Solución de control de acceso

SmartPSS Lite

Manual de usuario

V1.1.2

Prefacio

General

Este manual presenta las funciones y operaciones de la solución de control de acceso de la plataforma SmartPSS Lite (en adelante, "la Plataforma"). Lea atentamente antes de utilizar la plataforma 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
	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
	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.
	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
	Proporciona información adicional como complemento al texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.1.2	Se actualizaron las configuraciones de gestión de personas y control de acceso.	enero 2024
V1.1.1	Se actualizó el diseño de la página de inicio.	Septiembre 2023
V1.1.0	● Función de gestión de personas actualizada. ● Función de configuración del controlador de acceso actualizada.	diciembre 2022
V1.0.1	Imagen de visualización del personal actualizada.	agosto 2022
V1.0.0	Primer lanzamiento.	abril 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 otros.

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.

Tabla de contenido

1. Información general

La solución de control de acceso se utiliza con los dispositivos de control de acceso a través de la plataforma SmartPSS Lite, que resulta útil en escenarios pequeños y medianos, como controlar puertas de forma remota y configurar alarmas.

2 Guía de acceso

Puede configurar el control de acceso siguiendo la guía a continuación.

Procedimiento

Paso 1 Seleccionar**Control de acceso**en la barra

Paso 2 izquierda. Hacer clic**Guía**en la página de inicio.

Figura 2-1 Guía de acceso

Gestión de 3 personas

3.1 Agregar empresa

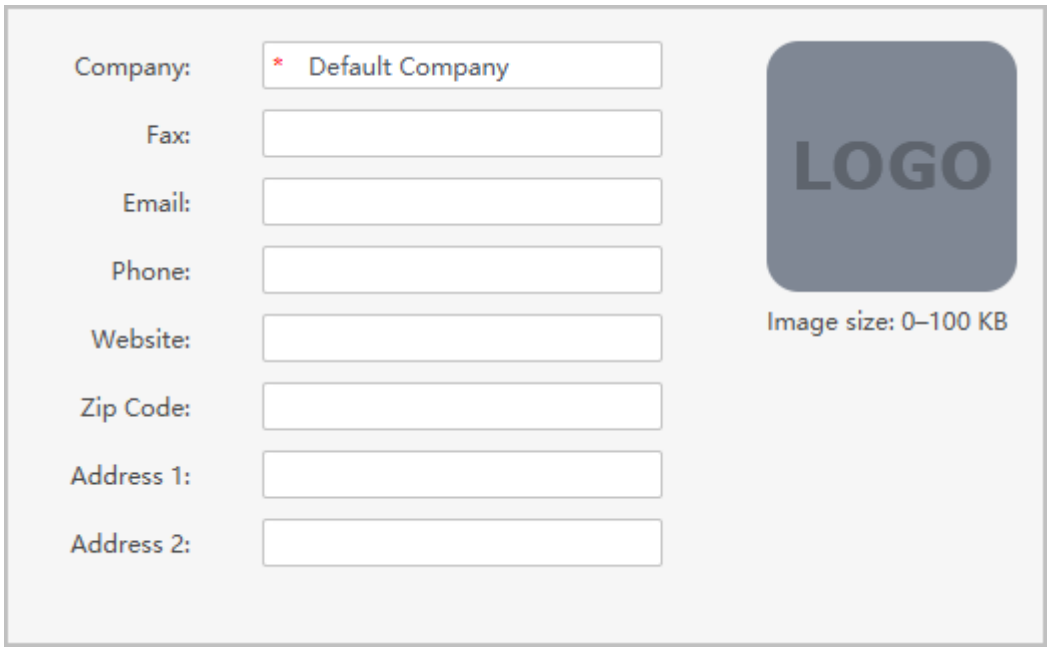
Procedimiento

Paso 1 Seleccionar**Persona**>**Compañía**. Configurar la información

Paso 2 de la empresa. Cargue el logotipo de la empresa y luego

Paso 3 haga clic en**DE ACUERDO**.

Figura 3-1 Agregar empresa



3.2 Agregar persona

Información de contexto

Seleccione uno de los métodos para agregar personal.

- Agregue personal uno por uno manualmente.
- Agregue personal en lotes.
- Extraiga información del personal de otros dispositivos.
- Importar información del personal desde el local.

3.2.1 Agregar departamentos

Procedimiento

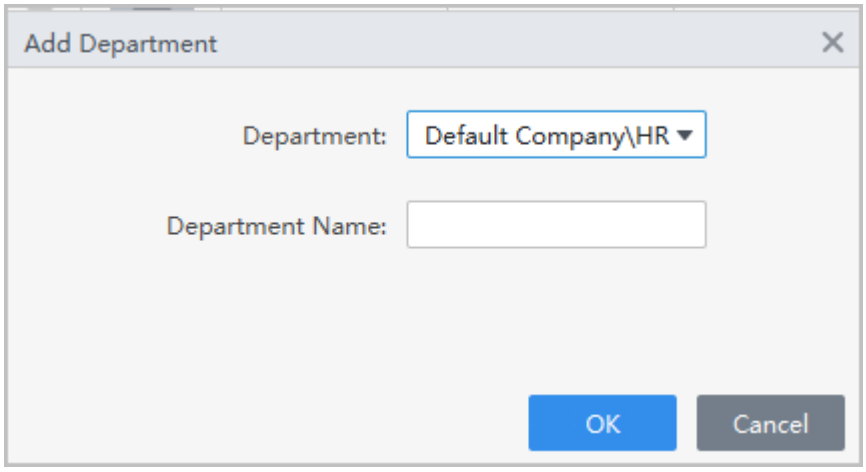
Paso 1 Seleccionar**Persona**>**Gestión de personas**.

Paso 2 En el árbol de organización del departamento, haga clic en .

Paso 3 Seleccione un departamento existente y luego ingrese el nombre del nuevo departamento. Hacer clic**DE**

Etapa 4 **ACUERDO**.

Figura 3-2 Agregar departamentos



Operaciones relacionadas

- Hacer clic para eliminar el departamento. para
- Hacer clic cambiar el nombre del departamento.

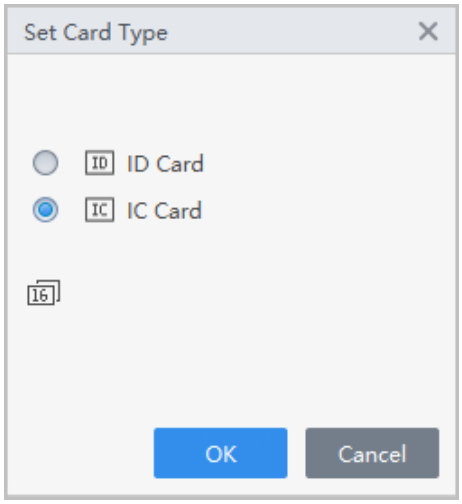
3.2.2 Configuración del tipo de tarjeta

Seleccionar**Persona**>**Gestión de personas**, y luego**Tipo de tarjeta**.

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

El sistema utiliza un número de tarjeta hexadecimal de forma predeterminada. Haga clic en para cambiarlo a tarjeta decimal el número.

Figura 3-3 Establecer tipo de tarjeta



3.2.3 Agregar personal uno por uno

Procedimiento

Paso 1 Seleccionar**Persona**>**Gestión de personas**y luego haga clic en**Agregar**.

Paso 2 Ingrese la información básica de la persona.

1. Seleccione**Información básica**.

2. Agregar información básica del personal.

3. Tome una instantánea o cargue una imagen y luego haga clic en**Finalizar**.

4. Configure los métodos de verificación de identidad.

- Configurar la clave

  Hacer clic**Agregar**para agregar la contraseña. Para los controladores de acceso de segunda generación, establezca contraseñas personales; para otros dispositivos, establezca contraseñas de tarjetas. Las nuevas contraseñas deben constar de 6 a 8 dígitos.

- Configurar tarjeta

  a. Clic para seleccionar**Dispositivo**o**Emisor de la tarjeta**como lector de tarjetas.

  b. Agregar tarjeta.

  C. Después de agregarla, puede seleccionar la tarjeta como tarjeta principal o tarjeta de coacción, reemplazar la tarjeta por una nueva o eliminarla.

  d. Haga clic para mostrar el código QR de la tarjeta.

  Solo el número de tarjeta de 8 dígitos en modo hexadecimal puede mostrar el código QR de la tarjeta.

- Configurar huella digital

  a. Clic para seleccionar**Dispositivo**o**Escáner de huellas dactilares**como recolector de huellas dactilares.

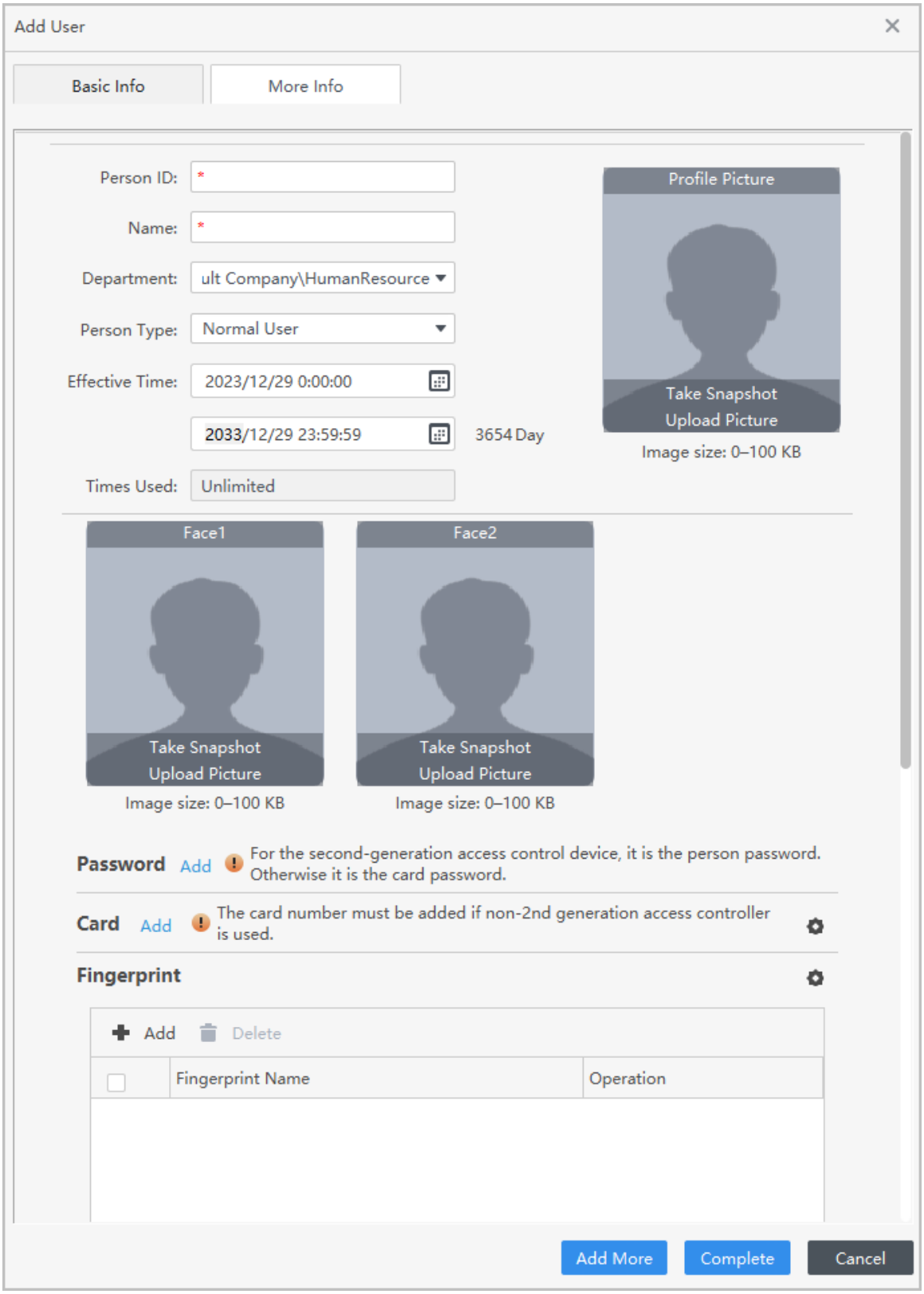
  b. Agregar huella digital. Seleccionar**Agregar**>**Agregar huella digital**y luego presione con el dedo el escáner tres veces seguidas.

- Configurar códigos de característica

  a. Haga clic en y luego seleccione un dispositivo.

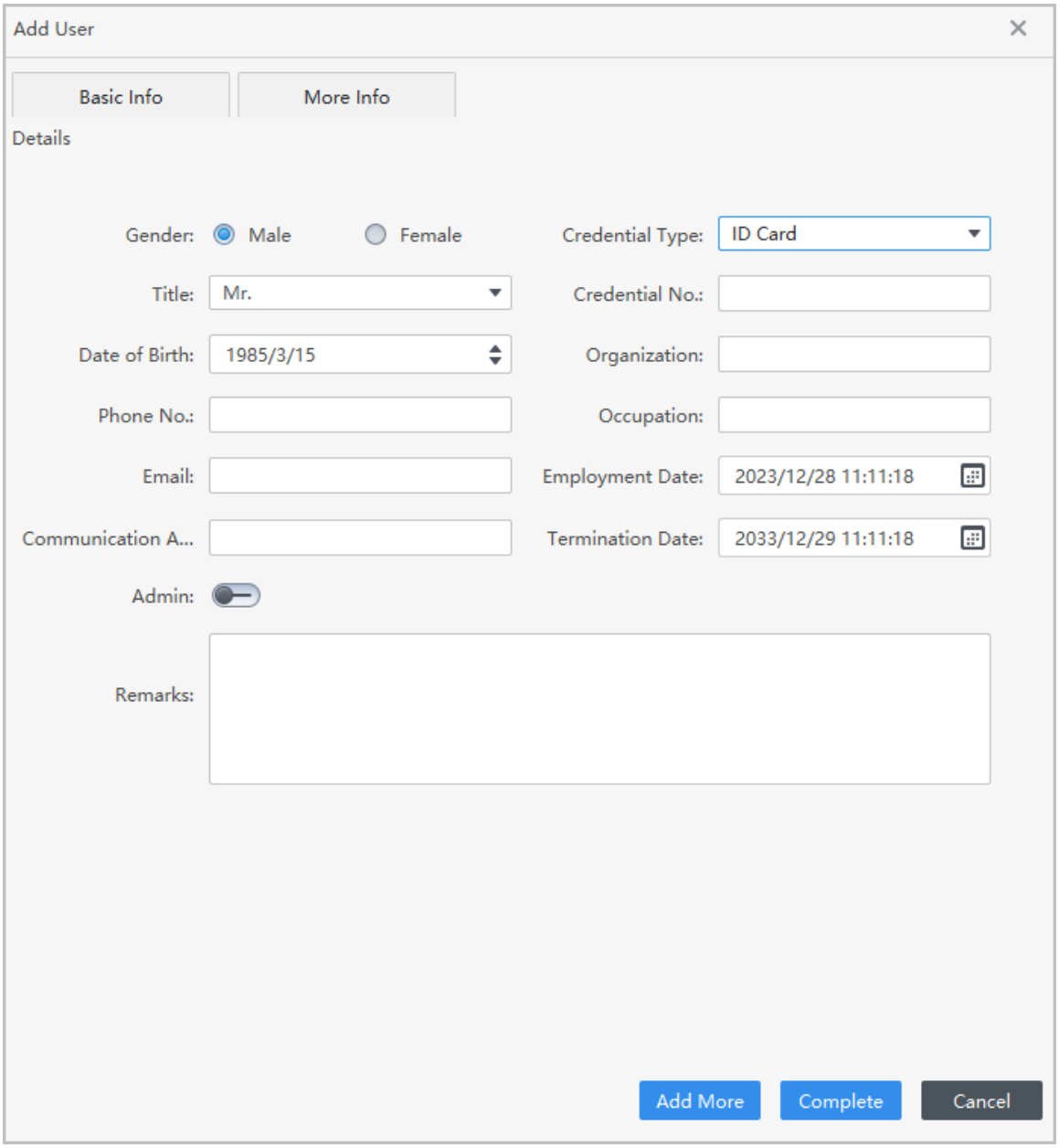
  b. Hacer clic**Extracto**, y luego el dispositivo extraerá los rasgos del rostro.

