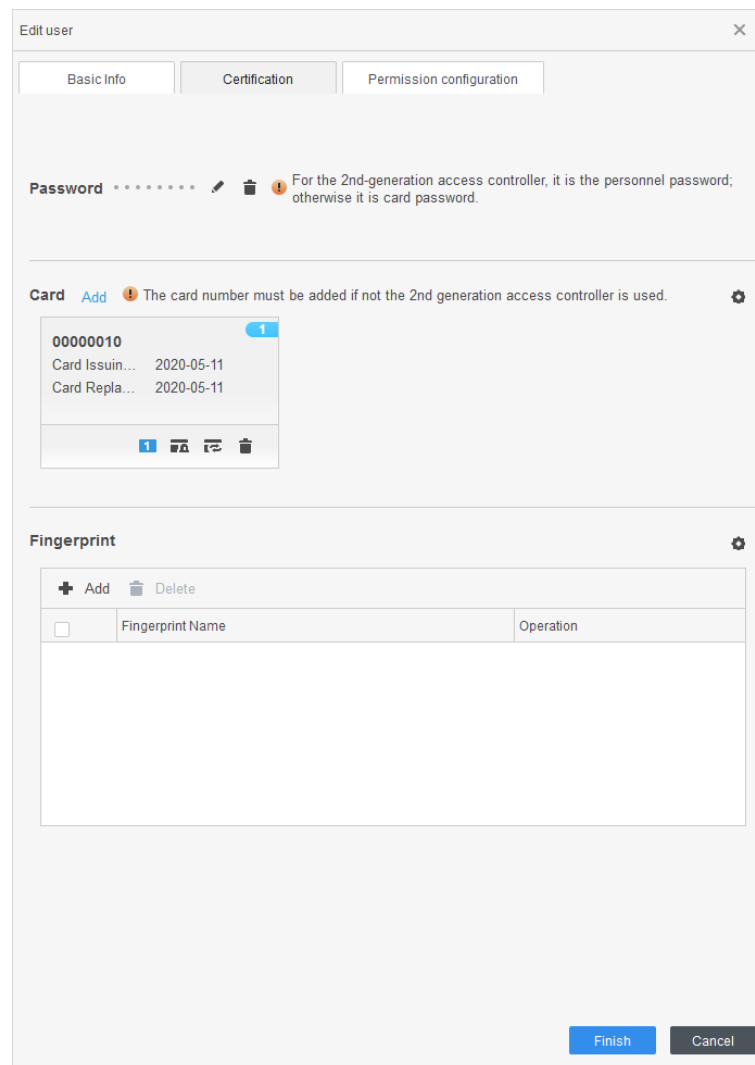
- 1) Haga clic  para configurar **Dispositivo** o **Escáner de huellas dactilares** al colector de huellas dactilares.
- 2) Haga clic **Agregar huella digital** y presione el dedo en el escáner tres veces seguidas.

Figure 3-7 Configurar la certificación



The screenshot shows the 'Edit user' window with the 'Certification' tab selected. It features three main sections: Password, Card, and Fingerprint. The Password section has a field with a masked password and a note: 'For the 2nd-generation access controller, it is the personnel password; otherwise it is card password.' The Card section includes an 'Add' button and a note: 'The card number must be added if not the 2nd generation access controller is used.' Below this is a card preview showing the number '00000010', 'Card Issuin...' with date '2020-05-11', and 'Card Repla...' with date '2020-05-11'. The Fingerprint section has an 'Add' button and a table with columns 'Fingerprint Name' and 'Operation'. At the bottom are 'Finish' and 'Cancel' buttons.

Step 5 Configurar los permisos para el usuario.

Para obtener más información, consulte "3.4 Configuración de permisos".

Figure 3-8 Configuración de permisos

Basic Info Certification **Permission configuration**

Permission group is a combination of various devices including attendance check and access control. After selecting the permission group, the personnel info will be sent to corresponding device and used for related functions of access control and attendance check.

Add Group

<input type="checkbox"/>	Permission Group	Memo
<input type="checkbox"/>	Permission Group1	
<input type="checkbox"/>	Permission Group2	

Step 6 Hacer clic **Terminar**.

3.3.2.2 Agregar lote

Puede agregar usuarios en lotes.

Step 1 Inicie sesión en SmartPSS AC. Hacer clic **Administrador de**

Step 2 **personal> Usuario> Agregar lote.**

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

Step 4 Hacer clic **Asunto** para empezar a emitir tarjetas.

El número de la tarjeta se leerá automáticamente. Hacer clic

Step 5 **Parada** después de emitir la tarjeta y luego haga clic en **está bien**.

Figure 3-9 Agregar usuarios en lotes

Batch Add ✕

Device
Card issuer Issue


Start No.: * 5 Quantity: * 10

Department:
Company\DepartmentB

Effective Time: 2020/4/30 0:00:00 📅 Expired Time: 2030/4/30 23:59:59 📅

Issue Card

ID	Card No.
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	

Step 6 En la lista de usuarios, haga clic en  para modificar información o agregar detalles de usuarios.

3.4 Configurar el permiso







3.4.1 Agregar grupo de permisos


Agregue un grupo de permisos, y luego puede agregar usuarios al grupo para asignarles varios permisos de acceso.

Step 1 Inicie sesión en SmartPSS AC. Hacer clic **Administrador de personal**>

Step 2 **Configuración de permisos.**

Figure 3-10 Lista de grupos de permisos

	Permission Group	Operation
<input type="checkbox"/>	Permission Group1	  
<input type="checkbox"/>	Permission Group2	  

Step 3 Hacer clic  para agregar un grupo de permisos.

Step 4 Establecer parámetros de permisos.

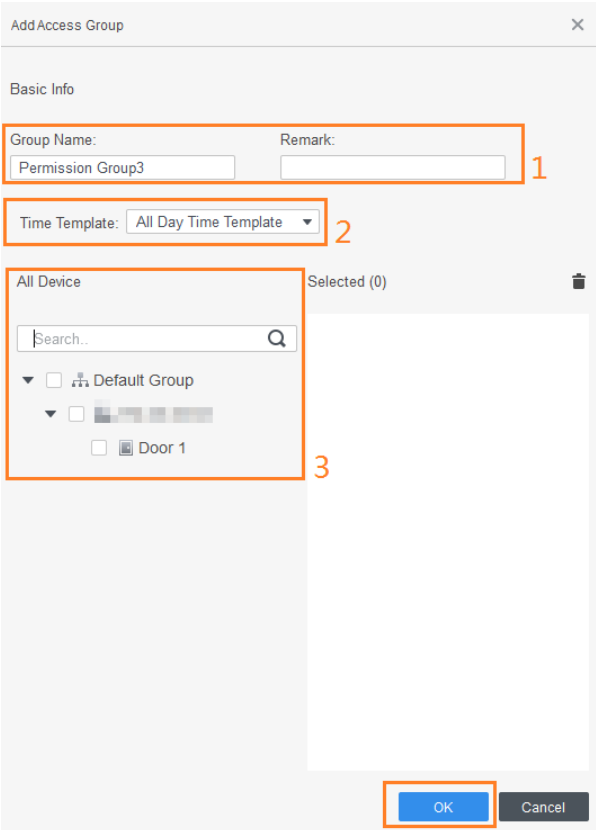
- 1) Ingrese el nombre del grupo y el comentario.
- 2) Seleccione la plantilla de tiempo necesaria.



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

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


Figure 3-11 Agregar grupo de permisos




Step 5 Hacer clic **está bien**.



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

Haga clic  para eliminar el grupo.

Hacer clic  para modificar la información del grupo.

