

Acceso bidireccional de dos puertas

Controlador

Guía de inicio rápido

V1.0.0

Recomendaciones de ciberseguridad

Acciones obligatorias a tomar en materia de ciberseguridad

1. Cambie las contraseñas y use contraseñas seguras:

La razón número uno por la que los sistemas son "pirateados" se debe a que tienen contraseñas débiles o predeterminadas. Se recomienda cambiar las contraseñas predeterminadas de inmediato y elegir una contraseña segura siempre que sea posible. Una contraseña segura debe estar compuesta por al menos 8 caracteres y una combinación de caracteres especiales, números y letras mayúsculas y minúsculas.

2. Actualizar firmware

Como es un procedimiento estándar en la industria de la tecnología, recomendamos mantener actualizado el firmware de la cámara NVR, DVR y IP para garantizar que el sistema esté actualizado con los últimos parches y correcciones de seguridad.

Recomendaciones "agradables de tener" para mejorar la seguridad de su red

1. Cambie las contraseñas regularmente

Cambie regularmente las credenciales de sus dispositivos para ayudar a garantizar que solo los usuarios autorizados puedan acceder al sistema.

2. Cambiar los puertos HTTP y TCP predeterminados:

- Cambiar los puertos HTTP y TCP predeterminados para los sistemas. Estos son los dos puertos que se utilizan para comunicarse y ver videos de forma remota.
- Estos puertos se pueden cambiar a cualquier conjunto de números entre 1025 y 65535. Evitar los puertos predeterminados reduce el riesgo de que personas externas puedan adivinar qué puertos está utilizando.

3. Habilite HTTPS/SSL:

Configure un certificado SSL para habilitar HTTPS. Esto encriptará toda la comunicación entre sus dispositivos y la grabadora.

4. Habilitar filtro IP:

Habilitar su filtro IP evitará que todos, excepto aquellos con direcciones IP específicas, accedan al sistema.

5. Cambiar la contraseña de ONVIF:

En el firmware anterior de la cámara IP, la contraseña de ONVIF no cambia cuando cambia las credenciales del sistema. Deberá actualizar el firmware de la cámara a la última revisión o cambiar manualmente la contraseña de ONVIF.

6. Reenviar solo los puertos que necesita:

- Solo reenvíe los puertos HTTP y TCP que necesita usar. No reenvíe una gran variedad de números al dispositivo. No DMZ la dirección IP del dispositivo.
- No necesita reenviar ningún puerto para cámaras individuales si todas están conectadas a una grabadora en el sitio; solo se necesita el NVR.

7. Deshabilite el inicio de sesión automático en SmartPSS:

Aquellos que usan SmartPSS para ver su sistema y en una computadora que usan varias personas deben deshabilitar el inicio de sesión automático. Esto agrega una capa de seguridad para evitar que los usuarios sin las credenciales adecuadas accedan al sistema.

8. Utilice un nombre de usuario y una contraseña diferentes para SmartPSS:

En el caso de que su cuenta de redes sociales, banco, correo electrónico, etc. se vea comprometida, no querrá que alguien recopile esas contraseñas y las pruebe en su sistema de videovigilancia. El uso de un nombre de usuario y una contraseña diferentes para su sistema de seguridad hará que sea más difícil para alguien adivinar cómo ingresar a su sistema.

9. Funciones de límite de las cuentas de invitados:

Si su sistema está configurado para varios usuarios, asegúrese de que cada usuario solo tenga derechos sobre las características y funciones que necesita usar para realizar su trabajo.

10. UPnP:

- UPnP intentará automáticamente reenviar puertos en su enrutador o módem. Normalmente esto sería algo bueno. Sin embargo, si su sistema reenvía automáticamente los puertos y deja las credenciales predeterminadas, puede terminar con visitantes no deseados.
- Si reenvió manualmente los puertos HTTP y TCP en su enrutador/módem, esta función debe desactivarse independientemente. Se recomienda deshabilitar UPnP cuando la función no se usa en aplicaciones reales.

11. SNMP:

Deshabilite SNMP si no lo está utilizando. Si está utilizando SNMP, debe hacerlo solo temporalmente, solo con fines de seguimiento y prueba.

12. Multidifusión:

La multidifusión se utiliza para compartir transmisiones de video entre dos grabadoras. Actualmente no hay problemas conocidos relacionados con la multidifusión, pero si no está utilizando esta función, la desactivación puede mejorar la seguridad de su red.

13. Verifique el Registro:

Si sospecha que alguien ha obtenido acceso no autorizado a su sistema, puede consultar el registro del sistema. El registro del sistema le mostrará qué direcciones IP se usaron para iniciar sesión en su sistema y a qué se accedió.

14. Bloquee físicamente el dispositivo:

Idealmente, desea evitar cualquier acceso físico no autorizado a su sistema. La mejor manera de lograr esto es instalar la grabadora en una caja de seguridad, un rack de servidor con llave o en una habitación que esté detrás de una cerradura y una llave.

15. Conecte las cámaras IP a los puertos PoE en la parte posterior de un NVR:

Las cámaras conectadas a los puertos PoE en la parte posterior de un NVR están aisladas del mundo exterior y no se puede acceder a ellas directamente.

16. Aislar NVR y red de cámaras IP

La red en la que reside su NVR y su cámara IP no debe ser la misma red que su red informática pública. Esto evitará que los visitantes o invitados no deseados obtengan acceso a la misma red que necesita el sistema de seguridad para funcionar correctamente.

Información reglamentaria

Información de la FCC



PRECAUCIÓN

Los cambios o modificaciones no aprobados expresamente por la parte responsable del cumplimiento podrían anular la autoridad del usuario para operar el equipo.

Condiciones de la FCC:

Este dispositivo cumple con la parte 15 de las normas de la FCC. La operación está sujeta a las siguientes dos condiciones:

- Este dispositivo no puede causar interferencias perjudiciales.
- Este dispositivo debe aceptar cualquier interferencia recibida, incluida la interferencia que pueda provocar un funcionamiento no deseado.

Cumplimiento de la FCC:

Este equipo ha sido probado y se encontró que cumple con los límites para un dispositivo digital, de conformidad con la parte 15 de las Reglas de la FCC. Este equipo genera, usa y puede irradiar energía de radiofrecuencia y, si no se instala y usa de acuerdo con la guía, puede causar interferencias dañinas en las comunicaciones por radio.






- Para dispositivos de clase A, estos límites están diseñados para brindar una protección razonable contra interferencias dañinas en un entorno comercial. Es probable que la operación de este equipo en un área residencial cause interferencias perjudiciales, en cuyo caso el usuario deberá corregir la interferencia por su propia cuenta.
- Para dispositivos de clase B, estos límites están diseñados para brindar una protección razonable contra interferencias dañinas en una instalación residencial. Sin embargo, no hay garantía de que no se produzcan interferencias en una instalación en particular. Si este equipo causa interferencias dañinas en la recepción de radio o televisión, lo que se puede determinar apagando y encendiendo el equipo, se recomienda al usuario que intente corregir la interferencia mediante una o más de las siguientes medidas:
 - Reorientar o reubicar la antena receptora.
 - Aumente la separación entre el equipo y el receptor.
 - Conecte el equipo a una toma de un circuito diferente al que está conectado el receptor.
 - Consulte al distribuidor o a un técnico experimentado en radio/TV para obtener ayuda.

General

Este documento detalla la estructura, instalación y cableado del controlador de acceso bidireccional de dos puertas.

Las instrucciones de seguridad

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

Palabras de advertencia	Sentido
 DANGER	Indica un peligro de alto potencial que, si no se evita, provocará la muerte o lesiones graves.
 WARNING	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 CAUTION	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
 TIPS	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
 NOTE	Proporciona información adicional como énfasis y complemento del texto.