Figura 3-4 Agregar información básica



Paso 3 Hacer clic**Más información**pestaña para agregar información ampliada del personal y luego haga clic en**Completo**.

Figura 3-5 Agregar más información



Etapa 4 Hacer clic**Completo**.

Después de completar la adición, puede hacer clic en la para modificar información o agregar detalles en la lista persona.

Operaciones relacionadas

- Hacer clic para modificar información o añadir detalles en la lista de personal.
- Hacer clic para eliminar toda la información de la persona.
- Hacer clic para congelar la tarjeta, y luego la tarjeta no se puede utilizar normalmente.

3.2.4 Agregar personal en lotes

Procedimiento

Paso 1 Seleccionar**Persona**>**Gestión de personas**y luego haga clic en**Agregar lote**. Seleccione

Paso 2 el tipo de dispositivo, configure el número de inicio, el número de tarjeta.

Paso 3 Establezca el departamento, la hora de vigencia y la hora de vencimiento de la tarjeta. Hacer

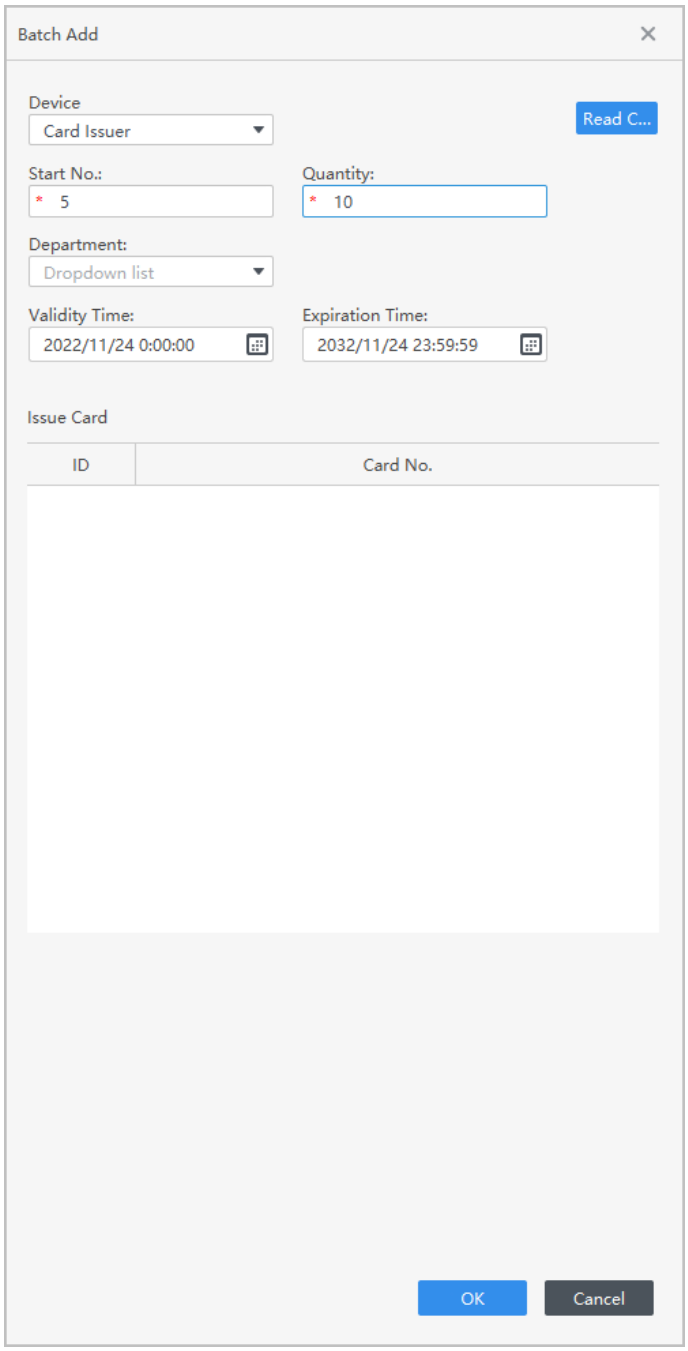
Etapa 4 clic**Leer tarjeta No.**.

Paso 5 Coloque las tarjetas en el emisor de la tarjeta o en el lector de tarjetas.

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

Paso 6 **ACUERDO**.

Figura 3-6 Agregar personal en lotes



3.2.5 Otras operaciones

3.2.5.1 Emisión de tarjetas en lotes

Puede emitir tarjetas al personal que se haya agregado pero que no tenga tarjeta.

Procedimiento

Paso 1 Seleccionar**Persona**>**Gestión de personas**.

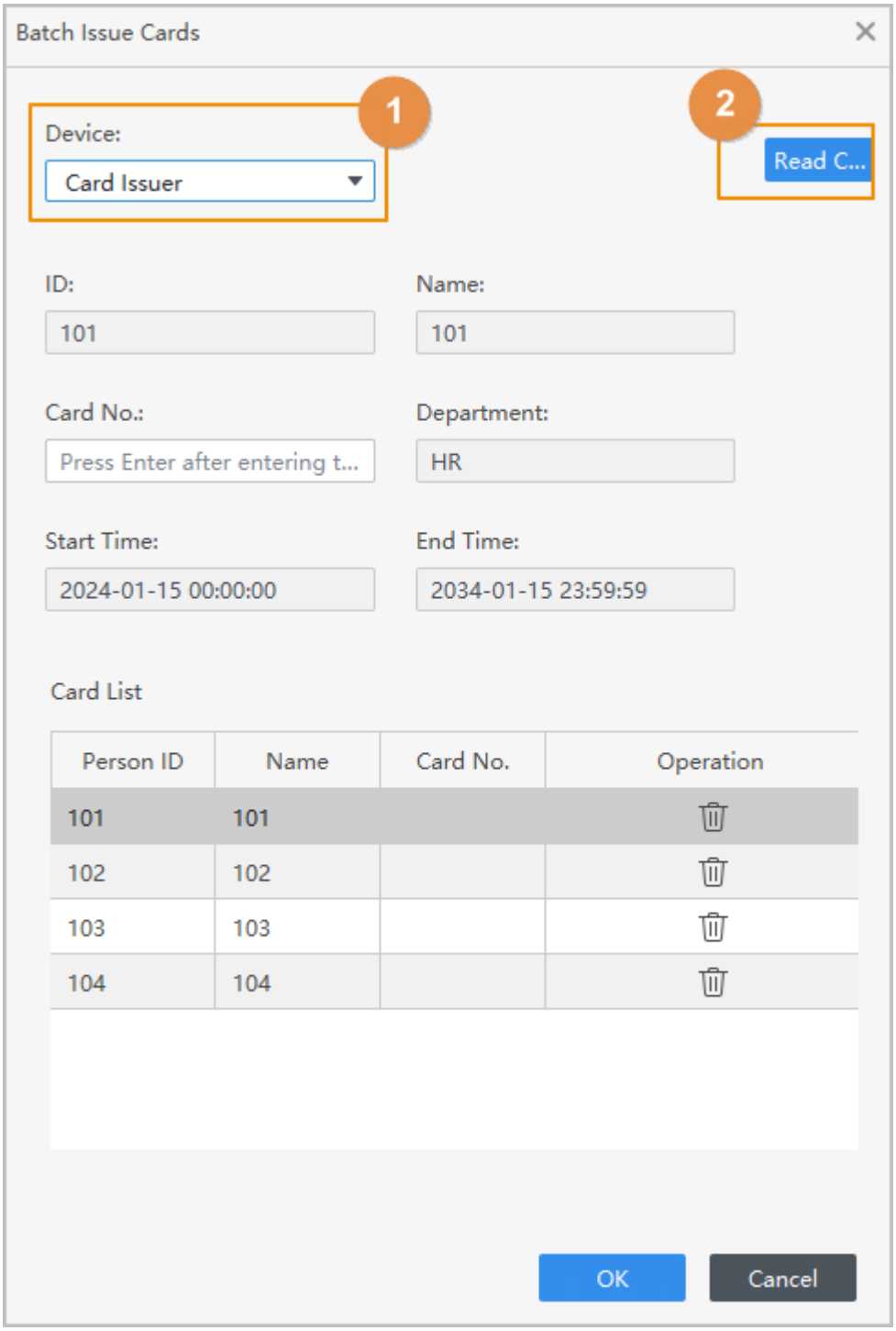
Paso 2 Seleccione personal y luego seleccione**Actualización por lotes**>**Tarjeta de emisión por lotes**.

Paso 3 Emitir tarjeta por lotes. El número de tarjeta puede leerse automáticamente mediante un lector de tarjetas o ingresarse manualmente.

- Utilice el emisor de la tarjeta o el dispositivo lector de tarjetas para leer automáticamente el número de la tarjeta.

  1. Seleccione el emisor de la tarjeta o un dispositivo lector de tarjetas y luego haga clic en**Leer tarjeta No.**.
  2. De acuerdo con la lista de pedidos, coloque en secuencia las tarjetas del personal correspondiente en el área de deslizamiento de tarjetas, y luego el sistema leerá y completará automáticamente el número de tarjeta.

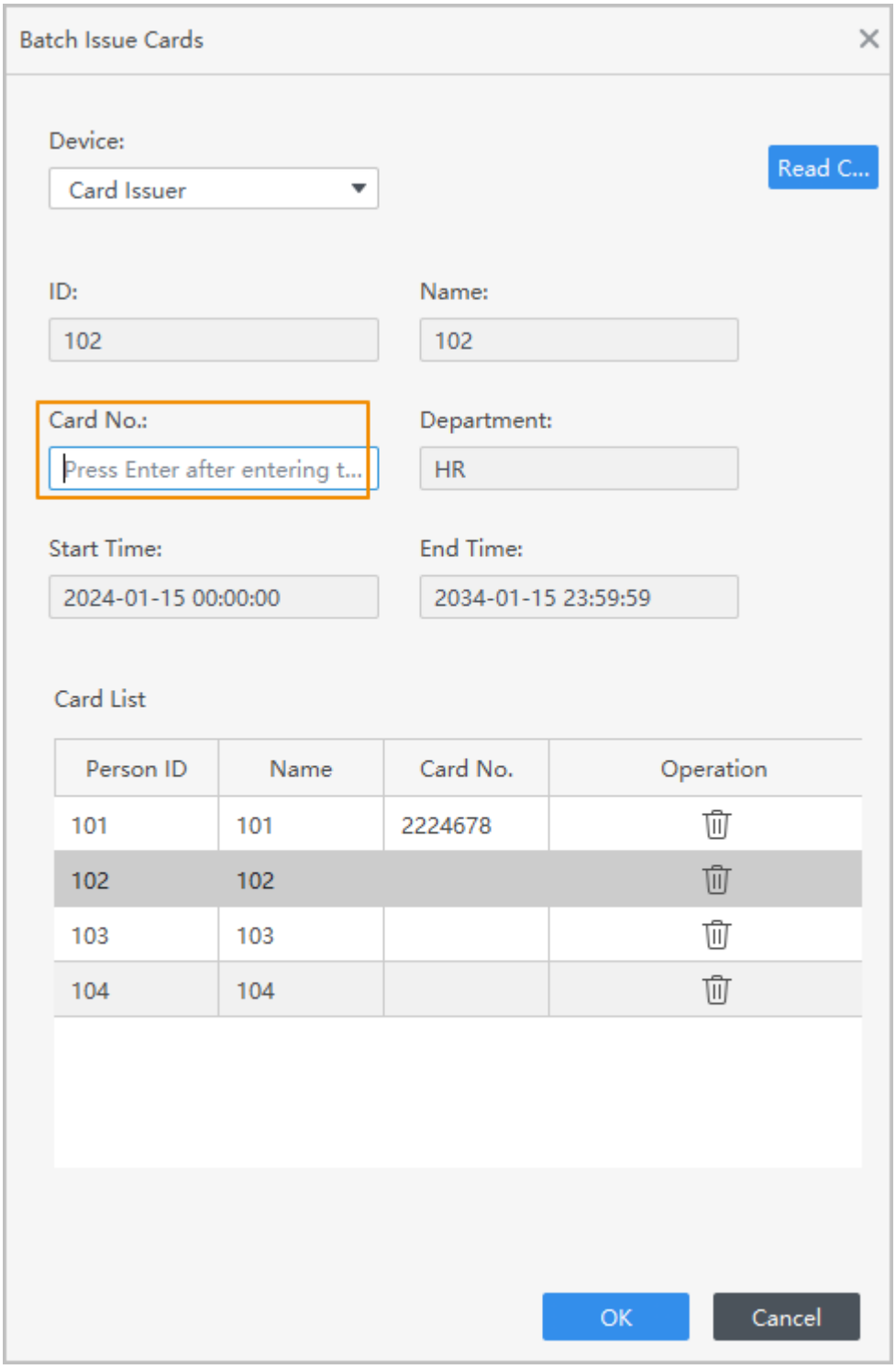
Figura 3-7 Leer automáticamente



- Ingresar manualmente

  1. Seleccione el personal en la lista de tarjetas y luego ingrese el número de tarjeta correspondiente.
  2. Presione el**Ingresar**llave.

Figura 3-8 Ingresar el número de tarjeta manualmente



Etapa 4 Hacer clic**DE ACUERDO**.

3.2.5.2 Extracción de información del personal

Extraiga usuarios de los dispositivos a la plataforma.

Procedimiento

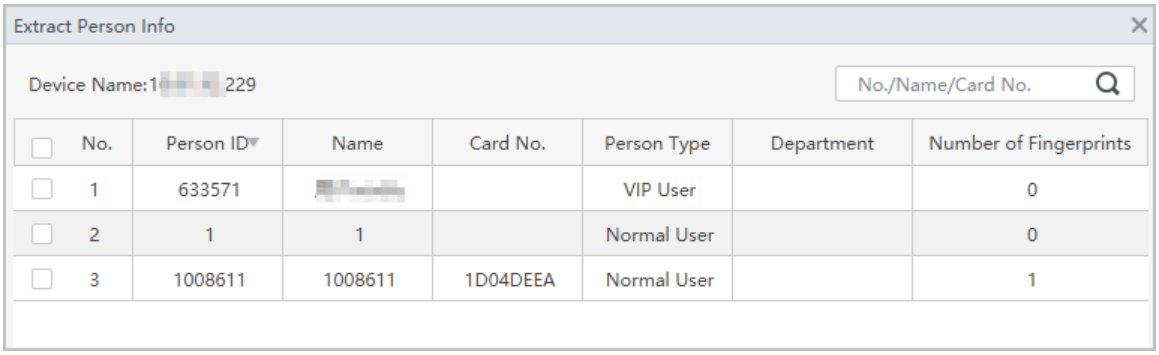
Paso 1 Seleccionar**Persona**>**Gestión de personas**y luego haga clic en**Extracto**

Paso 2 Seleccione un dispositivo y luego haga clic en**DE ACUERDO**.

Puede seleccionar extraer el usuario de**Todo**,**Éxito**o**Falla**en la lista desplegable junto a **Extracto**.

Paso 3 Seleccione personal y luego haga clic en**Extracto**para extraer los usuarios del dispositivo a la plataforma.

