# Controlador de acceso

## Manual de usuario

ZHEJIANG DAHUA VISIÓN TECNOLOGÍA CO., LTD. V1.0.5

# Prefacio

## General

Este manual presenta las funciones y operaciones del Controlador de acceso. 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 |
|---|---|---|
| V1.0.5 | Se actualizaron las descripciones de desbloqueo de contraseña. | noviembre 2023 |
| V1.0.4 | Actualizado agregando usuarios y configurando permisos. | junio 2023 |
| V1.0.3 | Se actualizó la descripción sobre cómo agregar usuarios. | abril 2023 |
| V1.0.2 | Se actualizaron los métodos de desbloqueo. | marzo 2023 |
| V1.0.1 | Se actualizó el cableado. | Septiembre 2022 |
| V1.0.0 | Primer lanzamiento. | Septiembre 2022 |

### Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otras personas, como su rostro, 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 al

medidas de implementación 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 controlador de acceso, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el Controlador de acceso y cumpla con las pautas al usarlo.

## Requisito de transporte

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

### Requisito de almacenamiento

Guarde el controlador de acceso en condiciones permitidas de humedad y temperatura.

### requerimientos de instalación

- No conecte el adaptador de corriente al controlador de acceso 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 controlador de acceso.
- No conecte el Controlador de acceso a dos o más tipos de fuentes de alimentación para evitar daños al Controlador de acceso.
- 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 controlador de acceso en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el Access Controller alejado de la humedad, el polvo y el hollín.
- Instale el controlador de acceso en una superficie estable para evitar que se caiga.
- Instale el controlador de acceso 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 Controlador de acceso.

- El Controlador de Acceso es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del controlador de acceso esté conectada a una toma de corriente con conexión a tierra protectora.

## 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 controlador de acceso mientras el adaptador esté encendido.

- Opere el controlador de acceso dentro del rango nominal de entrada y salida de energía.
- Utilice el controlador de acceso en las condiciones permitidas de humedad y temperatura.
- No deje caer ni salpique líquido sobre el Controlador de acceso y asegúrese de que no haya ningún objeto lleno de líquido sobre el Controlador de acceso para evitar que el líquido fluya hacia él.
- No desmonte el controlador de acceso sin instrucción profesional.

# Tabla de contenido

# 1 Descripción general del producto

## 1.1 Introducción del producto

Flexible y conveniente, el Controlador de acceso tiene un sistema fácil de usar que le permite acceder a los controladores en la página web a través de la dirección IP. Viene con un sistema de gestión de acceso profesional y hace que la conexión en red de los modos de control principal y secundario sea rápida y sencilla, satisfaciendo las necesidades de sistemas pequeños y avanzados.

### 1.2 Características principales

- Construido con material PC y ABS ignífugo, es a la vez resistente y elegante con una clasificación IK06.
- Admite conexión TCP e IP y PoE estándar.
- Accede a lectores de tarjetas mediante protocolos Wiegand y RS-485.
- Suministra energía a la cerradura a través de su fuente de alimentación de salida de 12 VDC, la cual tiene una corriente de salida máxima de 1000 mA.
- Admite 1000 usuarios, 5000 tarjetas, 3000 huellas dactilares y 300.000 registros.
- Múltiples métodos de desbloqueo que incluyen tarjeta, contraseña, huella digital y más. También puedes combinar estos métodos para crear tus propios métodos de desbloqueo personales.
- Se admiten varios tipos de eventos de alarma, como coacción, manipulación, intrusión, tiempo de espera de desbloqueo y tarjeta ilegal.
- Admite una amplia gama de usuarios, incluidos usuarios generales, de patrulla, VIP, invitados, incluidos en listas bloqueadas y más.
- Sincronización horaria manual y automática.
- Retiene los datos almacenados incluso cuando está apagado.
- Ofrece una variedad de funciones y el sistema se puede configurar. Los dispositivos también se pueden actualizar a través de la página web.
- Cuenta con modos de control principal y secundario. El modo de control principal ofrece gestión de usuarios, gestión y configuración de dispositivos de control de acceso y más opciones. Los dispositivos bajo modos de subcontrol se pueden agregar a múltiples plataformas.
- Un controlador principal puede conectarse y administrar hasta 19 subcontroladores.
- Watchdog protege el sistema para permitir que el dispositivo sea estable y funcione de manera eficiente.
- Se pueden agregar subcontroladores a SmartPSS Lite y DSS Pro.