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otros, como la cara, las huellas dactilares, el número de placa del automóvil, la dirección de correo electrónico, el número de teléfono, el GPS, etc. 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 al sujeto de los datos sobre la existencia de un área de vigilancia y proporcionar contacto relacionado.

Acerca de la guía

- La Guía es solo para referencia. Si hay inconsistencia entre la Guía y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por las operaciones que no cumplan con la Guía. La Guía se actualizaría de acuerdo con las últimas leyes y reglamentos de las regiones relacionadas. Para obtener información detallada, consulte el Manual del usuario en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el Manual del usuario 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 la Guía. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria. Todavía puede haber desviación en los datos técnicos, descripción de funciones y operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final.
- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir la Guía (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de compañías en la Guía son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio al cliente si ocurre algún problema al usar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

Medidas de seguridad y advertencias importantes

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

Requisito operativo

- No coloque ni instale el dispositivo en un área expuesta a la luz solar directa o cerca de un dispositivo generador de calor.
- No instale el dispositivo en un área húmeda, polvorienta o fuliginosa.
- Mantenga su instalación horizontal o instálela en lugares estables y evite que se caiga.
- Por favor, no gotee ni salpique líquidos sobre el dispositivo; no coloque en el dispositivo nada lleno de líquidos, para evitar que los líquidos fluyan hacia el dispositivo.
- Instale el dispositivo en lugares bien ventilados; no bloquee su abertura de ventilación.
- Use el dispositivo solo dentro del rango nominal de entrada y salida.
- Por favor, no desmonte el dispositivo arbitrariamente.
- Transporte, use y almacene el dispositivo dentro del rango permitido de humedad y temperatura.

Requisitos de energía

- Asegúrese de usar baterías de acuerdo con los requisitos; de lo contrario, puede provocar incendios, explosiones o quemar las baterías.
- ¡Para reemplazar las baterías, solo se puede usar el mismo tipo de baterías!
- ¡El producto debe usar cables eléctricos (cables de alimentación) recomendados por esta área, que deben usarse dentro de su especificación nominal!
- Utilice un adaptador de corriente estándar que coincida con el dispositivo. De lo contrario, el usuario asumirá las lesiones personales resultantes o daños al dispositivo.
- Utilice una fuente de alimentación que cumpla con los requisitos SELV (voltaje extra bajo de seguridad) y suministre energía con un voltaje nominal que cumpla con la fuente de alimentación limitada en IEC60950-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas del dispositivo.
- Los productos con estructura de categoría I se conectarán a la toma de salida de la red eléctrica, que está equipada con protección a tierra.
- El acoplador de electrodomésticos es un dispositivo de desconexión. Durante el uso normal, mantenga un ángulo que facilite la operación.

Tabla de contenido

Recomendaciones de ciberseguridad	I
Información reglamentaria	IV
Prólogo	V
Medidas de seguridad y advertencias importantes	VII
1 Visión de conjunto.....	1
1.1 Característica funcional	1
1.2 Dimension externa.....	1
2 Guía de instalación.....	3
2.1 Estructura del sistema.....	3
2.2 Instalación del dispositivo	3
2.3 Desmontaje.....	4
2.4 Diagrama de cableado	5
2.4.1 Descripción del cableado del controlador de acceso	5
2.4.2 Descripción del cableado del botón de salida/contacto de puerta	6
2.4.3 Descripción del cableado de la cerradura	7
2.4.4 Descripción del cableado del lector	8
2.4.5 Descripción del cableado de la entrada de alarma externa.....	8
2.4.6 Descripción del cableado de la salida de alarma externa	9
2.4.7 Descripción del cableado de la salida de alarma interna	10
2.4.8 Descripción de la regla de entrada y salida de alarma	11
2.5 Dip switch.....	11
2.6 Reiniciar.....	12
3 Configuración de PSS inteligente	13
3.1 Cliente de inicio de sesión	13
3.2 Agregar controlador de acceso.....	13
3.2.1 Búsqueda automática	13
3.2.2 Adición manual	15
4 Preguntas frecuentes	17
1. Pregunta: Después de encender, el indicador de encendido no se enciende o el zumbador no responde.	17
2. Pregunta: Después de conectar el lector con el dispositivo, la luz de pasar la tarjeta no se enciende y no responde después de pasar una tarjeta.	17
3. Pregunta: El software del cliente no detecta el dispositivo.	17
4. Pregunta: Después de deslizar la tarjeta, indica que la tarjeta no es válida	17
5. Pregunta: IP predeterminada del controlador de acceso.	17
6. Pregunta: Puerto predeterminado, nombre de usuario inicial y contraseña del controlador de acceso.	17
7. Pregunta: Actualización en línea del dispositivo.	17
8. Pregunta: Máx. distancia de cableado y distancia de transmisión del lector de tarjetas y el controlador	17

El controlador de acceso bidireccional de dos puertas 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, propiedades corporativas y comunidades inteligentes.

1.1 Característica funcional

Sus ricas funciones son las siguientes:

- Adopte un riel deslizante y un diseño controlado por bloqueo, instalación y mantenimiento convenientes.
- Integra alarma, control de acceso, video vigilancia y alarma contra incendios.
- Admite 4 juegos de lectores de tarjetas (que se pueden configurar como 2 lectores bidireccionales de una puerta).
- Admite 8 grupos de entrada de señal (botón de salida*2, contacto de puerta*2 y alarma de intrusión*4). Admite 6 grupos de salida de control (cerradura eléctrica * 2, salida de alarma externa * 2 y salida de alarma interna * 2).
- Con puerto RS485, puede extenderse para conectar el módulo de control.
- La capacidad de almacenamiento FLASH es de 16M (que puede extenderse a 32M). Soporte máx. 100.000 titulares de tarjetas y 150.000 registros de lectura de tarjetas.
- Admite alarma de intrusión ilegal, alarma de tiempo de espera de desbloqueo, tarjeta de coacción y configuración de código de coacción. También es compatible con la lista en blanco y negro y la configuración de la tarjeta de patrulla.
- Admite la configuración de un período de tiempo válido, la configuración de una contraseña y la configuración de la fecha de caducidad de las tarjetas. En cuanto a la tarjeta de huésped, se puede configurar su tiempo de uso.
- Admite 128 grupos de horarios y 128 grupos de horarios de vacaciones. Almacenamiento de datos permanente durante la interrupción, RTC integrado (compatible con DST), actualización en línea.

1.2 Dimension externa

Su apariencia y dimensión se muestran en la Figura 1-1 y la Figura 1-2. La unidad es mm.

Figure 1-1

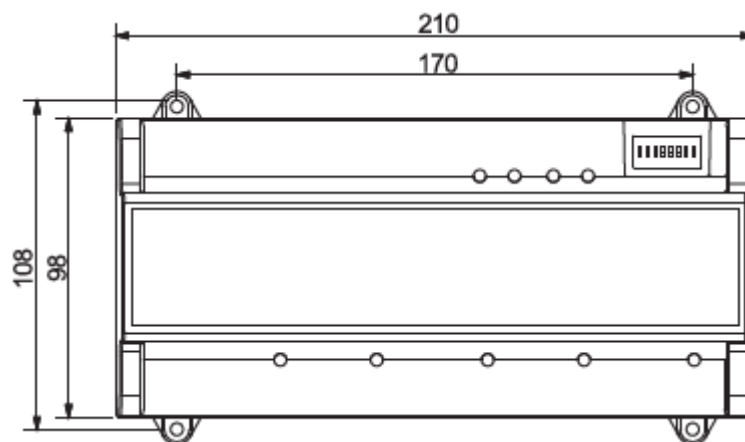
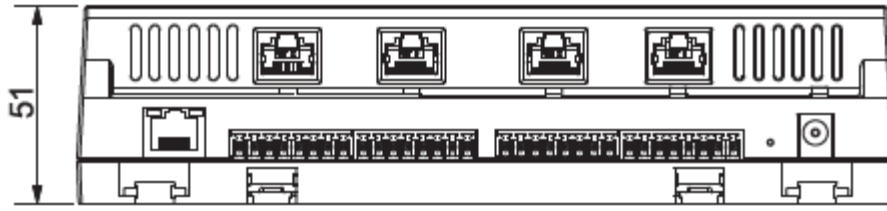


