Acceso bidireccional de dos puertas Controlador

Manual de usuario

V1.0.1

Prefacio

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 información relacionada. contacto.

Sobre el Manual

- El Manual es solo para referencia. Si hay inconsistencia entre el Manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por las operaciones que no cumplan con el Manual.
- El Manual 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 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 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 el Manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio al cliente si ocurre algún problema al usar el 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 el manual antes de utilizarlo para evitar peligros y pérdidas materiales. Siga estrictamente el manual durante la aplicación y consérvelo correctamente después de leerlo.

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

1 Visión de conjunto

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 Dimensión externa

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

Figura 1-1

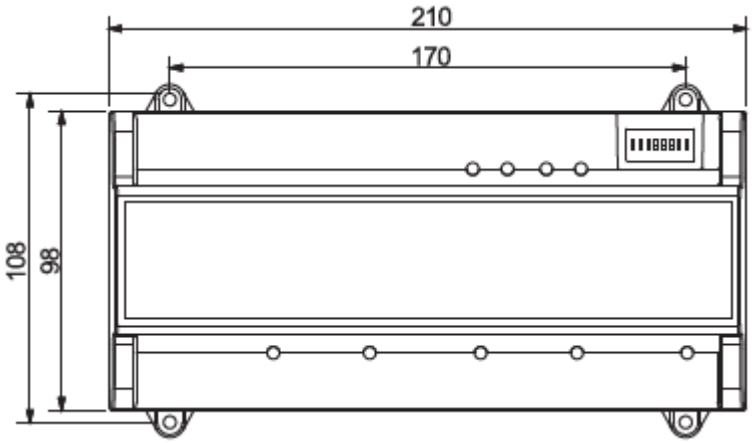
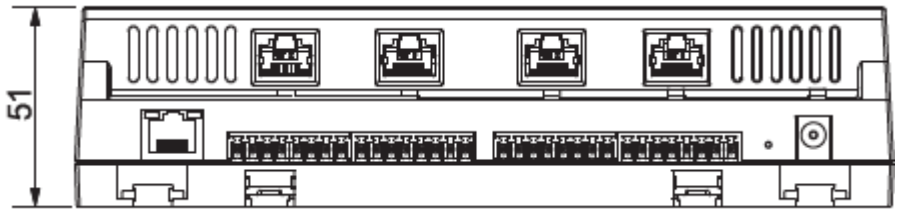


Figura 1-2

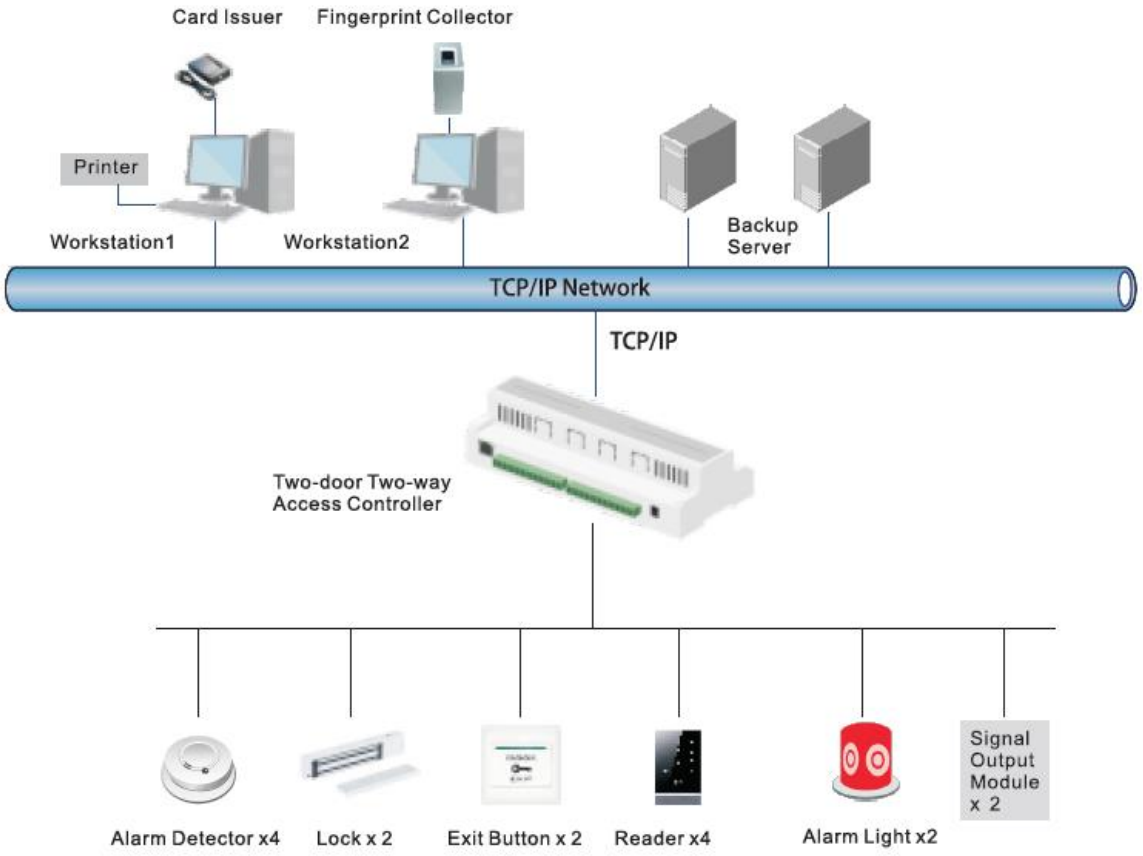


2 Guía de instalación

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.

Figura 2-1



2.2 Instalación del dispositivo

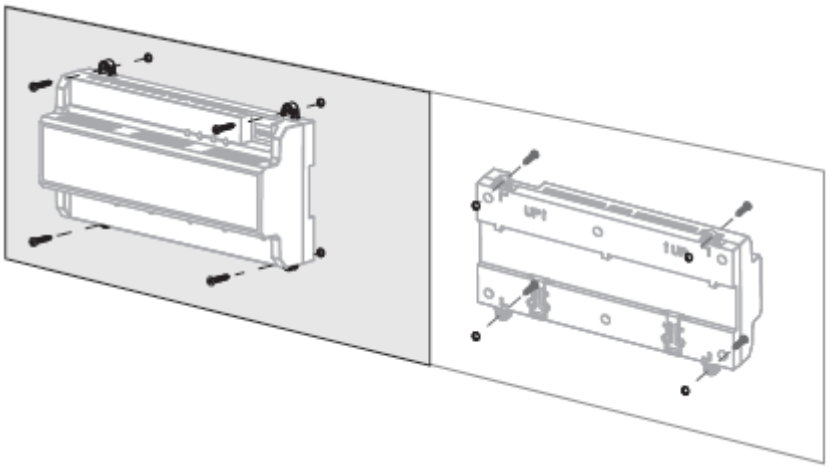
Hay dos modos de instalación.

- 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.

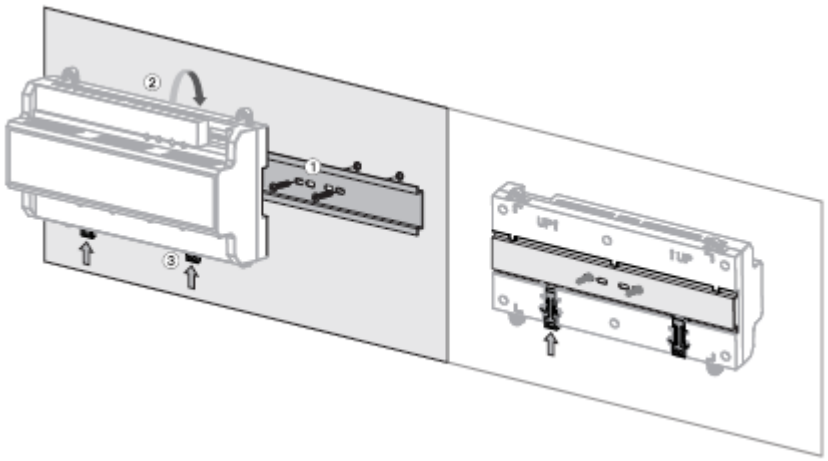
Figura 2-2



Modo 2

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

Figura 2-3



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

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

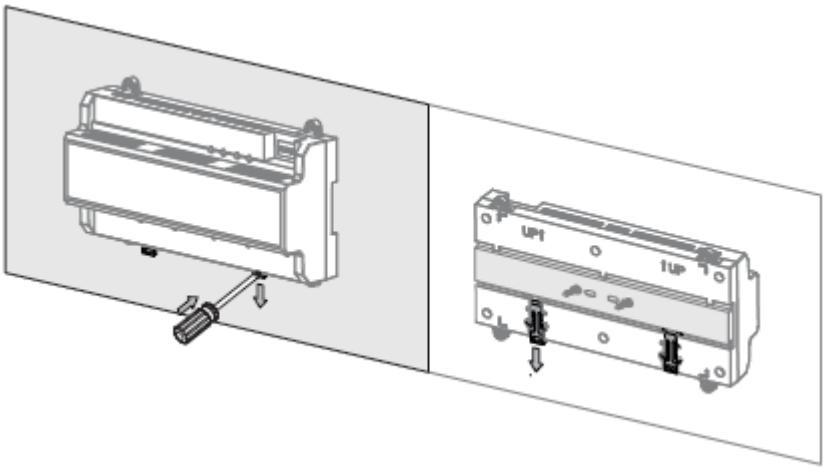
Paso 3 la unión a presión en la parte inferior del dispositivo hacia arriba. La instalación se completa cuando escucha el sonido de ajuste.