Haga doble clic en el nombre del grupo de permisos para ver la información del grupo.

3.4.2 Asignación de permisos

Asigne permisos a los usuarios y luego podrán desbloquear las puertas.

El método para configurar los permisos para el departamento y para los usuarios es similar. Esta sección toma a los usuarios como ejemplo.

Step 1 Inicie sesión en SmartPSS AC. Hacer clic **Administrador de personal**>

Step 2 **Configuración de permisos.**


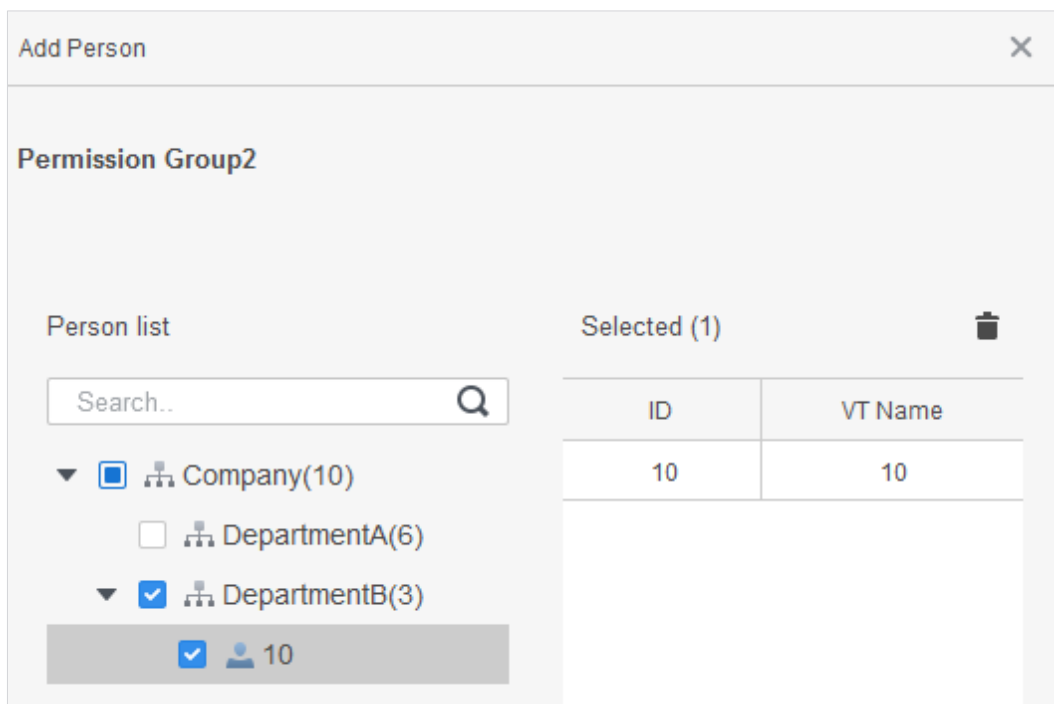
Step 3 Seleccione el grupo de permisos de destino y luego haga clic en .

Figure 3-12 Configurar permiso



Step 4 Seleccione el usuario que necesita tener permisos configurados. Hacer clic

Step 5 **está bien.**

3.5 Configuración del controlador de acceso

3.5.1 Configuración de funciones avanzadas

3.5.1.1 Desbloqueo de la primera tarjeta

Puede configurar varias primeras cartas. Solo después de que cualquier usuario de la primera tarjeta pase la tarjeta, otros usuarios podrán abrir la puerta con sus tarjetas.



La persona a la que se le otorgará el primer permiso de desbloqueo de la tarjeta debe ser **General** tipo de usuario y tener permisos de determinadas puertas. Establezca el tipo al agregar usuarios. Para obtener más información, consulte "3.3.2 Agregar usuario".

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

Step 1 Seleccione **Acceda a Configuración > Configuración avanzada**.

Step 2 Haga clic en el **Desbloqueo de la primera tarjeta** pestaña.

Step 3 Hacer clic **Agregar**.

Step 4 Configurar el **Desbloqueo de la primera tarjeta** parámetros y luego haga clic en **Ahorrar**.

Figure 3-13 Configuración de desbloqueo de la primera tarjeta

First Card Unlock configuration

Door: Door 1 Timezone: All Day Time Template

Status: Normal

Select Personnel

Dropdown list Search..

ID	Name
1	1
2	2
3	3



Selected(2) Clear

ID	Name	Operation
1	1	
2	2	

Save Cancel

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 desbloqueo de la primera tarjeta.
Zona horaria	Desbloqueo de la primera tarjeta es válido en el período de la plantilla de tiempo seleccionada. Después
Estado	Desbloqueo de la primera tarjeta está habilitado, la puerta está en el Modo normal o Siempre en modo abierto .
Usuario	Seleccione el usuario para tener la primera tarjeta. Admite la selección de varios usuarios para que tengan las primeras tarjetas. Cualquiera de ellos deslizar la primera tarjeta significa que el primer desbloqueo de la tarjeta está hecho.

Step 5 (Opcional) Haga clic en . El icono cambiando a  indica **Desbloqueo de la primera tarjeta** está habilitado. El recién agregado **Desbloqueo de la primera tarjeta** está habilitado de forma predeterminada.

3.5.1.2 Desbloqueo de múltiples tarjetas

En este modo, uno o varios grupos de usuarios tienen que pasar las tarjetas por un canal de control de acceso en una secuencia establecida para desbloquear la puerta.

Un grupo puede tener hasta 50 usuarios y una persona puede pertenecer a varios grupos.

Con el desbloqueo de múltiples tarjetas habilitado para un canal de control de acceso, puede haber hasta cuatro grupos de usuarios en el sitio al mismo tiempo para la verificación. El número total de usuarios puede ser 200 como máximo, con hasta 5 usuarios válidos.



El desbloqueo de la primera tarjeta tiene mayor prioridad que el desbloqueo de múltiples tarjetas, lo que significa que si ambas reglas están habilitadas, el sistema realiza primero el desbloqueo de la primera tarjeta.

Se recomienda agregar personas con permiso de desbloqueo de la primera tarjeta al grupo de desbloqueo de múltiples tarjetas.

No configure el **VIP** o **Patrulla** escriba para las personas del grupo de usuarios. Para obtener más información, consulte "3.3.2 Agregar usuario".