## 1.3 Escenarios de aplicación

Se utiliza ampliamente en parques, comunidades, centros de negocios y fábricas, y es ideal para lugares como edificios de oficinas, edificios gubernamentales, escuelas y estadios.

El controlador de acceso se puede configurar como controlador de acceso principal (en adelante denominado controlador principal) o en controlador de acceso secundario (en adelante denominado subcontrolador). Hay 2 métodos de conexión en red diferentes disponibles para el controlador de acceso. Puede seleccionar un método de red según sus necesidades.

Tabla 1-1 Métodos de conexión en red del controlador de acceso

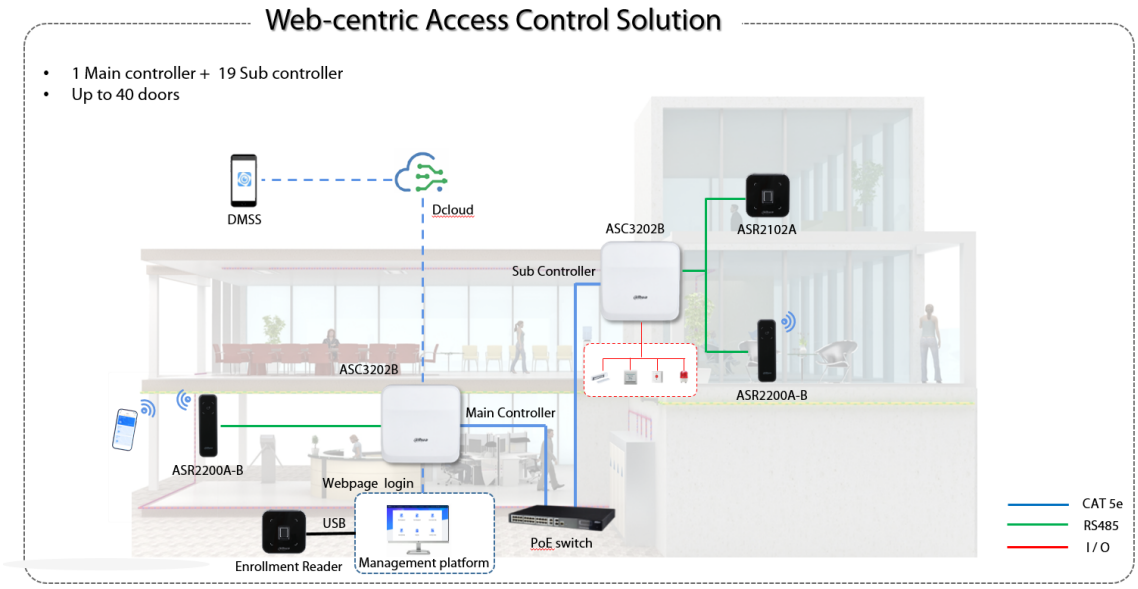
| Métodos de networking | Descripción |
| --- | --- |
| Controlador principal—Sub Controlador | El controlador principal viene con una plataforma de gestión (en adelante denominada la Plataforma). Los subcontroladores deben agregarse a la Plataforma del controlador principal. El controlador principal puede gestionar hasta 19 subcontroladores. Para obtener más información, consulte "2 Controlador principal-controlador secundario".<br><br>No recomendamos agregar otras plataformas de administración en este método de networking. |
| SmartPSS Lite—Subcontrolador | Es necesario agregar subcontroladores a una plataforma de administración independiente, como SmartPSS Lite. La plataforma puede gestionar hasta 64 puertas si cada subcontrolador conecta 2 puertas. Para obtener más información, consulte "3 controladores Smart PSS Lite-Sub". |

# 2 Controlador principal-Subcontrolador

## 2.1 Diagrama de red

El controlador principal viene con una plataforma de gestión (en adelante denominada la plataforma). Es necesario agregar el subcontrolador a la plataforma de gestión del controlador principal. El controlador principal puede gestionar hasta 19 subcontroladores.