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.

Figura 2-4

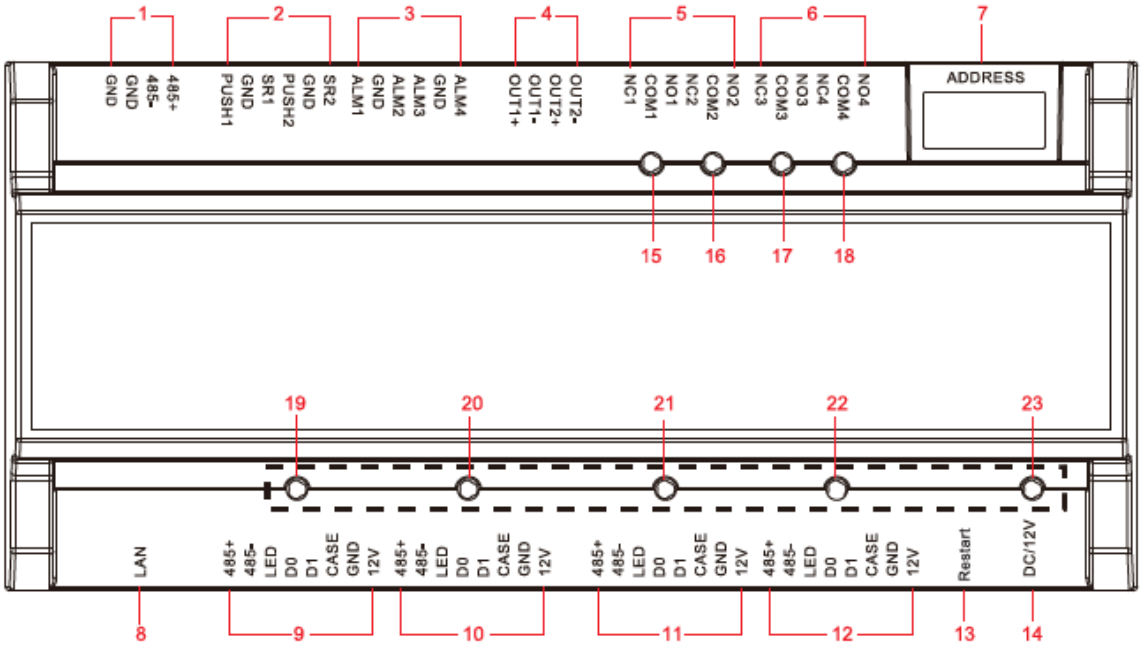


2.4 Diagrama de cableado

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 externo para dar una alarma. El diagrama de cableado del dispositivo se muestra en la Figura 2-5.

Figura 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 dieciséis	Indicador de estado de bloqueo
17 18	Indicador de estado de alarma
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.

Figura 2-6

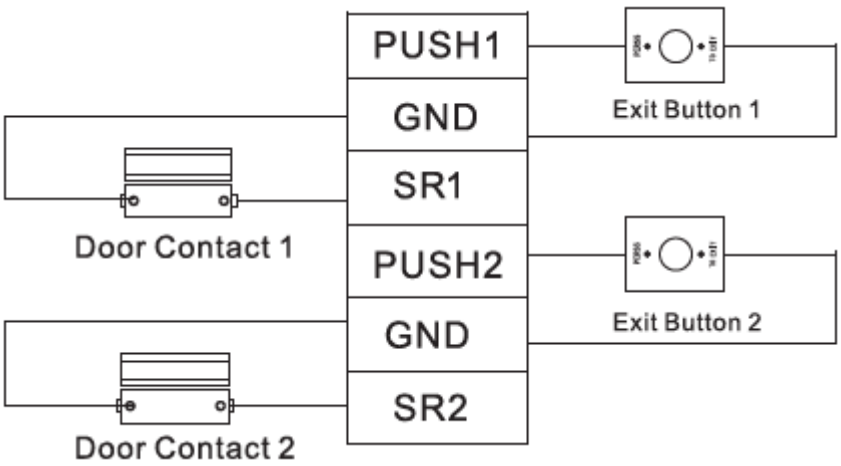


Tabla 2-3

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.

Figura 2-7

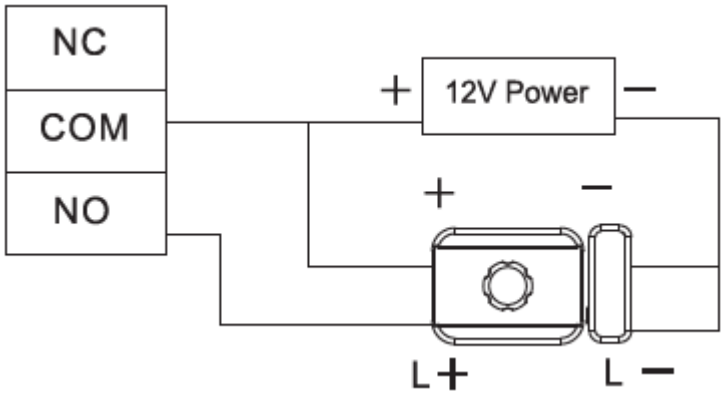


Figura 2-8

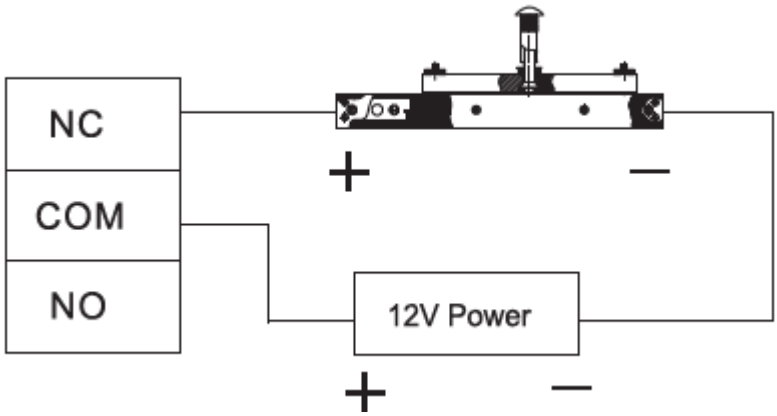


Figura 2-9

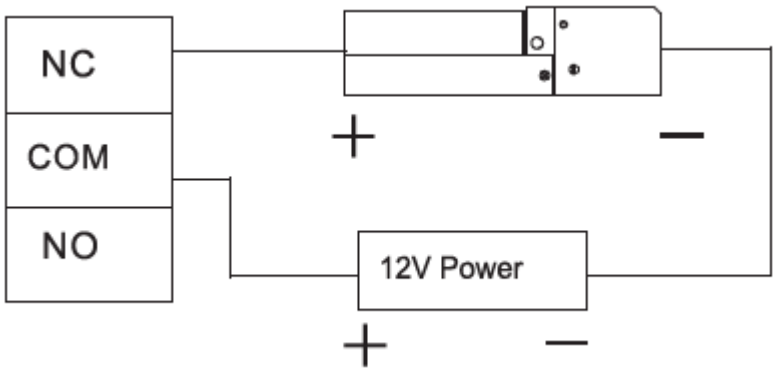


Tabla 2-4

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.

Figura 2-10

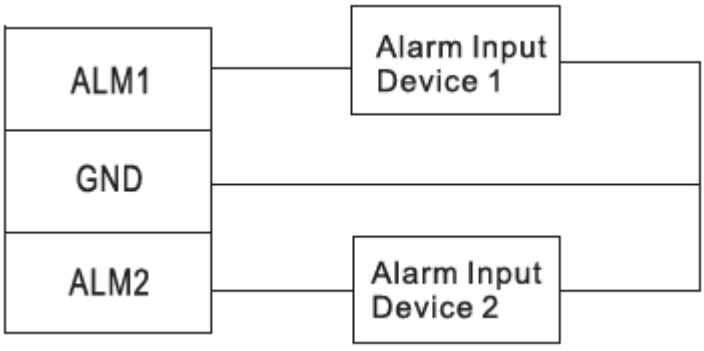


Tabla 2-7

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

Puerto	Terminal de cableado		Descripción
	ALM2	Puerto de entrada de alarma 2	NOTE La alarma externa puede vincular la puerta Estado abierto y cerrado. - ALARMA1 ~ ALARMA2 la alarma externa vincula todas las puertas para que estén normalmente abiertas. - ALARMA3 ~ ALARMA4 la alarma externa vincula todas las puertas para que estén normalmente cerradas.
	ALM3	Puerto de entrada de alarma 3	
	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

Con salida de alarma externa de 2 canales, después de que se activa 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.