Figura 3-9 Extraer usuarios



Resultados

Los usuarios que se extraigan exitosamente de los dispositivos se mostrarán en la**Gestión de personas**página.

3.2.5.3 Importación de información del personal

Importar información del personal a la plataforma.

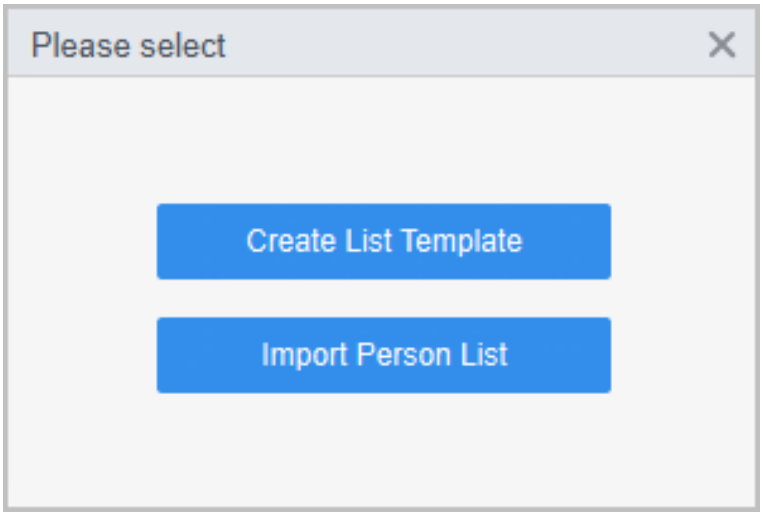
Procedimiento

Paso 1 Hacer clic**Persona**>**Gestión de personas**y luego haga clic en**Importar**.

Paso 2 Hacer clic**Crear plantilla de lista**para descargar una plantilla. Complete la

Paso 3 plantilla y luego haga clic**Importar lista de personas**.

Figura 3-10 Importar información del personal



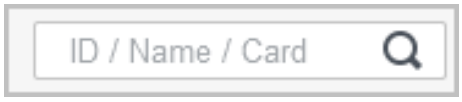
3.2.5.4 Exportación de información del personal

Seleccionar**Persona**>**Gestión de personas**, seleccione personal y luego haga clic en**Exportar**para exportar información del personal a su computadora.

3.2.5.5 Búsqueda de personal

Seleccionar**Persona**>**Gestión de personas**, busca personal por DNI, nombre o tarjeta.

Figura 3-11 Búsqueda de personal



3.2.5.6 Pantalla de personal

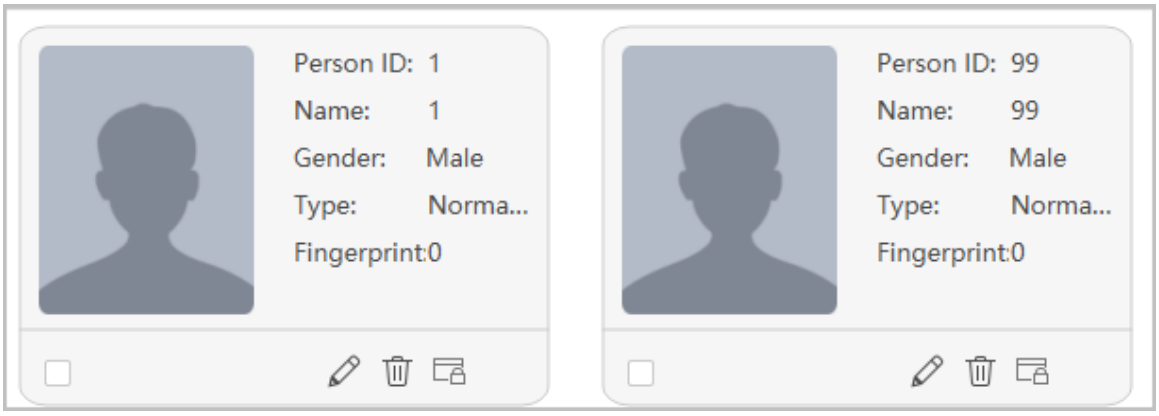
Puede seleccionar modos de visualización: visualización de tarjeta y visualización de lista.

Hacer clic para exhibir en tarjetas; hacer clic para mostrar en la lista. Figura

3-12 Mostrar en la lista

Image	Person ID	Name	Person Type	Department	Verification Method	Operation
	1	1	Normal User	Default Compa...	1 0 0 0	
	99	99	Normal User	HR	0 0 0 0	
	100	100	Normal User	HR	0 1 0 0	

Figura 3-13 Visualización en tarjeta



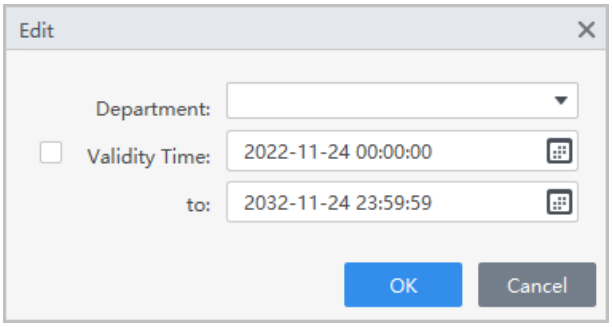
3.2.5.7 Edición de personal en lotes

Procedimiento

Paso 1 Seleccionar**Persona**>**Gestión de personas**.

Paso 2 Seleccione personal y luego seleccione**Actualización por lotes**>**Edición por lotes**para editar departamento y período de validez en lotes.

Figura 3-14 Editar departamento



3.3 Colección de personas

Cuando se actualiza la información del usuario o se agregan nuevos usuarios, el dispositivo de control de acceso enviará automáticamente la información del usuario a la plataforma de administración.

Requisitos previos

La función de inserción de información de la persona está habilitada en el dispositivo de control de acceso.

Esta función solo está disponible en modelos seleccionados de dispositivo de control de acceso.

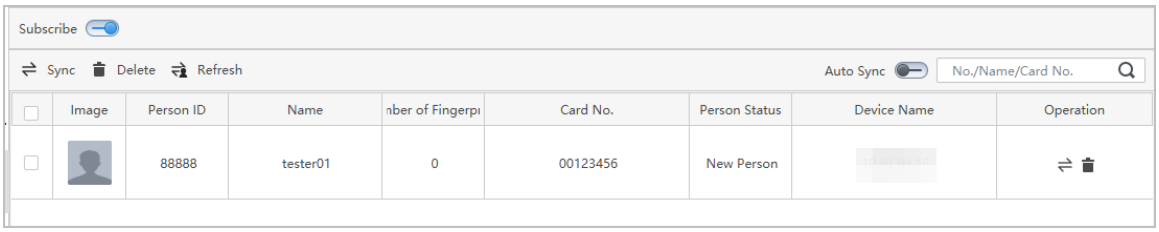
Procedimiento

Paso 1 Seleccionar**Persona**>**Colección de personas**.

Paso 2 Encender**Suscribir**.

Paso 3 Si agregó un nuevo usuario o modificó la información del usuario en el dispositivo de control de acceso, el usuario será enviado automáticamente a la plataforma de administración.

Figura 3-15 Suscribir usuarios



Etapa 4 Puedes hacer clic para sincronizar el usuario con la página de administración de personas.

Si el usuario que es enviado a la plataforma tiene la misma identificación personal o la misma tarjeta que cualquier usuario existente en la**Gestión de personas**página, el sistema generará un conflicto información. Puedes hacer clic para ver detalles.

Figura 3-16 Conflicto de ID de persona

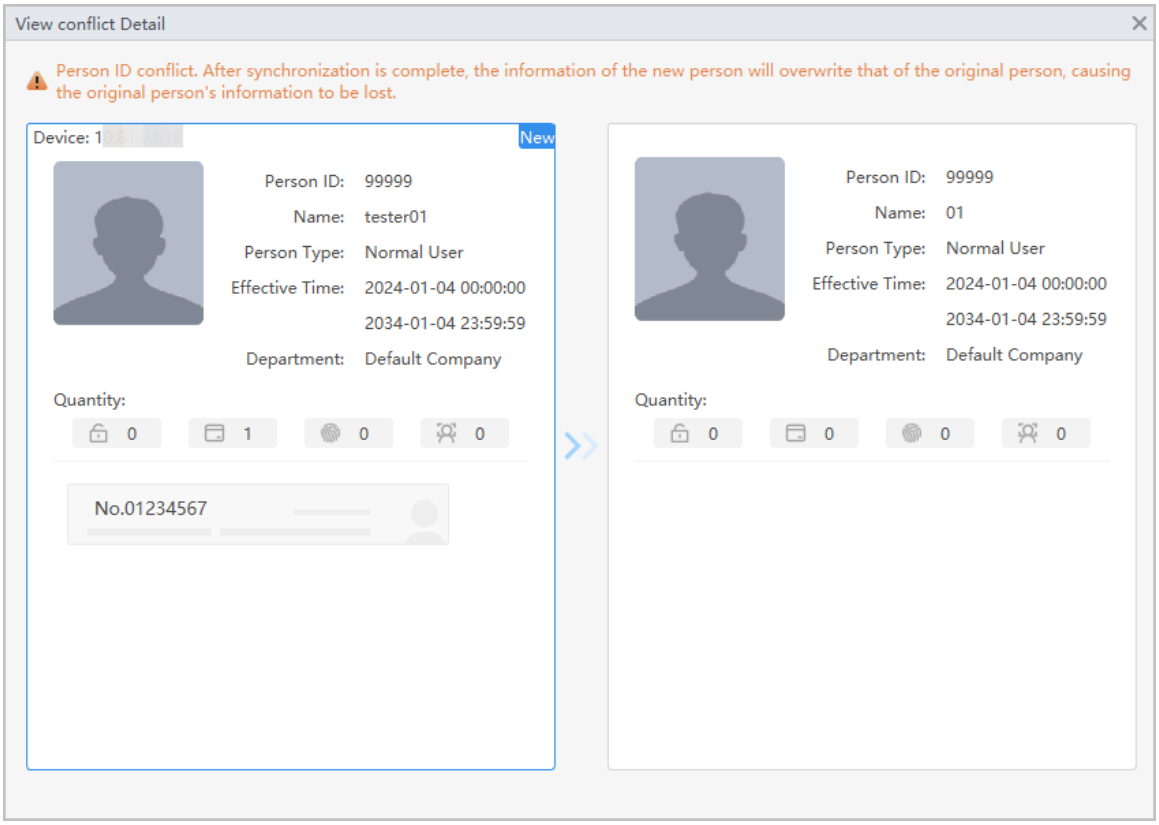


Figura 3-17 Conflicto de número de tarjeta

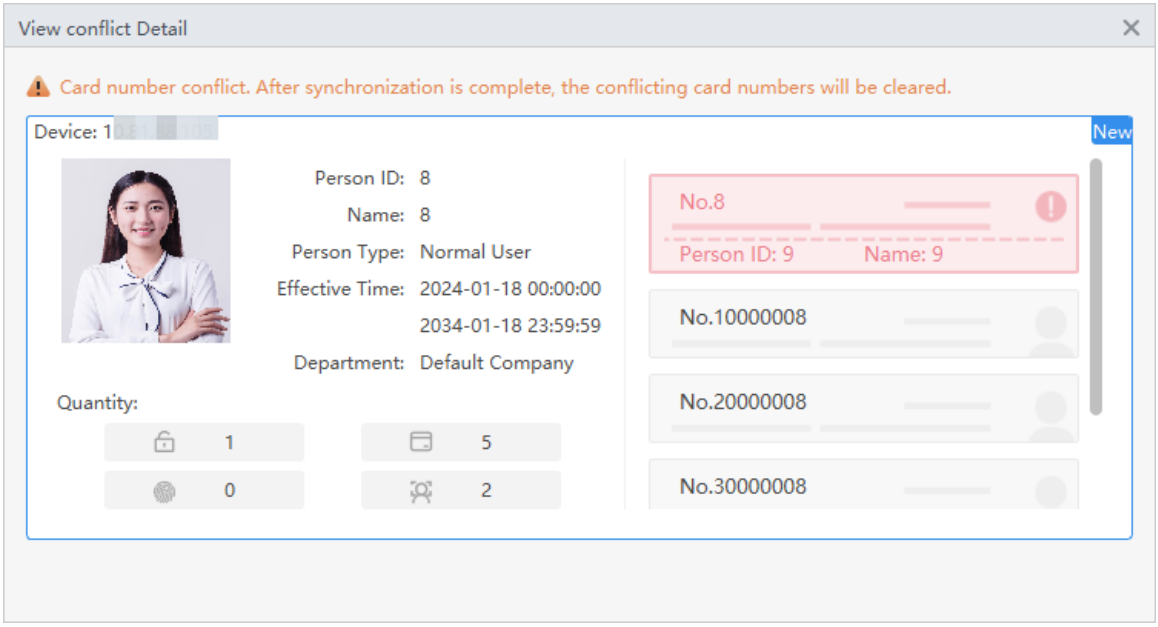
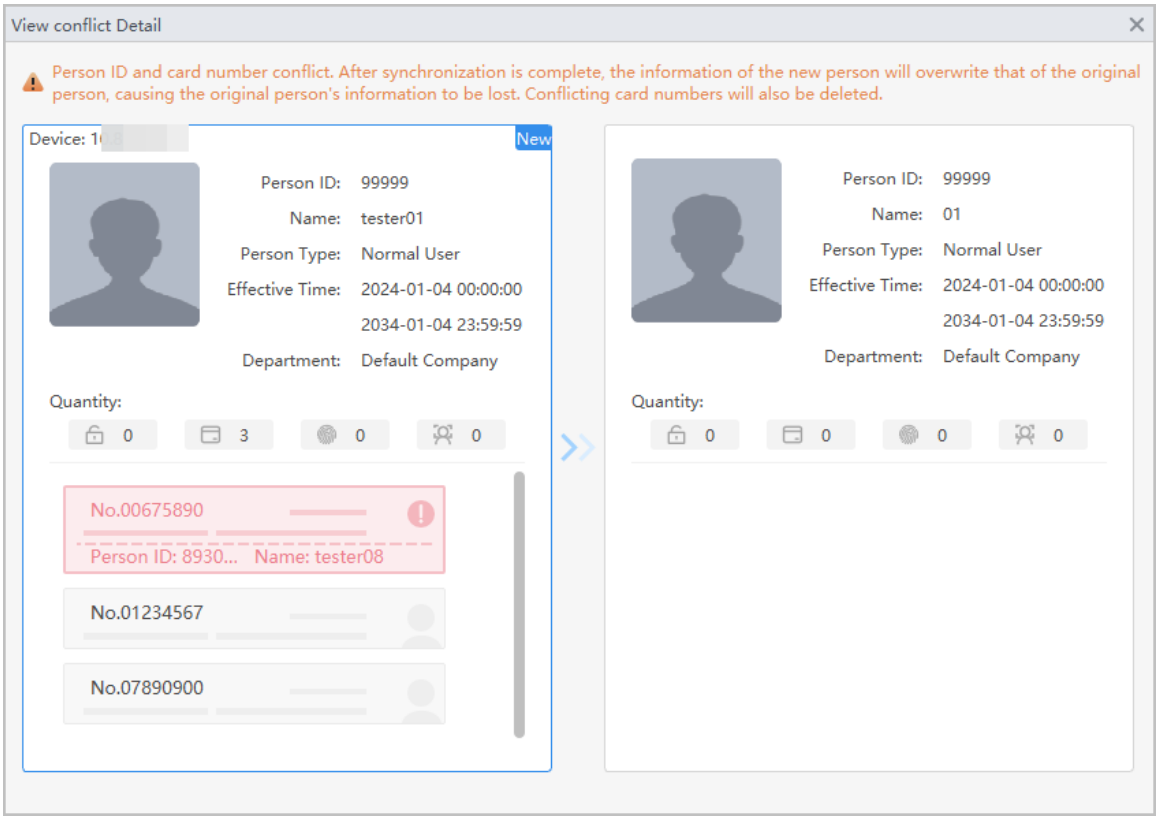


Figura 3-18 Conflicto entre ID de persona y número de tarjeta



Operaciones relacionadas

- Sincronizar usuarios en lotes: seleccione usuarios y luego haga clic en**Sincronizar**,Los usuarios seleccionados se sincronizarán automáticamente con**Gestión de personas**página.
- Sincronizar usuarios automáticamente: Habilitar**Sincronización automática**,Si los usuarios que ingresan a la plataforma no tienen la misma identificación personal o la misma tarjeta que ningún usuario existente en la**Gestión de personas**página, y los usuarios se sincronizarán automáticamente con**Gestión de personas** página.
- Actualizar: actualiza a los usuarios con información de conflicto.