Figure 1-2

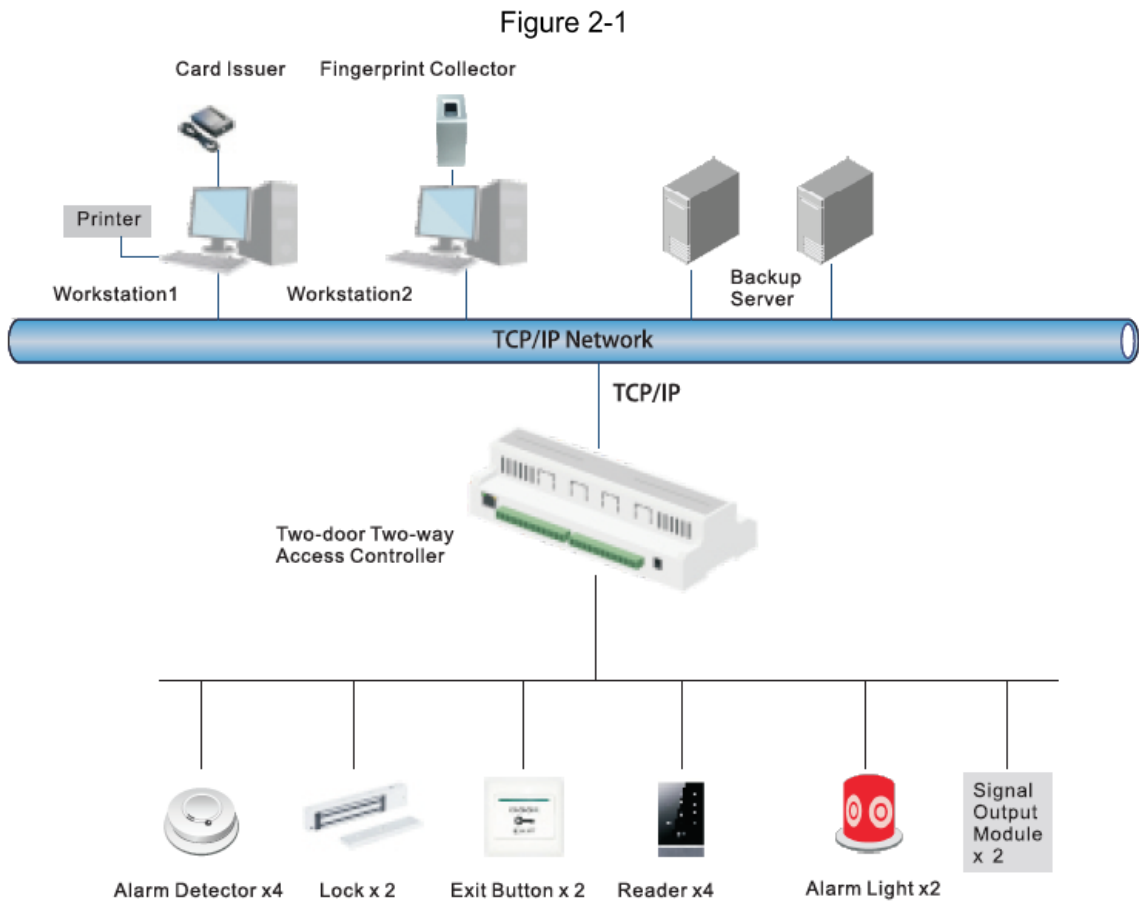


2

Guía de instalación

2.1 Estructura del sistema

La estructura del sistema del controlador de acceso bidireccional de dos puertas, cerradura de puerta y lector se muestra en la Figura 2-1.



2.2 Instalación del dispositivo

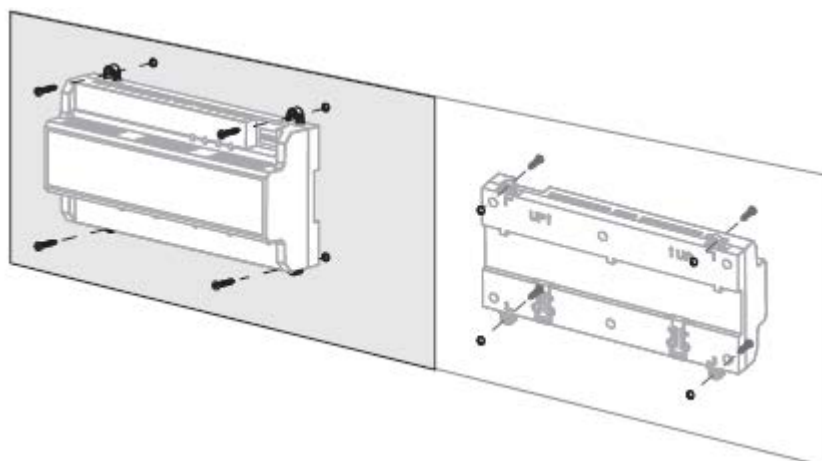
Hay dos modos de instalación.

- Modo 1: fije todo el dispositivo a la pared con tornillos.
- Modo 2: con riel guía en forma de U, cuelgue todo el dispositivo en la pared (el riel guía en forma de U es un accesorio opcional).

Modo 1

El diagrama de instalación se muestra en la Figura 2-2.

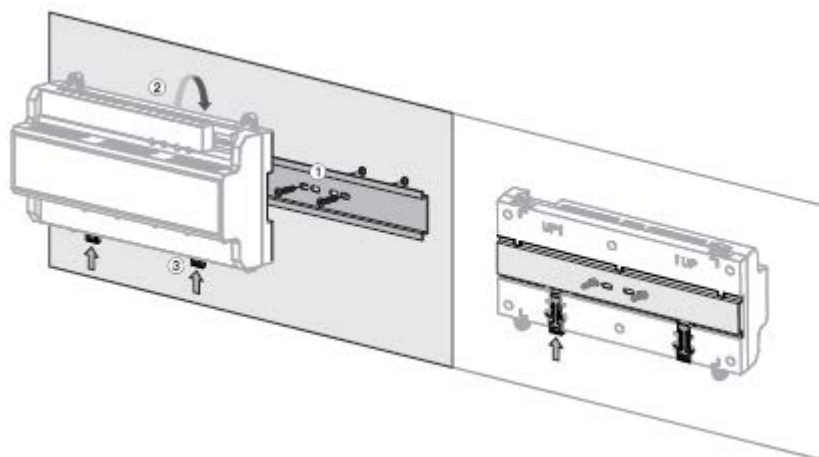
Figure 2-2



Modo 2

El diagrama de instalación se muestra en la Figura 2-3.

Figure 2-3



Step 1 Fije el riel guía en forma de U a la pared con tornillos.

Step 2 Abrache la parte trasera superior del dispositivo en la ranura superior del riel guía en forma de U. Empuje

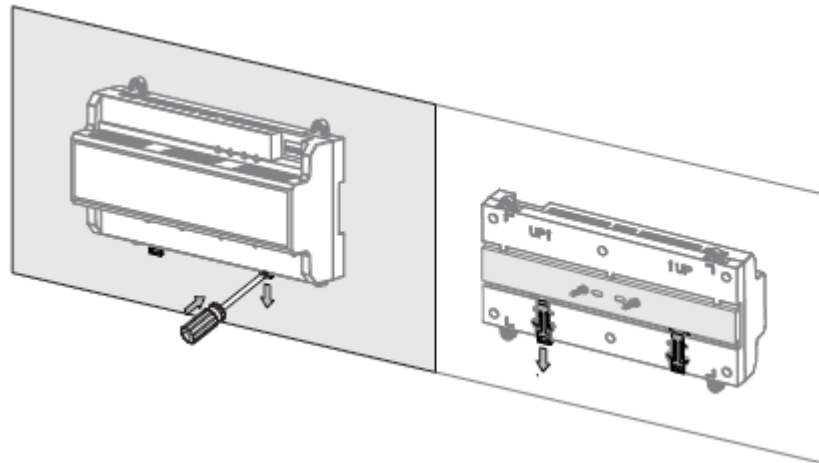
Step 3 la unión a presión en la parte inferior del dispositivo hacia arriba. La instalación se completa cuando escucha el sonido de ajuste.