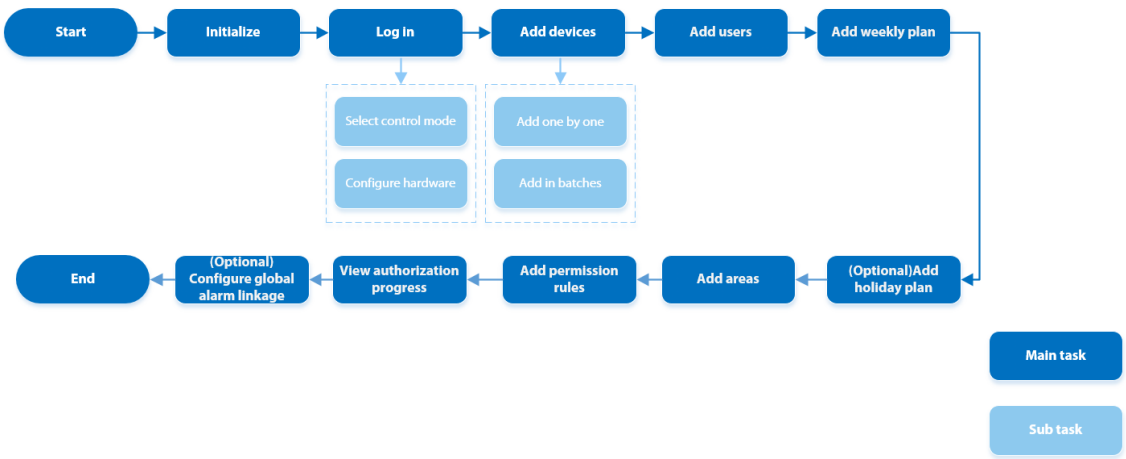
Figura 2-1 Diagrama de red




## 2.2 Configuraciones del controlador principal

### 2.2.1 Diagrama de flujo de configuración

Figura 2-2 Diagrama de flujo de configuración



# 2.2.2 Inicialización

Inicialice el controlador principal cuando inicie sesión en la página web por primera vez o después de que se restablezca a sus valores predeterminados de fábrica.

## Requisitos previos

Asegúrese de que la computadora utilizada para iniciar sesión en la página web esté en la misma LAN que el controlador principal.