4 Configuración de permisos

4.1 Agregar áreas de permiso

Un área es una colección de permisos de acceso a puertas. Cree un área y luego vincule a los usuarios al área para que puedan obtener los permisos de acceso establecidos para el área.

Procedimiento

Paso 1 Seleccionar**Configuración de control de acceso**>**Configuración de área**.

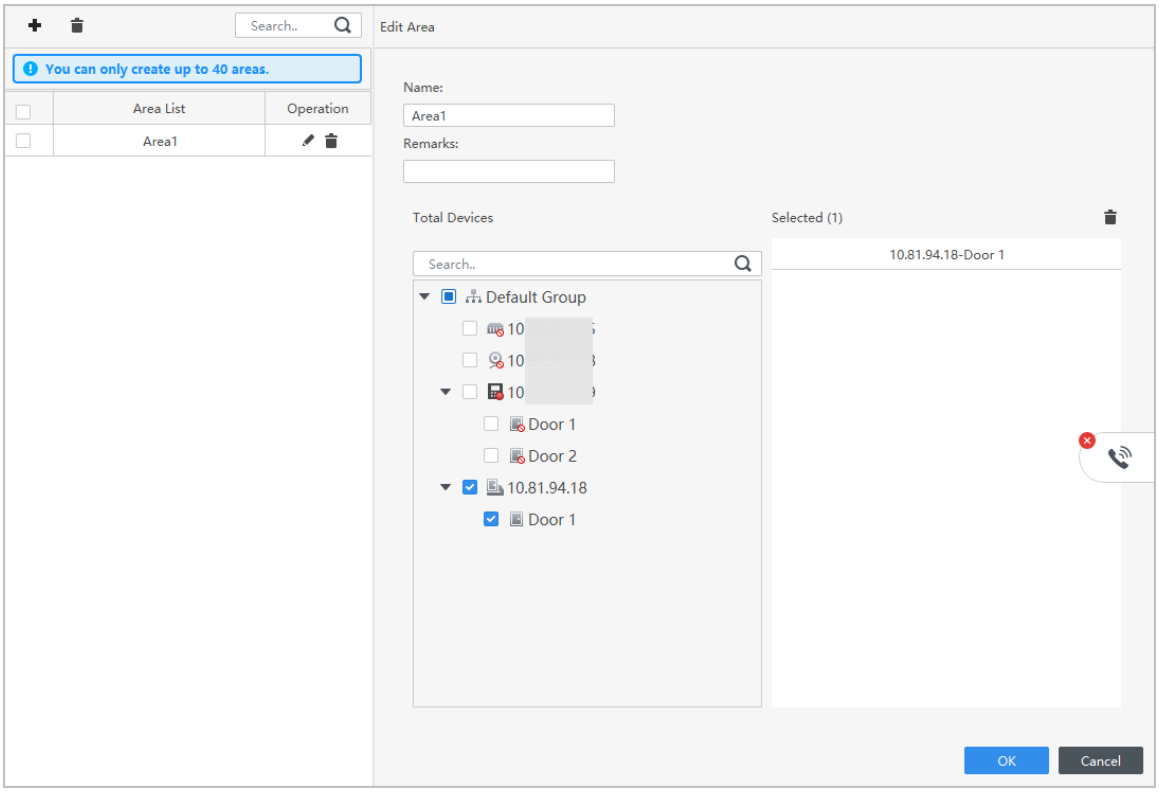
Paso 2 Haga clic para agregar un área de permiso.

Puedes agregar hasta 40 áreas.

Paso 3 Configure el área de permisos.

1. Ingrese el nombre del área y el comentario.
2. Seleccione canales de puerta, como la puerta 1.
3. Haga clic**DE ACUERDO**.

Figura 4-1 Agregar área de permiso



Operaciones relacionadas

- : Elimina el área de permiso.
- : Modifica la información del área.

4.2 Asignación de permisos

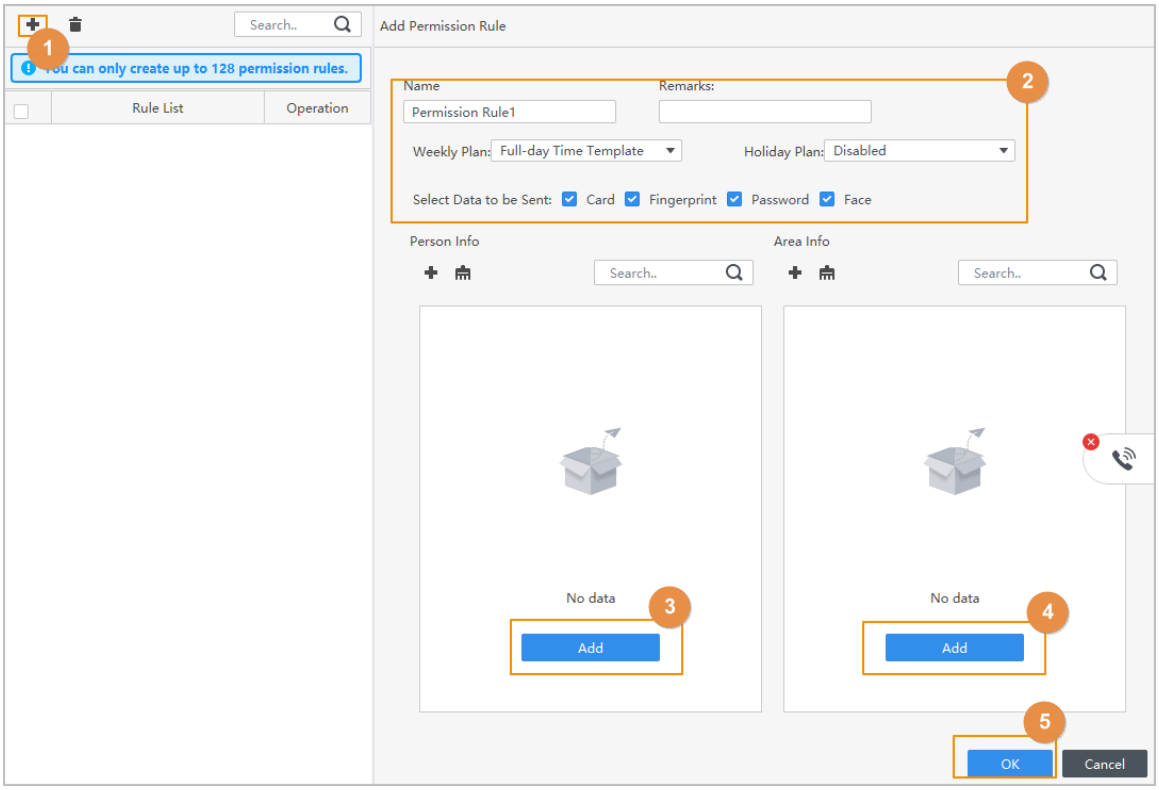
El método para configurar permisos para el departamento y el personal es similar y aquí se utiliza el departamento como ejemplo.

Procedimiento

Paso 1 Seleccionar**Configuración de control de acceso**>**Configuración de permisos**. Haga

Paso 2 clic para agregar una regla de permiso.

Figura 4-2 Asignar reglas de permisos



Paso 3 Ingrese el nombre de la regla de permiso, seleccione el plan de tiempo y los métodos de desbloqueo. En el**Información de**

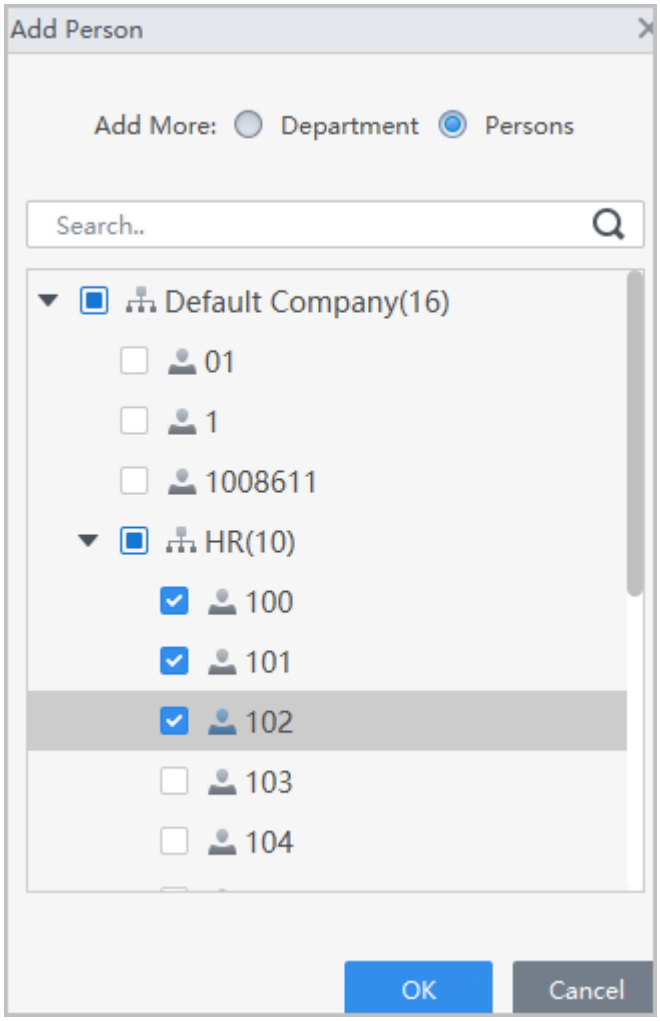
Etapa 4 **la persona**área, haga clic**Agregar**para seleccionar personal y luego haga clic en**DE ACUERDO**.

Puede seleccionar personal del departamento o usuarios individuales.

- Departamento: A todo el personal del departamento se le asignarán permisos de acceso.
- Usuario: Solo a los usuarios seleccionados se les asignarán permisos de acceso.

Cuando desee asignar permiso a una nueva persona o cambiar los permisos de acceso para una persona existente, simplemente puede agregar el usuario a un departamento existente o vincularlo con un rol existente; se le asignarán automáticamente los permisos de acceso establecidos para el departamento o rol. .

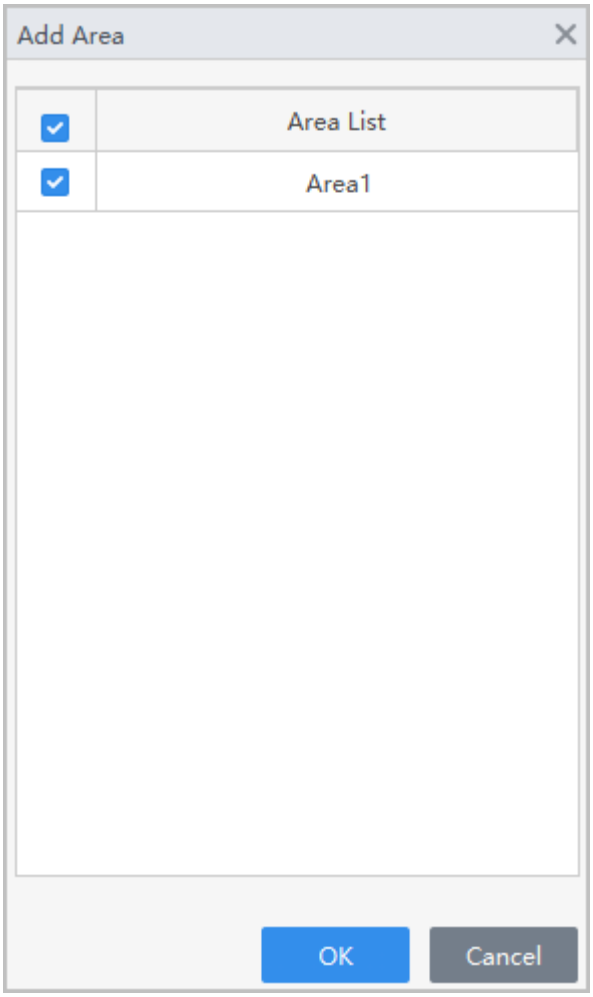
Figura 4-3 Agregar usuarios



Puedes hacer clic + para crear nuevas áreas de permiso. Para obtener detalles sobre la creación de áreas de permiso, consulte "4.1 Agregar áreas de permiso".

Paso 5 En el**Información del área**,hacer clic**Agregar**para seleccionar un área y luego haga clic en**DE ACUERDO**.

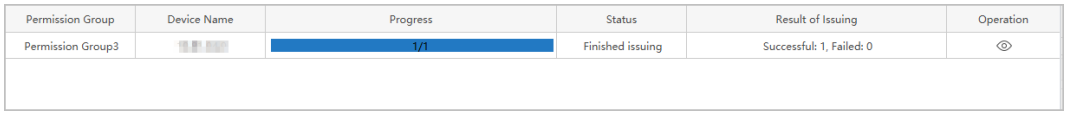
Figura 4-4 Agregar área



Paso 6 Hacer clic**DE ACUERDO**.

Paso 7 Si la autorización falló, haga clic en en la lista para ver el posible motivo.

Figura 4-5 Progreso de la autorización



4.3 Ver el progreso de la autorización

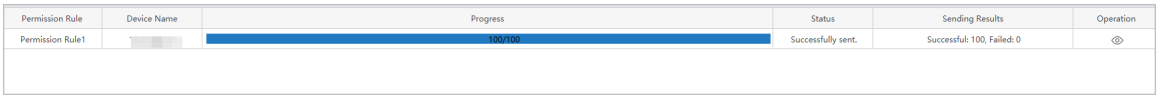
Después de asignar permisos de acceso a los usuarios, puede ver el proceso de autorización.

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración de control de acceso**>**Progreso de la autorización**.

Paso 2 Ver el progreso de la autorización.

Figura 4-6 Progreso de la autorización



Paso 3 (Opcional) Si la autorización falló, puede hacer clic en las  para ver detalles sobre el error tareas de autorización y reenviarlas.

5 Configuración de plantilla de tiempo

5.1 Agregar planes semanales

El plan semanal se utiliza para establecer el calendario de desbloqueo para la semana. La plataforma ofrece una plantilla predeterminada con un horario diurno completo. También puedes crear tus propias plantillas.