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

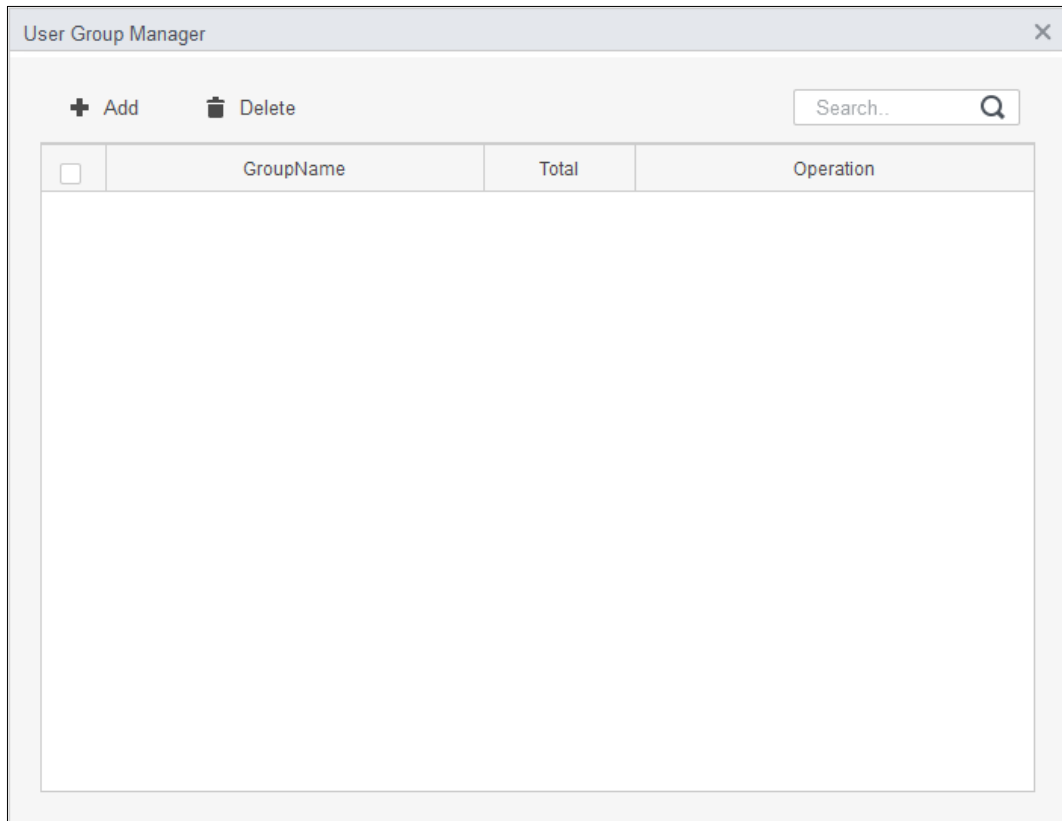
Step 1 Seleccione **Acceda a Configuración > Configuración avanzada**.

Step 2 Haga clic en el **Desbloqueo de múltiples tarjetas** pestaña.

Step 3 Agregar grupo de usuarios.

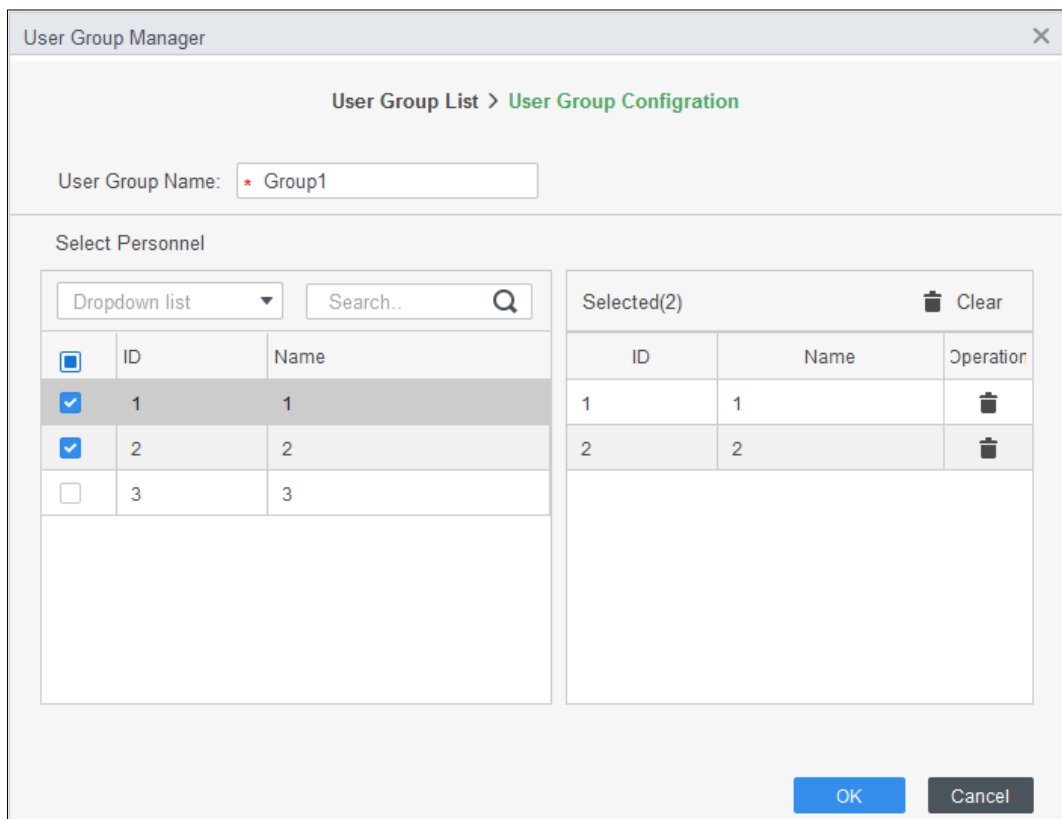
1) Haga clic en **Grupo de usuario**.

Figure 3-14 Administrador de grupo de usuarios



2) Haga clic en **Agregar**.

Figure 3-15 Configuración del grupo de usuarios



3) Configurar **Nombre del grupo de usuarios**. Seleccionar usuarios de **Lista de usuarios** y haga clic en **está bien**. Puede seleccionar hasta 50 usuarios.

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

Step 4 Configure los parámetros de desbloqueo de múltiples tarjetas.

1) Haga clic en **Agregar**.

Figure 3-16 Configuración de desbloqueo de múltiples tarjetas (1)

Multi-card Unlock configuration

Door:

User Group List

<input type="checkbox"/>	User Group Name	Count
<input type="checkbox"/>	Group1	2

Selected (0) Clear

User Group Name	Count	Valid Count	Unlock Mode	Operation
-----------------	-------	-------------	-------------	-----------

OK Cancel

2) Seleccione la puerta.

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

Figure 3-17 Configuración de desbloqueo de múltiples tarjetas (2)

Multi-card Unlock configuration

Door:

User Group List



<input type="checkbox"/>	User Group Name	Count
<input checked="" type="checkbox"/>	Group1	2
<input checked="" type="checkbox"/>	Group2	2

Selected (2) Clear

User Group Name	Count	Valid Count	Unlock Mode	Operation
Group1	2	1	Card	↑ ↓ 🗑️
Group2	2	2	Card	↑ ↓ 🗑️

OK Cancel

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



Haga clic en  o  para ajustar la secuencia de grupo para desbloquear la puerta.

El recuento válido se refiere a la cantidad de usuarios en cada grupo que deben estar en el sitio para pasar sus tarjetas. Tome la Figura 3-17 como ejemplo. La puerta se puede desbloquear solo después de que una persona del grupo 1 y 2 personas del grupo 2 hayan robado sus tarjetas.



Se permiten hasta cinco usuarios válidos.

5) Haga clic en **está bien**.

Step 5 (Opcional) Haga clic en . El icono cambiando a  indica **Desbloqueo de múltiples tarjetas** está habilitado. El recién agregado **Desbloqueo de múltiples tarjetas** está habilitado de forma predeterminada.

3.5.1.3 Anti-passback

La función anti-passback requiere que una persona salga de las puertas específicas. Para la misma persona, un registro de entrada debe emparejarse con un registro de salida. Si alguien ha entrado siguiendo a otra persona, lo que significa que no hay registro de entrada, esta persona no puede abrir la puerta.

Step 1 Seleccione **Acceda a Configuración> Configuración avanzada**.

Step 2 Hacer clic **Agregar**.

Step 3 Configure los 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 es un minuto.

