Acceso independiente

Manual de usuario

V1.0.4

Prefacio

General

Este manual presenta las funciones y operaciones de Access Standalone (en adelante, el "Dispositivo"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para consultarlo en el futuro.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

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

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.4	Se actualizó el desbloqueo de la tarjeta.	marzo 2024
V1.0.3	Se actualizaron los modos de desbloqueo.	noviembre 2023
V1.0.2	Se actualizaron los modos de desbloqueo.	marzo 2023
V1.0.1	Se actualizaron las configuraciones en la plataforma.	noviembre 2022
V1.0.0	Primer lanzamiento.	enero 2022

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otras personas, como su rostro, audio, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: Proporcionar una identificación clara y visible para informar a las personas sobre la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del Manual

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

Salvaguardias y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del Dispositivo, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el Dispositivo y cumpla con las pautas al usarlo.

Requisito de transporte

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

Requisito de almacenamiento

Guarde el dispositivo en condiciones permitidas de humedad y temperatura.

requerimientos de instalación

- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- Cumpla estrictamente con el código y las normas locales de seguridad eléctrica. Asegúrese de que el voltaje ambiental sea estable y cumpla con los requisitos de suministro de energía del dispositivo.
- No conecte el Dispositivo a dos o más tipos de fuentes de alimentación para evitar daños al Dispositivo.
- El uso inadecuado de la batería podría provocar un incendio o una explosión.

- El personal que trabaja en alturas debe tomar todas las medidas necesarias para garantizar la seguridad personal, incluido el uso de casco y cinturones de seguridad.
- No coloque el Dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- Instale el dispositivo sobre una superficie estable para evitar que se caiga.
- Instale el dispositivo en un lugar bien ventilado y no bloquee su ventilación.
- Utilice un adaptador o fuente de alimentación de gabinete proporcionado por el fabricante.
- Utilice los cables de alimentación recomendados para la región y cumplan con las especificaciones de potencia nominal.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en el estándar IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de suministro de energía están sujetos a la etiqueta del dispositivo.
- El Dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del Dispositivo esté conectada a una toma de corriente con conexión a tierra de protección.

Requisitos de operación

- Compruebe si la fuente de alimentación es correcta antes de su uso.
- No desenchufe el cable de alimentación en el costado del dispositivo mientras el adaptador esté encendido.
- Opere el dispositivo dentro del rango nominal de entrada y salida de energía.
- Utilice el dispositivo en condiciones permitidas de humedad y temperatura.
- 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 él.
- No desmonte el dispositivo sin instrucción profesional.

Tabla de contenido

Prefacio..... I Medidas de seguridad y advertencias importantes..... III 1 Descripción general del producto..... 1

1.1 Dimensiones.....1

1.2 Estructura..... 2

2 Instalación..... ... 3

3 Diagrama de red.....5

4 Cableado..... 6

5 Configuración Local..... 8

5.1 Menú principal..... 8

5.2 Cambiar la contraseña de administrador..... 8

5.3 Agregar usuarios..... 9

5.4 Eliminación de usuarios..... 9

5.5 Configuración de modos de desbloqueo..... 10

5.6 Configuración de la duración de apertura de la puerta.....11

5.7 Configurar modos de trabajo.....11

5.8 Configuración del detector de puerta..... 11

5.9 Restauración a los valores predeterminados de fábrica..... 11

6 Configuración inteligente de PSS Lite..... 13

6.1 Instalación e inicio de sesión..... 13

6.2 Agregar dispositivos..... 13

6.2.1 Agregar uno por uno..... 13

6.2.2 Agregar lotes.....14

6.3 Gestión de usuarios..... 15

6.3.1 Configurar el tipo de tarjeta..... 15

6.3.2 Agregar usuarios.....dieciséis

6.3.3 Asignación de permiso de acceso.....20

6.4 Gestión de acceso..... 22

6.4.1 Apertura y cierre de puerta de forma remota..... 22

6.4.2 Configuración de Siempre abierto y Siempre cerrado.....23

6.4.3 Monitoreo del estado de la puerta..... 24

7 Preguntas frecuentes..... 25

Apéndice 1 Recomendaciones de ciberseguridad..... 26

1 Descripción general del producto

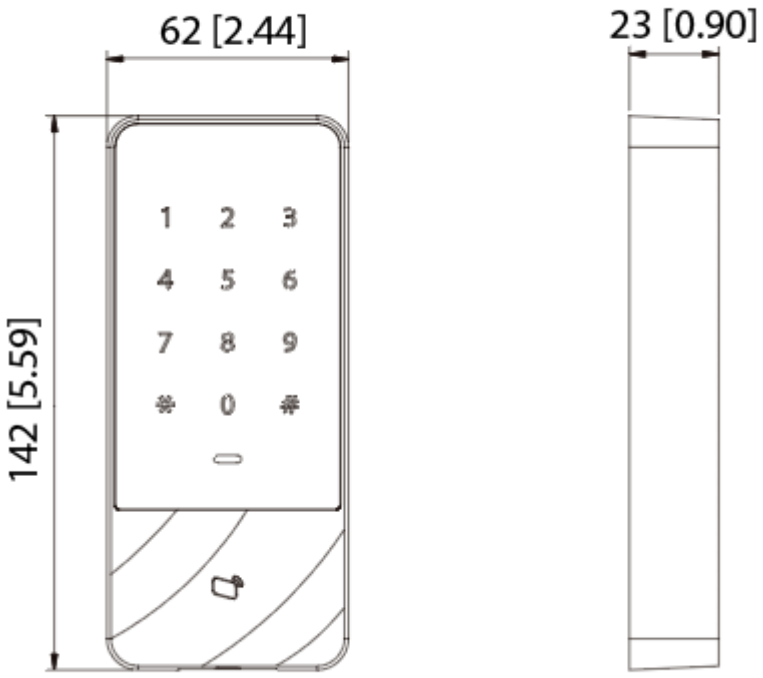
El Dispositivo está destinado a la gestión de acceso en un área controlada. Con una apariencia elegante y un grado de impermeabilidad IPX6, se puede usar en exteriores.

Tiene las siguientes características principales:

- Admite teclado táctil y protocolo TCP/IP.
- Admite 30.000 tarjetas válidas y puede almacenar hasta 60.000 registros.
- Admite desbloquear la puerta a través de los siguientes modos:
  - ◇ Tarjeta
  - ◇ ID de usuario + Tarjeta de
  - ◇ contraseña + Contraseña)
  - ◇ Tarjeta o (ID de usuario + Contraseña)
- Admite alarma de horas extras, alarma de intrusión, alarma de coacción y alarma de manipulación.
- Admite tarjeta de invitado, tarjeta de coacción, tarjeta de lista de bloqueo/lista de permitidos y tarjeta de patrulla.
- Admite 128 grupos de horarios, 128 grupos de períodos y 128 grupos de períodos festivos.