## Procedimiento

Paso 1 Abra un navegador, vaya a la dirección IP (la dirección IP es 192.168.1.108 por defecto) del controlador principal.

Le recomendamos utilizar la última versión de Chrome o Firefox.

Paso 2 Seleccione un idioma y luego haga clic en**Próximo**.

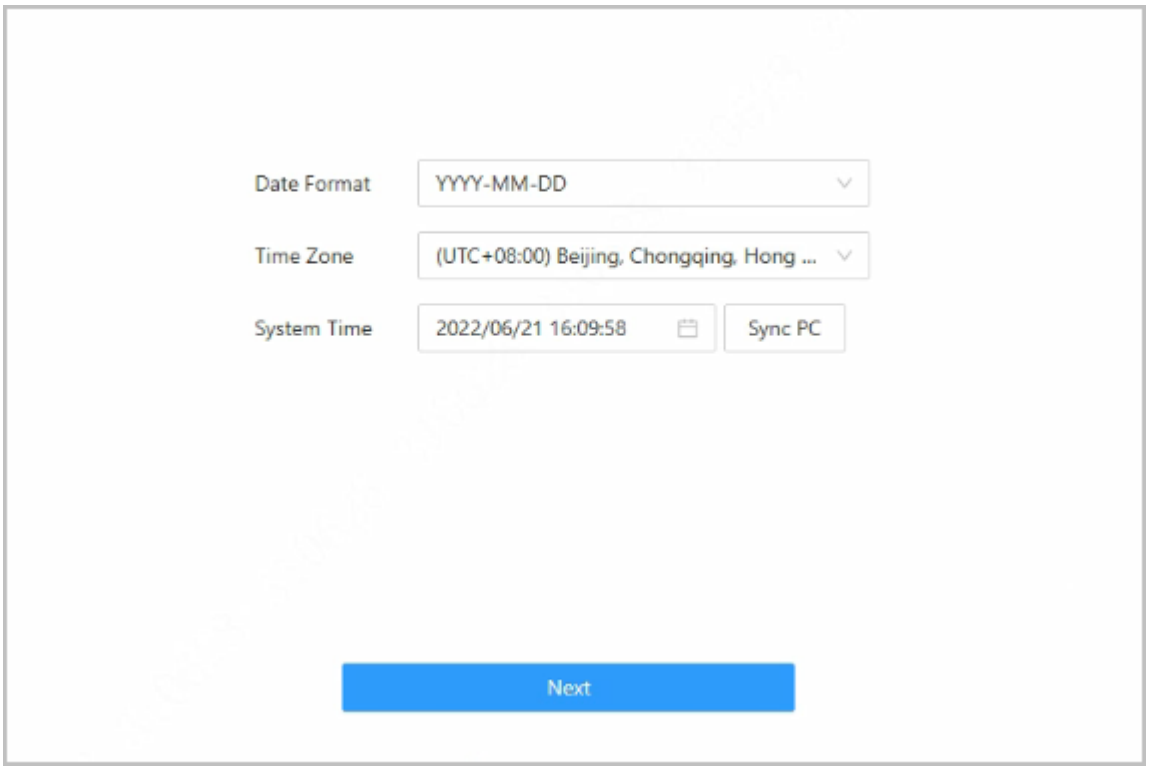
Paso 3 Lea atentamente el acuerdo de licencia de software y la política de privacidad, seleccione**He leído y acepto los términos del Acuerdo de licencia de software y la Política de privacidad.**,y luego haga clic**Próximo**.