Figura 2-11

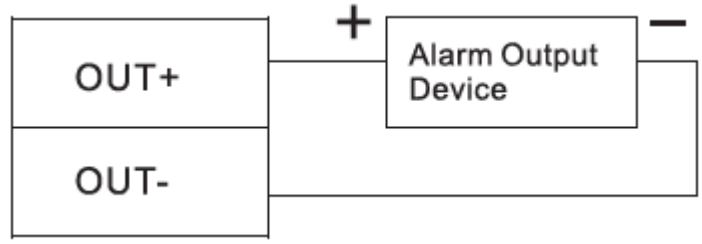


Figura 2-12

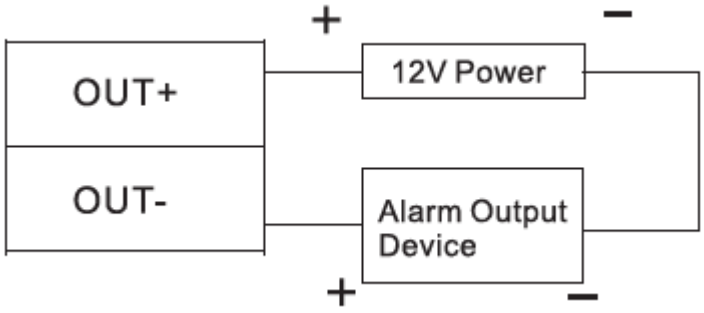


Tabla 2-8

Puerto	Terminal de cableado		Descripción
Externo salida de alarma	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.

Figura 2-13

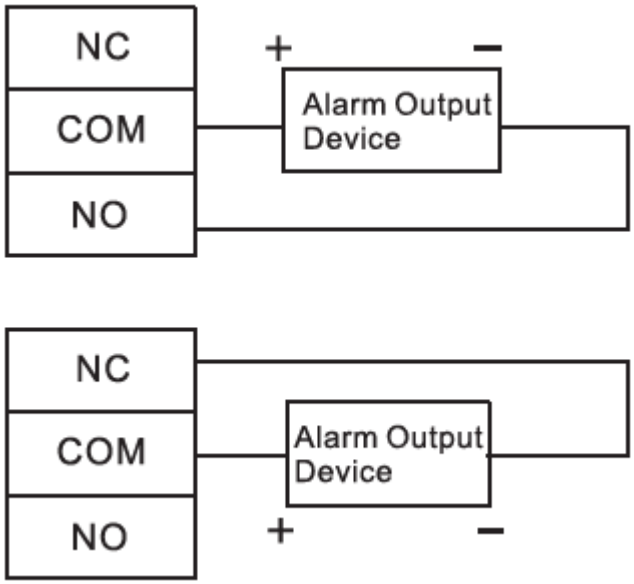


Figura 2-14

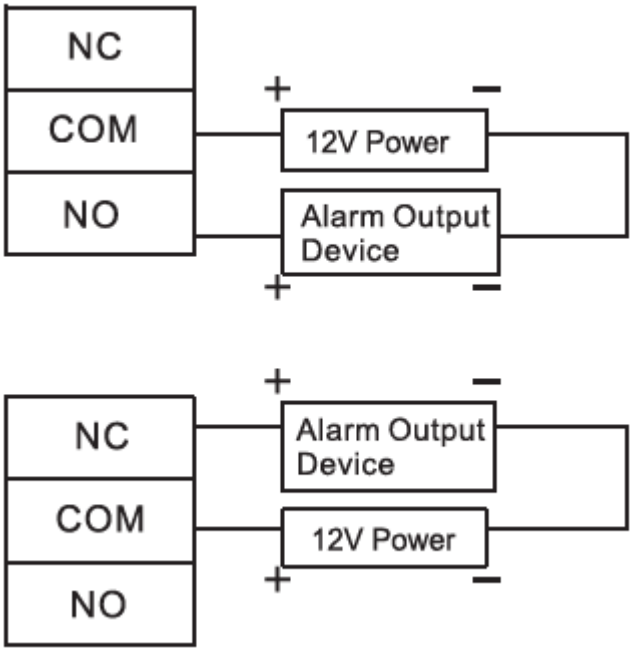


Tabla 2-9

Puerto	Terminal de cableado		Descripción
Interno salida de alarma	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	Alarma interna Los puertos de salida son capaz de conectar audible y visual sirenas
	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, la alarma continúa durante 15 s. Consulte la Tabla 2-10 para conocer las reglas detalladas de entrada y salida de alarma.

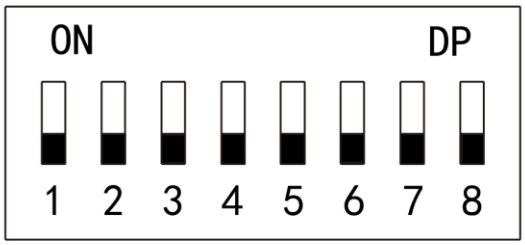
Tabla 2-10

Tipo de alarma	Entrada de señal de alarma Puerto	Señal de alarma Puerto de salida	Estado de alarma
Externo entrada de alarma	ALM1	SALIDA1	Vincule todas las puertas para que estén normalmente abiertas.
	ALM2		
	ALM3	SALIDA2	Enlace todas las puertas para que estén normalmente cerradas.
	ALM4		
Alarma interna aporte	SR1	SALIDA1	El tiempo de espera de la puerta y la alarma de intrusión activan una alarma externa para dar una alarma.
	SR2	SALIDA2	
	RS-485/CAJA	SALIDA1	La alarma de manipulación del lector activa una alarma externa para dar una alarma.
	RS-485/CAJA	SALIDA2	

2.5 Interruptor DIP

Operar con interruptor DIP.

Figura 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 correr. Llevar a cabo la inicialización 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.

Paso 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.

Figura 3-1

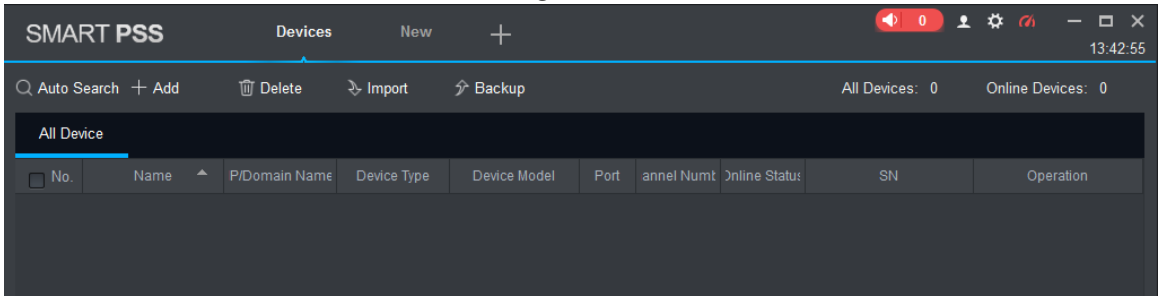
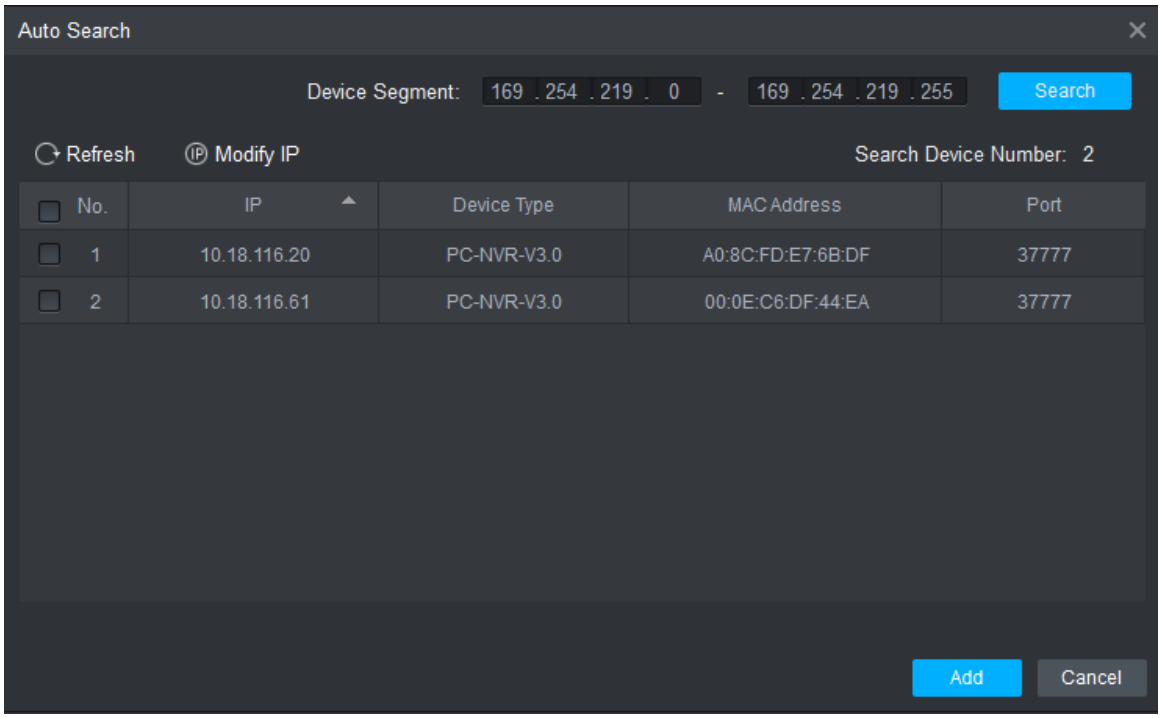


Figura 3-2



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

El sistema muestra los resultados de la búsqueda.