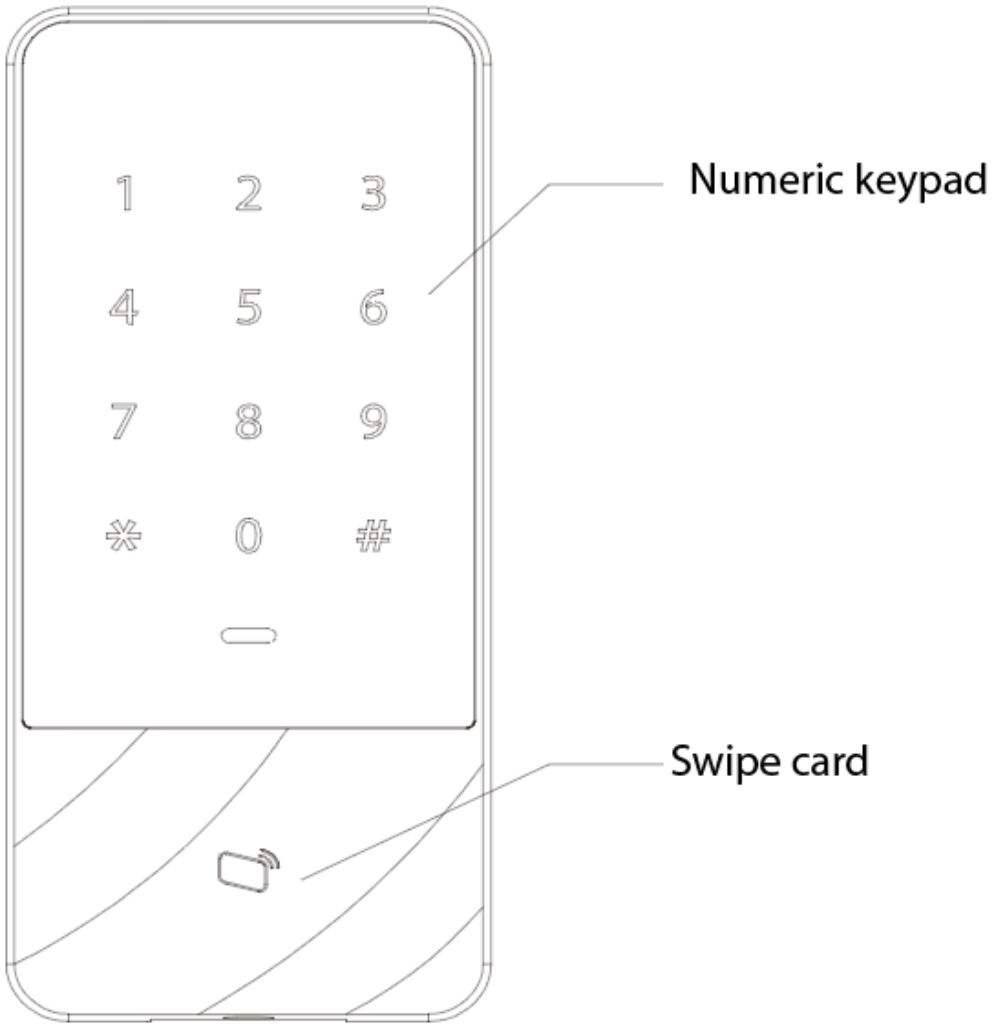
1.1 Dimensiones

Figura 1-1 Dimensiones (mm [pulgadas])



1.2 Estructura

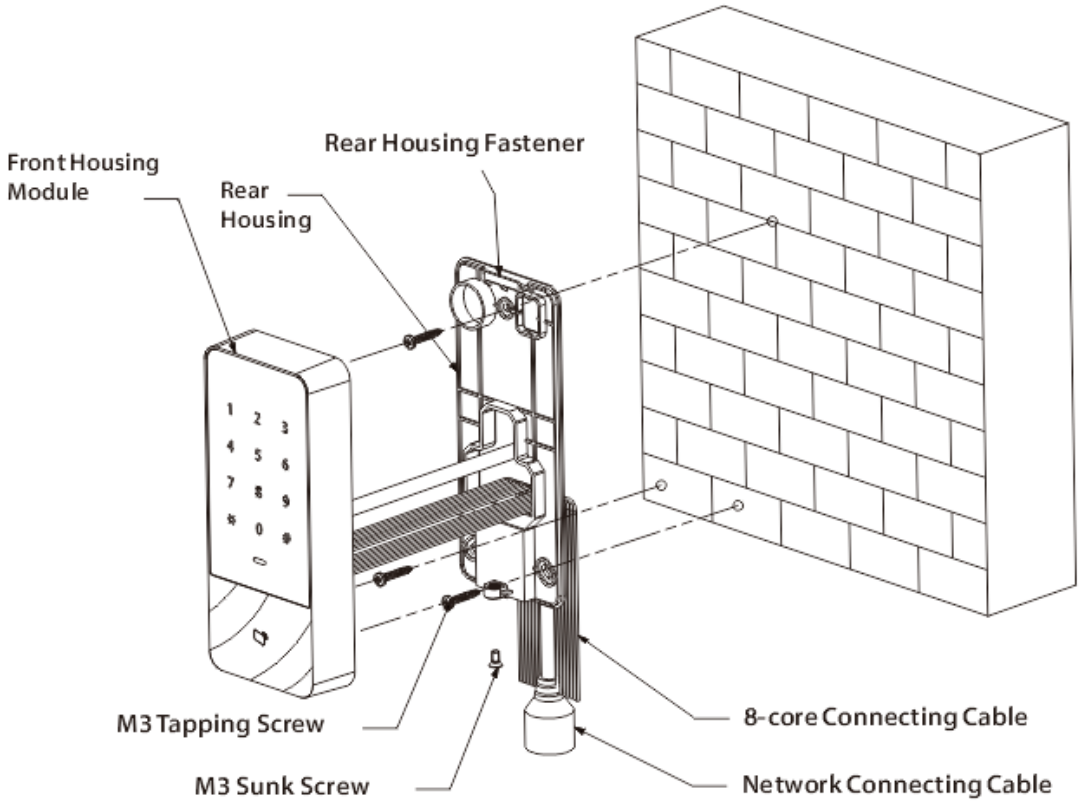
Figura 1-2 Estructura



2 Instalación

Información de contexto

Figura 2-1 Instalación



Procedimiento

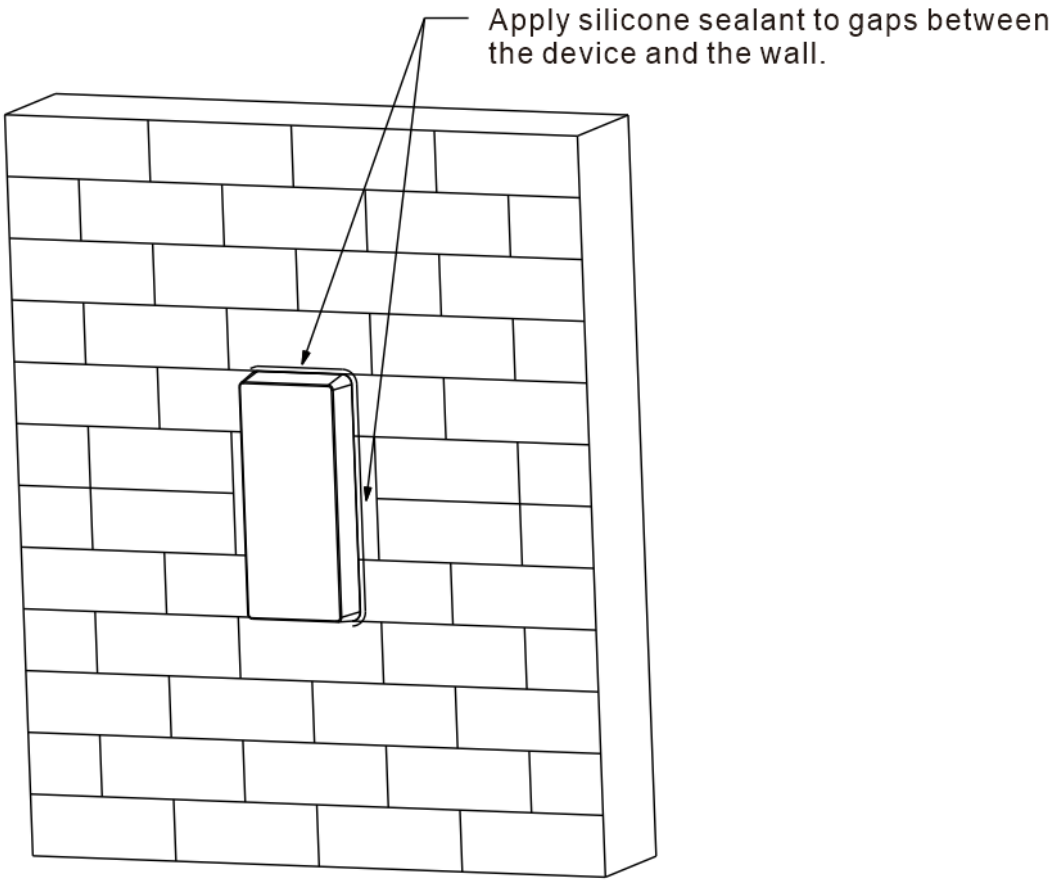
Paso 1 Fije la carcasa trasera a la pared con tornillos autorroscantes M3; Deje un espacio para el cable de conexión de red entre la carcasa trasera y la pared.

Paso 2 Pase el cable de conexión de red y los dos cables de conexión de 8 núcleos a través de la ranura de la carcasa trasera y la pared, y luego apriete los tornillos de rosca M3.

Paso 3 Fije la parte superior del módulo de la carcasa frontal al sujetador de la carcasa trasera y luego apriete los tornillos hundidos M3 en la parte inferior para fijarlos.

Etapa 4 Aplique sellador de silicona a los espacios entre el dispositivo y la pared.