Etapa 4 Establezca la contraseña y la dirección de correo electrónico.

- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de los siguientes caracteres: letras mayúsculas y minúsculas, números y caracteres especiales (excluidos ' " ; : &). Establezca una contraseña de alta seguridad siguiendo las indicaciones sobre la seguridad de la contraseña.
- Mantenga la contraseña segura después de la inicialización y cámbiela periódicamente para mejorar la seguridad.

Paso 5 Configure la hora del sistema y luego haga clic en**Próximo**.

Figura 2-3 Configurar la hora



Paso 6 (Opcional) Seleccionar**Comprobación automática de actualizaciones**,y luego haga clic**Terminado**.

El sistema verifica automáticamente si hay alguna versión superior disponible e informa al usuario que actualice el sistema. El sistema busca automáticamente nuevas actualizaciones y le informa cuando hay una nueva disponible.

Paso 7 Hacer clic**Terminado**.

El sistema accede automáticamente a la página de inicio de sesión después de que la inicialización sea exitosa.

## 2.2.3 Iniciar sesión

Para iniciar sesión por primera vez durante la inicialización, debe seguir el asistente de inicio de sesión para configurar el tipo de controlador principal y su hardware.

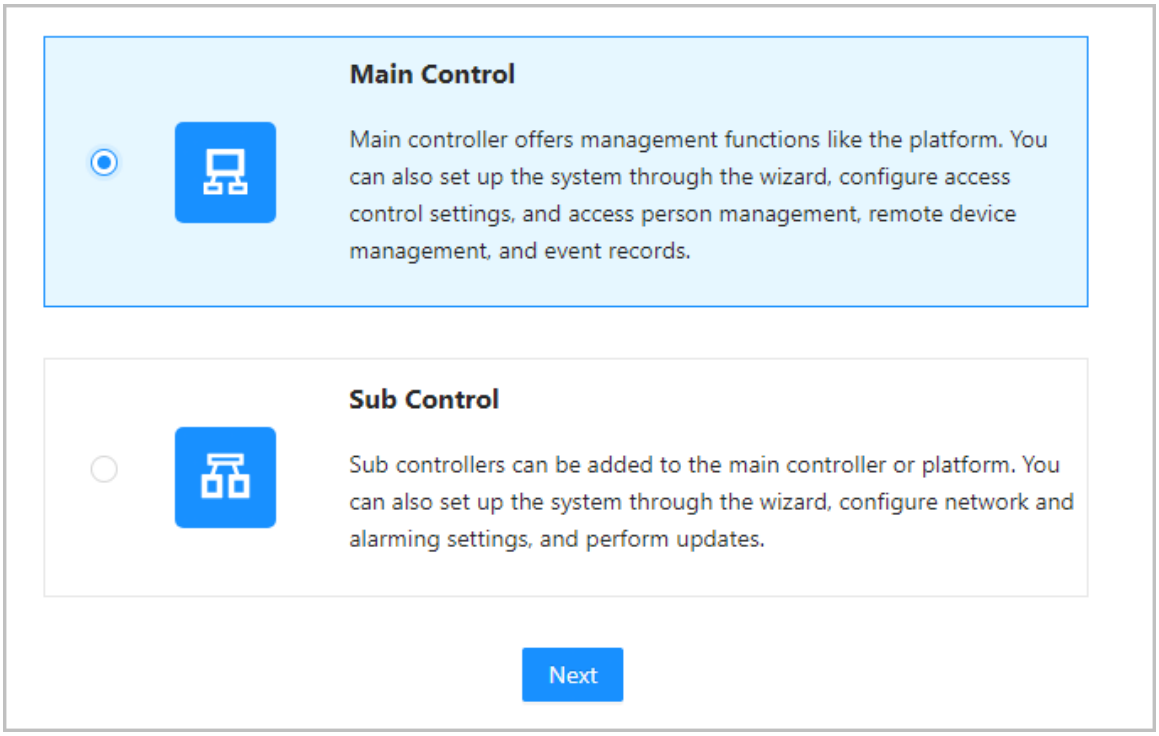
Procedimiento

Paso 1 En la página de inicio de sesión, ingrese el nombre de usuario y la contraseña.

- El nombre del administrador predeterminado es admin y la contraseña es la que estableció durante la inicialización. Le recomendamos cambiar la contraseña de administrador periódicamente para aumentar la seguridad de la plataforma.
- Si olvida la contraseña de inicio de sesión del administrador, puede hacer clic en**¿Has olvidado tu contraseña?**.

Paso 2 Seleccionar**Control principal**,y luego haga clic**Próximo**.

Figura 2-4 Tipo de controlador de acceso




- Control Principal: El controlador principal viene con una plataforma de gestión. Puede administrar todos los subcontroladores, configurar el control de acceso, acceder a la administración personal en la plataforma y más.
- Subcontrol: los subcontroladores deben agregarse a la plataforma de administración del controlador principal u otras plataformas de administración como DSS Pro o SmartPSS Lite. Puede realizar las configuraciones en la página web del subcontrolador.

Paso 3 Seleccione el número de puertas y luego ingrese el nombre de la puerta.

Etapa 4 Configurar los parámetros de las puertas.