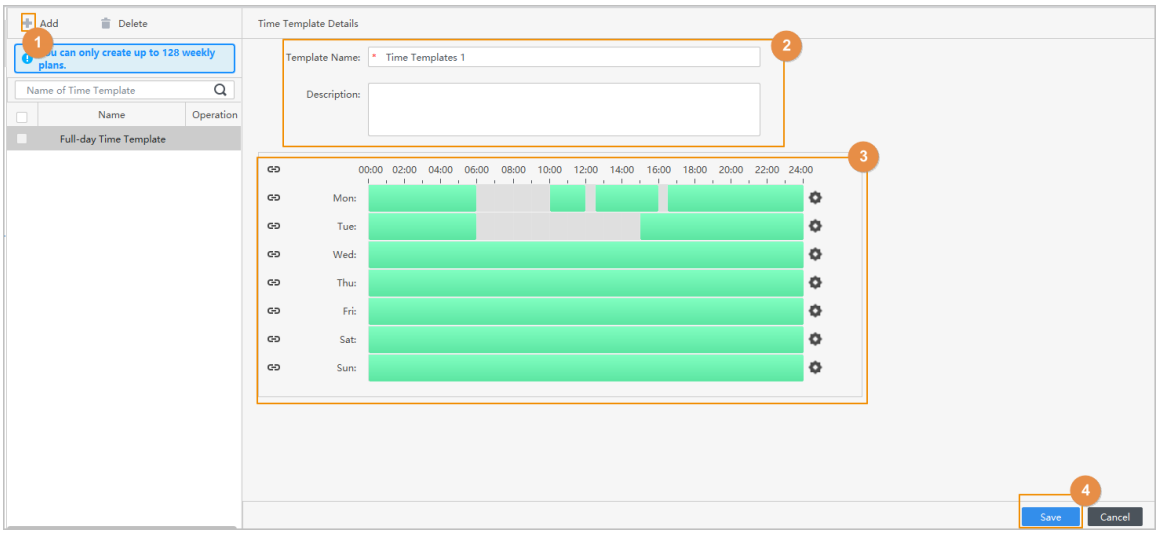
Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración de control de acceso**>**Plan semanal**y luego haga clic en .

- La plantilla de tiempo predeterminada de día completo no se puede modificar.
- Puedes crear hasta 128 planes semanales.

Paso 2 Ingrese el nombre de la plantilla de tiempo.

Figura 5-1 Crear el plan semanal



Paso 3 Ajuste el período de tiempo para cada día.

- Cuando el puntero del mouse se convierte en un bolígrafo, puede mantenerlo presionado y arrastrarlo para seleccionar un rango de tiempo.
- Cuando el puntero del mouse se convierte en un borrador, puede mantener presionado y arrastrar para cancelar la selección de un rango de tiempo.

También puedes hacer clic para aplicar el periodo de tiempo configurado a otros días.

Sólo puedes configurar hasta 4 tramos horarios para cada día.

Etapa 4 Hacer clic**Ahorrar**.

5.2 Agregar planes de vacaciones (opcional)

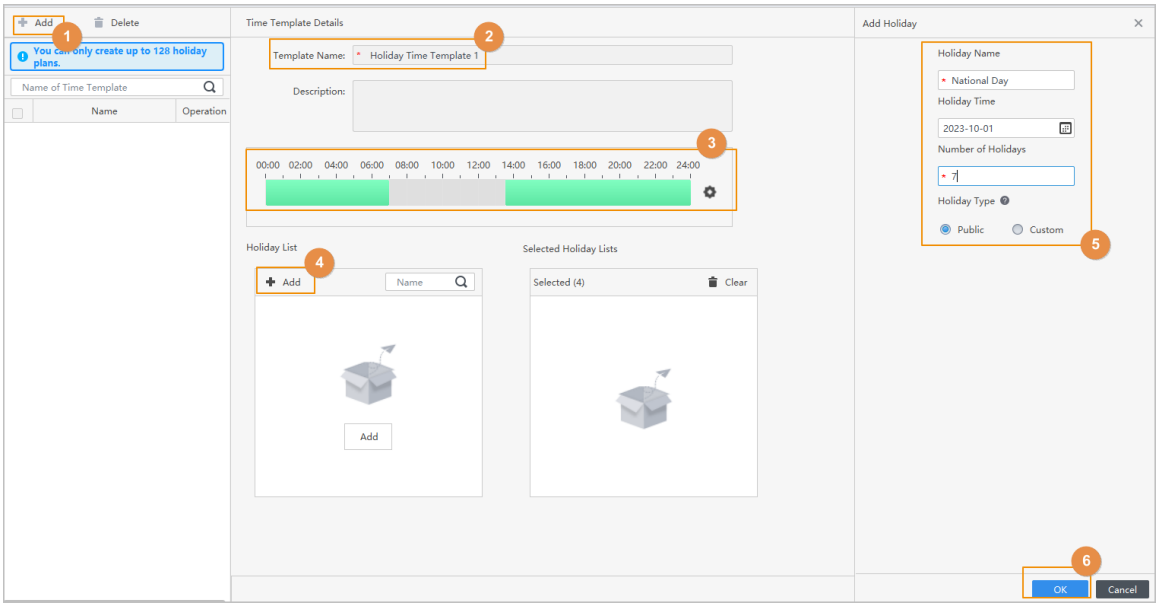
El plan de vacaciones se utiliza para establecer los horarios de desbloqueo para los días festivos.

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración de control de acceso**>**Plan de vacaciones**y luego haga clic en .

Puede crear hasta 128 planes de vacaciones.

Figura 5-2 Crear plan de vacaciones



Paso 2 Introduzca el nombre del plan de vacaciones.

Paso 3 Ajuste el período de tiempo para cada día.

- Cuando el puntero del mouse se convierte en un bolígrafo, puede mantenerlo presionado y arrastrarlo para seleccionar un rango de tiempo.
- Cuando el puntero del mouse se convierte en un borrador, puede mantener presionado y arrastrar para cancelar la selección de un rango de tiempo.

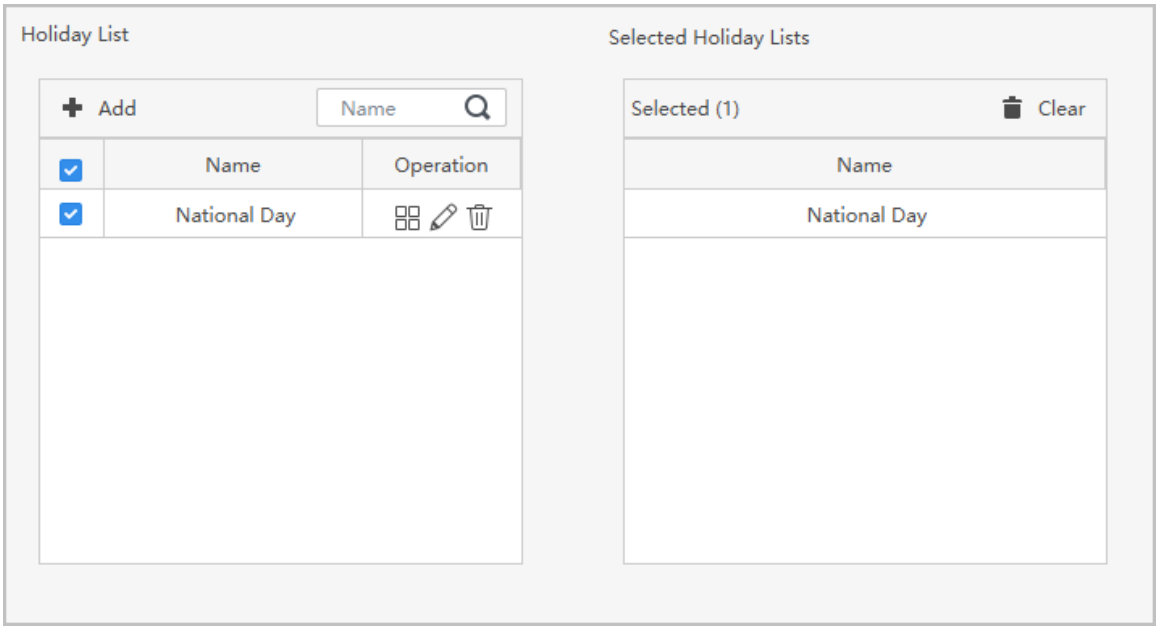
Sólo puedes configurar hasta 4 tramos horarios para cada día.

Etapa 4 Hacer clic**Agregar**para agregar días festivos al plan de vacaciones y luego haga clic en**DE ACUERDO**.

- Público: Las vacaciones se compartirán con todos sus planes de vacaciones.
- Personalizado: las vacaciones solo se utilizan en el plan de vacaciones actual.

Paso 5 Seleccione días festivos y luego haga clic en**Aplicar**.

Figura 5-3 Seleccionar días festivos



6 Configuración de funciones avanzadas

6.1 Configurar el desbloqueo de la primera tarjeta

Defina a ciertas personas como los primeros titulares de la tarjeta; otros usuarios pueden verificar sus identidades para desbloquear la puerta solo después de que los primeros titulares de la tarjeta verifiquen sus identidades primero.

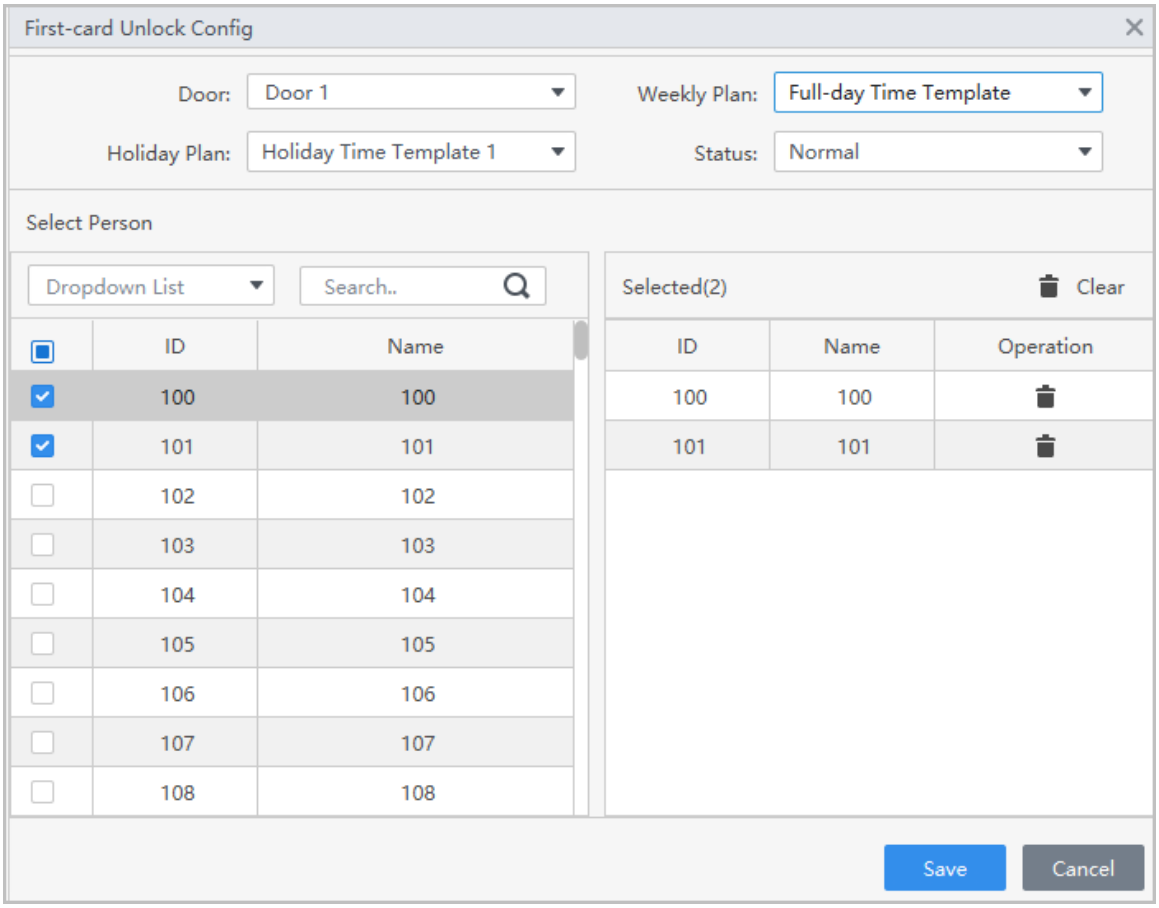
Procedimiento

Paso 1 Seleccionar**Configuración de control de acceso**>**Desbloqueo de primera tarjeta**.

Paso 2 Hacer clic**Agregar**.

Paso 3 Seleccione un canal de puerta.

Figura 6-1 Agregar titulares de primera tarjeta



Etapa 4 Selecciona el plan semanal y el plan vacacional.

La primera tarjeta es válida sólo durante el tiempo definido.

Paso 5 Seleccione el estado de la puerta.

- Normal: los usuarios que no son de primera tarjeta deben verificar sus identidades para desbloquear la puerta después de que los usuarios de primera tarjeta otorgan acceso en el controlador de acceso.
- Normalmente abierta: la puerta permanece abierta después de que los usuarios con la primera tarjeta otorgan acceso al controlador de acceso.

Paso 6 Seleccione usuarios de primera tarjeta y luego haga clic en**Ahorrar**.

6.2 Configurar el desbloqueo de múltiples tarjetas

Los usuarios deben verificar sus identidades en el controlador de acceso en una secuencia establecida antes de que se desbloquee la puerta.

Información de contexto

No recomendamos agregar usuarios de primera tarjeta a grupos de desbloqueo de varias personas.

Procedimiento

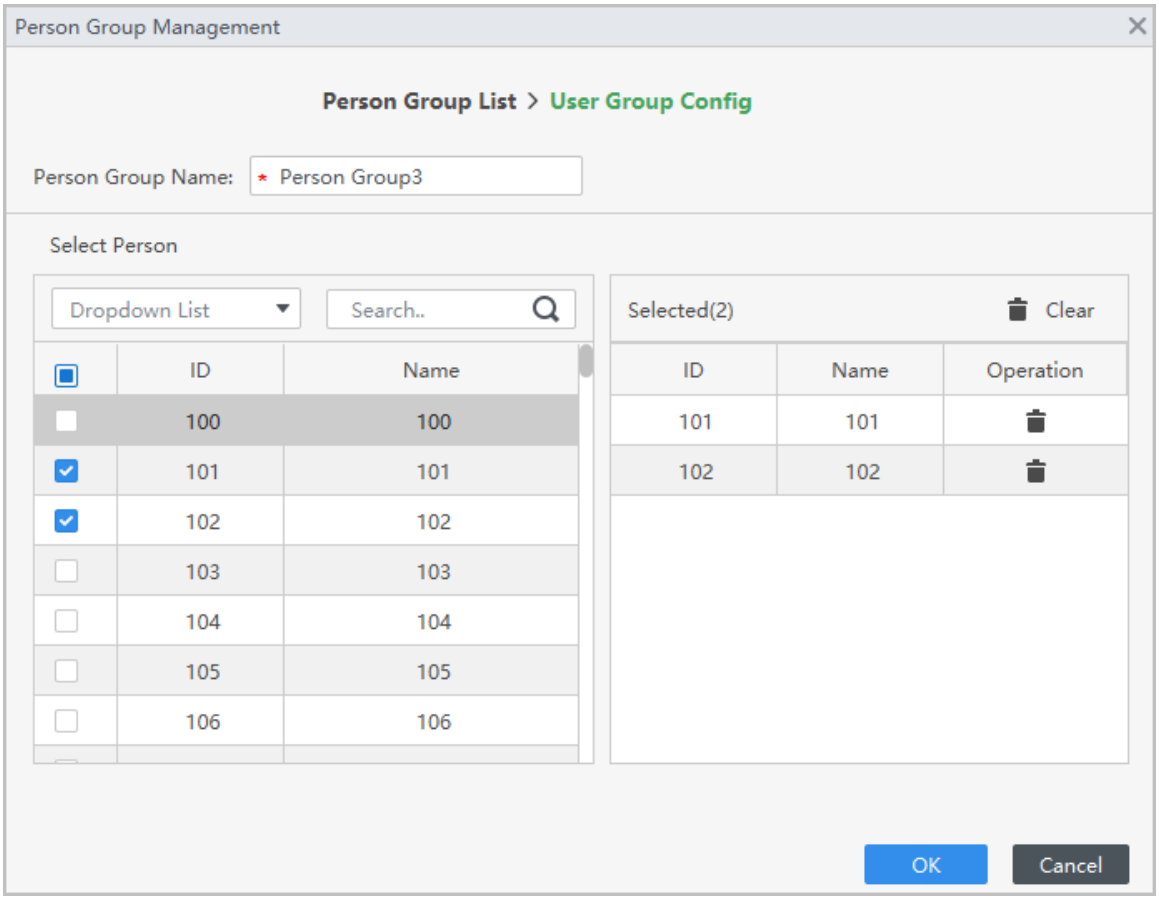
Paso 1 Seleccionar**Configuración de control de acceso**>**Desbloqueo multitarjeta**.