2.3 Desmontaje

Si el dispositivo está instalado con el modo 2, desmóntelo de acuerdo con la Figura 2-4.

Alinee un destornillador con la junta a presión, presiónelo hacia abajo y la junta a presión se levantará, de modo que todo el dispositivo se pueda desarmar sin problemas.

Figure 2-4

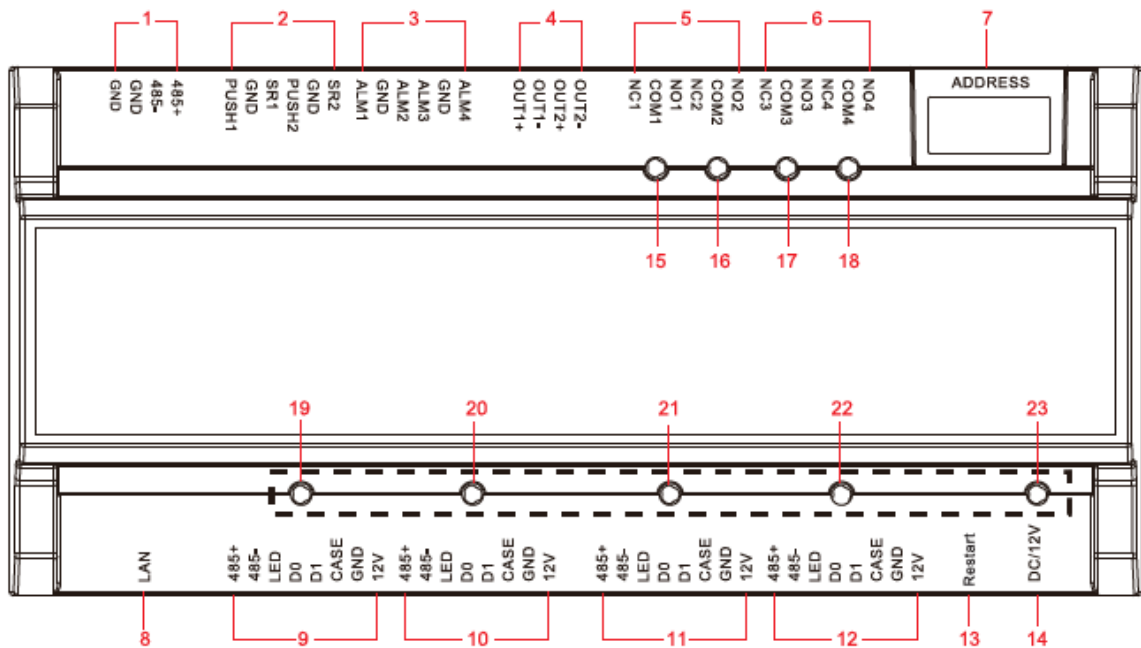


2.4 Diagrama de cableado

2.4.1 Descripción del cableado del controlador de acceso

Este dispositivo admite entrada o salida bidireccional de dos puertas. En caso de entrada de alarma, active el dispositivo de salida de alarma externa para dar una alarma. El diagrama de cableado del dispositivo se muestra en la Figura 2-5.

Figure 2-5



Las interfaces se describen en la Tabla 2-1.

Tabla 2-1

No.	Descripción del puerto	No.	Descripción del puerto
1	Comunicación RS485	8	TCP/IP, puerto de plataforma de software
2	Pulsador de salida y contacto de puerta	9	Lector entrada puerta 1
3	Entrada de alarma externa	10	Lector de salida de la puerta 1
4	Salida de alarma externa	11	Lector entrada puerta 2
5	Salida de potencia de bloqueo	12	Lector de salida de la puerta 2
6	Salida de alarma interna	13	Reiniciar

No.	Descripción del puerto	No.	Descripción del puerto
7	Dip switch	14	Puerto de alimentación de 12 V CC

Las luces indicadoras se describen en la Tabla 2-2.

Tabla 2-2

No.	Descripción
15	Indicador de estado de bloqueo
dieciséis	
17	Indicador de estado de alarma
18	
19	Indicador de detección de lector de entrada de la puerta 1
20	Indicador de detección de lector de salida de la puerta 1
21	Indicador de detección de lector de entrada de puerta 2
22	Indicador de detección de lector de salida de la puerta 2
23	Indicador de encendido

2.4.2 Descripción del cableado del botón de salida/contacto de puerta

Los terminales de cableado correspondientes del botón de salida y el contacto de la puerta se muestran en la Figura 2-6. Consulte la Tabla 2-3 para ver las descripciones de los terminales de cableado.

Figure 2-6

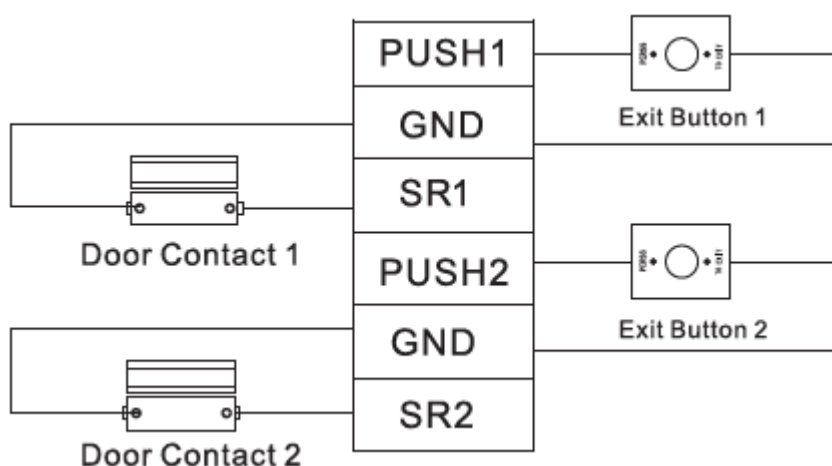


Tabla 2-3

Puerto	Terminal de cableado	Descripción
Botón de salida + puerta contacto	EMPUJAR1	Botón de salida de la puerta 1
	TIERRA	Compartido por el botón de salida de la puerta 1 y la entrada de contacto de puerta de la puerta 1
	SR1	Entrada de contacto de puerta de la puerta 1
	PUSH2	Botón de salida de la puerta 2
	TIERRA	Compartido por el botón de salida de la puerta 2 y la entrada de contacto de puerta de la puerta 2
	SR2	Entrada de contacto de puerta de la puerta 2

2.4.3 Descripción del cableado de la cerradura

Admite 4 grupos de salidas de control de bloqueo; los números de serie después de los terminales representan las puertas correspondientes. Elija un modo de conexión adecuado según el tipo de bloqueo, como se muestra en la Figura 2-7, la Figura 2-8 y la Figura 2-9. Consulte la Tabla 2-4 para ver las descripciones de los terminales de cableado.