NOTE

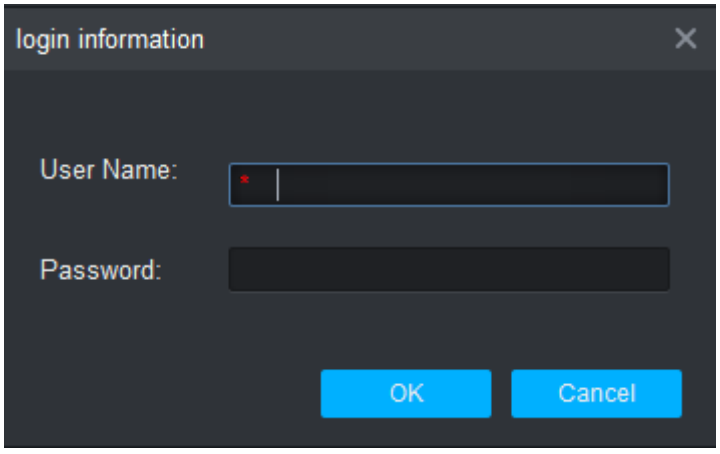
- Haga clic en "Actualizar" para actualizar la información del dispositivo.
- Seleccione un dispositivo, haga clic en "Modificar IP" para modificar la dirección IP del dispositivo. para específicos operaciones, consulte el Manual del usuario de Smart PSS Client.

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

Etapa 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.

Figura 3-3



Paso 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. Consulte la Tabla 3-1 para obtener más información.

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".

Figura 3-4

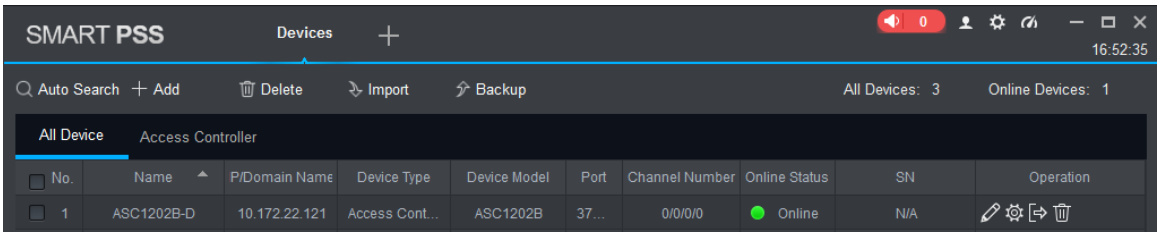


Tabla 3-1

Icono	Descripción
	Haga clic en este ícono para ingresar a la interfaz "Modificar dispositivo" y modificar la información del dispositivo, incluido el nombre del dispositivo, IP/nombre de dominio, puerto, nombre de usuario y contraseña. Alternativamente, haga doble clic en el dispositivo para ingresar a la interfaz "Modificar dispositivo".
	Haga clic en este ícono para ingresar a la interfaz de "Configuración del dispositivo" y configurar la cámara del dispositivo, la red, el evento, el almacenamiento y la información del sistema.
y	- Cuando el dispositivo está en línea, el ícono es . Haga clic en este icono para salir iniciar sesión, y este icono se convierte en . - Cuando el dispositivo está fuera de línea, el ícono es . Haga clic en este icono para iniciar sesión (con la información correcta del dispositivo), y este icono se convierte en .
	Haga clic en este icono para eliminar el dispositivo.

3.2.2 Adición manual

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

Paso 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.

Figura 3-5

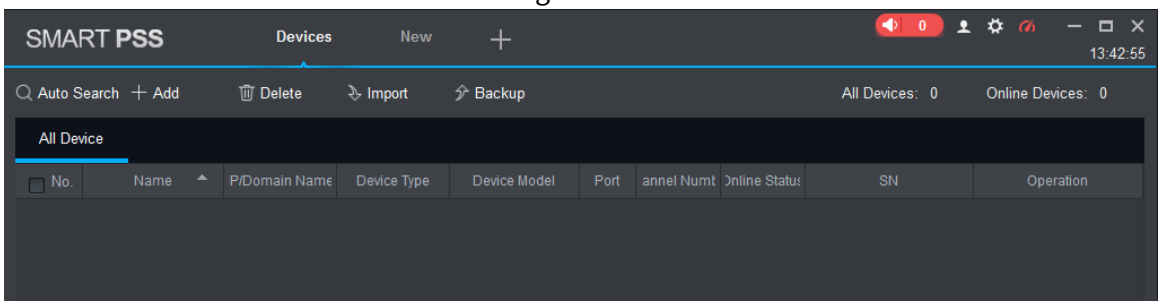
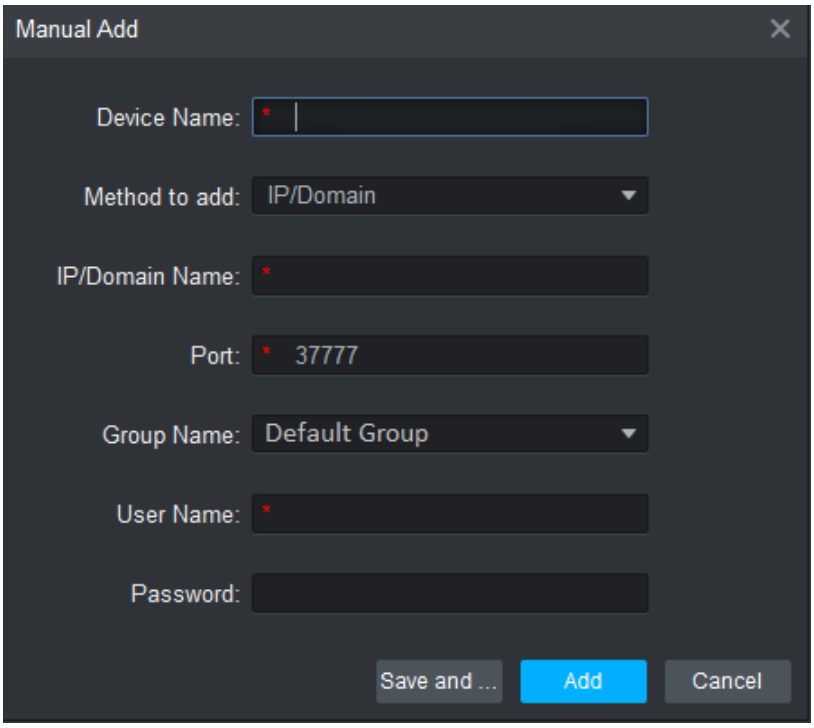


Figura 3-6



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

Tabla 3-2

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.

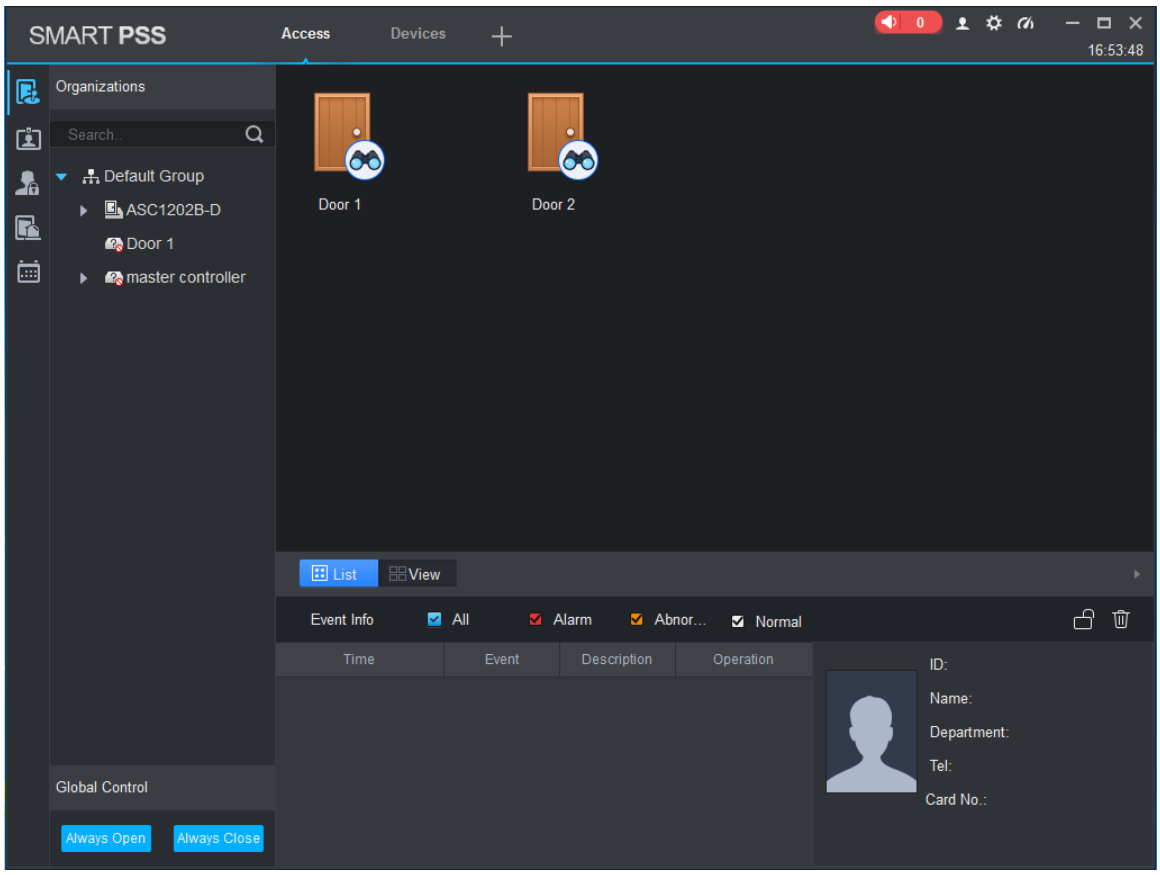
Paso 3 Haga clic en "Agregar" para agregar un dispositivo.