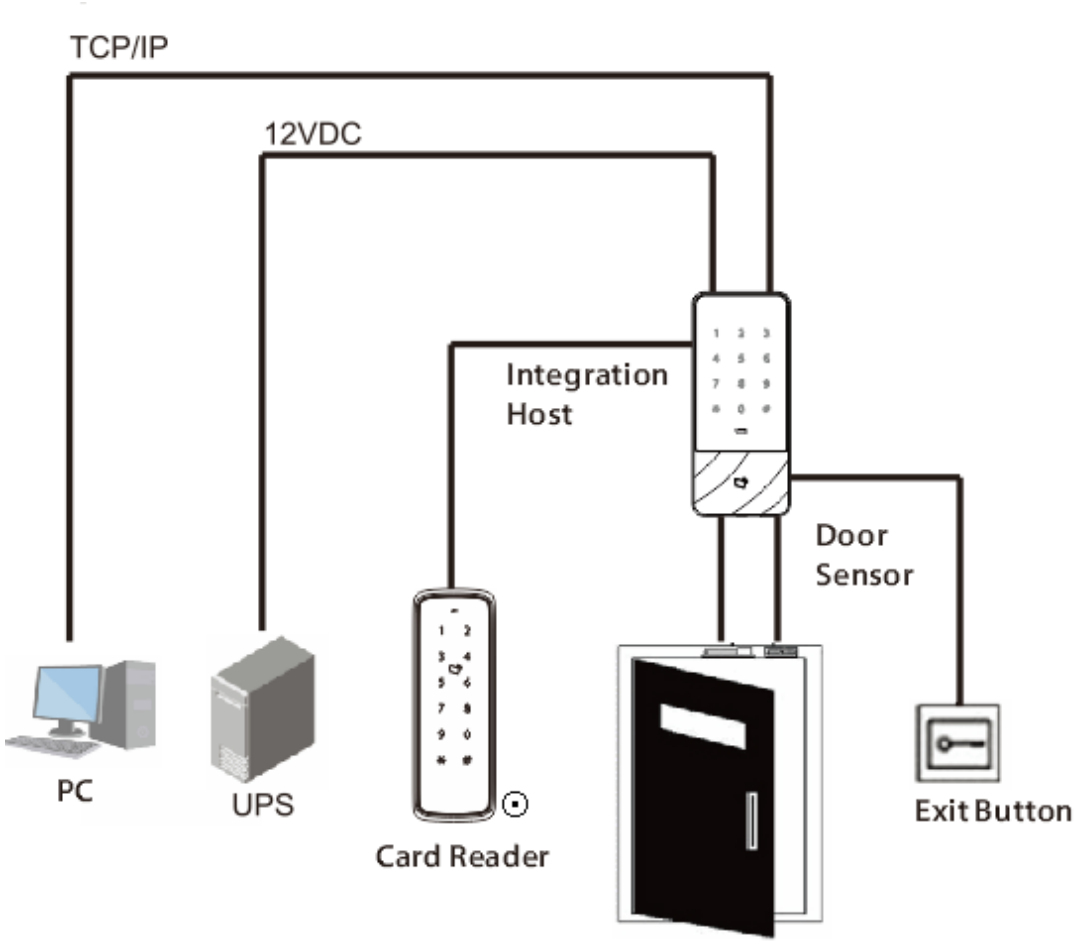
Figura 2-2 Aplicar silicona



3 Diagrama de red

A continuación se muestra el diagrama de red de un sistema de control de acceso básico.

Figura 3-1 Diagrama de red



4 cableado

Figura 4-1 Cableado

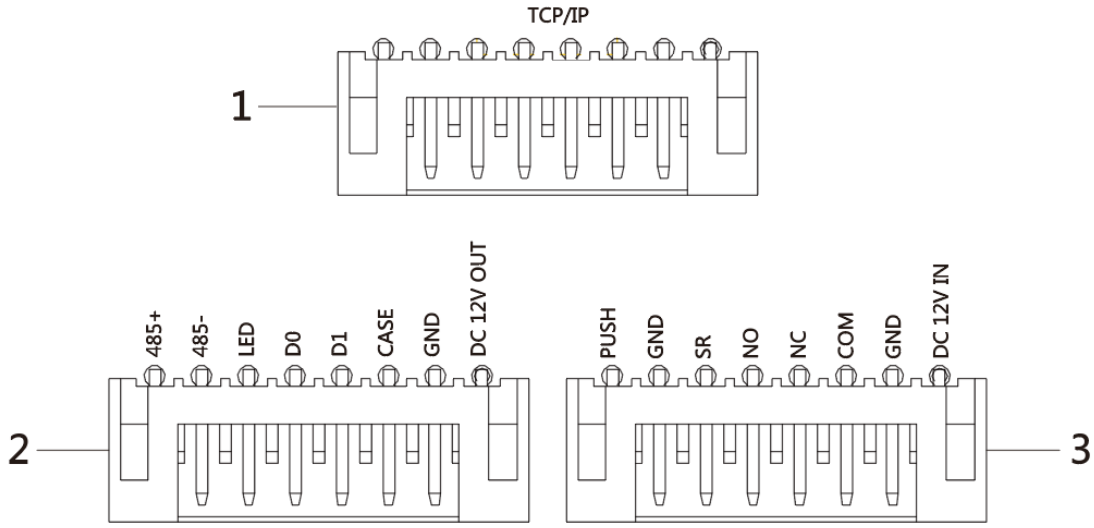


Tabla 4-1 Descripción del cableado

No.	Puerto	Descripción
1	RJ45	TCP/IP (puerto de red).
2	485+	Conecta lector de tarjetas RS-485.
	485-	
	CONDUJO	Conecta el cable LED del lector de tarjetas para transmitir señales indicadoras.
	D0	Conecta el lector de tarjetas Wiegand.
	D1	
	CASO	Conecta las señales antimanipulación del lector de tarjetas.
	Tierra	Conecta el cable de tierra.
	SALIDA DE 12 VCC	Alimentación de 12VDC del lector.
3	EMPUJAR	Conecta el botón de salida de la puerta.
	Tierra	Conecta el cable a tierra, que comparten el detector de puerta y el botón de salida de la puerta.
	SR	Conecta el detector de puerta.
	NO	Conecta el puerto NO de la cerradura de la puerta.
	CAROLINA DEL NORTE	Conecta el puerto NC de la cerradura de la puerta.
	COM	Conecta el puerto COM de la cerradura de la puerta.
	Tierra	Conecta el cable de tierra.

No.	Puerto	Descripción
	ENTRADA DE 12 VCC	Entrada de alimentación de 12 VCC.

5 Configuración local

5.1 Menú principal

Procedimiento

Paso 1 Toque la pantalla para activar el dispositivo y toque**#**.

La luz indicadora es azul fija y el teclado numérico se enciende, lo que significa que el dispositivo se activa.

Paso 2 Ingrese la contraseña de administrador y luego toque**#**.

Paso 3 Después de ingresar al menú principal, puede tocar las teclas numéricas para configurar los parámetros.

Tabla 5-1 Descripción del menú principal

Tecla numérica	Descripción
0	Modifique la contraseña de administrador.
1	Agregar usuarios.
2	Eliminar usuarios.
3	Establecer modos de desbloqueo.
4	Configure el tiempo de espera del relé de bloqueo de la puerta.
5	Configure el modo de trabajo.
6	Habilite el sensor de puerta.
9	Restaurar los valores de fábrica.

- La contraseña de administrador predeterminada es 88888888.
- La luz indicadora parpadea en azul, lo que significa que ingresa al menú principal con éxito.
- El indicador está en rojo fijo. Después de que suene el timbre tres veces, la luz indicadora se vuelve azul fija, lo que significa que se ingresó una contraseña incorrecta.
- Después de las configuraciones, toque*****para ir a la página anterior.
- En el menú principal, toque*****para salir del menú principal.

5.2 Cambiar la contraseña de administrador

Cambie la contraseña de administrador periódicamente para mejorar la seguridad de la cuenta.

Procedimiento

Paso 1 Ingrese al menú

Paso 2 principal. grifo**0**y**#**.

Paso 3 Ingrese la nueva contraseña y toque**#**. Confirme la

Etapa 4 nueva contraseña y luego toque**#**.

- La luz indicadora es de color verde fijo y el timbre suena una vez, lo que significa que la contraseña se cambió correctamente.
- La luz indicadora es roja fija y el timbre suena tres veces, lo que significa que la contraseña no se cambia.

5.3 Agregar usuarios

Procedimiento

Paso 1 Ingrese al menú principal. grifo**1**y

Paso 2 **#**para agregar un usuario.

1. Agregar ID de usuario: ingrese la ID de usuario y luego toque**#**.

   Si el ID de usuario ya existe, no se puede agregar.

2. Agregar una tarjeta: desliza una tarjeta y luego toca**#**.

   - Si no desea agregar una tarjeta, toque**#**para omitir este paso.
   - Sólo se permite una tarjeta por usuario.

3. Agregar contraseña: ingresa una contraseña y toca**#**.

   - Si no desea establecer una contraseña, toque**#**para omitir este paso.
   - Establezca la contraseña si no agregó el número de tarjeta. Si no se establece la contraseña, no se puede agregar el usuario.

Paso 3 RepetirPaso 2 para agregar más usuarios.

La luz indicadora es de color verde fijo y el timbre suena una vez, lo que significa que el usuario se agregó correctamente. La luz indicadora es de color rojo fijo y el timbre suena 3 veces, lo que significa que el usuario agrega una falla.

Después de agregar usuarios, el sistema permanece en**Agregar usuario**pantalla. Grifo*****para volver al menú principal.