Figura 2-5 Configurar los parámetros de la puerta

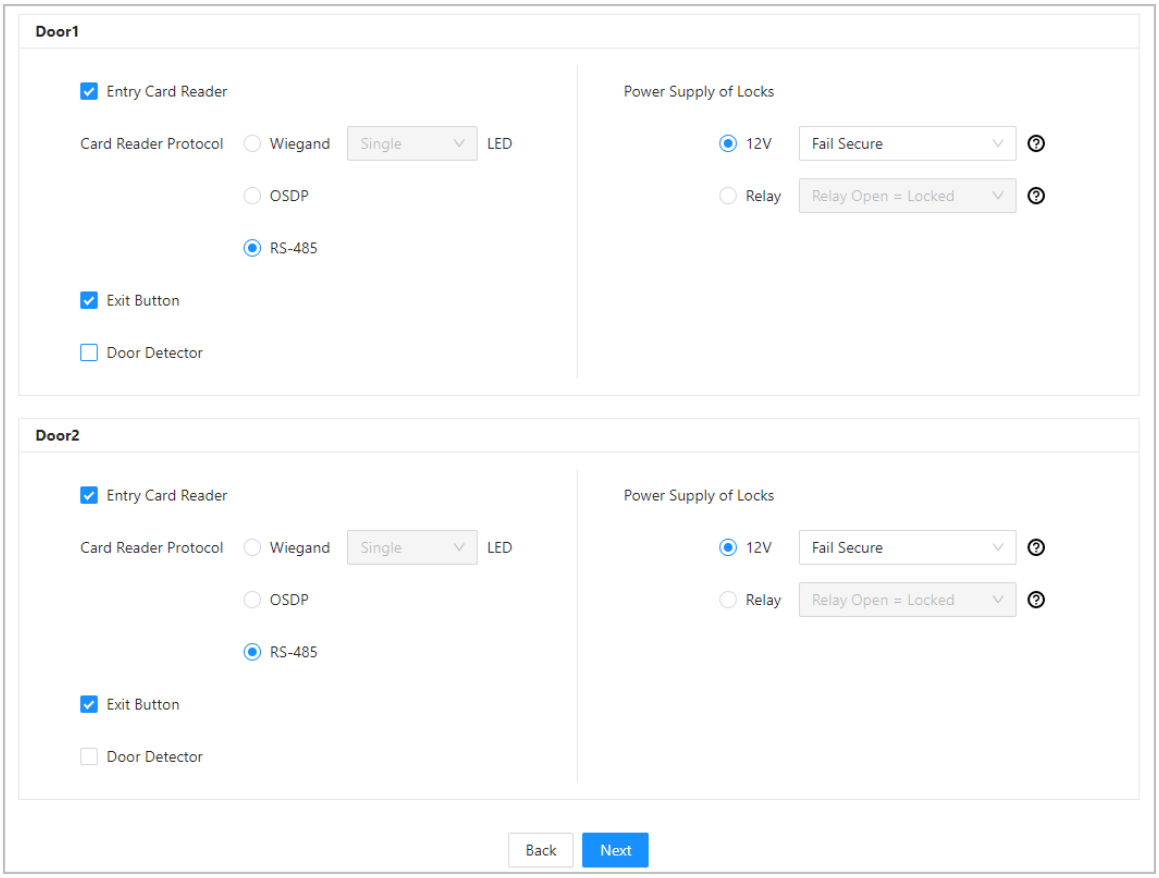



Tabla 2-1 Descripción del parámetro

| Parámetro | Descripción |
|---|---|
| Lector de tarjetas de entrada | Seleccione el protocolo del lector de tarjetas.<br>● Wiegand: Se conecta a un lector Wiegand. Puede conectar el cable LED al puerto LED del controlador y el lector emitirá un pitido y parpadeará cuando la puerta se desbloquee.<br>● OSDP: Se conecta a un lector OSDP.<br>● RS-485: Se conecta a un lector RS-485. |
| Botón Salir | Se conecta a un botón de salida. |
| Detector de puerta | Se conecta a un detector de puerta. |

| Parámetro | Descripción |
|---|---|
| Fuente de alimentación de cerraduras | ● 12 V: El controlador proporciona energía a la cerradura.<br>◇ A prueba de fallos: cuando se interrumpe o falla la energía, la puerta permanece bloqueada.<br>◇ A prueba de fallos: cuando se interrumpe o falla la energía, la puerta se desbloquea automáticamente para permitir que las personas salgan.<br>● Relé: El relé suministra energía a la cerradura.<br>◇ Relé abierto = bloqueado: configura la cerradura para que permanezca bloqueada cuando el relé está abierto.<br>◇ Relé abierto = desbloqueado: configura el bloqueo para que se desbloquee cuando el relé está abierto.<br>El bloqueo electromagnético se desbloquea en un instante y se vuelve a bloquear inmediatamente cuando el controlador de acceso está en el reinicio suave. |

Paso 5 Configurar los parámetros de control de acceso.

Paso 6 En**Configuración de desbloqueo**,seleccionar**O**o**Y**de**Método de combinación**.

- O: Utilice uno de los métodos de desbloqueo seleccionados para autorizar la apertura de la puerta.
- Y: Utilice todos los métodos de desbloqueo seleccionados para autorizar la apertura de la puerta.

La tarjeta Bluetooth no se puede seleccionar cuando configura el método de combinación en**Y**.

Paso 7 Seleccione los métodos de desbloqueo y luego configure los demás parámetros.