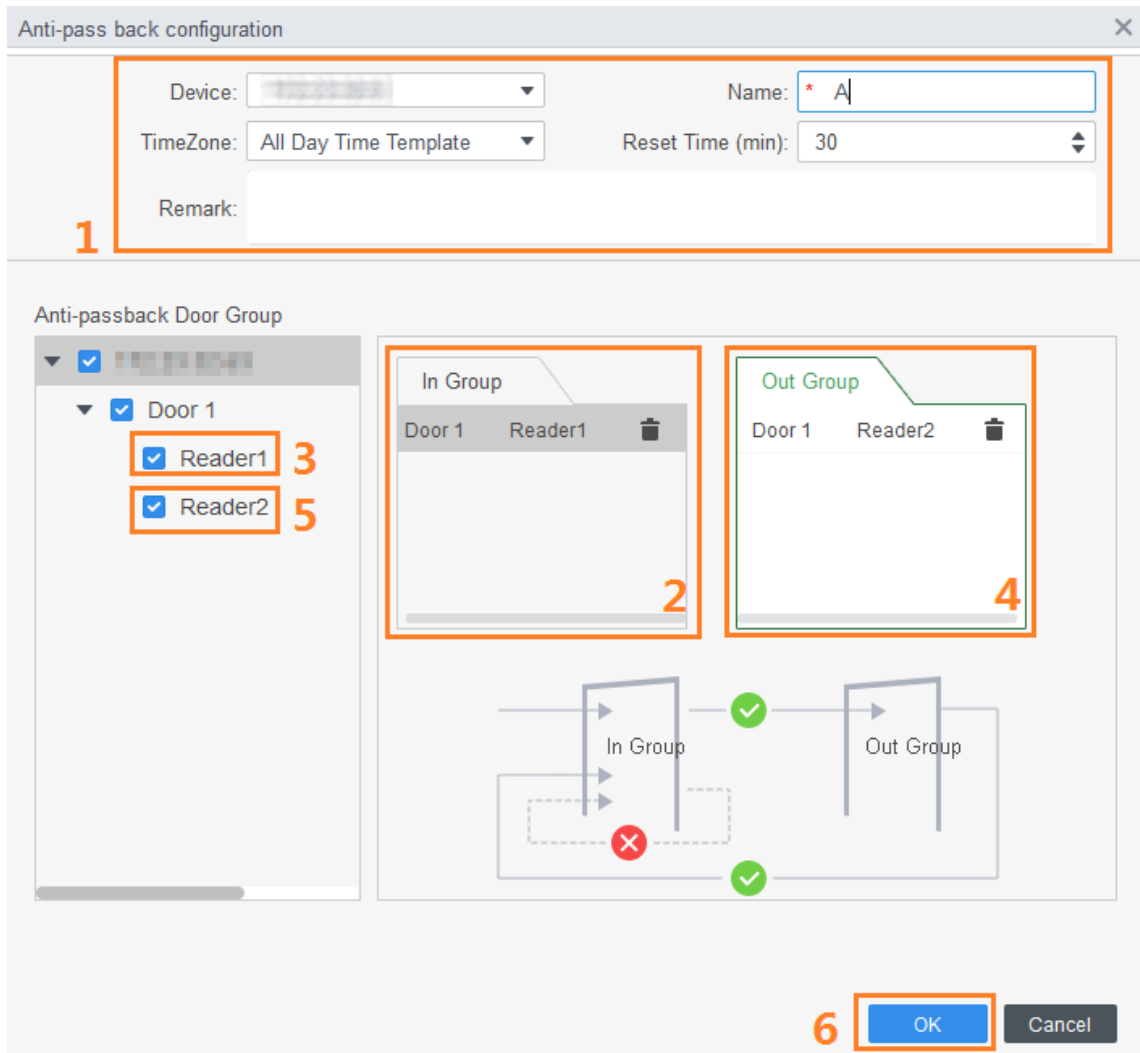
Por ejemplo, establezca el tiempo de reinicio en 30 minutos. Si un miembro del personal ha entrado pero no ha salido, la alarma antirretorno se activará cuando este personal tiende a entrar de nuevo dentro de los 30 minutos. El segundo deslizamiento de este personal solo es válido después de 30 minutos.



4) Haga clic en **En grupo** y seleccione el lector correspondiente. Y luego haga clic en **Fuera de grupo** y seleccione el lector correspondiente.

5) Haga clic en **está bien**.

La configuración se emitirá en el dispositivo y surtirá efecto.

Figure 3-18 Configuración anti-pass back



Step 4 (Opcional) Haga clic en . El icono cambiando a  indica **Anti-passback** está habilitado. El recién agregado **Anti-passback** está habilitado de forma predeterminada.

3.5.1.4 Bloqueo entre puertas

Un controlador central de A&C admite dos grupos de desbloqueo entre puertas, y cada grupo de puertas puede agregar hasta 4 puertas.

Step 1 Seleccione **Acceda a Configuración > Configuración avanzada**.

Step 2 Haga clic en el **Entrelazar** pestaña.

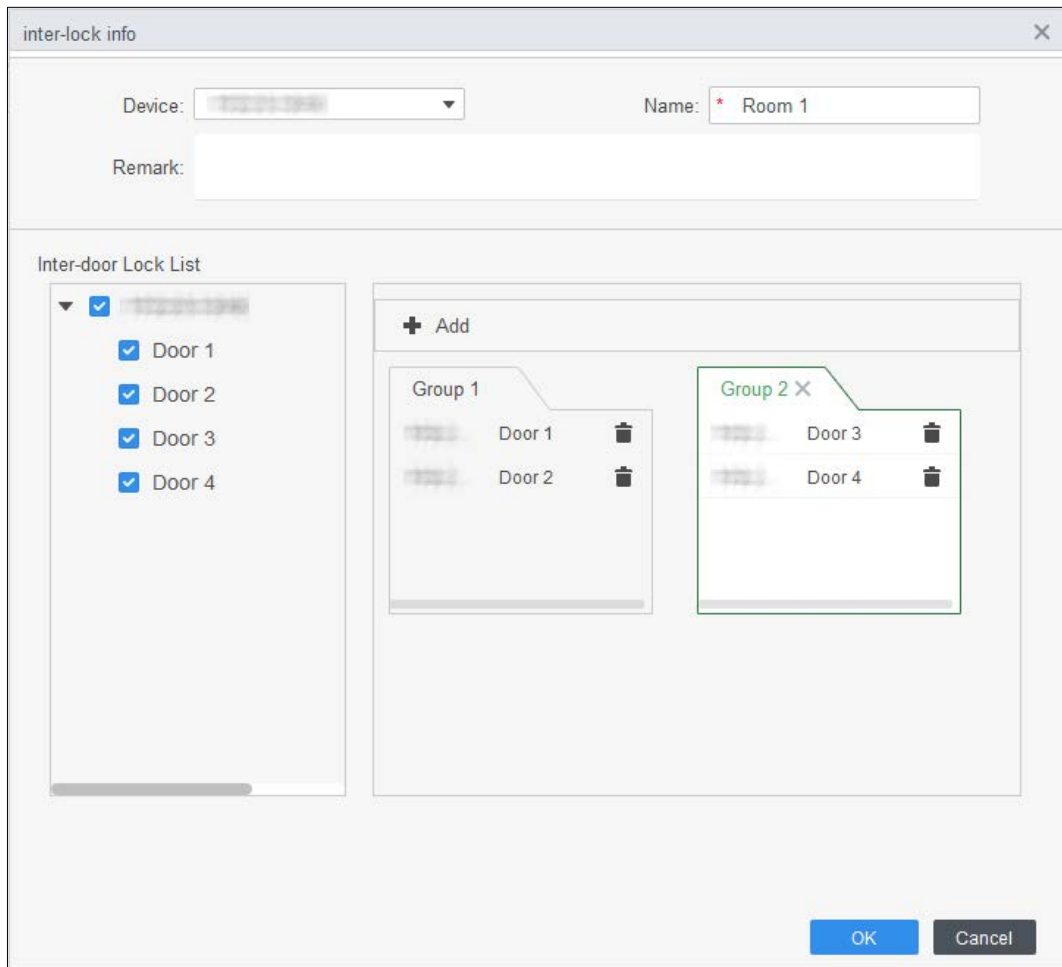
Step 3 Hacer clic **Agregar**.