5.4 Eliminar usuarios

Elimine usuarios y no tendrán permisos para desbloquear la puerta.

Procedimiento

Paso 1 Ingrese al menú

Paso 2 principal. grifo**2**y**#**.

- Desliza la tarjeta y toca**#**para eliminar al usuario.
- Ingrese el ID de usuario y toque**#**para eliminar al usuario.
- Ingrese 0000 y toque**#**para eliminar a todos los usuarios.

- La luz indicadora es de color verde fijo y el timbre suena una vez, lo que significa que el usuario se ha eliminado correctamente. La luz indicadora es roja fija y el timbre suena 3 veces, lo que

significa que el usuario no se agregó correctamente. Después de la eliminación, el sistema permanece en el **Borrar usuario**pantalla. Grifo*****para volver al menú principal.

5.5 Configuración de modos de desbloqueo

Configure los modos de desbloqueo de puertas, como desbloqueo mediante tarjeta, ID de usuario + contraseña, tarjeta + contraseña y tarjeta o (ID de usuario + contraseña).

Procedimiento

Paso 1 Ingrese al menú

Paso 2 principal. grifo**3**y**#**.

Paso 3 Configurar el modo de desbloqueo.

Tabla 5-2 Configurar el modo de desbloqueo

Modo de desbloqueo	Método de desbloqueo
Tarjeta (por defecto): toca**0**y**#**.	Pase la tarjeta por el lector de tarjetas para desbloquear la puerta.
Tarjeta + contraseña: toque**1**y**#**.	Pase la tarjeta y luego ingrese la contraseña y toque **#**para desbloquear la puerta.
ID de usuario + contraseña: toque**2**y**#**.	Ingrese el ID de usuario y toque**#**y luego ingrese la contraseña y toque**#**para desbloquear la puerta.
Tarjeta o (ID de usuario + contraseña): toque**3**y**#**.	Pase la tarjeta para desbloquear la puerta o ingrese la identificación del usuario y toque**#**y luego ingrese la contraseña y toque**#**para desbloquear la puerta.
Contraseña pública: puede configurar la contraseña pública en SmartPSS Lite o DSS Pro y luego enviar la contraseña pública al dispositivo. ● DSS Pro puede enviar hasta 500 contraseñas públicas al dispositivo. ● SmartPSS Lite solo puede enviar una contraseña pública al Dispositivo. Si cambia la contraseña pública, la contraseña anterior se sobrescribirá con la nueva.	Ingrese la contraseña pública y luego toque**#**. La contraseña pública no está limitada por los modos de desbloqueo.

Después de las configuraciones, el sistema regresa al menú principal automáticamente. Grifo*****para salir del menú principal.

- La contraseña de coacción es ID de usuario más 1. Por ejemplo, si la contraseña de usuario es 12345, la contraseña de coacción es 12346. Si la contraseña de usuario es 56789, la contraseña de coacción es 56780.
- Para activar la función de contraseña de coacción, instale e inicie sesión en el cliente SmartPSS Lite y vaya a **Configuración de acceso**>**Acceder a la configuración**y habilite la contraseña de coacción. Para obtener más información, consulte el manual del usuario de SmartPSS Lite. Independientemente de los modos de desbloqueo, si ingresa la ID de usuario y la contraseña de coacción, se activará una alarma de coacción y se enviarán mensajes de alarma a la plataforma de administración.

5.6 Configuración de la duración de apertura de la puerta

La puerta permanece abierta durante un período definido para que las personas puedan acceder antes de que se vuelva a cerrar automáticamente.

Procedimiento

Paso 1 Ingrese al menú

Paso 2 principal. grifo**4**y**#**.

Paso 3 Introduzca el tiempo (entre 1 s y 600 s) y toque**#**.

Después de la configuración, el sistema vuelve al menú principal automáticamente. grifo*****para salir del menú principal.

5.7 Configurar modos de trabajo

El Dispositivo tiene 2 modos de trabajo. Puede funcionar como controlador de acceso o lector de tarjetas.

Procedimiento

Paso 1 Ingrese al menú

Paso 2 principal. grifo**5**y**#**.

Paso 3 Seleccione el modo de trabajo.

- Controlador de acceso: controla el acceso después de que las personas verifican sus identidades.

  Grifo**0**y**#**.
- Lector: Sólo lee tarjeta.

  Grifo**1**y**#**.

Después de las configuraciones, el sistema regresa al menú principal automáticamente. Grifo*****para salir del menú principal.

5.8 Configuración del detector de puerta

El detector de puerta puede monitorear el estado de la puerta y activar una alarma cuando la puerta se abre de manera anormal.

Procedimiento

Paso 1 Ingrese al menú

Paso 2 principal. Grifo**6**y**#**.

Paso 3 Configurar el detector de puerta.

- Desactivar (predeterminado): toque**0**y**#**.
- Habilitar: toque**1**y**#**.

Después de las configuraciones, el sistema regresa al menú principal automáticamente. Grifo*****para salir del menú principal.

5.9 Restauración a los valores predeterminados de fábrica

Procedimiento

Paso 1 Ingrese al menú

Paso 2 principal. grifo**9**y**#**.

Paso 3 Ingresar**000**,y luego toque**#**.

El dispositivo se reiniciará automáticamente.

Operaciones relacionadas

Si olvidó la contraseña de administrador, puede restaurar el dispositivo a los valores predeterminados de fábrica mediante los siguientes métodos;

- Restauración parcial: Restaura solo la contraseña.

  El dispositivo suena una vez después de encenderlo y luego tocar***0***en 30s.
- Restauración completa: restaura todas las configuraciones a los valores predeterminados de fábrica.

  El dispositivo suena una vez después de encenderlo y luego tocar***00000***en 30s.

El indicador es de color verde fijo y el timbre suena una vez, lo que significa que el dispositivo se restauró correctamente.

El indicador está en rojo fijo y el timbre suena 3 veces, lo que significa que la restauración falló.

6 Configuración inteligente de PSS Lite

Esta sección presenta cómo administrar y configurar el dispositivo a través de Smart PSS Lite. Para obtener más información, consulte el manual del usuario de Smart PSS Lite.

6.1 Instalación e inicio de sesión

Instale e inicie sesión en Smart PSS Lite. Para obtener más información, consulte el manual de usuario de Smart PSS Lite.

Procedimiento

Paso 1 Obtenga el paquete de software del Smart PSS Lite del soporte técnico y luego instale y ejecute el software según las instrucciones.

Paso 2 Inicialice Smart PSS Lite cuando inicie sesión por primera vez, incluida la configuración de contraseña y preguntas de seguridad.

Establezca la contraseña para el primer uso y luego configure preguntas de seguridad para restablecer su contraseña cuando la haya olvidado.

Paso 3 Ingrese su nombre de usuario y contraseña para iniciar sesión en Smart PSS Lite.

6.2 Agregar dispositivos

Debe agregar el dispositivo a Smart PSS Lite. Puedes agregarlos en lotes o individualmente.

6.2.1 Agregar uno por uno

Puede agregar dispositivos uno por uno ingresando sus direcciones IP o nombres de dominio.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Administrador de dispositivos**y haga clic

Paso 3 **Agregar**. Ingrese la información del dispositivo.

Figura 6-1 Información del dispositivo

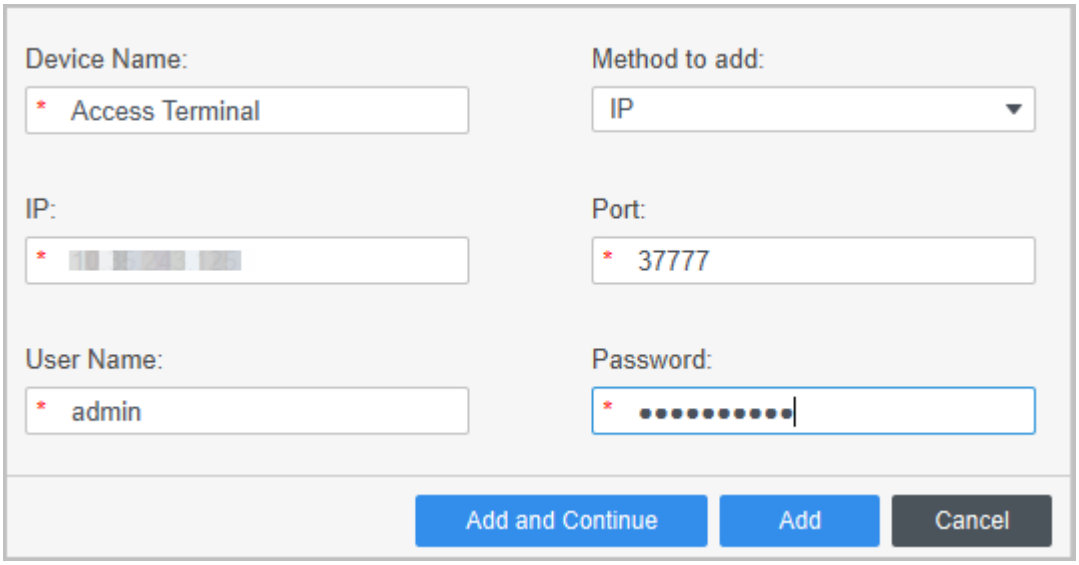


Tabla 6-1 Parámetros del dispositivo Descripción

Parámetro	Descripción
Nombre del dispositivo	Ingrese un nombre del dispositivo. Le recomendamos que le ponga el nombre de su área de instalación.
Método para agregar	Seleccionar**IP**para agregar el dispositivo ingresando su dirección IP.
IP	Ingrese la dirección IP del dispositivo.
Puerto	El número de puerto es 37777 de forma predeterminada.
Usuario Contraseña	Ingrese el nombre de usuario y contraseña del dispositivo.