El sistema muestra la lista de dispositivos agregados, como se muestra en la Figura 3-4. Consulte la Tabla 3-1 para obtener más detalles. 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".

Figura 3-7

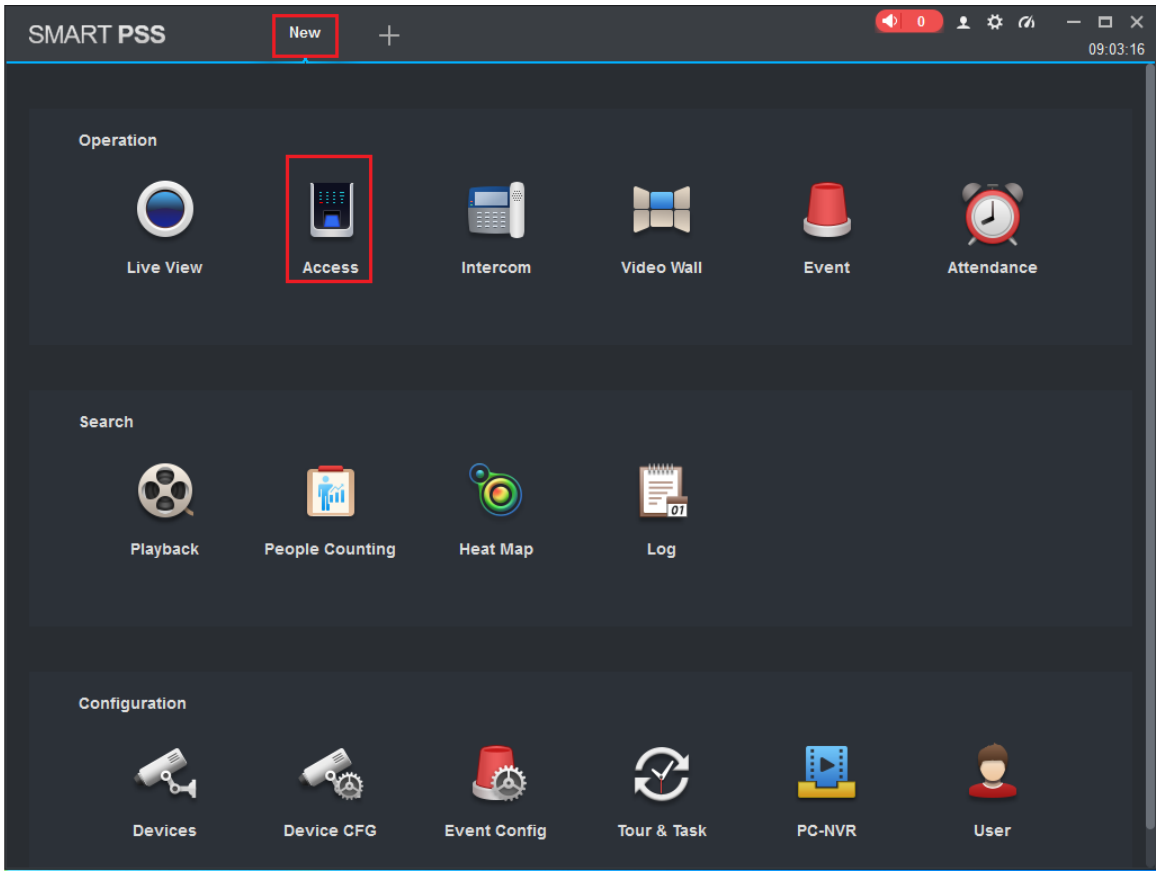


3.3 Agregar usuario

Agregue usuarios y enlace con tarjetas, para distribuir la autoridad.

En la interfaz "Nueva", haga clic en "Acceso" para ingresar a la interfaz "Acceso" y complete la configuración de acceso aquí.

Figura 3-8



3.3.1 Tipo de tarjeta

CAUTION

El tipo de tarjeta será el mismo que el emisor de la tarjeta; de lo contrario, no puede leer el número de tarjeta.

En la interfaz de "Acceso", haga  y luego haga clic  para configurar el tipo de tarjeta, como se muestra en la figura clic en 3-9 y en la Figura 3-10.

Figura 3-9

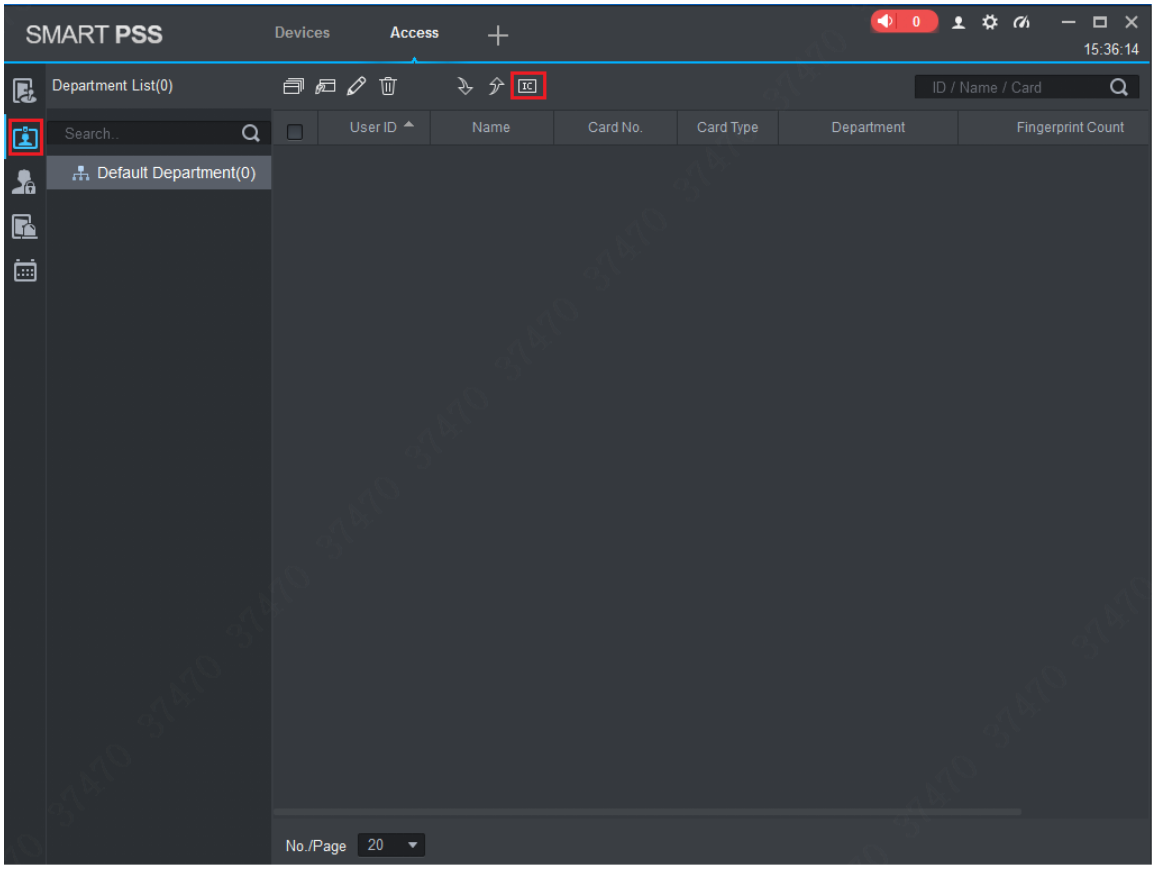
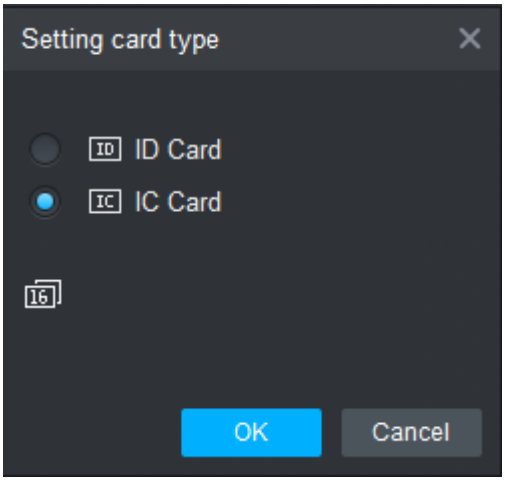


Figura 3-10



3.3.2 Adición única

Agregue un solo usuario, envíe una tarjeta e ingrese la información del usuario.

Paso 1 En la interfaz de "Acceso", haga clic en  y luego haga clic en  , como se muestra en la Figura 3-11.

El sistema muestra el cuadro de diálogo "Agregar usuario", como se muestra en la Figura 3-12.