Step 4 Configure los parámetros y haga clic en **está bien**.

- 1) Seleccione el dispositivo e ingrese el nombre del dispositivo.
- 2) Ingrese comentario.
- 3) Haga clic en **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 en **está bien**.

Figure 3-19 Configuración de bloqueo entre puertas



Step 5 (Opcional) Haga clic en . El icono cambiando a , lo cual indica **Cerradura de puerta** es activado.

El recién agregado **Cerradura de puerta** está habilitado de forma predeterminada.

3.5.2 Configuración de Access Controller

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

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

Step 2 Haga clic en la puerta que debe configurarse.

Step 3 Configure los parámetros.

Figure 3-20 Configurar puerta de acceso

Access Door Config

Door: * Door 1

Reader Direction Config: IN Reader1 ⇌ OUT

Status: Normal Always Open Always Close

Keep OpenTimezone: Unopened

Keep Close Timezone: Unopened

Alarm: Intrusion Overtime Duress

Door Sensor:

Administrator Password: *

Remote Verification:

Unlock Hold Interval: 3 Second

Close Timeout: 15 Second

Unlock Mode: or

Card Fingerprint Face Password

Save Cancel

Figure 3-21 Desbloquear por período de tiempo

Timezone set

Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Timezone 1 00:00 — 06:00 Unlock Mode Card / Fingerprint / Face / Password

Timezone 2 06:00 — 10:00 Unlock Mode Card + Fingerprint



Timezone 3 10:00 — 12:00 Unlock Mode Password

Timezone 4 12:00 — 23:00 Unlock Mode Fingerprint

All

OK Cancel

Tabla 3-3 Parámetros de la puerta de acceso

Parámetro	Descripción
Puerta	Ingrese el nombre de la puerta.
Dirección del lector Config	Hacer clic  para establecer la dirección del lector de acuerdo con situaciones reales.
Estado	<p>Establecer el estado de la puerta, incluido Normal, siempre abierto y Siempre cerca.</p>  <p>No es el estado real de la puerta porque el SmartPSS-AC solo puede enviar comandos al dispositivo. Si desea conocer el estado real de la puerta, habilite el sensor de puerta.</p>
Mantener la zona horaria abierta	Seleccione la plantilla de tiempo cuando la puerta esté siempre abierta.
Manténgase cerca de la zona horaria	Seleccione la plantilla de tiempo cuando la puerta esté siempre cerrada.
Alarma	Habilite la función de alarma y configure el tipo de alarma, incluida la intrusión, las horas extraordinarias y la coacción. Cuando se activa la alarma, 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 configure la contraseña de administrador. Puede acceder ingresando la contraseña.
Verificación remota	Habilite la función y configure la plantilla de tiempo, y luego el acceso de la persona debe ser verificado de forma remota a través del SmartPSS-AC durante los períodos de la plantilla.
Desbloquear intervalo de espera	Establezca el intervalo de retención de desbloqueo. La puerta se cerrará automáticamente cuando se acabe el tiempo.
Cerrar tiempo de espera	Configure el tiempo de espera para la alarma. Por ejemplo, establezca el tiempo de espera de cierre en 60 segundos. Si la puerta no se cierra durante más de 60 segundos, se cargará el mensaje de alarma.
Modo de desbloqueo	<p>Seleccione el modo de desbloqueo según sea necesario.</p> <ul style="list-style-type: none"> ● Seleccione Y, y seleccione métodos de desbloqueo. Puede abrir la puerta combinando los métodos de desbloqueo seleccionados. ● Seleccione O y seleccione métodos de desbloqueo. Puede abrir la puerta de una de las formas que haya configurado. ● Seleccione Desbloquear por período de tiempo y seleccione el modo de desbloqueo para cada período de tiempo. La puerta solo se puede abrir con los métodos seleccionados dentro del período definido.

Step 4 Hacer clic **Ahorrar** y luego la configuración se emitirá en el dispositivo y entrará en vigencia.

3.5.3 Visualización de eventos históricos

Los eventos históricos de puertas incluyen los que ocurrieron en SmartPSS-AC y dispositivos de puerta. Antes de ver, extraiga los eventos históricos en los dispositivos de la puerta para asegurarse de que se busquen todos los eventos.

Step 1 Agregue el personal necesario al SmartPSS-AC. Hacer clic **Configuración de**

Step 2 **acceso> Evento histórico** en la página de inicio. Clickea en el **Administrador**

Step 3 **de acceso** interfaz.

Step 4 Extraiga eventos del dispositivo de la puerta al local. Hacer clic **Extraer**, establecer la hora, seleccionar el dispositivo de la puerta y luego hacer clic en **Extraer ahora**.



Puede seleccionar varios dispositivos a la vez para extraer eventos.

Figure 3-22 Extraer eventos

Time	User ID	Name	Card No.	Device	Door	Event	Verification Method	Access direction	Operation
2020-06-18 10:45:42				BCDFDE66	1	External Alarm			
2020-06-18 10:34:12				BCDFDE66	1	Tamper Alarm			
2020-06-18 10:31:17				BCDFDE66	1	Door Unlocked Alarm			
2020-06-18 10:13:20				BCDFDE66	1	Close Door			
2020-06-18 10:13:17				BCDFDE66	1	Duress			
2020-06-18 10:13:17				BCDFDE66	1	Door is unlocked			
2020-06-18 10:13:17				BCDFDE66	1	Card Unlock	Card	IN	
2020-06-18 10:01:25				BCDFDE66	1	Internal Alarm			
2020-06-18 08:54:08				BCDFDE66	1	Internal Alarm			
2020-06-18 08:53:31				BCDFDE66	1	Internal Alarm			
2020-06-18 08:53:16				BCDFDE66	1	Internal Alarm			
2020-06-18 08:53:09				BCDFDE66	1	Internal Alarm			
2020-06-18 08:53:08				BCDFDE66	1	Internal Alarm			
2020-06-18 08:52:37				BCDFDE66	1	Internal Alarm			
2020-06-18 08:52:35				BCDFDE66	1	Internal Alarm			
2020-06-18 08:52:11				BCDFDE66	1	Internal Alarm			
2020-06-18 08:39:14	30080	30080	134	BCDFDE66	1	Face Recognition	Face Recog...	IN	
2020-06-18 08:39:05	30080	30080	134	BCDFDE66	1	Face Recognition	Face Recog...	IN	
2020-06-18 08:32:42				BCDFDE66	1	Unregistered or lost	Face Recog...		
2020-06-18 08:30:55				BCDFDE66	1	Close Door			

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

Figure 3-23 Buscar eventos por condiciones de filtrado


The image shows a vertical search interface. At the top is a search bar with the text "Search.." and a magnifying glass icon. Below it are two dropdown menus: the first is labeled "Default Group" and the second is partially obscured. A third dropdown menu is highlighted in grey and labeled "Door 1". Below these are several filter sections: "Event:" with two dropdown menus (one showing "Abnormal" and the other "All"); "Time:" with a date and time range "05/07 00:00-05/07 23:59" and a calendar icon; "User ID/C..." with a text input field containing "1"; "Name:" with a text input field containing "1"; and "Departme..." with a dropdown menu showing "Company\DepartmentA". At the bottom is a blue button labeled "Search".