Etapa 4 Hacer clic**Agregar**.

El dispositivo agregado se muestra en la**Dispositivos**página. Puedes hacer clic**Agregar y continuar**para agregar más dispositivos.

6.2.2 Agregar en lotes

Le recomendamos que utilice la función de búsqueda automática cuando agregue dispositivos deseados en lotes. Asegúrese de que los dispositivos que agregue deben estar en el mismo segmento de red.

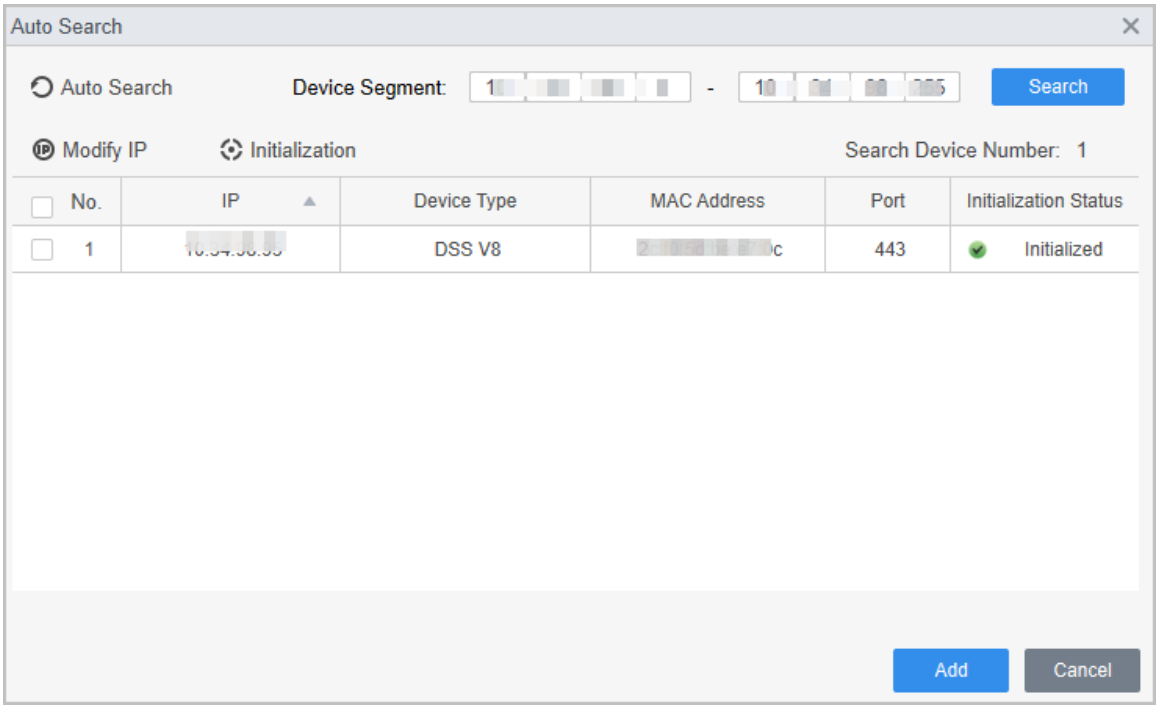
Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Administrador de dispositivos**y buscar dispositivos.

- Hacer clic**Auto búsqueda**, para buscar dispositivos en la misma LAN.
- Ingrese el rango del segmento de red y luego haga clic en**Buscar**.

Figura 6-2 Búsqueda automática



Se mostrará una lista de dispositivos.

Seleccione un dispositivo y luego haga clic en**Modificar IP**para modificar su dirección IP.

Paso 3 Seleccione el dispositivo que desea agregar a Smart PSS Lite y luego haga clic en**Agregar**.

Etapa 4 Ingrese el nombre de usuario y la contraseña del dispositivo.

Puede ver el dispositivo agregado en el**Dispositivos**página.

El dispositivo inicia sesión automáticamente en Smart PSS Lite después de agregarlo.**En línea**se muestra después de iniciar sesión correctamente.

6.3 Gestión de usuarios

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

6.3.1 Configurar el tipo de tarjeta

Configure el tipo de tarjeta antes de asignar tarjetas a los usuarios. Por ejemplo, si la tarjeta asignada es una tarjeta de identificación, configure el tipo de tarjeta en Tarjeta de identificación.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Solución de acceso**>**Gerente de Personal**>**Usuario**. Sobre el

Paso 3 **Tipo de emisión de tarjeta**y luego seleccione un tipo de tarjeta.

Asegúrese de que el tipo de tarjeta sea el mismo que la tarjeta realmente asignada; de lo contrario, el número de la tarjeta no podrá leerse.

Etapa 4 Hacer clic**DE ACUERDO**.

6.3.2 Agregar usuarios

6.3.2.1 Agregar uno por uno

Puede agregar usuarios uno por uno.

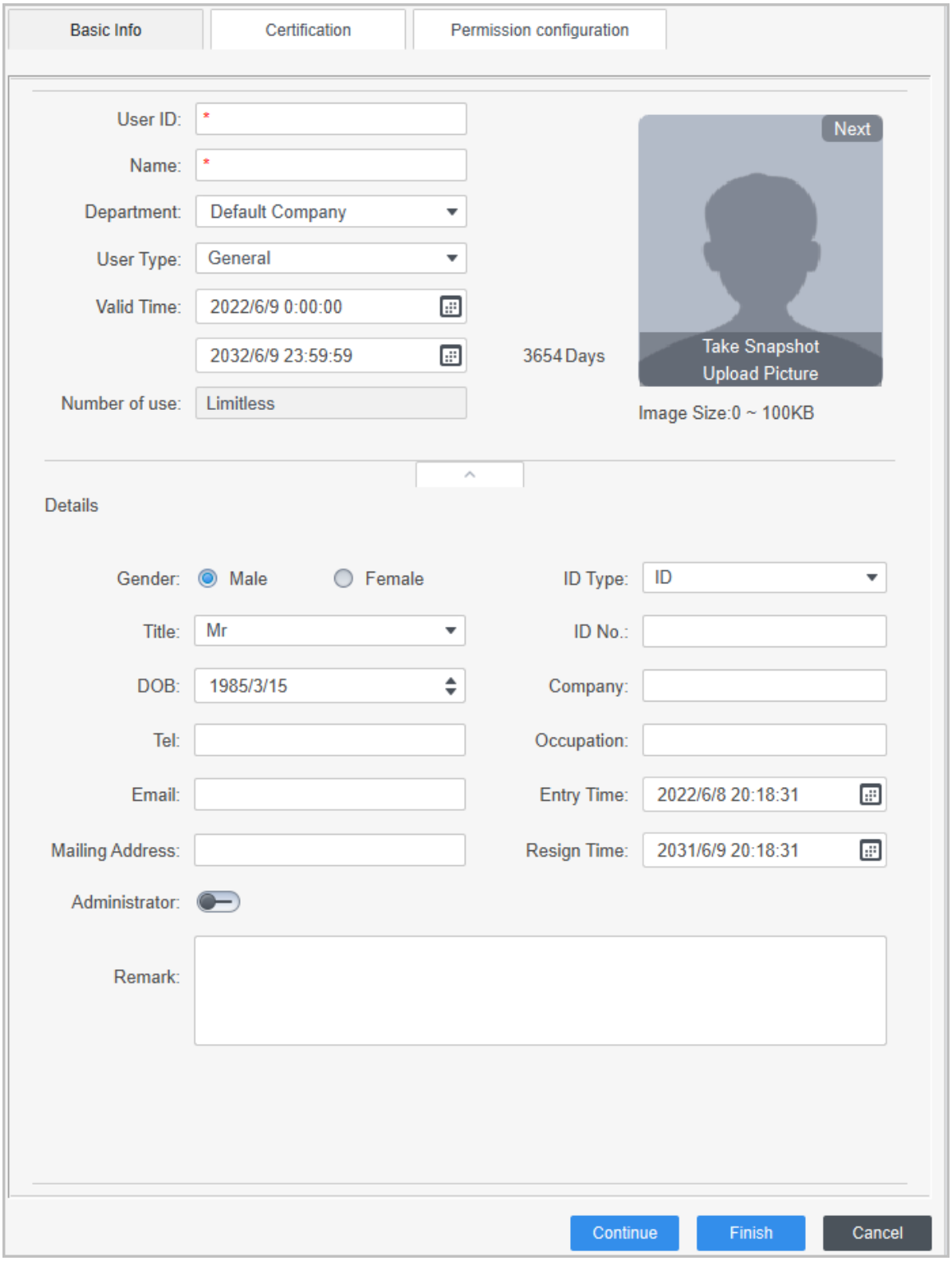
Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Solución de acceso**>**Gerente de Personal**>**Usuario**>**Agregar**.