Figura 3-11

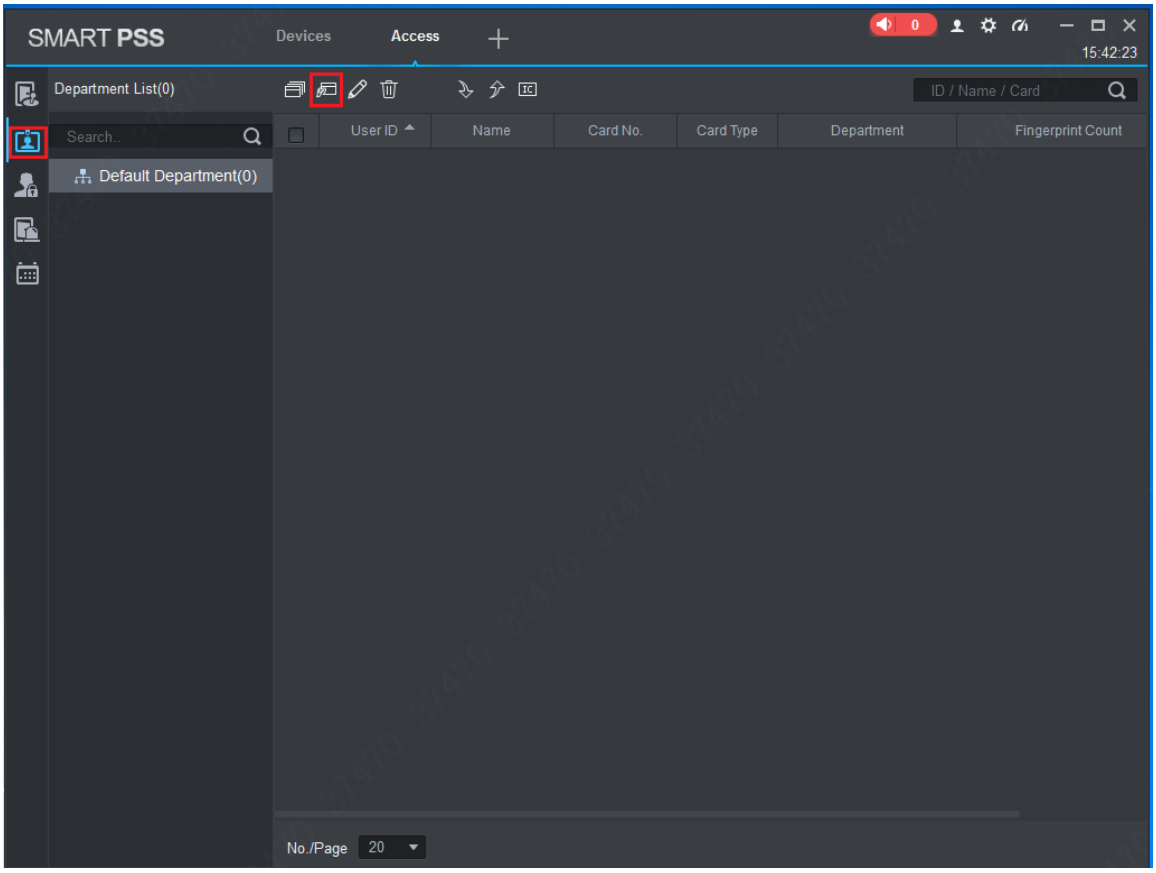
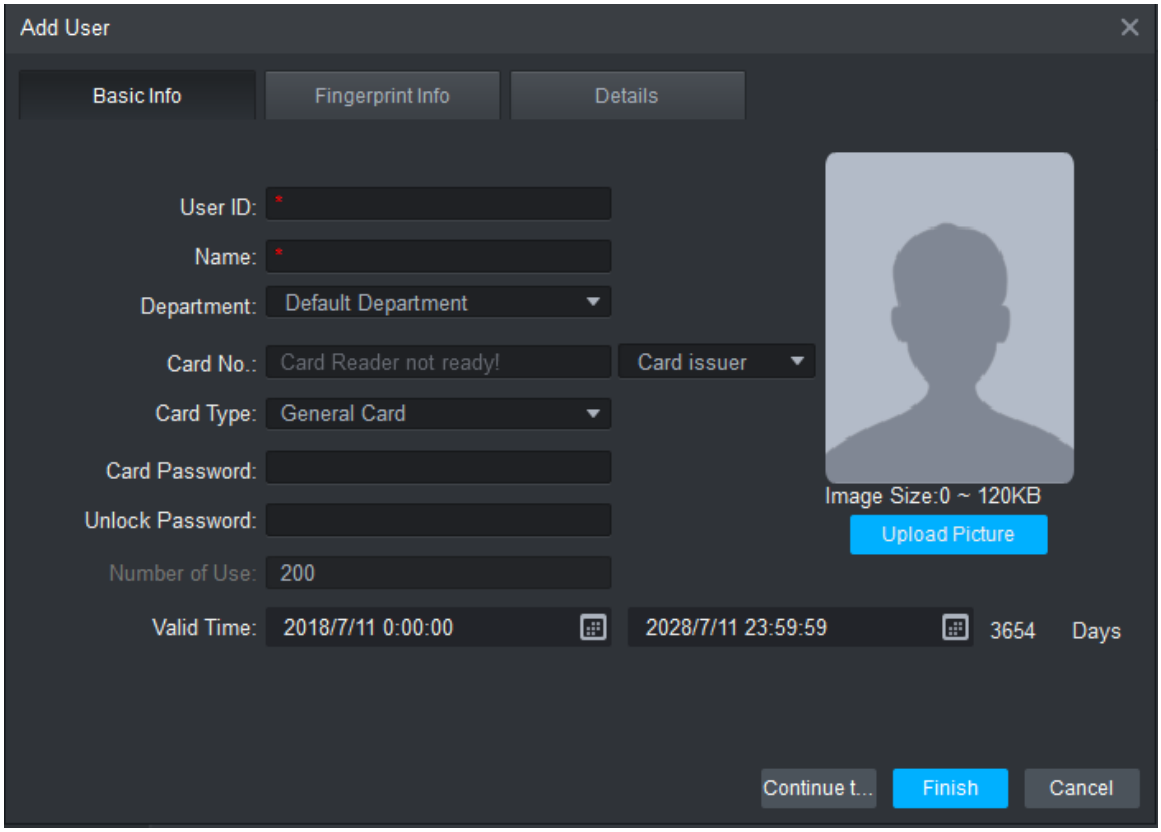


Figura 3-12



Paso 2 Agregue información de usuario manualmente, incluida información básica, información de huellas dactilares y detalles. Consulte la Tabla 3-3 para obtener más detalles.

Tabla 3-3

Parámetro	Descripción
Información básica	- ID de usuario (obligatorio). - Nombre (obligatorio). - Departamento (asociación de automóviles). - Número de tarjeta: entrada por lector de tarjetas o entrada manual. - Tipo de tarjeta: tarjeta general, tarjeta VIP, tarjeta de invitado, tarjeta de patrulla, tarjeta de lista negra y tarjeta de coacción. - Contraseña Tarjeta: se utiliza para abrir la puerta con tarjeta + contraseña. - Contraseña de desbloqueo: se utiliza para abrir la puerta con contraseña. - Número de Uso: solo aplica para tarjeta de huésped. - Tiempo de validez: establece el tiempo de validez de la tarjeta, que es de 10 años por defecto. - Imagen: imagen de usuario, máx. 120K. NOTE Número de tarjeta y el ID de usuario no se puede repetir.
Información de huellas dactilares	Recoger huellas dactilares con lector de huellas dactilares y lector de acceso. - máx. 2 huellas dactilares para cada persona. - Soporte para ingresar el nombre de la huella digital.
Detalles	Complete la información detallada del usuario de acuerdo con los parámetros de la interfaz.

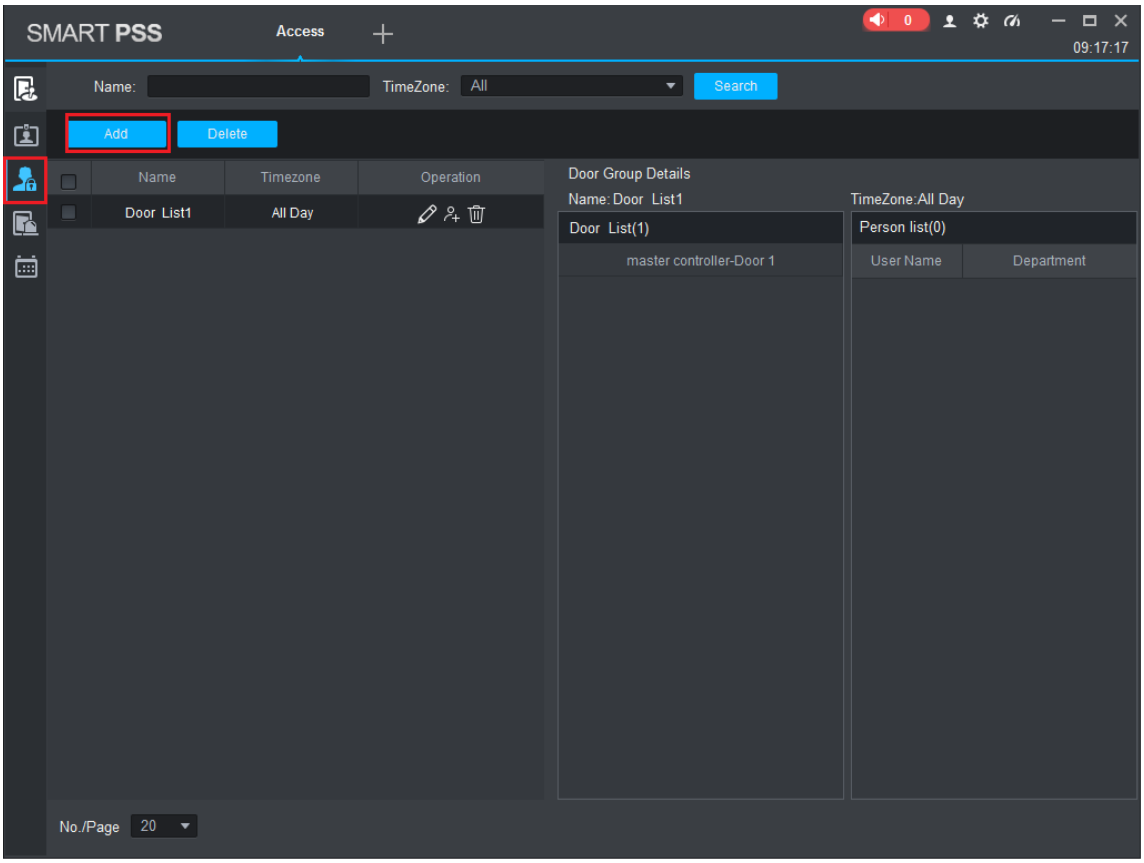
Paso 3 Haga clic en "Finalizar" para terminar de agregar los usuarios.