Figure 2-7

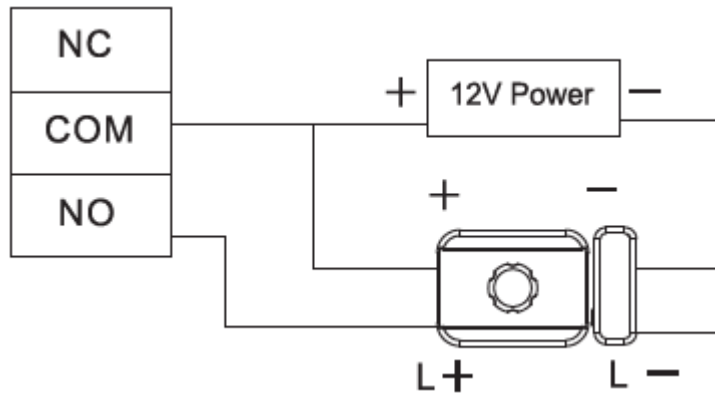


Figure 2-8

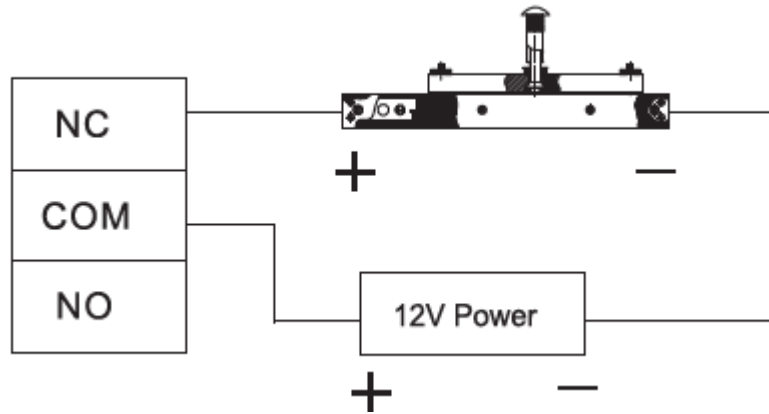


Figure 2-9

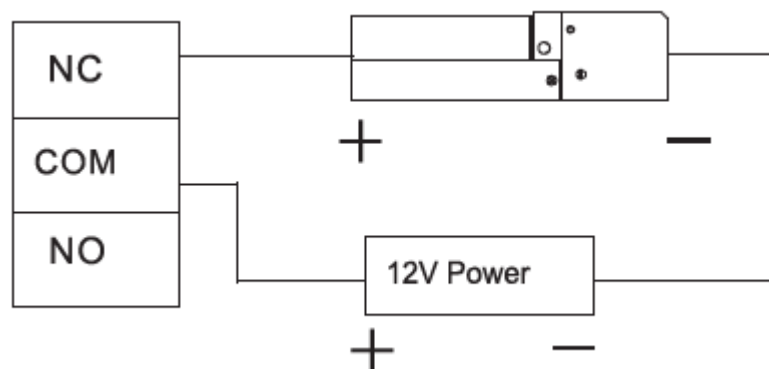


Tabla 2-4

Puerto	Terminal de cableado	Descripción
Salida de control de bloqueo Puerto	NC1	Control de bloqueo de la puerta 1
	COM1	
	NO1	
	NC2	Control de bloqueo de la puerta 2
	COM2	

Puerto	Terminal de cableado	Descripción
	NO2	

2.4.4 Descripción del cableado del lector



NOTE

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

Consulte la Tabla 2-5 para ver las descripciones de los terminales de cableado correspondientes a los lectores. Tome la puerta 1 por ejemplo; otros lectores son iguales. Consulte la Tabla 2-6 para ver las descripciones de las especificaciones y la longitud del cable del lector.

Tabla 2-5

Puerto	Terminal de cableado	Color de cable	Descripción
Lector de entrada de puerta 1	485+	Púrpura	485 lector
	485-	Amarillo	
	LED	marrón	Lector Wiegand
	D0	Verde	
	D1	blanco	
	CASO	Azul	
	TIERRA	Negro	Fuente de alimentación del lector
12V	rojo		

Tabla 2-6

Tipo de lector	Modo de conexión	Longitud
485 Lector	Cable de red CAT5e, conexión 485	100m
Lector Wiegand	Cable de red CAT5e, conexión Wiegand	100m

2.4.5 Descripción del cableado de la entrada de alarma externa

La conexión de entrada de alarma externa de 4 canales se muestra en la Figura 2-10. Consulte la Tabla 2-7 para ver las descripciones de los terminales de cableado.

Figure 2-10

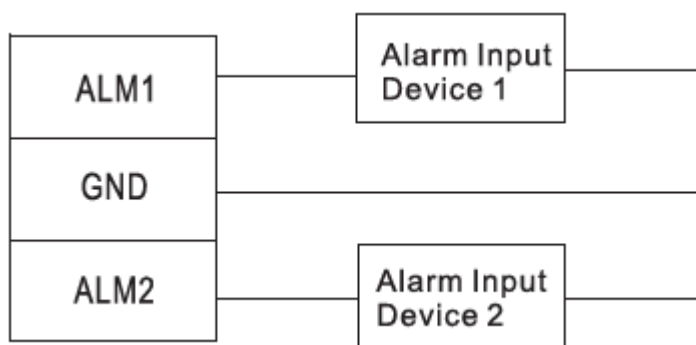


Tabla 2-7

Puerto	Terminal de cableado	Descripción
Externo alarma aporte	ALM1	Puerto de entrada de alarma 1
	TIERRA	Compartido por el puerto de entrada de alarma 1 y 2
	ALM2	Puerto de entrada de alarma 2
		Los puertos de entrada de alarma externa pueden conectar un detector de humo y un detector de infrarrojos, etc.

Puerto	Terminal de cableado		Descripción
	ALM3	Puerto de entrada de alarma 3	<p> NOTE</p> <p>La alarma externa puede vincular la puerta Estado abierto y cerrado.</p> <p>- ALARMA1 ~ ALARMA2 la alarma externa conecta todas las puertas estar normalmente abierto.</p> <p>- ALARMA3 ~ ALARMA4 la alarma externa vincula todas las puertas para que estén normalmente cerradas.</p>
	TIERRA	Compartido por los puertos de entrada de alarma 3 y 4	
	ALM4	Puerto de entrada de alarma 4	

2.4.6 Descripción del cableado de la salida de alarma externa

Después de que la salida de alarma externa de 2 canales active una alarma, el dispositivo de salida de alarma emite una alarma durante 15 s.

Hay dos modos de conexión de salida de alarma externa, dependiendo del dispositivo de alarma. Por ejemplo, IPC puede usar el Modo 1, mientras que la sirena audible y visual puede usar el Modo 2, como se muestra en la Figura 2-11 y la Figura 2-12. Consulte la Tabla 2-8 para obtener descripciones sobre los terminales de cableado.

Figure 2-11

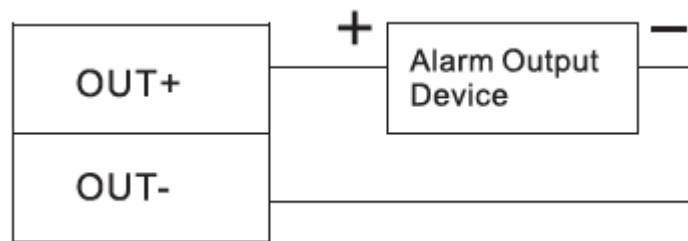


Figure 2-12

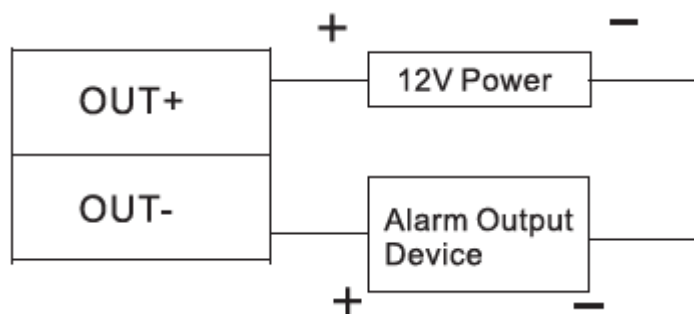


Tabla 2-8

Puerto	Terminal de cableado		Descripción
Alarma externa producción	SALIDA1+	ALM1/ALM2 activa la salida de alarma.	Salida de alarma externa Los puertos son capaces de conectar audio y sirenas visuales.
	SALIDA1-		
	SALIDA2+	ALM3/ALM4 activa la salida de alarma.	
	SALIDA2-		

2.4.7 Descripción del cableado de la salida de alarma interna

Con salida de alarma interna de 2 canales, después de que la entrada de alarma interna (como el tiempo de espera de la puerta) activa una alarma, el dispositivo de salida de alarma emite una alarma durante 15 s.