Paso 2 Hacer clic**Agregar**para agregar puertas a la lista de dispositivos.

Paso 3 Hacer clic**Grupo de personas**,y luego haga clic**Agregar**para agregar grupos de desbloqueo multipersona.

1. Crea un nombre para el grupo.
2. Seleccione usuarios de departamentos o roles.
3. Haga clic**DE ACUERDO**.

Figura 6-2 Agregar grupos

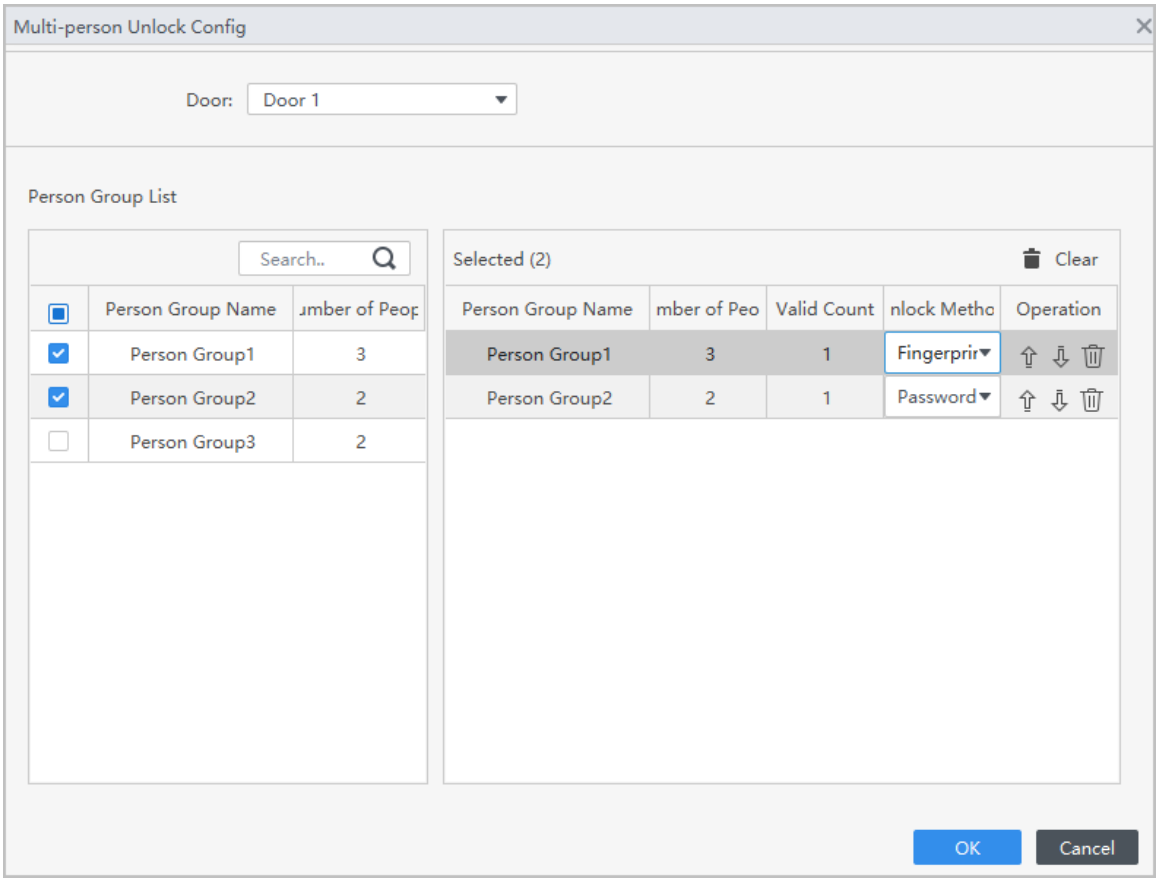


Etapa 4 Hacer clic Add y seleccione una puerta.

Paso 5 Seleccione grupos y luego haga clic**DE ACUERDO**.

Puedes agregar hasta 4 grupos por cada puerta. Cada grupo puede tener hasta 50 usuarios.

Figura 6-3 Configurar el desbloqueo para varias personas



Paso 6 Configure los parámetros de desbloqueo múltiple. 1.

Ingrese el recuento válido.

El recuento válido indica la cantidad de personas de cada grupo que necesitan verificar sus identidades en el controlador de acceso antes de que se desbloquee la puerta. Por ejemplo, si el recuento válido se establece en 2 para un grupo, 2 personas cualesquiera del grupo deberán verificar sus identidades para desbloquear la puerta.

El número válido oscila entre 1 y 5 en cada grupo.

2. Seleccione el método de desbloqueo.

Los usuarios del grupo deben verificar sus identidades a través de los métodos de desbloqueo definidos.

3. (Opcional) Haga clic en o para cambiar la secuencia de grupos.

Si se agregan más de un grupo, los usuarios deben verificar sus identidades de acuerdo con la secuencia definida de grupos.

Paso 7 Hacer clicDE ACUERDO.

6.3 Anti-passback

6.3.1 Configurar Anti-passback

Los usuarios deben verificar sus identidades tanto para entrar como para salir; de lo contrario, se activará una alarma anti-passback. Evita que el titular de una tarjeta pase una tarjeta de acceso a otra persona para que obtenga

entrada. Cuando el anti-passback está habilitado, el titular de la tarjeta debe abandonar el área segura antes de que el sistema le permita otra entrada.

Información de contexto

- Si una persona entra después de haber sido autorizada y sale sin estar autorizada, se activará una alarma cuando intente ingresar nuevamente y al mismo tiempo se le negará el acceso.
- Si una persona sin estar autorizada y sale después de haber sido autorizada, se activará una alarma cuando intente ingresar nuevamente y al mismo tiempo se le negará el acceso.

Procedimiento

Paso 1 Seleccionar**Configuración de control de acceso**>**Anti-retroceso**.

Paso 2 Hacer clic**Anti-pase hacia atrás**y luego haga clic en**Agregar**.

Paso 3 Seleccione un dispositivo de control de acceso y luego ingrese un nombre para el grupo anti-passback.

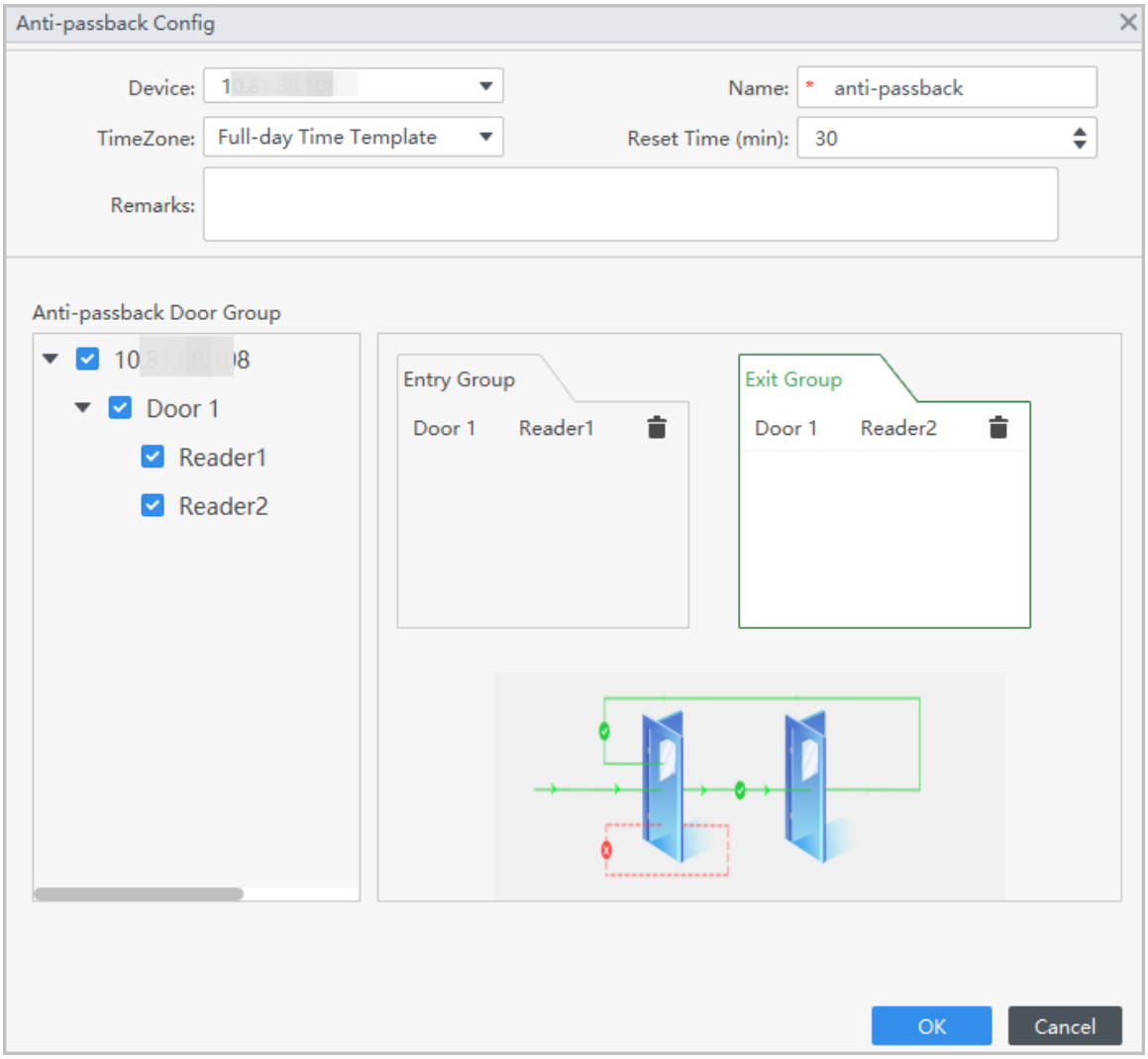
Etapa 4 Seleccione una zona horaria.

El anti-passback es efectivo durante el tiempo definido. Introduzca

Paso 5 el tiempo de reinicio.

Especifique una hora en la que se restablecerá el estado anti-passback de todo el personal. Por ejemplo, si el tiempo de reinicio se establece en 30 minutos, cuando una persona ingresa después de haber sido autorizada y sale sin autorización, si intenta ingresar nuevamente en 30 minutos, se activará una alarma anti-passback.

Figura 6-4 Configurar anti-passback



Paso 6 Seleccione el grupo de entrada y luego seleccione lectores de tarjetas. Seleccione el

Paso 7 grupo de salida y luego seleccione lectores de tarjetas. (Opcional) Puedes hacer clic

Paso 8 **Agregar nuevo grupo**para agregar más grupos.

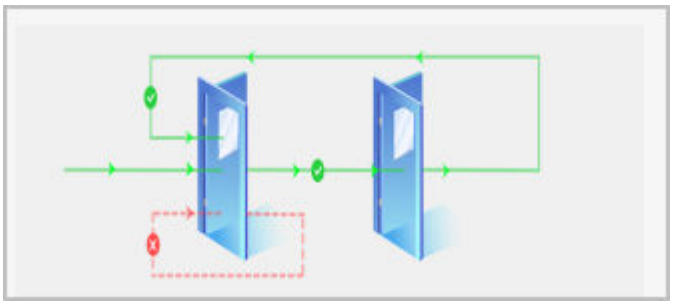
Puede agregar más de un lector a un grupo y los usuarios pueden deslizar el dedo hacia cualquiera de los lectores para obtener acceso.

Paso 9 Hacer clic**Aplicar**.

Resultados

El número de grupo indica la secuencia de tarjetas magnéticas. La tarjeta debe utilizarse siguiendo la secuencia específica de grupos. Por ejemplo, debe pasar la tarjeta en un lector del grupo de entrada 1 y luego en un lector del grupo de salida 2. Siempre que pase la tarjeta siguiendo la secuencia establecida, el sistema funciona bien.

Figura 6-5 Función anti-passback



6.3.2 Configuración del Anti-passback global

Los usuarios deben verificar sus identidades en los dispositivos siguiendo la secuencia establecida; de lo contrario, se activará una alarma anti-passback.

Procedimiento

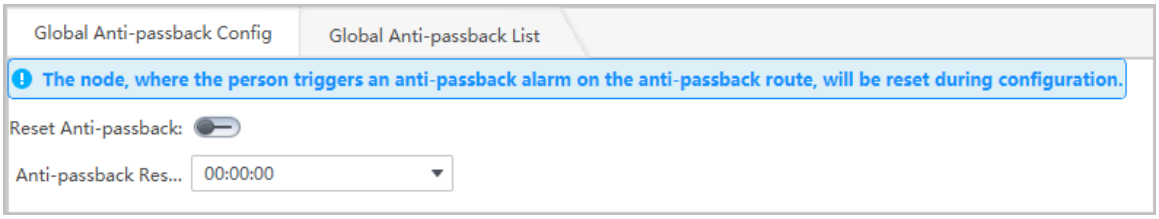
Paso 1 Seleccionar**Configuración de control de acceso**>**Anti-pase hacia atrás**.

Paso 2 Hacer clic**Anti-passback global**y luego haga clic en**Configuración global anti-passback**. Habilite

Paso 3 el reinicio de la función Anti-passback e ingrese el tiempo de reinicio.