3.4 Agregar grupo de puertas

Divida las puertas en grupos y manéjelos juntos.

Paso 1 En la interfaz de "Acceso", haga clic  , y luego haga clic en "Nivel de acceso", como se muestra en la Figura en 3-13.

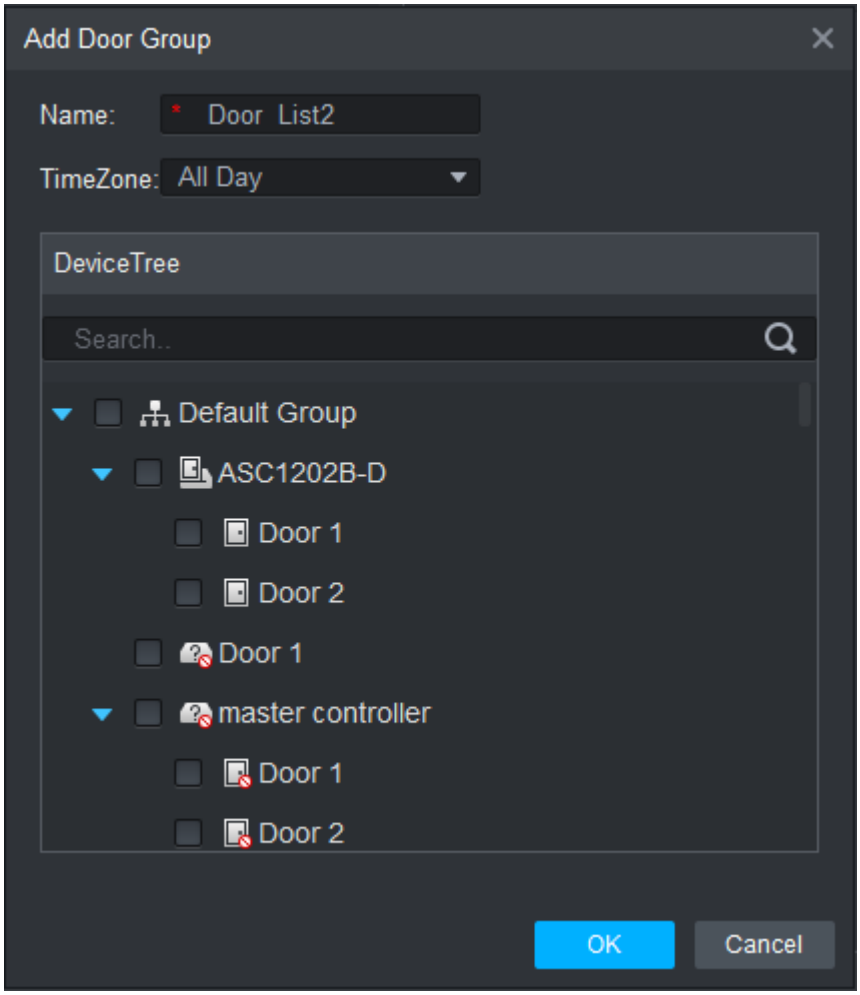
Figura 3-13



Paso 2 Haga clic en "Agregar".

El sistema muestra el cuadro de diálogo "Agregar grupo de puertas", como se muestra en la Figura 3-14.

Figura 3-14



Paso 3 Ingrese su nombre"; seleccione "Zona horaria" y puertas a gestionar. Haga clic en

Etapa 4 "Aceptar" para completar la adición.

3.5 Autorizar

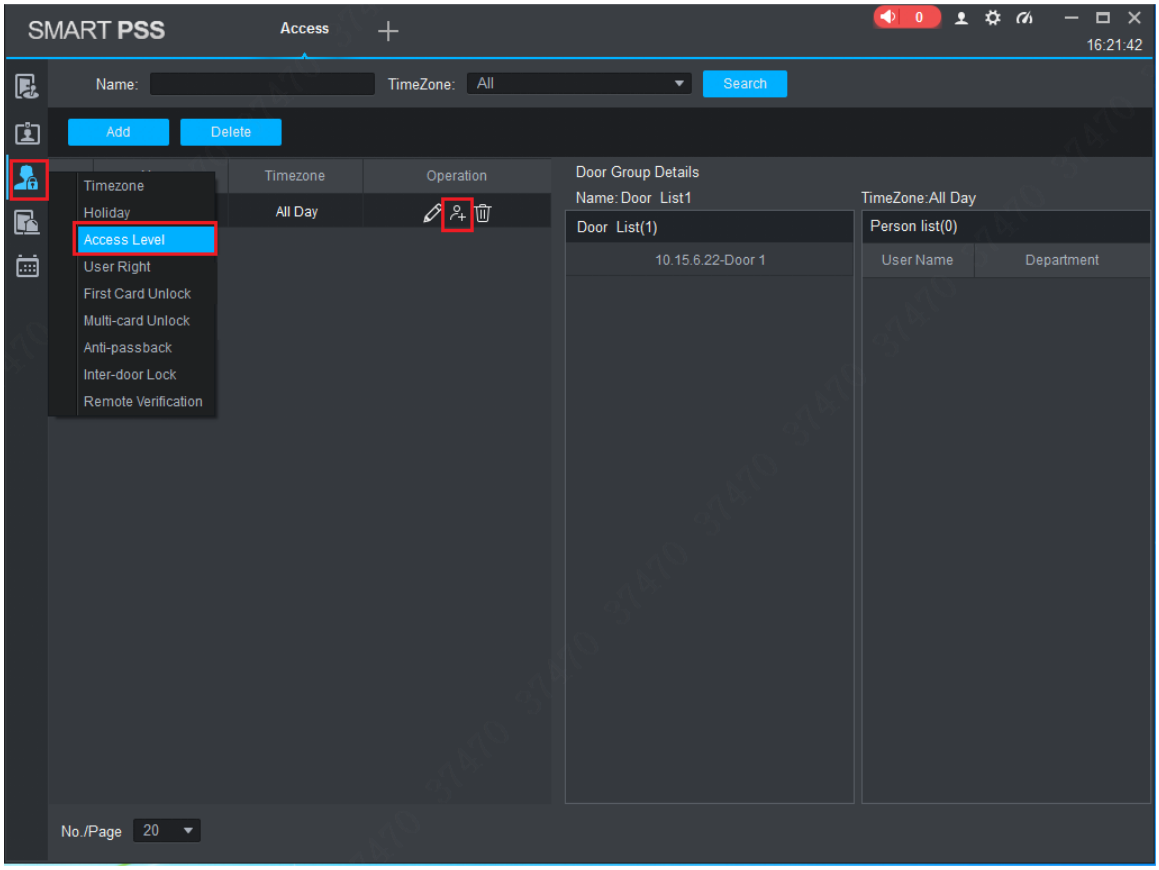
Otorgue autorizaciones a los usuarios según el grupo de puertas y el usuario.

3.5.1 Autorizar según Grupo de Puerta

Seleccione un grupo de puertas, agregue los usuarios correspondientes al grupo, para que todos los usuarios del grupo obtengan autorización de todas las puertas del grupo.

Paso 1 En la interfaz de "Acceso", haga clic  , y luego haga clic en "Nivel de acceso", como se muestra en la Figura en 3-15.