Paso 3 Hacer clic**Información básica**pestaña, e ingrese la información básica del usuario, y luego importe la imagen de la cara.

Figura 6-3 Agregar información básica



Etapa 4 Haga clic en el**Certificación**pestaña para agregar información de certificación del usuario.

- Configurar contraseña: la contraseña debe constar de 1 a 8 dígitos.
- Configurar tarjeta: El número de tarjeta se puede leer automáticamente o ingresar manualmente. Para leer el número de tarjeta automáticamente, seleccione un lector de tarjetas y luego coloque la tarjeta en el lector de tarjetas.

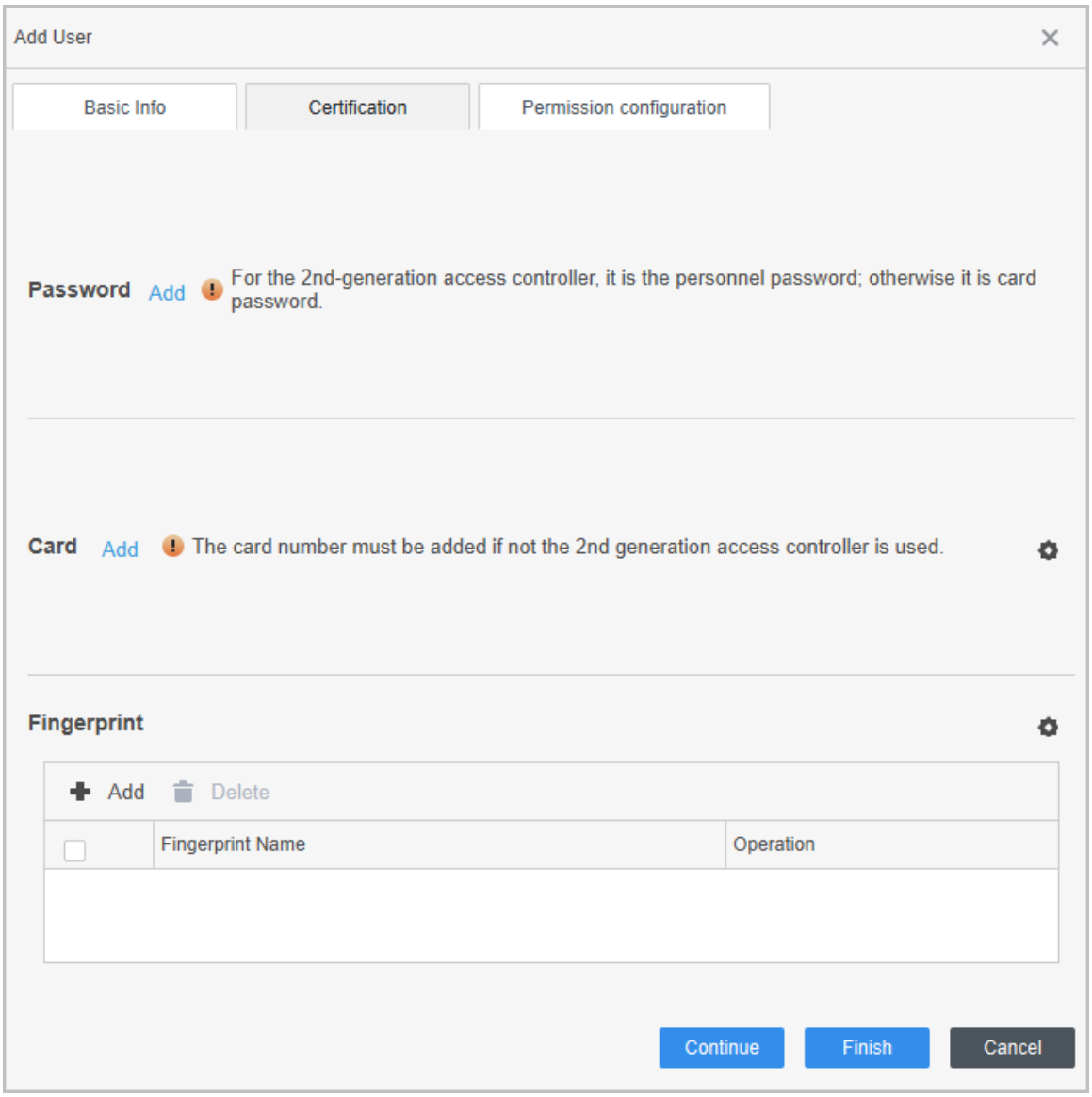
Solo puedes agregar una tarjeta para un usuario.

1. Sobre el**Tarjeta**área, haga clic y seleccione**Emisor de la tarjeta**y luego haga clic en**DE ACUERDO**.
2. Haga clic**Agregar**, pase una tarjeta por el lector de tarjetas.

   Se muestra el número de tarjeta.

3. Haga clic**DE ACUERDO**.

Figura 6-4 Agregar certificaciones



Paso 5 Configurar permisos para el usuario. Para obtener más información, consulte "6.3.3 Asignación de permiso de acceso".

Paso 6 Hacer clic**Finalizar**.

6.3.2.2 Agregar en lotes

Puede agregar usuarios en lotes.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

Paso 3 Seleccionar**Emisor de la tarjeta**desde el**Dispositivo**lista y luego configure los parámetros.