Step 6 (Opcional) Haga clic en **Exportar**, y luego opere de acuerdo con las instrucciones para guardar los eventos de puerta buscados en el local.

3.6 Gestión de Acceso

3.6.1 Apertura y cierre de puertas de forma remota

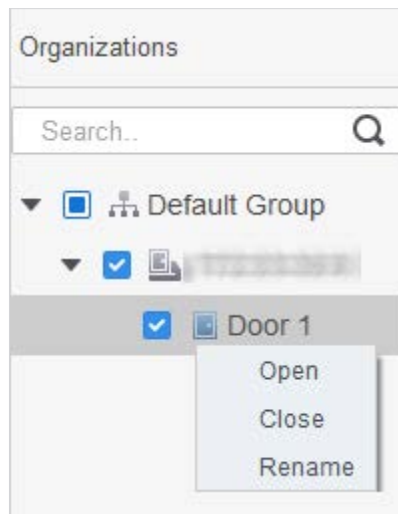
Después de la configuración de acceso, puede controlar la puerta de forma remota a través de SmartPSS AC.

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

Step 2 Controla la puerta de forma remota. Hay dos métodos.

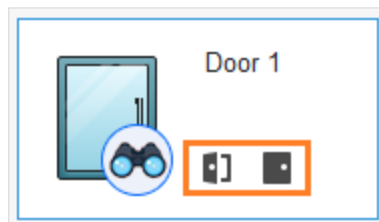
Método 1: seleccione la puerta, haga clic derecho y seleccione **Abierto**.

Figure 3-24 Control remoto (método 1)



Método 2: haga clic en  o  para abrir o cerrar la


Figure 3-25 puerta. Control remoto (método 2)



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



Filtrado de eventos: seleccione el tipo de evento en el **Información del evento**, y la lista de eventos muestra eventos de los tipos seleccionados. Por ejemplo, seleccione **Alarma**, y la lista de eventos solo muestra eventos de alarma.

Bloqueo de actualización de eventos: haga clic en  junto a **Información del evento** para bloquear o desbloquear la lista de eventos, y entonces los eventos en tiempo real no se pueden ver.

Eliminación de eventos: haga clic en  junto a **Información del evento** para borrar todos los eventos de la lista de eventos.

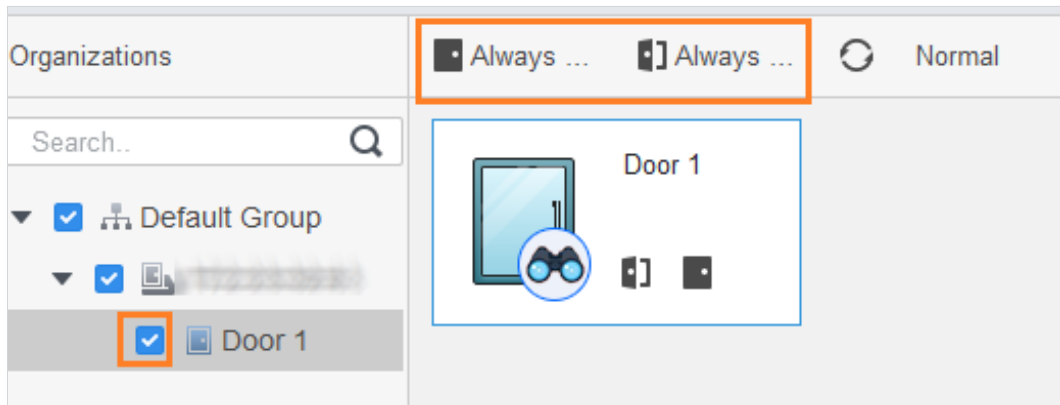
3.6.2 Configurar siempre abierto y siempre cerrado

Después de configurar siempre abierto o siempre cerrado, la puerta está abierta o cerrada todo el tiempo y no se puede controlar manualmente. Si desea volver a controlar manualmente la puerta, haga clic en **Normal** para restablecer el estado de la puerta.

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


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

Figure 3-26 Establecer siempre abierto o siempre cerrado



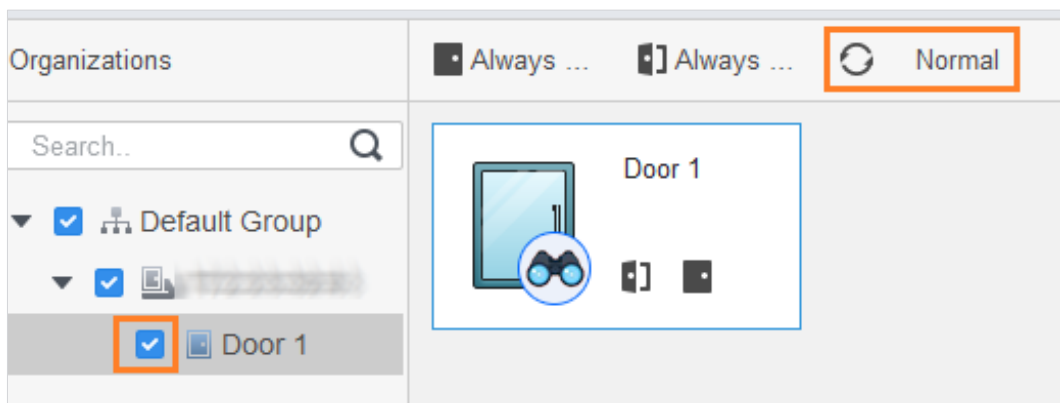
3.6.3 Restablecimiento del estado de la puerta

Hacer clic **Normal** para restablecer el estado de la puerta, si desea volver a controlar manualmente la puerta cuando haya hecho clic **Siempre abierto** o **Siempre cerca**.

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

Step 2 Seleccione la puerta necesaria y luego haga clic en **Normal**. Siga las instrucciones en pantalla para operar.

Figure 3-27 Restablecer el estado de la puerta



3.7 Configuración de eventos

Mediante la configuración de eventos, puede establecer vínculos de software, como sonido de alarma, envío de correo y vínculos de alarma.

Configure los enlaces de alarma externa conectados al controlador de acceso, como la alarma de humo. Configure los vínculos de los eventos del controlador de acceso.

- ◇ Alarmevent
- ◇ 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 de funciones avanzadas".


Step 1 Hacer clic **Configuración de eventos** en la página de inicio. Seleccione la puerta necesaria y

Step 2 seleccione **AlarmEvent** > **Evento de intrusión**.

Step 3 Haga clic junto a **Alarma de intrusión** para habilitar la función. Configure las

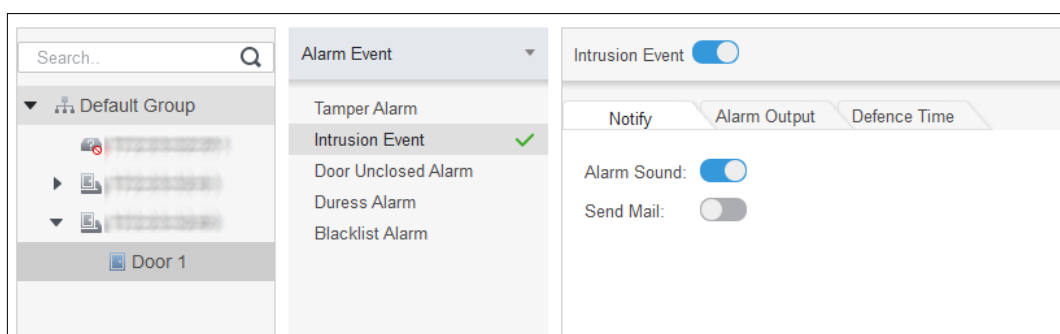
Step 4 acciones de vinculación de alarmas de intrusión según sea necesario.