Figura 3-15

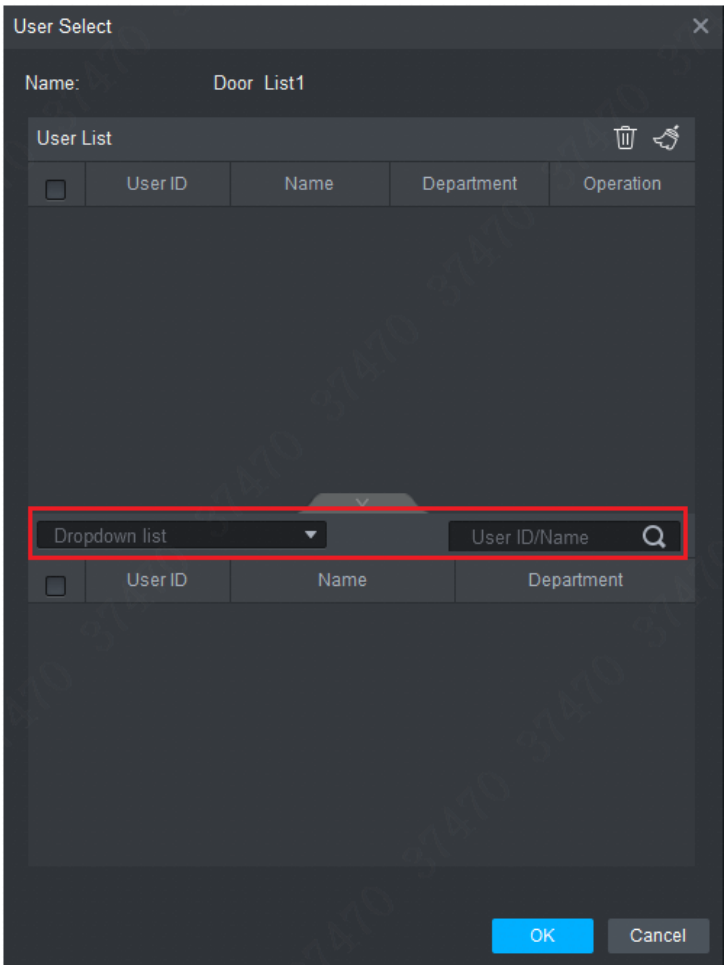


Paso 2 Hacer clic  .

El sistema muestra el cuadro de diálogo "Selección de usuario".

Paso 3 Seleccione el departamento del usuario de la lista desplegable o ingrese la ID o el nombre del usuario directamente, como se muestra en la Figura 3-16.

Figura 3-16



Etapa 4 En la lista de búsqueda, seleccione el usuario y agréguelo a la lista de usuarios. Haga clic

Paso 5 en "Aceptar" para finalizar la autorización.

NOTE

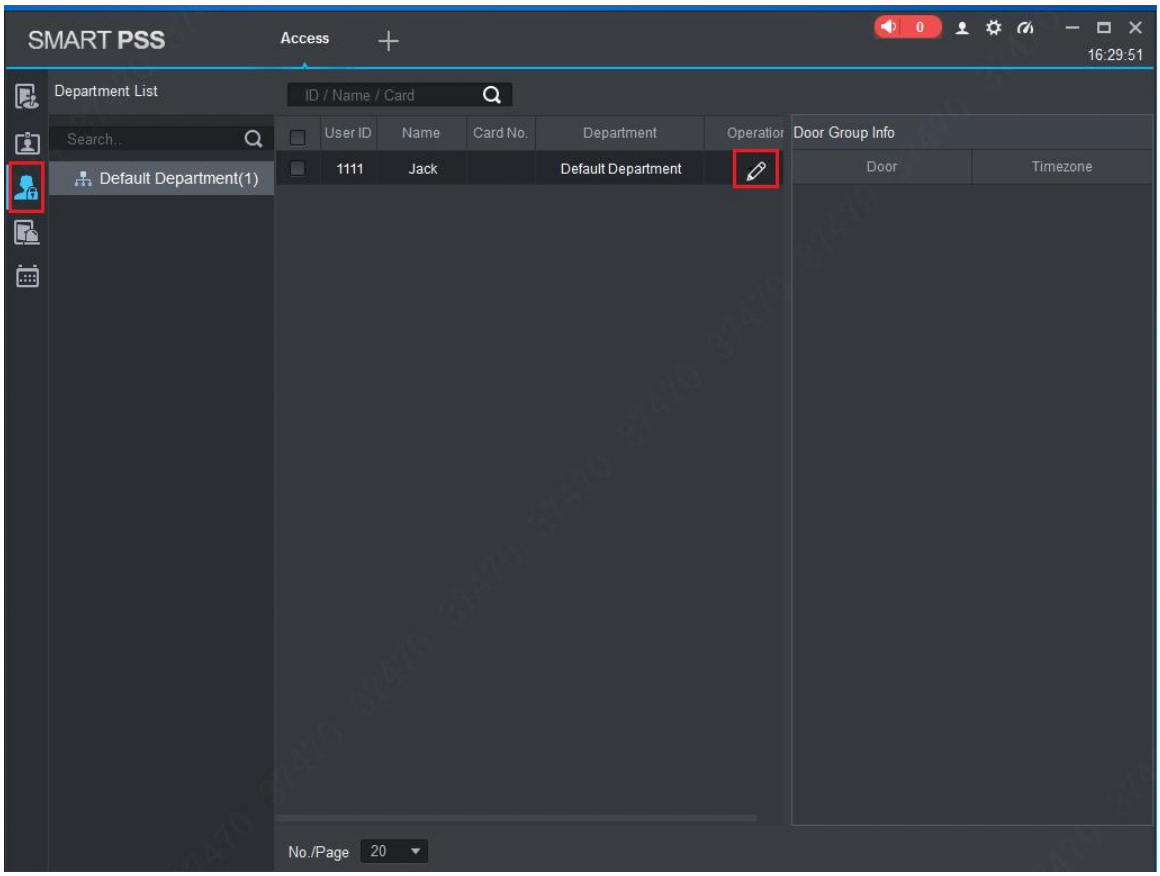
- La lista de búsqueda filtra la información del usuario sin número de tarjeta.
- En la lista de usuarios, cancele el usuario agregado y elimine la autoridad del usuario.

3.5.2 Autorizar según usuario

Seleccione un usuario, distribuya el grupo de puertas y otorgue autorización de grupo de puertas al usuario.

Paso 1 En la interfaz de "Acceso", haga clic en  y luego haga clic en "Derecho de usuario", como se muestra en la Figura 3-17.

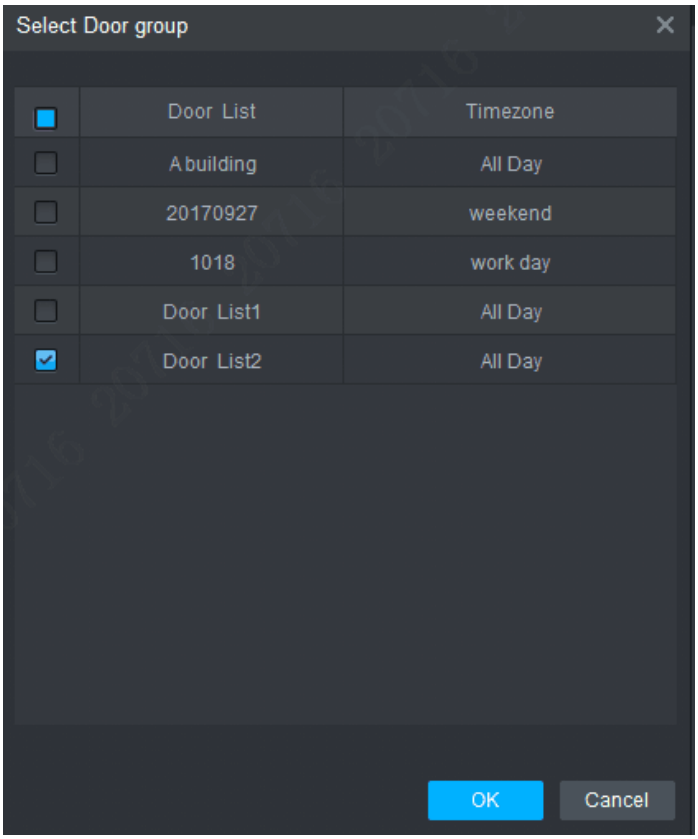
Figura 3-17



Paso 2 Hacer clic  .

El sistema muestra el cuadro de diálogo "Seleccionar grupo de puertas", como se muestra en la Figura 3-18.

Figura 3-18



Paso 3 Seleccione el grupo de puertas y haga clic en "Aceptar" para finalizar la autorización.

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.

Apéndice 1 Recomendaciones sobre ciberseguridad

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

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

1. Usar contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Actualice el firmware y el software del cliente a tiempo

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

- Le sugerimos que descargue y utilice la última versión del software del cliente.

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

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

2. Cambie las contraseñas regularmente

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

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

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

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilitar HTTPS

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

7. Habilitar lista blanca

Le sugerimos que habilite la función de lista blanca para evitar que todos, excepto aquellos con direcciones IP específicas, accedan al sistema. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del equipo adjunto a la lista blanca.

8. Enlace de dirección MAC

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

9. Asigne cuentas y privilegios de manera razonable

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios razonablemente y asígneles un conjunto mínimo de permisos.

10. Deshabilite los servicios innecesarios y elija modos seguros

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

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

- SNMP：Elija SNMP v3 y configure contraseñas de cifrado y contraseñas de autenticación seguras.
- SMTP：Elija TLS para acceder al servidor de buzones.
- FTP：Elija SFTP y configure contraseñas seguras.
- Punto de acceso AP：Elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

11. Transmisión encriptada de audio y video

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

Recordatorio: la transmisión encriptada causará cierta pérdida en la eficiencia de la transmisión.

12. Auditoría segura

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

13. Registro de red

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

14. Construya un entorno de red seguro

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

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde una red externa.

- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere usar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.