Figura 6-5 Agregar usuarios en lotes

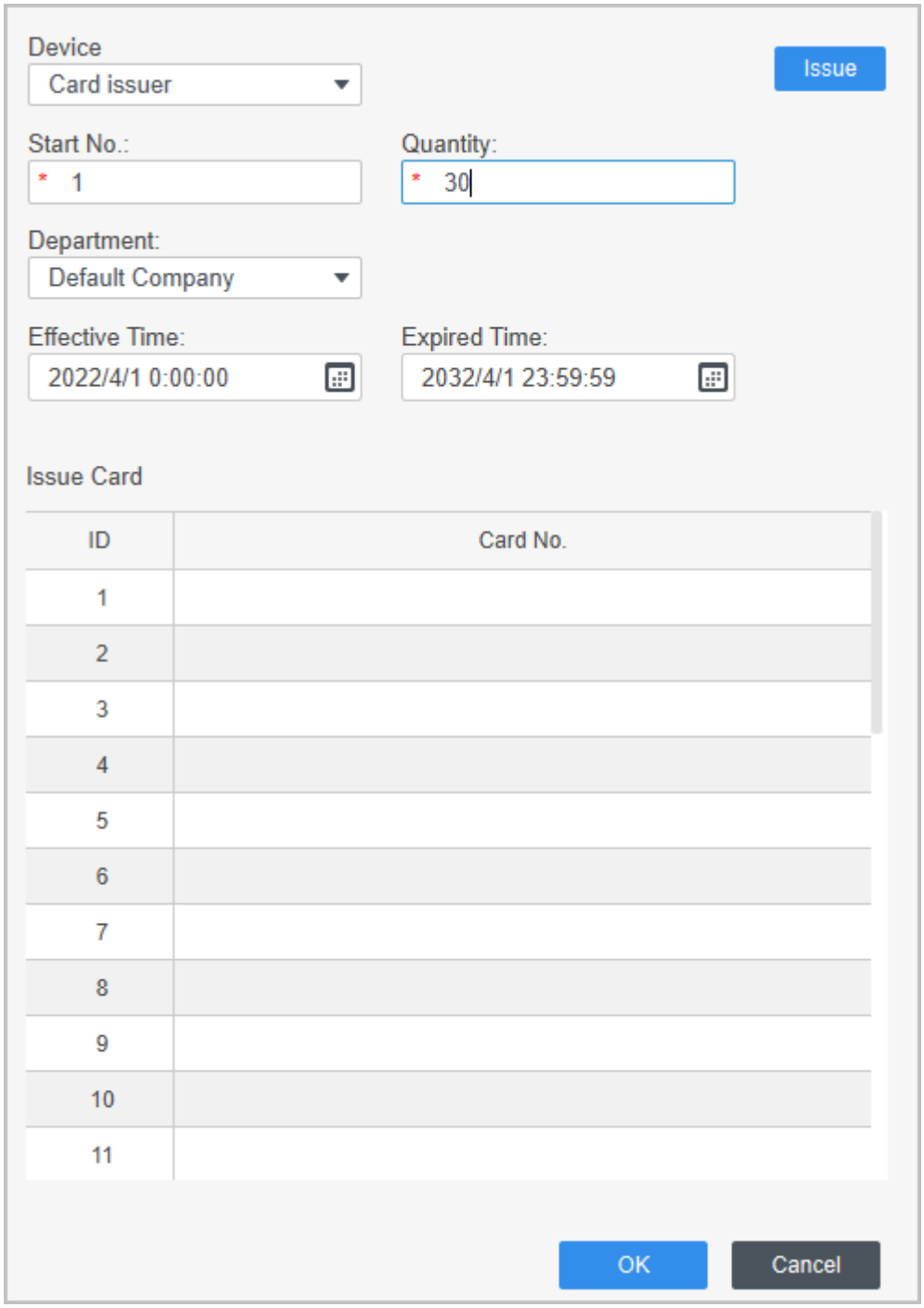


Tabla 6-2 Parámetros para agregar usuarios en lotes

Parámetro	Descripción
Empezar no.	La ID de usuario comienza con el número que usted definió.
Cantidad	La cantidad de usuarios que desea agregar.
Departamento	Seleccione el departamento al que pertenece el usuario.

Parámetro	Descripción
Tiempo efectivo/tiempo vencido	Los usuarios pueden desbloquear la puerta dentro del período definido.

Etapa 4 Hacer clic**Asunto**.

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

Paso 5 **ACUERDO**.

Paso 6 Sobre el**Usuario**página, haga clic  para completar la información del usuario.

6.3.3 Asignación de permiso de acceso

Cree un grupo de permisos que sea una colección de permisos de acceso a puertas y luego asocie usuarios con el grupo para que puedan desbloquear las puertas correspondientes.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Solución de acceso**>**Gerente de Personal**>**Configuración de permisos**.

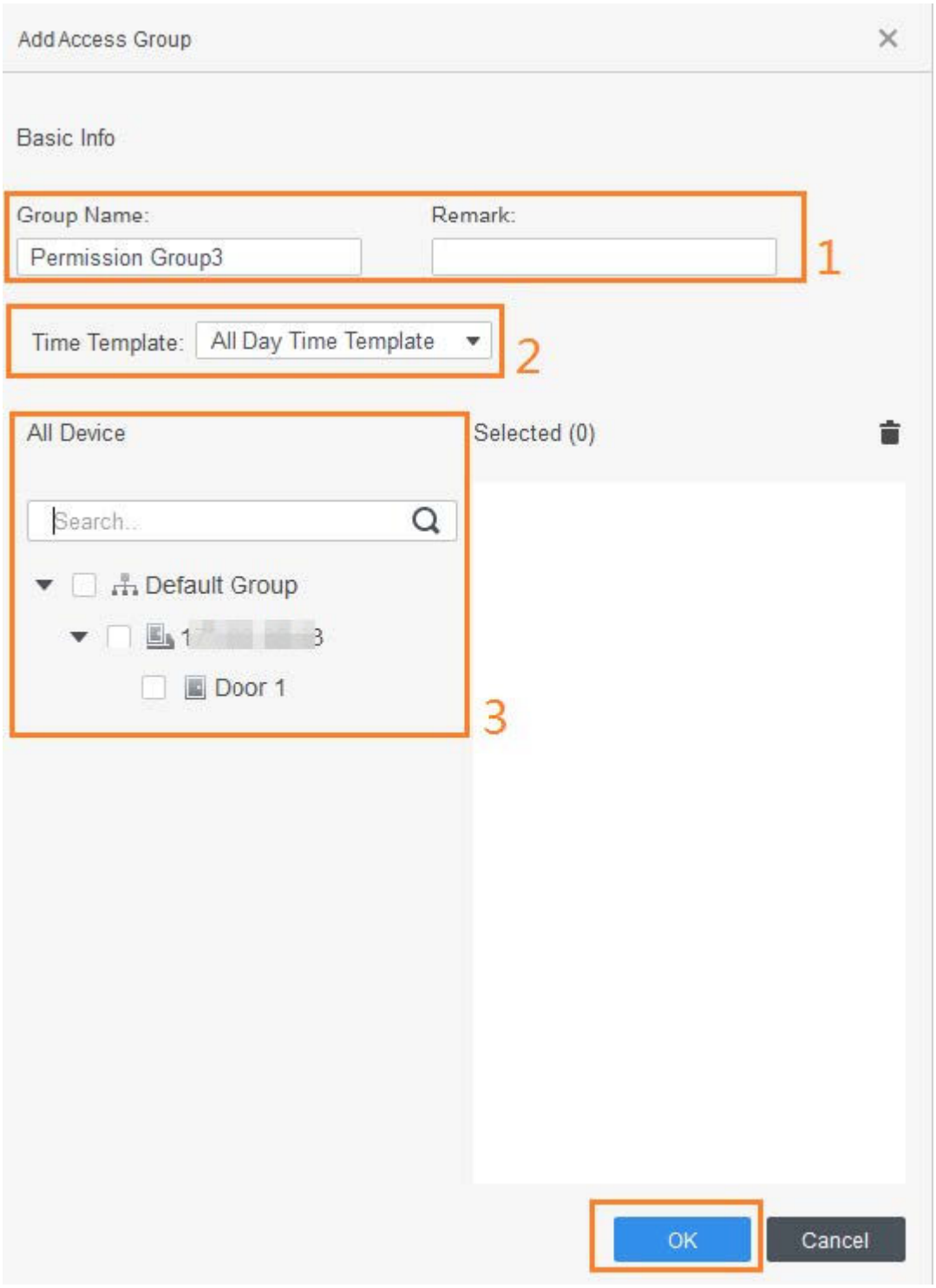
Paso 3 Haga clic.

Etapa 4 Ingrese el nombre del grupo, los comentarios (opcional) y seleccione una plantilla de tiempo.

Paso 5 Seleccione el dispositivo de control de acceso.

Paso 6 Hacer clic**DE ACUERDO**.

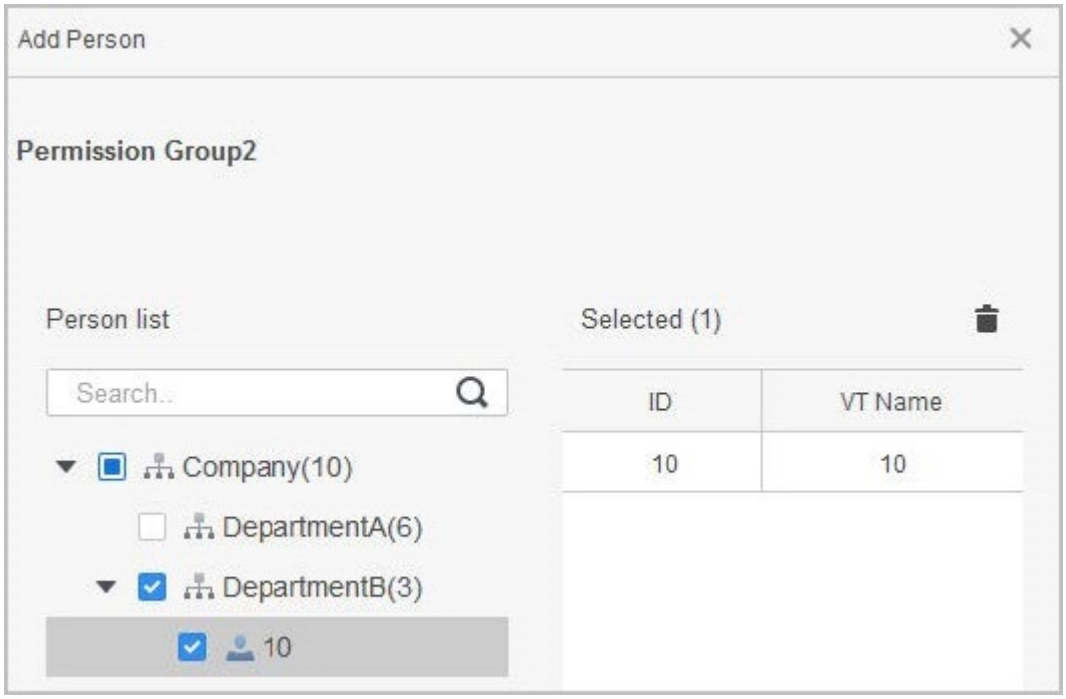
Figura 6-6 Crear un grupo de permisos



Paso 7 Hacer clic del grupo de permisos que agregó.