Habilita el sonido de la alarma.

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

- 1) Habilitar **Enviar correo** y confirme para configurar SMTP. los **Ajustes del sistema** se muestra la interfaz. Configure
- 2) los parámetros de SMTP, como la dirección del servidor, el número de puerto y el modo de cifrado. Cuando ocurre un evento de intrusión, el sistema envía automáticamente correos electrónicos de alarma al receptor especificado.

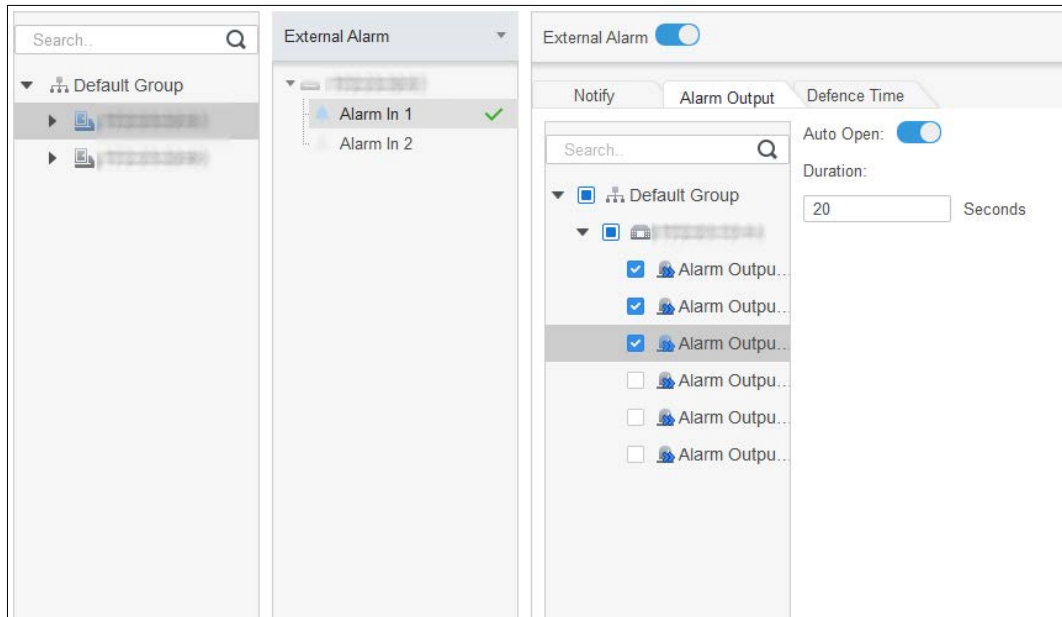
Figure 3-28 Configurar alarma de intrusión



Configure la E / S de alarma.

- 1) Haga clic en el **Salida de alarma** pestaña.
- 2) Seleccione el dispositivo que admite la entrada de alarma, seleccione la interfaz de entrada de alarma y luego habilite **Alarma externa**.
- 3) Seleccione el dispositivo que admita la salida de alarma, luego seleccione la interfaz de salida de alarma.
- 4) Habilitar **Apertura automática** para el enlace de alarma. Establezca la duración.
- 5)

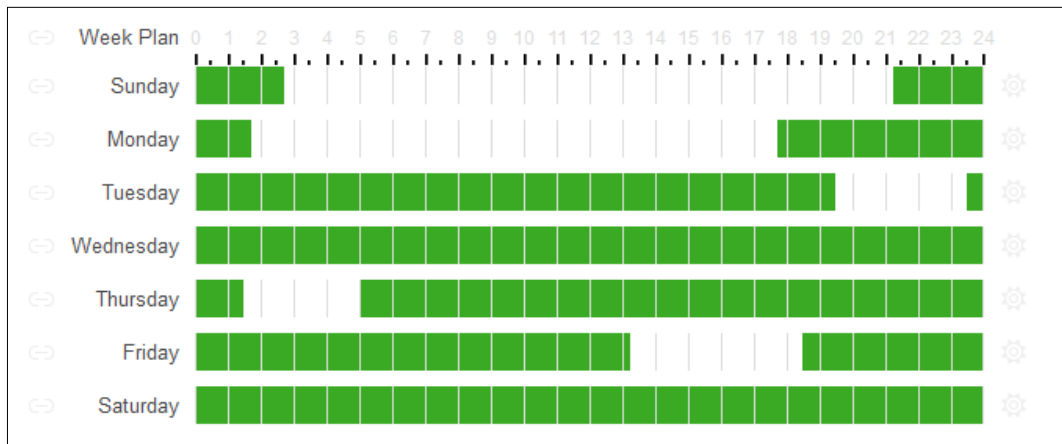
Figure 3-29 Configurar enlace de alarma



Establece tiempo de defensa. Hay dos métodos.

Método 1: mueva el cursor para establecer períodos de tiempo. Cuando el cursor es un lápiz, haga clic para agregar puntos; cuando el cursor es borrador, haga clic para menos puntos. La zona verde son los periodos con defensa.

Figure 3-30 Establecer tiempo de defensa (método 1)




Método 2: haga clic en  para establecer períodos y, a continuación, haga clic en **está bien**.

Figure 3-31 Establecer tiempo de defensa (método 2)

The screenshot shows a dialog box titled "Time Editor" with a close button (X) in the top right corner. It contains six rows, each labeled "Timezone 1" through "Timezone 6". Each row has two time input fields separated by a hyphen. The values are: Timezone 1 (0:00:00 - 2:45:00), Timezone 2 (11:30:00 - 14:15:00), Timezone 3 (21:15:00 - 23:59:59), Timezone 4 (0:00:00 - 0:00:00), Timezone 5 (0:00:00 - 0:00:00), and Timezone 6 (0:00:00 - 0:00:00). Below the rows is a "Check All" checkbox which is checked. Underneath is a horizontal line, followed by seven day checkboxes: Sun (checked), Mon, Tue, Wed, Thu, Fri, and Sat. At the bottom right are "OK" and "Cancel" buttons.

Step 5 (Opcional) Haga clic en **Copiar a**, seleccione el controlador de acceso al que se aplicará y luego haga clic en **está bien**.

Step 6 Hacer clic **Ahorrar**.

4 Configuración de ConfigTool

ConfigTool se utiliza principalmente para configurar y mantener el dispositivo.



No use ConfigTool y SmartPSS AC al mismo tiempo, de lo contrario podría causar una búsqueda anormal del dispositivo.


4.1 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, la herramienta no puede encontrar el dispositivo.

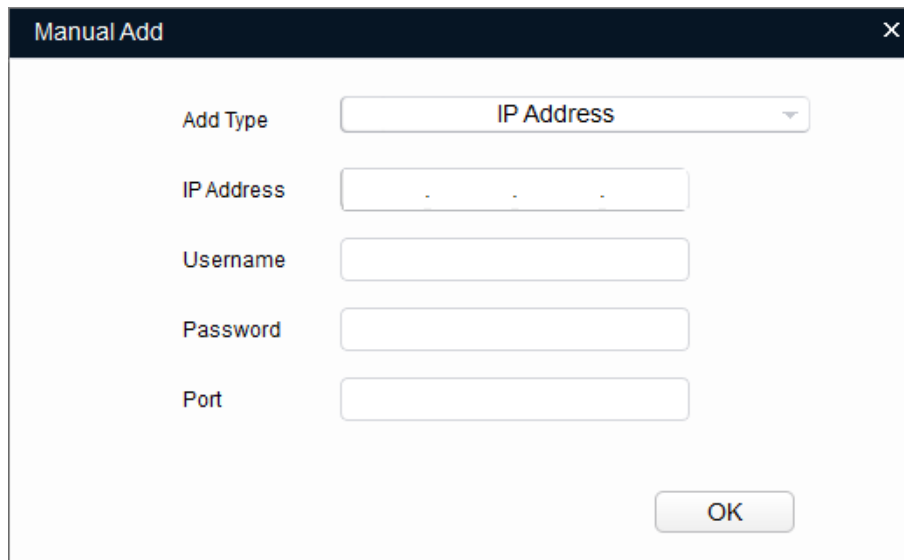
4.1.1 Agregar un dispositivo

Step 1 Hacer clic .