Durante la conexión del dispositivo de salida de alarma, seleccione NC/NO según el estado normalmente cerrado o normalmente abierto.

- NC representa el estado normalmente cerrado. NO
- representa el estado normalmente abierto.

Hay dos modos de conexión de salida de alarma interna, dependiendo del dispositivo de alarma. Por ejemplo, IPC puede usar el Modo 1, mientras que la sirena audible y visual puede usar el Modo 2, como se muestra en la Figura 2-13 y la Figura 2-14. Consulte la Tabla 2-9 para obtener descripciones sobre los terminales de cableado.

Figure 2-13

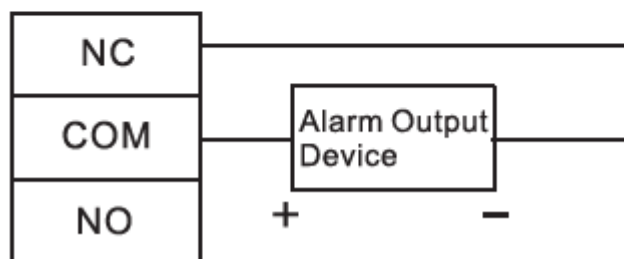
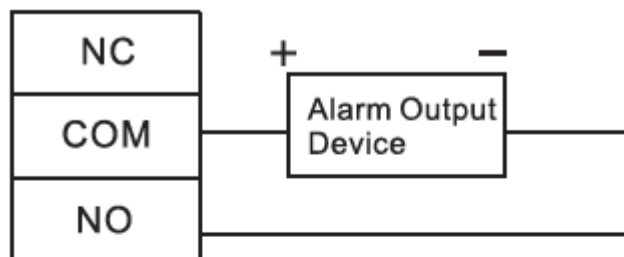


Figure 2-14

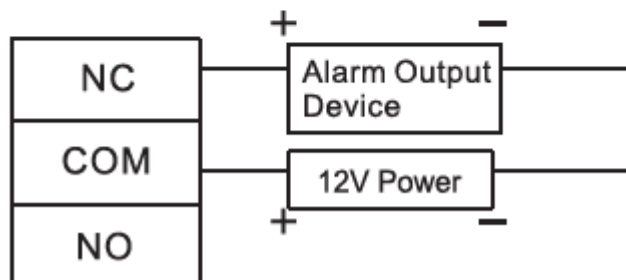
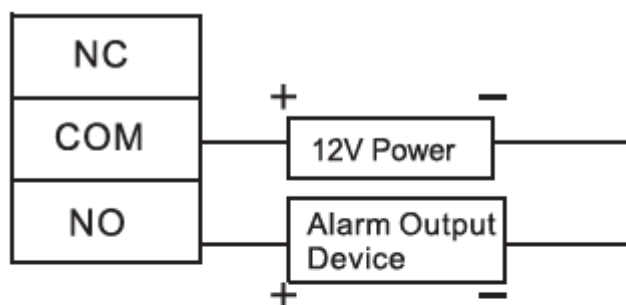


Tabla 2-9

Puerto	Terminal de cableado		Descripción
Alarma interna producción	NC3	● Salida de alarma de sabotaje del lector de entrada y salida de la puerta 1 Salida de alarma de tiempo de espera e intrusión de la puerta 1	Salida de alarma interna Los puertos son capaces de conectar audio y sirenas visuales.
	COM3		
	NUMERO 3		
	NC4	● Salida de alarma de sabotaje del lector de entrada y salida de la puerta 2 Salida de alarma de tiempo de espera e intrusión de la puerta 2	
	COM4		
NO. 4			

2.4.8 Descripción de la regla de entrada y salida de alarma

En caso de evento de alarma, el controlador de acceso puede controlar el acceso y el estado de la alarma externa.

Consulte la Tabla 2-10 para conocer las reglas detalladas de entrada y salida de alarma.

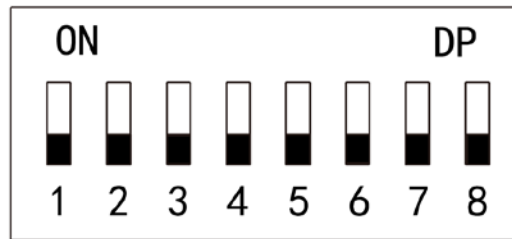
Tabla 2-10



Alarma Escribe	Evento de alarma	Señal de alarma Puerto de entrada	Señal de alarma Puerto de salida	Estado de alarma
Externo alarma aporte	gatillo no. 1 detector de alarma	ALM1	SALIDA1	La alarma n.º 1 emite una alarma y vincula todas las puertas para que estén normalmente abiertas.
	gatillo no. 2 detectores de alarma	ALM2		
	gatillo no. 3 detectores de alarma	ALM3	SALIDA2	La alarma n.º 2 emite una alarma y vincula todas las puertas para que estén normalmente cerradas.
	gatillo no. 4 detectores de alarma	ALM4		
Interno alarma aporte	alarma de intrusión o alarma de tiempo de espera de desbloqueo de no. 1 puerta	SR1	SALIDA1	La alarma n.º 1 da una alarma.
	alarma de intrusión o alarma de tiempo de espera de desbloqueo de no. 2 puertas	SR2	SALIDA2	La alarma n.º 2 da una alarma.
	Alarma de sabotaje de no. 1 lector de puerta	RS-485/CAJA	SALIDA1	La alarma n.º 1 da una alarma.
	Alarma de sabotaje de no. lector de 2 puertas	RS-485/CAJA	SALIDA2	La alarma n.º 2 da una alarma.

2.5 Dip switch

Operar con interruptor DIP.

Figure 2-15



-  el interruptor está en la posición ON, lo que significa 1.
-  el interruptor está en la parte inferior, lo que significa 0.
- 1~8 son todos 0; el sistema se inicia normalmente.
- 1~8 son todos 1; el sistema ingresa al modo BOOT después del inicio.
- 1, 3, 5 y 7 son 1, mientras que los demás son 0. Después de reiniciar, el sistema restaura los valores predeterminados de fábrica.
- 2, 4, 6 y 8 son 1, mientras que los demás son 0. Después de reiniciar, el sistema restaura los valores predeterminados de fábrica, pero se conserva la información del usuario.

2.6 Reiniciar

Inserte una aguja en el orificio de reinicio, presiónela una vez para reiniciar el dispositivo.

 **NOTE**

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

3

Configuración de PSS inteligente

El controlador de acceso se gestiona con el cliente Smart PSS, para realizar el control y la configuración correcta de una puerta y grupos de puertas.


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

NOTE

El cliente Smart PSS ofrece diferentes puertos para diferentes versiones. Consulte el puerto real.

3.1 Cliente de inicio de sesión



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

3.2 Agregar controlador de acceso

Agregar controlador de acceso en Smart PSS; seleccione "Búsqueda automática" y "Agregar".

3.2.1 Búsqueda automática

Los dispositivos deben estar en el mismo segmento de red.

Step 1 En la interfaz de "Dispositivos", haga clic en "Búsqueda automática", como se muestra en la Figura 3-1. El sistema muestra la interfaz de "Búsqueda automática", como se muestra en la Figura 3-2.