Paso 8 Seleccione usuarios para asociarlos con el grupo de permisos.

Figura 6-7 Agregar usuarios a un grupo de permisos



Paso 9 Hacer clic**DE ACUERDO**.

Los usuarios del grupo de permisos pueden desbloquear la puerta después de una verificación de identidad válida.

6.4 Gestión de acceso

6.4.1 Apertura y cierre de puertas de forma remota

Puede monitorear y controlar la puerta de forma remota a través de Smart PSS Lite. Por ejemplo, puede abrir o cerrar la puerta de forma remota.

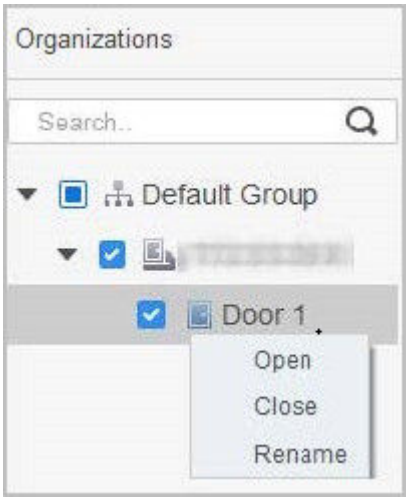
Procedimiento

Paso 1 Hacer clic**Solución de acceso**>**Administrador de acceso**en la página de inicio.

Paso 2 Controla remotamente la puerta.

- Seleccione la puerta, haga clic derecho y seleccione**Abierto**o**Cerca**.

Figura 6-8 Puerta abierta



- Haga clic en o para abrir o cerrar la puerta.

Operaciones relacionadas

- Filtrado de eventos: seleccione el tipo de evento en el**Información del evento**y la lista de eventos muestra el tipo de evento seleccionado, como eventos de alarma y eventos anormales.
- Bloqueo de actualización de eventos: haga clic para bloquear la lista de eventos y luego la lista de eventos dejará de actualizarse. Haga clic para desbloquear.
- Eliminación de eventos: haga clic para borrar todos los eventos en la lista de eventos.

6.4.2 Configuración de Siempre abierto y Siempre cerrado

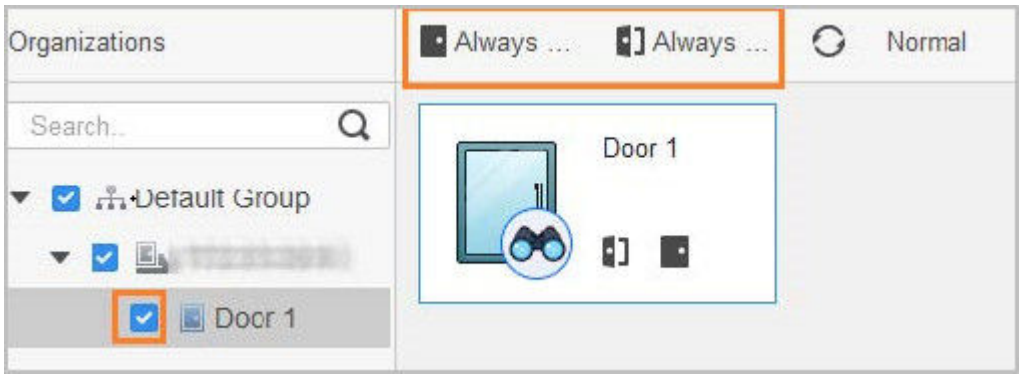
Después de configurar siempre abierta o siempre cerrada, la puerta permanece abierta o cerrada todo el tiempo.

Procedimiento

Paso 1 Hacer clic**Solución de acceso**>**Administrador de acceso**en la página de inicio.

Paso 2 Hacer clic**Siempre abierto**o**Siempre cerca**para abrir o cerrar la puerta.

Figura 6-9 Siempre abierto o cerrado



La puerta permanecerá abierta o cerrada todo el tiempo. Puedes hacer clic**Normal**para restaurar el control de acceso al estado normal, y luego la puerta se abrirá o cerrará según los métodos de verificación configurados.

6.4.3 Monitoreo del estado de la puerta

Procedimiento

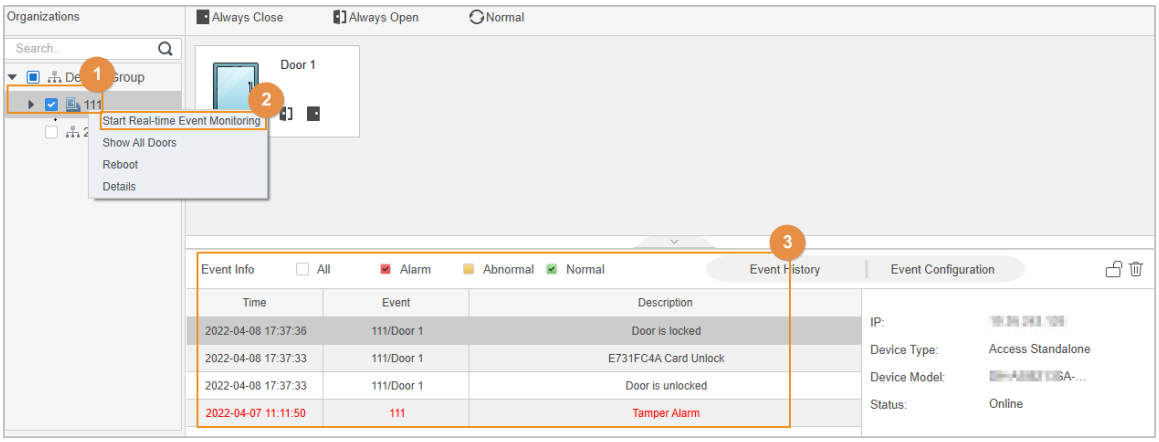
Paso 1 Hacer clic**Solución de acceso**>**Administrador de acceso**en la página de inicio.

Paso 2 Seleccione el dispositivo en el árbol de dispositivos, haga clic derecho en el dispositivo y luego seleccione**Iniciar monitoreo de eventos en tiempo real**.

Los eventos de control de acceso en tiempo real se mostrarán en la lista de eventos.

Hacer clic**Detener monitor**, los eventos de control de acceso en tiempo real no se mostrarán.

Figura 6-10 Monitorear el estado de la puerta



Operaciones relacionadas

- Mostrar todas las puertas: muestra todas las puertas controladas por el dispositivo.
- Reiniciar: reinicia el dispositivo.
- Detalles: vea los detalles del dispositivo, como la dirección IP, el modelo y el estado.

7 preguntas frecuentes

¿Cómo cambiar la IP si olvidó la IP del Dispositivo?

1. Restaure el dispositivo a los valores predeterminados de fábrica.

   Para obtener más información, consulte "5.9 Restauración a los valores predeterminados de fábrica".

   Después de restaurar los valores predeterminados de fábrica, el dispositivo pasará a un estado no inicializado y su IP se restaurará a 192.168.0.2.
2. Conecte el dispositivo a su computadora, inicialice el dispositivo con Configtool.

   - Asegúrese de que el dispositivo y la computadora estén en la misma red.
   - Asegúrese de que Configtool esté descargado e instalado en su computadora.
3. Cambie la IP del dispositivo a través de Configtool.

Apéndice 1 Recomendaciones de ciberseguridad

Acciones obligatorias que se deben tomar para la seguridad básica de la red de dispositivos:

1.**Utilice contraseñas seguras**

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

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

Recomendaciones "es bueno tener" para mejorar la seguridad de la red de su dispositivo:

1.Protección física

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

2.**Cambie las contraseñas con regularidad**

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de que las adivinen o las descifren.

3.**Establecer y actualizar contraseñas Restablecer información oportunamente**

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

4.**Habilitar bloqueo de cuenta**

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

5.**Cambiar HTTP predeterminado y otros puertos de servicio**

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

6.**Habilitar HTTPS**

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

7.**Enlace de dirección MAC**

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

8.**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. **Deshabilite los servicios innecesarios y elija modos seguros**

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

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

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

10. **Transmisión cifrada de audio y vídeo**

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

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

11. **Auditoría segura**

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

12. **Registro de red**

Debido a la capacidad de almacenamiento limitada del dispositivo, el registro almacenado es limitado. Si necesita guardar el registro durante un período prolongado, se recomienda habilitar la función de registro de red para garantizar que los registros críticos estén sincronizados con el servidor de registro de red para su seguimiento.

13. **Construya un entorno de red seguro**

Para garantizar mejor la seguridad del dispositivo y reducir los posibles riesgos cibernéticos, recomendamos:

- Deshabilite la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa.
- La red debe dividirse y aislarse según las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere utilizar VLAN, red GAP y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts permitidos para acceder al dispositivo.