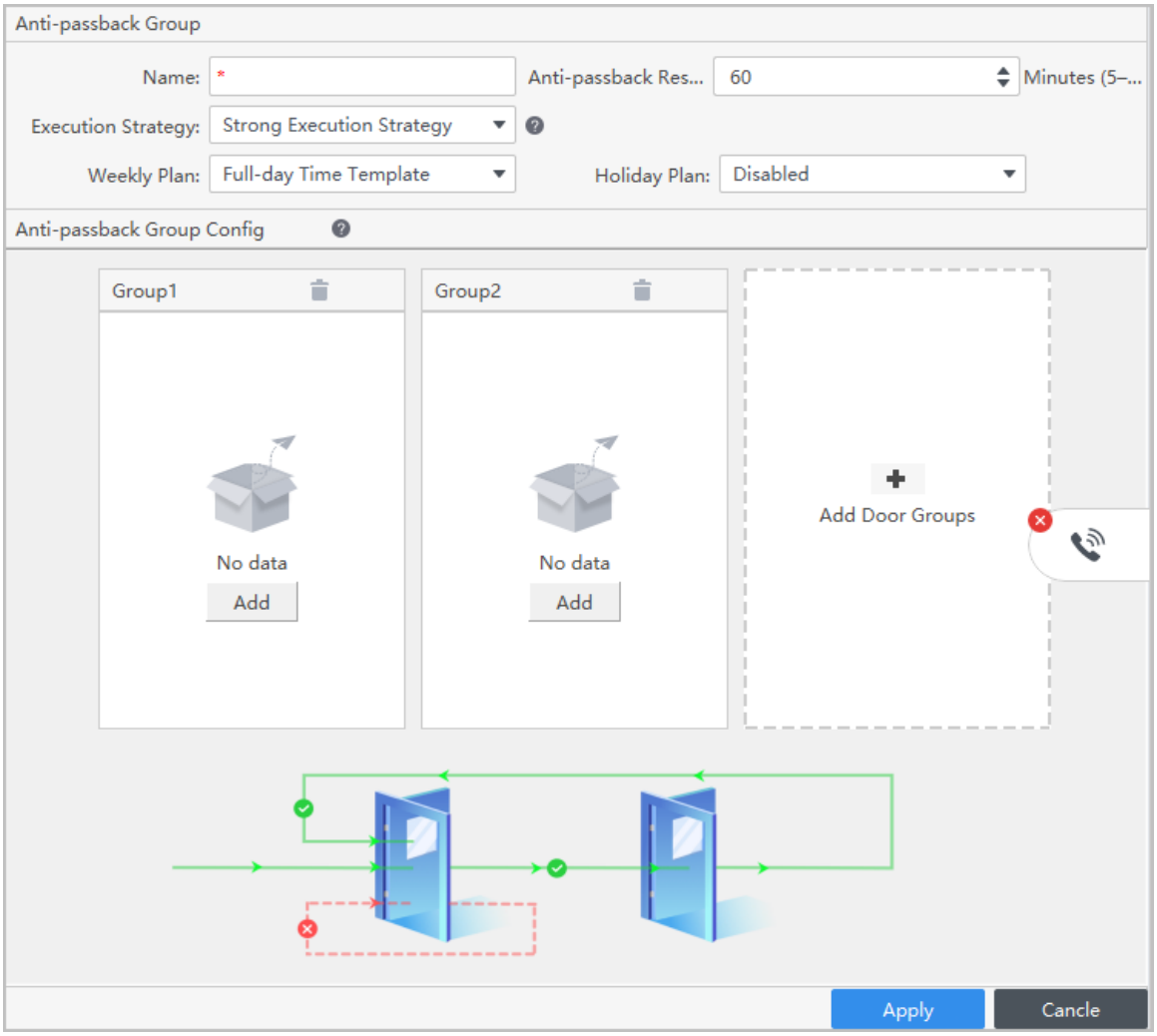
Especifique una hora en la que se restablecerá el estado anti-passback de todo el personal.

Figura 6-6 Restablecer anti-passback



Etapa 4 Hacer clic**Lista global anti-passback**,y luego haga clic**Agregar**.

Figura 6-7 Configurar anti-passback



Paso 5 Ingrese el nombre y configure el tiempo de reinicio.

Especifique una hora en la que se restablecerá el estado anti-passback de todo el personal. Por ejemplo, si el tiempo de reinicio se establece en 30 minutos, cuando se activa una alarma anti-passback, el usuario debe esperar 30 minutos antes de poder deslizar el dedo para abrir la puerta.

Paso 6 Seleccione el modo de ejecución.

- Ejecución sólida: el dispositivo realiza la función anti-passback incluso cuando se desconecta.
- Ejecución débil: el dispositivo no realiza la función anti-passback cuando se desconecta.

Paso 7 Seleccione el plan semanal y el plan de vacaciones.

El anti-passback es efectivo durante el tiempo definido. En el grupo

Paso 8 1, haga clic**Agregar**y luego seleccione lectores de tarjetas. En el

Paso 9 grupo 2, haga clic**Agregar**y luego seleccione lectores de tarjetas.

Se deben agregar al menos 2 grupos.

Paso 10 (Opcional) Puedes hacer clic**Agregar grupos de puertas**para agregar más grupos.

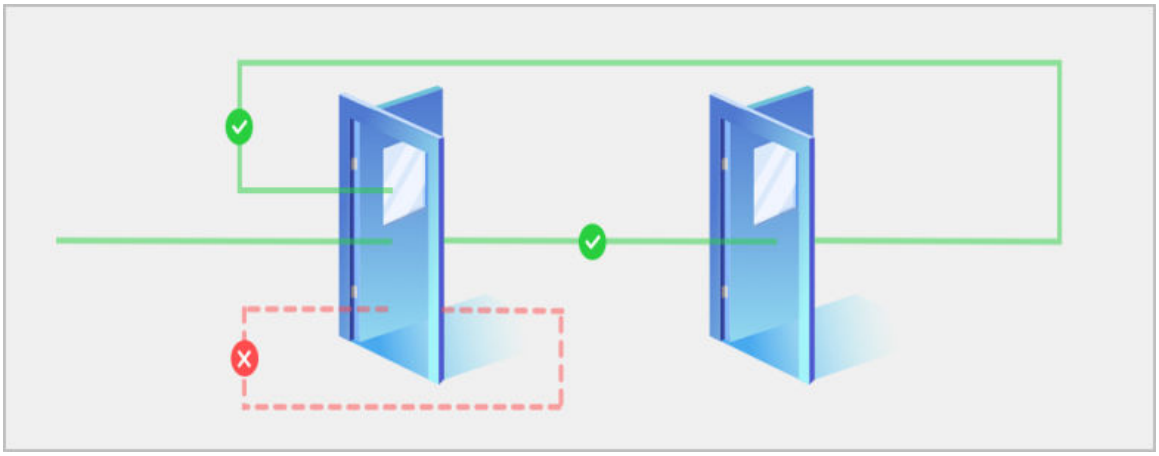
Puede agregar más de un lector a un grupo y los usuarios pueden deslizar el dedo hacia cualquiera de los lectores para obtener acceso.

Paso 11 Hacer clic**Aplicar**.

Resultados

El número de grupo indica la secuencia de tarjetas magnéticas. La tarjeta debe utilizarse siguiendo la secuencia específica de grupos. Por ejemplo, debe pasar la tarjeta en un lector del grupo 1, luego en un lector del grupo 2, y luego en un lector del grupo 3, etc. Siempre que pases la tarjeta siguiendo la secuencia establecida, el sistema funciona bien.

Figura 6-8 Función anti-passback



6.4 Configuración del interbloqueo entre grupos

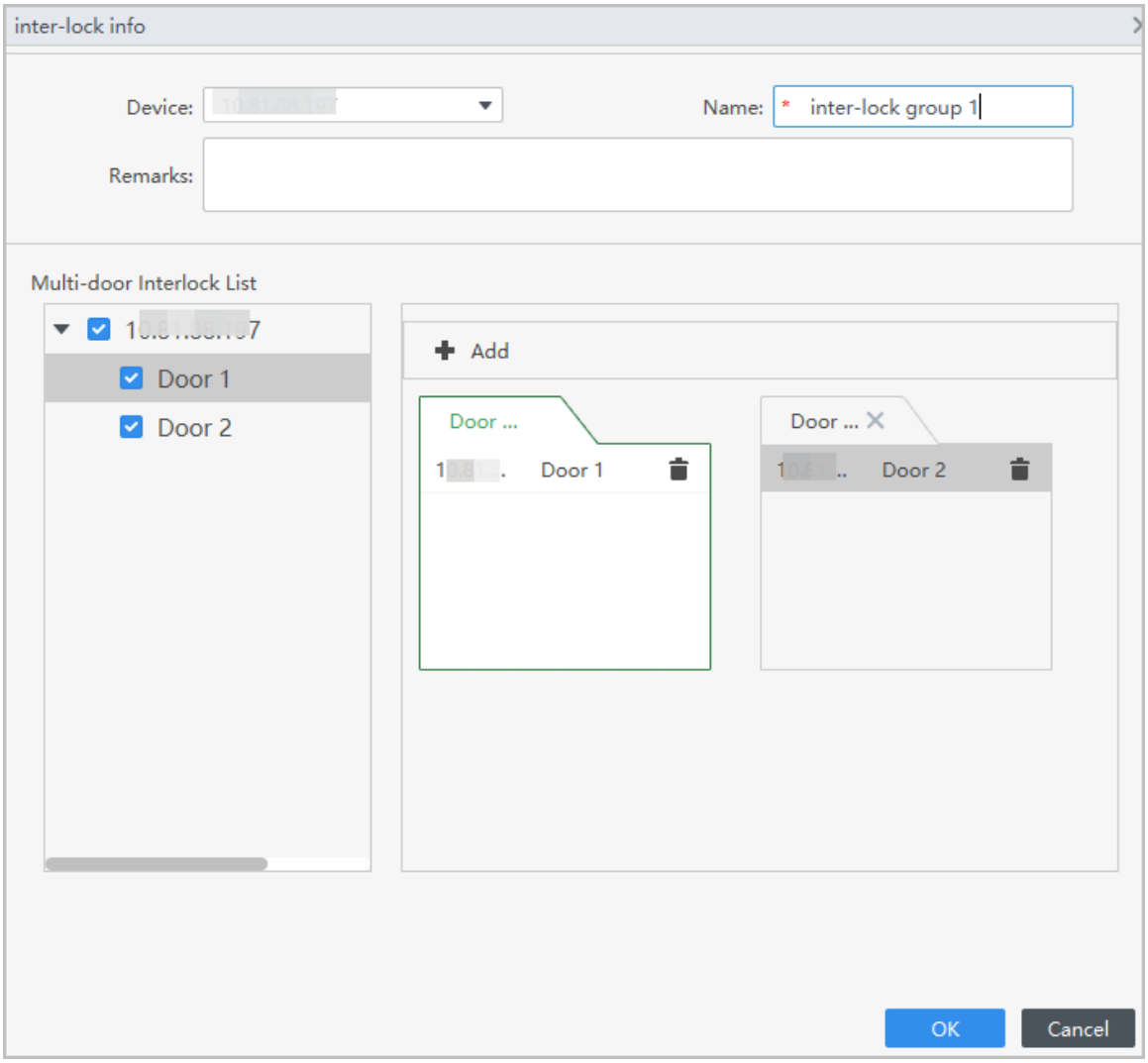
Si alguna puerta de un grupo está desbloqueada, las puertas de los otros grupos no se pueden abrir.

Procedimiento

Paso 1 Seleccionar**Configuración de control de acceso**>**Cerradura entre puertas**.

Paso 2 Hacer clic**Agregar**y luego agregue un grupo de enclavamiento.

Figura 6-9 Interbloqueo entre grupos



Paso 3 Seleccione un dispositivo de control de acceso y luego ingrese un nombre para el grupo de interbloqueo. En el

Etapa 4 grupo 1, haga clic**Agregar**para agregar puertas al grupo. En el grupo 2, haga clic**Agregar**para agregar puertas

Paso 5 al grupo. Hacer clic**Aplicar**.

Paso 6

Resultados

Si alguna puerta de un grupo está desbloqueada, las puertas del otro grupo no podrán abrirse.

7 Configuración de los parámetros de la puerta

Procedimiento

Paso 1 Seleccionar**Configuración de control de acceso**>**Parámetros de la**

Paso 2 **puerta**. Configurar parámetros básicos para el control de acceso.

Figura 7-1 Parámetros básicos

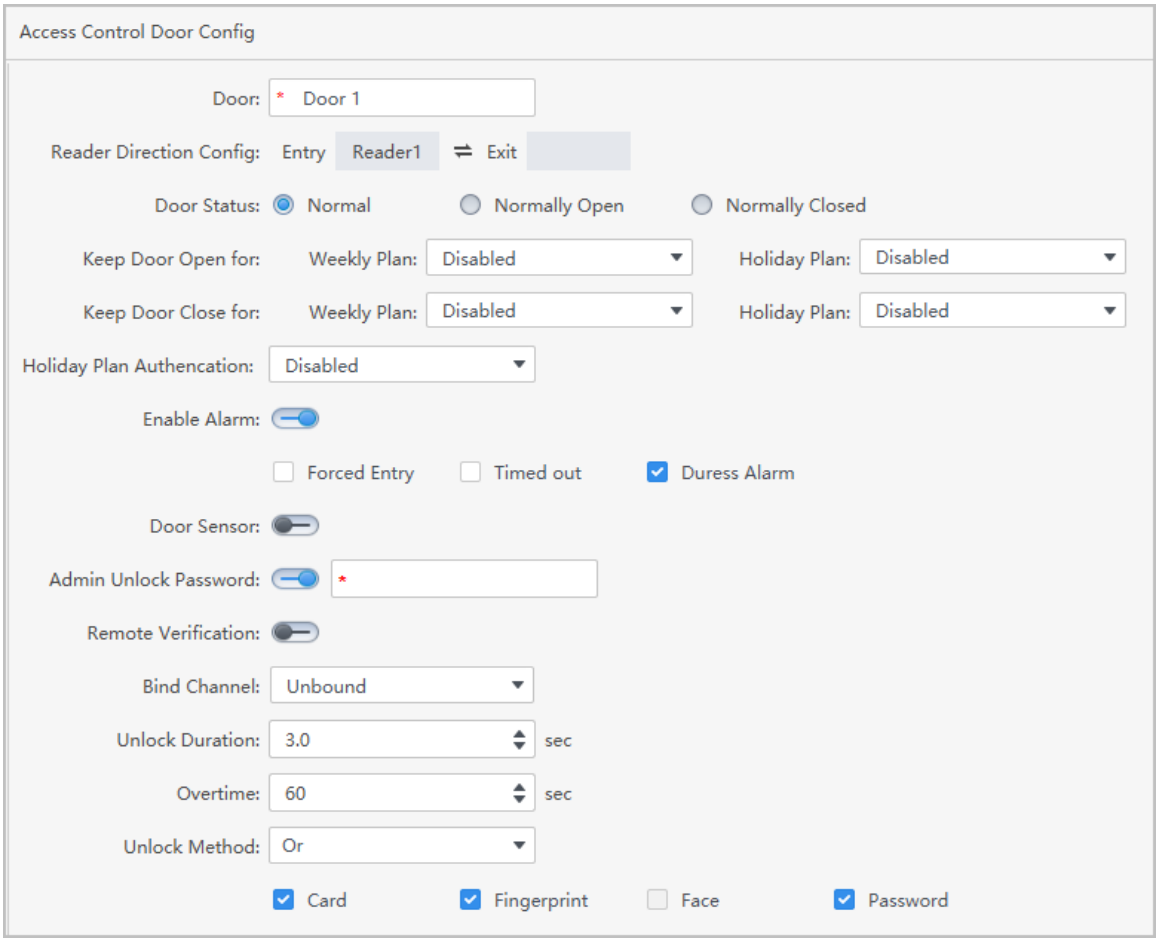


Tabla 7-1 Descripción de los parámetros básicos

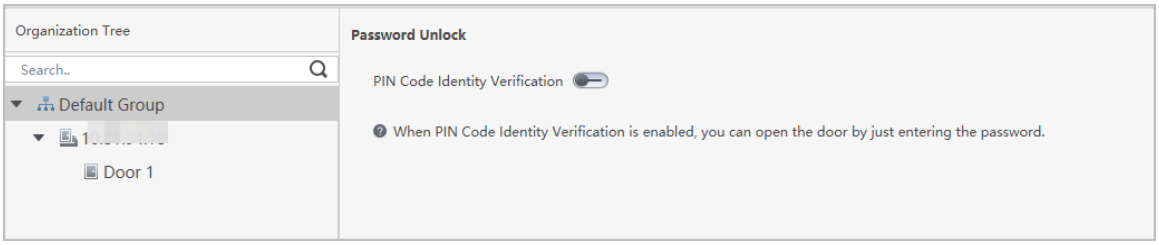
Parámetro	Descripción
Nombre	El nombre de la puerta.
Dirección del lector	Hacer clic ⇌ para configurar el lector como lector de tarjetas "entrada" o lector de tarjetas "salida".
Estado de la puerta	Establecer el estado de la puerta. ● **Normal**:La puerta se desbloquea solo después de una verificación de identidad válida. ● **Siempre abierto**:La puerta permanece abierta todo el tiempo. ● **Siempre cerrado**:La puerta permanece cerrada todo el tiempo.
Mantenga la puerta abierta durante	La puerta permanece abierta durante el plan semanal definido o el plan de vacaciones.
Mantenga la puerta cerrada durante	La puerta permanece cerrada durante el plan semanal definido o el plan de vacaciones.