Figure 3-1

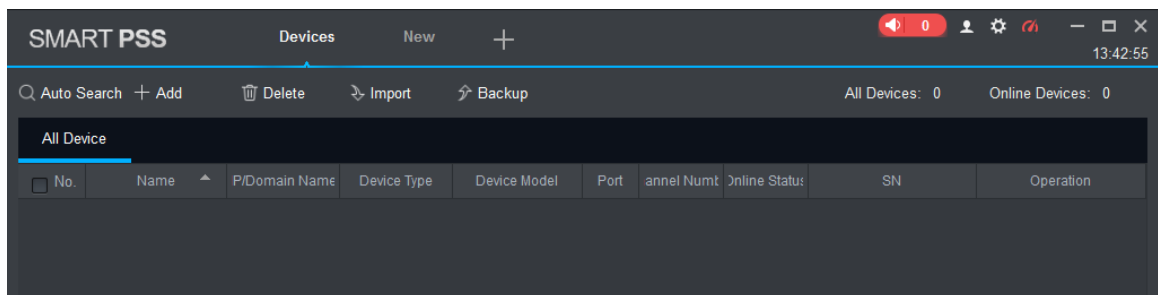
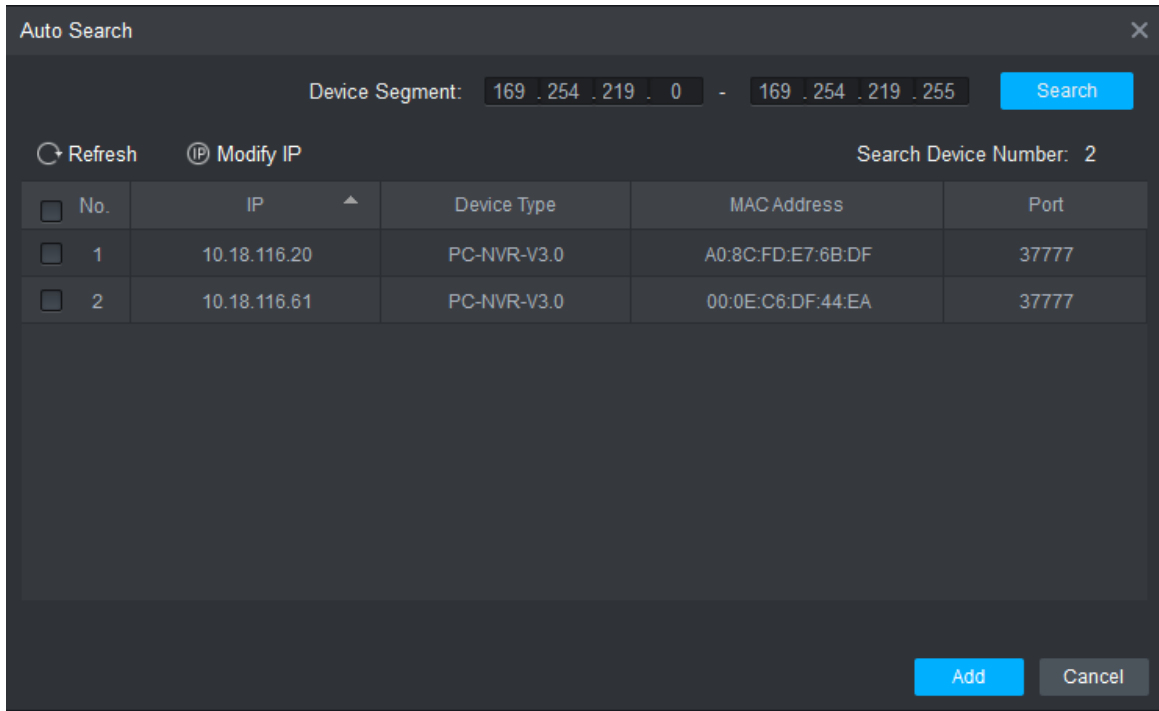


Figure 3-2



Step 2 Introduzca el segmento del dispositivo y haga clic en "Buscar".

El sistema muestra los resultados de la búsqueda.



NOTE

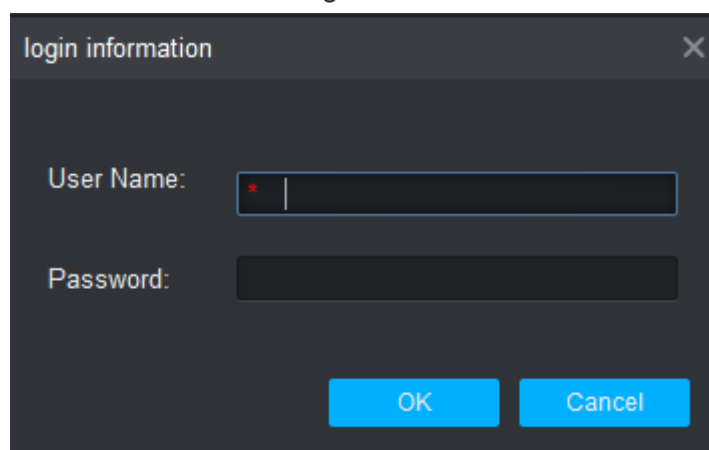
- Haga clic en "Actualizar" para actualizar la información del dispositivo.
- Seleccione un dispositivo, haga clic en "Modificar IP" para modificar la dirección IP del dispositivo. para específicos operaciones, consulte el Manual del usuario de Smart PSS Client.

Step 3 Seleccione el dispositivo que debe agregarse y haga clic en "Agregar". El sistema muestra "Prompt".

Step 4 Haga clic en Aceptar".

El sistema muestra el cuadro de diálogo "Información de inicio de sesión", como se muestra en la Figura 3-3.

Figure 3-3



Step 5 Ingrese "Nombre de usuario" y "Contraseña" para iniciar sesión en el dispositivo y haga clic en "Aceptar". El sistema muestra la lista de dispositivos agregados, como se muestra en la Figura 3-4.

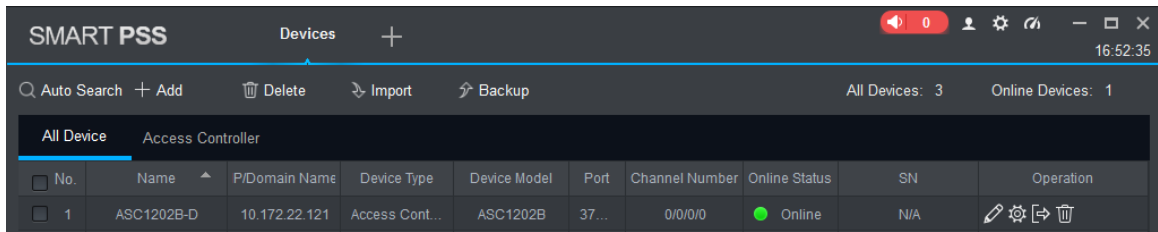


NOTE

- Después de completar la adición, el sistema permanece en la interfaz de "Búsqueda automática". Puede continuar agregando más dispositivos o hacer clic en "Cancelar" para salir de "Búsqueda automática" interfaz.

- Después de completar la adición, Smart PSS inicia sesión en el dispositivo automáticamente. En caso de inicio de sesión exitoso, el estado en línea muestra "En línea". De lo contrario, muestra "Fuera de línea".

Figure 3-4



3.2.2 Adición manual

Para agregar dispositivos, primero se debe conocer la dirección IP del dispositivo o el nombre de dominio.

Step 1 En la interfaz de "Dispositivos", haga clic en "Agregar", como se muestra en la Figura 3-5.

El sistema muestra la interfaz "Adición manual", como se muestra en la Figura 3-6.