Step 2 Hacer clic **Agregar manual**.

Step 3 Seleccione **Dirección IP** de **AddType**.

Figure 4-1 Adición manual (dirección IP)



Step 4 Configure los parámetros del dispositivo.

Tabla 4-1 Parámetros de adición manual

AddMethod	Parámetro	Descripción
Dirección IP	Dirección IP	La dirección IP del dispositivo. Es 192.168.1.108 por defecto.

AddMethod	Parámetro	Descripción
	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 **está bien**.

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

4.1.2 Agregar varios dispositivos

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

4.1.2.1 Agregar mediante búsqueda

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



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

Step 1 Hacer clic 

Figure 4-2 Configuración

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

Buscar segmento actual

Selecciona el **Búsqueda de segmento actual** casilla de verificación. Ingrese el nombre de usuario en el **Nombre de usuario** cuadro y la contraseña en el **Contraseña** caja. El sistema buscará los dispositivos en consecuencia.

Buscar otro segmento

Selecciona el **Búsqueda de otro segmento** casilla de verificación. Ingrese la dirección IP en el **Iniciar IP** caja y **IP final** caja respectivamente. Ingrese el nombre de usuario en el **Nombre de usuario** cuadro y la contraseña en el **Contraseña** caja. El sistema buscará los dispositivos en consecuencia.

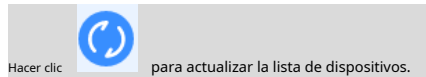


Si selecciona el **Búsqueda de segmento actual** y el **Búsqueda de otro segmento** casillas de verificación juntas, el sistema busca dispositivos en ambas condiciones.

El nombre de usuario y la contraseña son los que se utilizan para iniciar sesión cuando desea cambiar la IP, configurar el sistema, actualizar el dispositivo, reiniciar el dispositivo y más.

Step 3 Hacer clic **OK** para comenzar a buscar dispositivos.

Los dispositivos buscados se mostrarán en la lista de dispositivos en la interfaz de usuario principal.




El sistema guarda las condiciones de búsqueda al salir del software y reutiliza las mismas condiciones cuando se inicia el software la próxima vez.

4.1.2.2 Agregar mediante la importación de DeviceTemplate

Puede agregar los dispositivos completando e importando una plantilla de Excel. Puede importar 1000 dispositivos como máximo.



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

Step 1 Exportar plantilla de dispositivo. Hacer clic , seleccione un dispositivo, haga clic en **Exportar**, y luego sigue el guía en pantalla para guardar el archivo de plantilla localmente.

Step 2 Complete la plantilla. Abra el archivo de plantilla, siga la información del dispositivo existente para completar la información de los dispositivos que desea agregar.

Step 3 Importe la plantilla. Hacer clic **Importar**, seleccione la plantilla y haga clic en **Abierto**.

El sistema comienza a importar los detalles de los dispositivos. Una vez completada la importación, se muestra un aviso de éxito.

Step 4 Hacer clic **está bien**.

Los dispositivos recién importados aparecen en la lista de dispositivos.

4.2 Configuración de Access Controller



Las interfaces y los parámetros de este manual son solo de referencia y pueden diferir de los reales.

Step 1 Hacer clic  en la barra de menú.

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 la interfaz de inicio de sesión se lo solicita, ingrese el nombre de usuario y la contraseña, y luego haga clic en **está bien**.

Step 4 Configure los parámetros del controlador de acceso.

Figure 4-3 Configurar controlador de acceso

The screenshot shows a configuration window for an access controller. It contains the following elements:

- Channel:** A dropdown menu with '0' selected.
- Card No.:** A dropdown menu with 'No Convert' selected.
- Tcp Port:** A text input field containing '37777' and a 'Save' button to its right.
- System Log:** A text input field and a 'Get' button to its right.
- CommPort:** A dropdown menu with '0' selected.
- Bitrate:** A dropdown menu with '9600' selected.
- OSDPEnable:** A toggle switch currently in the 'off' position.

Canal: Seleccione el canal para configurar los parámetros.

No de tarjeta: Configure la regla de procesamiento del número de tarjeta del controlador de acceso. Está **No convertir** por defecto. Cuando el resultado de la lectura de la tarjeta no coincida con el número de la tarjeta enviada, seleccione **Byte Revertir** o **HIDpro Convert**.

Byte Revertir: Cuando el controlador de acceso funciona con lectores de terceros y el resultado de la lectura de la tarjeta no coincide con el número de la tarjeta enviada. Por ejemplo, el resultado de la lectura de la tarjeta es hexadecimal 12345678 mientras que el número de tarjeta enviada es hexadecimal 78563412, puede seleccionar **Byte Revertir** para igualarlos.

Conversión de HIDpro: Cuando el controlador de acceso funciona con lectores HID Wiegand y el resultado de la lectura de la tarjeta no coincide con el número de la tarjeta enviada, por ejemplo, el resultado de la lectura de la tarjeta es hexadecimal 1BAB96 mientras que el número de la tarjeta enviada es hexadecimal 78123456, puede seleccionar **HIDpro Revertir** para igualarlos.

Puerto TCP: Modifique el número de puerto TCP del dispositivo.


SysLog: Hacer clic **Obtener** para seleccionar una ruta de almacenamiento para los registros del sistema.

CommPort: Seleccione el lector para configurar 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 9,600 por defecto.

OSDPEnable: 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 que necesita para sincronizar el configurado parámetros a, y luego haga clic en **Config**.

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

4.3 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 4-4 Contraseña del dispositivo

Modify Password

Old Password

New Password

Weak
Medium
Strong

Confirm Password

*After you have set new password, please set password again in "Search setting".

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 4-2 Parámetros de contraseña

Parámetro	Descripción
Contraseña anterior	Ingrese la contraseña anterior del dispositivo. Para asegurarse de que la contraseña anterior se ingrese correctamente, puede hacer clic en Cheque 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 **OK** para completar la modificación.

Appendix 1 Recomendaciones de ciberseguridad

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

Acciones obligatorias que deben tomarse para la seguridad de la red de equipos básicos:

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Actualice el firmware y el software cliente inTime

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

Recomendaciones "Es bueno tener" para mejorar la seguridad de la red de su equipo:

1. Protección física

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

2. Cambie las contraseñas con regularidad

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

3. Establecer y actualizar la información de restablecimiento de contraseñas

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

4. Habilite el bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilite HTTPS

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

7. Enlace de dirección MAC

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

8. Asignar cuentas y privilegios de forma razonable

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

9. Desactive los servicios innecesarios y elija los modos seguros

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

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

SNMP: elija SNMP v3 y configure contraseñas de cifrado y contraseñas de autenticación seguras.

SMTP: elija TLS para acceder al servidor de buzones de correo.

FTP: elija SFTP y configure contraseñas seguras.

Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

10. Transmisión encriptada de audio y video

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

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

11. Auditoría segura

Verificar usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo está conectado sin autorización.

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

13. Construya un entorno de red seguro

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

Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la 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, 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.