Parámetro	Descripción
Plan de vacaciones Autenticación	El estado de la puerta es**Normal**en vacaciones cuando esta función está habilitada. La prioridad es la siguiente: mantener la puerta abierta para el plan de vacaciones > mantener la puerta cerrada para el plan de vacaciones > autenticación del plan de vacaciones > mantener la puerta abierta para el plan semanal > mantener la puerta cerrada para el plan semanal.
Activar la alarma	● Entrada forzada: cuando el detector de puerta está habilitado, se activará una alarma de intrusión si la puerta se abre de manera anormal. ● Tiempo de espera agotado: se activa una alarma de tiempo de espera cuando la puerta permanece desbloqueada por más tiempo que el valor definido. ● Coacción: Se activará una alarma cuando se utilice una tarjeta de coacción, una contraseña de coacción o una huella digital de coacción para desbloquear la puerta.
Sensor de puerta	Cuando el detector de puerta está habilitado, se activará una alarma de intrusión si la puerta se abre de manera anormal.
Contraseña de desbloqueo de administrador	Puede desbloquear la puerta simplemente ingresando la contraseña de desbloqueo del administrador.
Verificación Remota	El administrador debe otorgar acceso a la plataforma después de que el personal verifique sus identidades en el dispositivo y luego se abrirá la puerta.
Canal de enlace	Seleccione un canal de video y luego podrá ver el video en vivo asociado con la puerta.
Duración de la puerta	Después de que se le conceda acceso a una persona, la puerta permanecerá desbloqueada durante un tiempo definido para que pueda pasar. Va desde 0,2 sa 600 segundos.
Tiempo de espera de desbloqueo	Se activa una alarma de tiempo de espera cuando la puerta permanece desbloqueada durante más tiempo que el valor definido.
Método de desbloqueo	Admite desbloqueo mediante tarjeta, huella digital, rostro o contraseña.

Operaciones relacionadas

Verificación de identidad con código PIN: cuando esta función está habilitada, las personas pueden desbloquear la puerta simplemente ingresando la contraseña.

Figura 7-2 Verificación de identidad del código PIN



8 Visualización de registros de control de acceso

Los eventos de puerta del historial incluyen aquellos que ocurren en el cliente SmartPSS Lite y en los dispositivos de puerta. Antes de ver eventos, extraiga el historial de eventos en los dispositivos de puerta para asegurarse de que se busquen todos los eventos.

Procedimiento

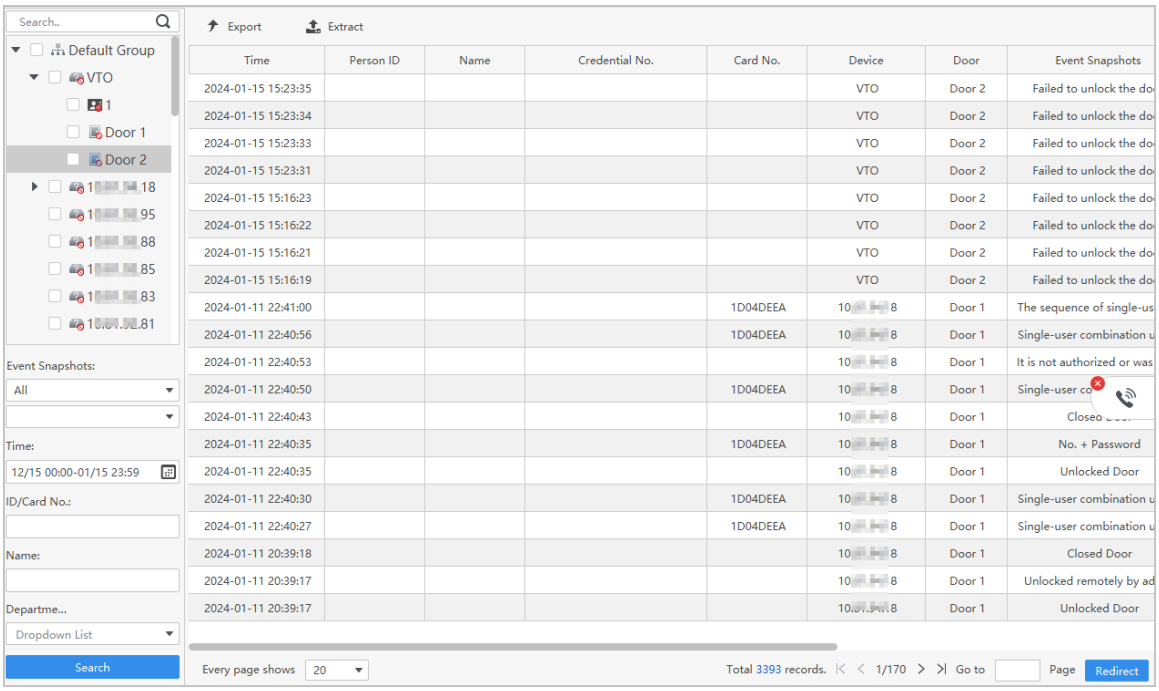
Paso 1 Hacer clic**Registro de control de acceso**en la página de inicio.

Paso 2 Hacer clic**Extracto**,configure la hora, seleccione el dispositivo de control de acceso y luego haga clic en**Extraer ahora**.

Los eventos de control de acceso en los dispositivos se extraerán a la plataforma.

- Puede seleccionar varios dispositivos a la vez para extraer eventos.
- Si la zona horaria de la computadora admite DST (horario de verano), el evento de acceso informado a la plataforma tendrá un retraso de 1 hora con respecto a la hora UTC (hora universal coordinada) del dispositivo.

Figura 8-1 Extraer eventos



Paso 3 Seleccione un dispositivo, establezca las condiciones del filtro y luego haga clic en

Etapa 4 **Buscar**. (Opcional) Haga clic**Exportar**y luego guárdelo en su computadora.

9 Monitoreo de control de acceso

Procedimiento

Paso 1 Hacer clic**Monitoreo de control de acceso**en la página de inicio.

Paso 2 Gestiona la puerta.

Figura 9-1 Monitorear la puerta

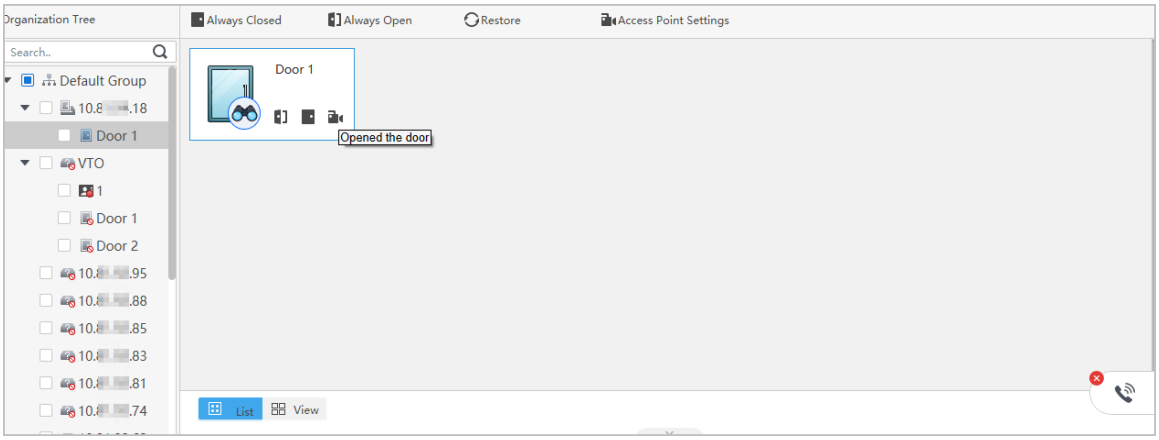


Tabla 9-1 Descripción de los parámetros

Función	Descripción
Controlar remotamente la puerta	Controla remotamente la puerta. ● Método 1: haga clic derecho en una puerta y luego seleccione**Abierto**o**Cerca**. ● Método 2: haga clic en o para abrir o cerrar la puerta.
	Vea el vídeo capturado por la cámara del controlador de acceso o la cámara externa vinculada. Si no puede ver video en tiempo real, significa que el dispositivo de control de acceso no tiene cámara y no está conectado a una cámara externa. Configure una cámara externa para el controlador de acceso. Para obtener más información, consulte "7 Configuración de los parámetros de la puerta". Si desea ver varios videos en vivo al mismo tiempo, haga clic en View y luego arrastre el dispositivo de control de acceso en la organización árbol a Windows, o haga doble clic en el dispositivo de control de acceso en el árbol de la organización.
Siempre abierto	Después de configurar siempre abierta o siempre cerrada, la puerta está abierta o cerrada todo el tiempo y no se puede controlar manualmente. Si desea controlar manualmente la puerta nuevamente, haga clic en**Normal**para restablecer el estado de la puerta.
Siempre cerrado	
Restaurar	
Configuración del punto de acceso	Configure dispositivos (NVR, IPC, IVSS y más) que admitan el reconocimiento de objetivos como punto de control de acceso. Después de la configuración, los registros de desbloqueo de puertas se cargarán en la plataforma.

Paso 3 Haga clic derecho en un dispositivo de control de acceso para administrar el dispositivo.

Figura 9-2 Administrar el dispositivo

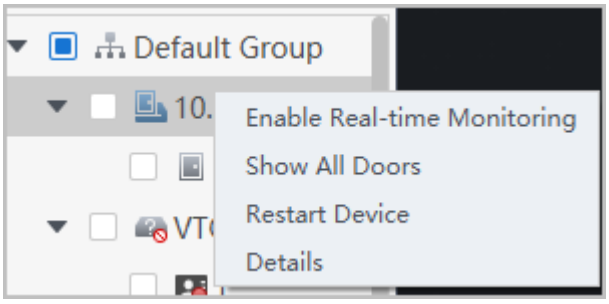


Tabla 9-2 Descripción de los parámetros

Parámetro	Descripción
Habilitar monitoreo en tiempo real	Inicie el monitoreo de eventos en tiempo real.
Mostrar todas las puertas	Muestra todas las puertas conectadas al dispositivo de control de acceso.
Reiniciar el dipositivo	Reinicie el dispositivo de control de acceso.
Detalles	Vea la información del dispositivo, como la versión y más.

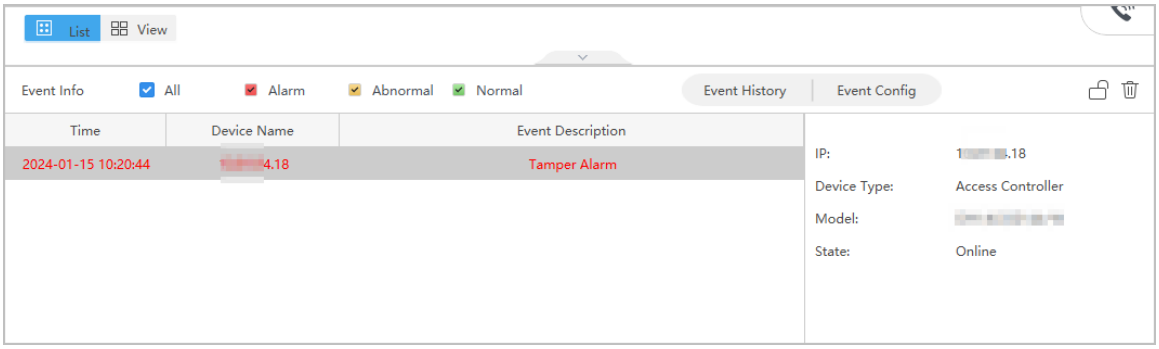
Etapa 4 Ver el estado de la puerta en**Información del evento**lista. Para obtener más información, consulte "8 Visualización de registros de control de acceso".

Operaciones relacionadas

Hacer clic para abrir el**Información del evento**lista.

- Ver información de control de acceso: puede ver información de acceso en tiempo real en el**Información del evento** lista. La información se borrará después de que se reinicie la plataforma.
- Filtrar eventos: seleccione el tipo de evento en el**Información del evento**,y la lista de eventos muestra eventos de los tipos seleccionados. Por ejemplo, seleccione**Alarma**y la lista de eventos solo muestra eventos de alarma.
- Bloquear o desbloquear la lista de eventos: haga clic en el lado derecho de**Información del evento**para bloquear o desbloquear la lista de eventos y luego los eventos en tiempo real no se podrán ver.
- Eliminar eventos: haga clic en el lado derecho de**Información del evento**para borrar todos los eventos en la lista de eventos.
- Hacer clic**Historial de eventos**saltar a la**Registro de control de acceso**página y haga clic**Configuración de eventos** saltar a la**Configuración de eventos**página.

Figura 9-3 Información del evento



Apéndice 1 Recomendaciones de ciberseguridad

Las medidas necesarias para garantizar la ciberseguridad básica de la plataforma:

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.**Personaliza la respuesta a la pregunta de seguridad**

La configuración de las preguntas de seguridad debe garantizar la diferencia de respuestas, elegir diferentes preguntas y personalizar diferentes respuestas (se prohíbe que todas las preguntas tengan la misma respuesta) para reducir el riesgo de que la pregunta de seguridad sea adivinada o descifrada.

Medidas de recomendación para mejorar la ciberseguridad de la plataforma:

1.**Habilitar IP/MAC vinculante de cuenta**

Se recomienda habilitar el mecanismo IP/MAC de vinculación de cuentas y configurar la IP/MAC del terminal donde se encuentra el cliente de uso común como una lista de permitidos para mejorar aún más la seguridad del acceso.

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.**Activar el mecanismo de bloqueo de cuenta**

La función de bloqueo de cuenta está habilitada de fábrica de forma predeterminada y se recomienda mantenerla activada para proteger la seguridad de su cuenta. Después de que el atacante haya fallado en varios intentos de contraseña, la cuenta correspondiente y la IP de origen se bloquearán.

4.**Asignación razonable de cuentas y permisos**

De acuerdo con las necesidades comerciales y de administración, agregue razonablemente nuevos usuarios y asigne razonablemente un conjunto mínimo de permisos para ellos.

5.**Cerrar servicios no esenciales y restringir la forma abierta de servicios esenciales**

Si no es necesario, se recomienda desactivar NetBIOS (puerto 137, 138, 139), SMB (puerto 445), escritorio remoto (puerto 3389) y otros servicios en Windows, y Telnet (puerto 23) y SSH (puerto 22). bajo Linux. Al mismo tiempo, cierre el puerto de la base de datos al exterior o ábralo solo a una dirección IP específica, como MySQL (puerto 3306), para reducir los riesgos que enfrenta la plataforma.

6.**Parchear el sistema operativo/componentes de terceros**

Se recomienda detectar periódicamente vulnerabilidades de seguridad en el sistema operativo y componentes de terceros, y aplicar los parches oficiales a tiempo.

7.**Auditoría de seguridad**

- Verifique a los usuarios en línea: se recomienda verificar a los usuarios en línea de manera irregular para identificar si hay usuarios ilegales iniciando sesión.
- Ver el registro de la plataforma: al ver el registro, puede obtener la información de IP del intento de iniciar sesión en la plataforma y la información de operación clave del usuario que inició sesión.

8.**El establecimiento de un entorno de red seguro**

Para proteger mejor la seguridad de la plataforma y reducir los riesgos de ciberseguridad, se recomienda:

- Siga el principio de minimización, restrinja los puertos que la plataforma asigna externamente mediante firewalls o enrutadores y solo asigne los puertos que sean necesarios para los servicios.

- Según los requisitos reales de la red, separe las redes: si no hay requisitos de comunicación entre las dos subredes, se recomienda utilizar VLAN, gatekeeper, etc. para dividir la red y lograr el efecto de aislamiento de la red.