Figure 3-5

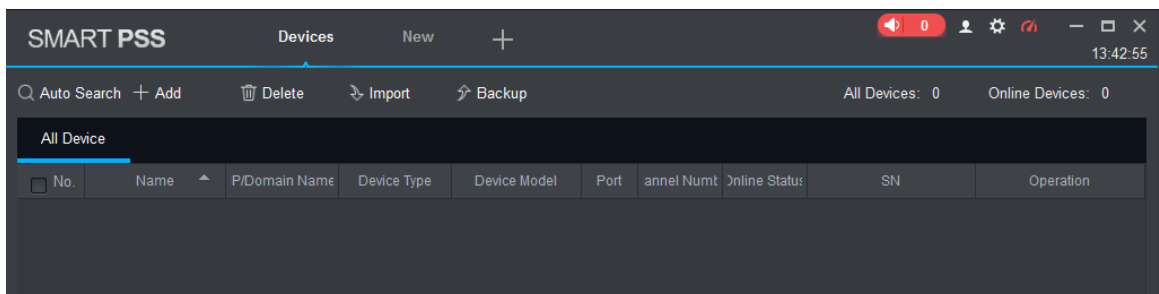


Figure 3-6

Manual Add ✕

Device Name:

Method to add: IP/Domain ▼

IP/Domain Name:

Port:

Group Name: Default Group ▼

User Name:

Password:

Step 2 Establecer parámetros del dispositivo. Para obtener descripciones de parámetros específicos, consulte la Tabla 3-1.

Tabla 3-1

Parámetro	Descripción
Nombre del dispositivo	Se sugiere que el nombre del dispositivo sea nombrado por la zona de monitoreo, para facilitar el mantenimiento.
Método para agregar	Seleccione "IP/Nombre de Dominio" . Agregue dispositivos según la dirección IP del dispositivo o el nombre de dominio.
IP/Nombre de Dominio	Dirección IP o nombre de dominio del dispositivo.
Puerto	Número de puerto del dispositivo. El número de puerto predeterminado es 37777. Complételo de acuerdo con las condiciones reales.
Nombre del grupo	Seleccione el grupo del dispositivo.
Nombre de usuario y contraseña	Nombre de usuario y contraseña del dispositivo.

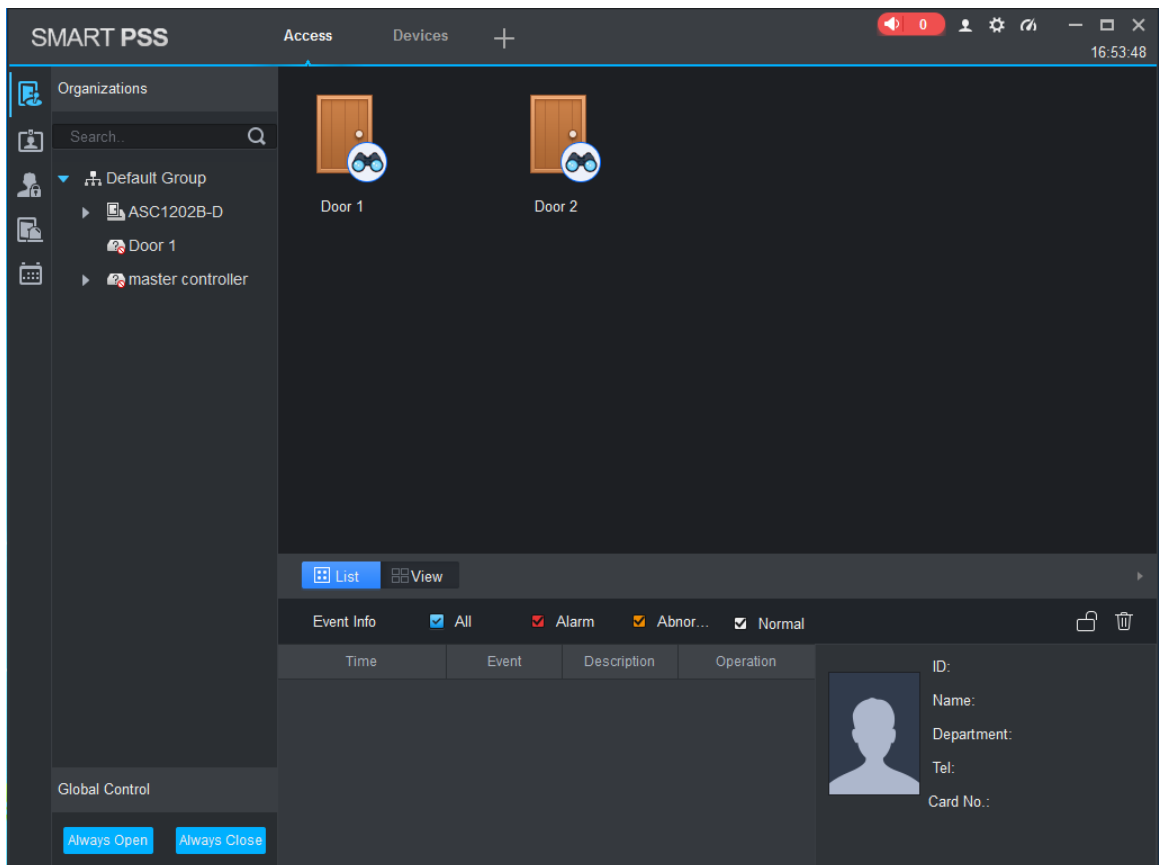
Step 3 Haga clic en "Agregar" para agregar un dispositivo.

El sistema muestra la lista de dispositivos agregados, como se muestra en la Figura 3-4. Las puertas del controlador agregado se muestran en la pestaña "Acceso", como se muestra en la Figura 3-7.

 **NOTE**

- Para agregar más dispositivos, haga clic en "Guardar y continuar", agregue dispositivos y quédese en "Manual Añadir" interfaz.
- Para cancelar la adición, haga clic en "Cancelar" y salga de la interfaz "Adición manual".
- Después de completar la adición, Smart PSS inicia sesión en el dispositivo automáticamente. En caso de inicio de sesión exitoso, el estado en línea muestra "En línea". De lo contrario, muestra "Fuera de línea".

Figure 3-7



Para problemas no incluidos a continuación, comuníquese con el personal de servicio al cliente local o consulte al personal de servicio al cliente de la sede. Estaremos siempre a su servicio.

1. Pregunta: Después de encender, el indicador de encendido no se enciende o el zumbador no responde.

Respuesta: Verifique si el enchufe de alimentación está insertado en su lugar. Por favor, sáquelo e insértelo de nuevo.

2. Pregunta: Después de conectar el lector con el dispositivo, la luz de pasar la tarjeta no se enciende y no responde después de pasar una tarjeta.

Respuesta: Verifique si el conector del lector está insertado en su lugar. Sáquelo e insértelo de nuevo; compruebe si la luz de contacto del lector se enciende.

3. Pregunta: El software del cliente no detecta el dispositivo.

Respuesta: compruebe si el conector TCP/IP está conectado correctamente y si la IP del dispositivo está en el mismo segmento de red.

4. Pregunta: Después de deslizar la tarjeta, indica que la tarjeta no es válida.

Respuesta: Verifique si este número de tarjeta se ha agregado en el controlador.

5. Pregunta: IP predeterminada del controlador de acceso.

Respuesta: La dirección IP predeterminada es 192.168.0.2.

6. Pregunta: Puerto predeterminado, nombre de usuario inicial y contraseña del controlador de acceso.

Respuesta: El puerto predeterminado es 37777, el nombre de usuario inicial es admin y la contraseña es 123456.

7. Pregunta: Actualización en línea del dispositivo.

Respuesta: conecte el dispositivo y la plataforma a través de la red y actualícelo en la plataforma.

8. Pregunta: Máx. distancia de cableado y distancia de transmisión del lector de tarjetas y el controlador.

Respuesta: Depende del tipo de cable de red y si necesita fuente de alimentación del relé de control.

Conectado con cable de red CAT5E, el valor típico es:

- RS485, 100m.
- Wiegand, 100m.