Figura 2-6 Configuración de desbloqueo

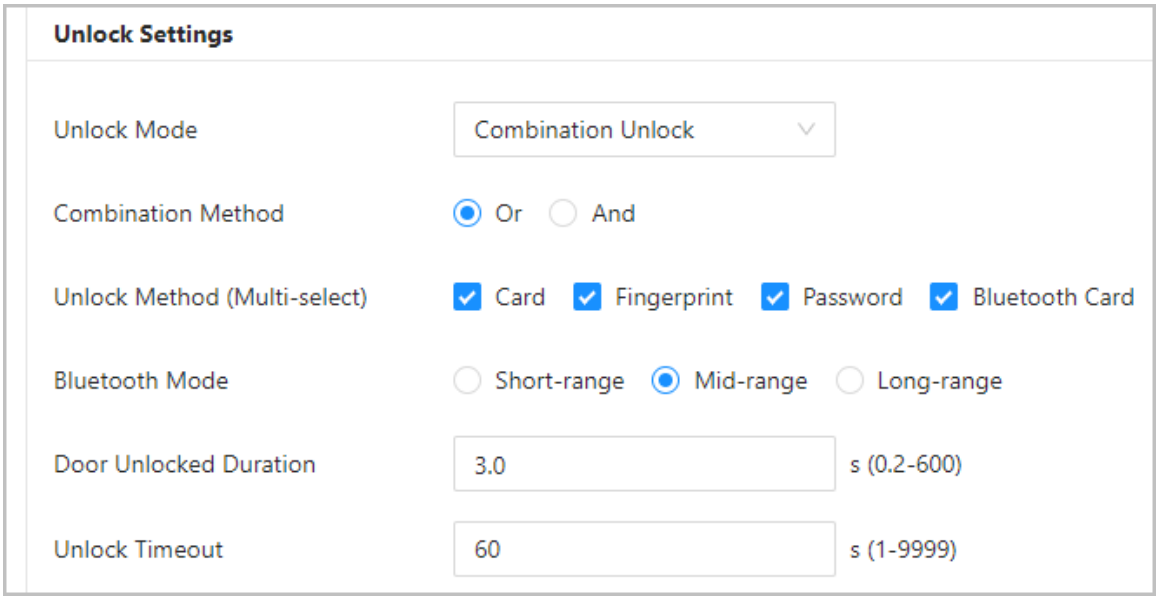



Tabla 2-2 Descripción de la configuración de desbloqueo

| Parámetro | Descripción |
|---|---|
| Método de desbloqueo (selección múltiple) | Admite desbloqueo mediante tarjeta, huella digital, contraseña o tarjeta Bluetooth. La función de tarjeta Bluetooth está desactivada de forma predeterminada. |

| Parámetro | Descripción |
|---|---|
| Modo Bluetooth | La tarjeta Bluetooth debe estar a cierta distancia del dispositivo de control de acceso para intercambiar datos y desbloquear la puerta. A continuación se detallan las gamas más adecuadas para ello.<br>● Corto alcance: el alcance de desbloqueo de Bluetooth es inferior a 0,2 m.<br>● Alcance medio: El alcance de desbloqueo de Bluetooth es inferior a 2 m.<br>● Largo alcance: el alcance de desbloqueo de Bluetooth es inferior a 10 m.<br>⚠<br>El rango de desbloqueo de Bluetooth puede variar según los modelos de su teléfono y el entorno. |
| Duración del desbloqueo 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. Varía de 0,2 sa 600 s. |
| 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. |

Paso 8 En**Configuración de alarma**, configure los parámetros de la alarma.

Figura 2-7 Alarma

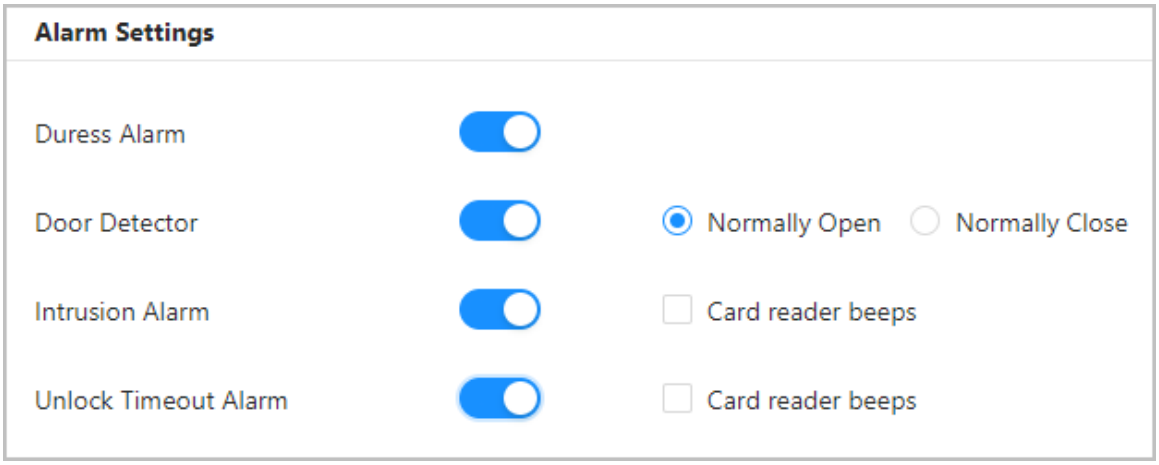



Tabla 2-3 Descripción de los parámetros de alarma

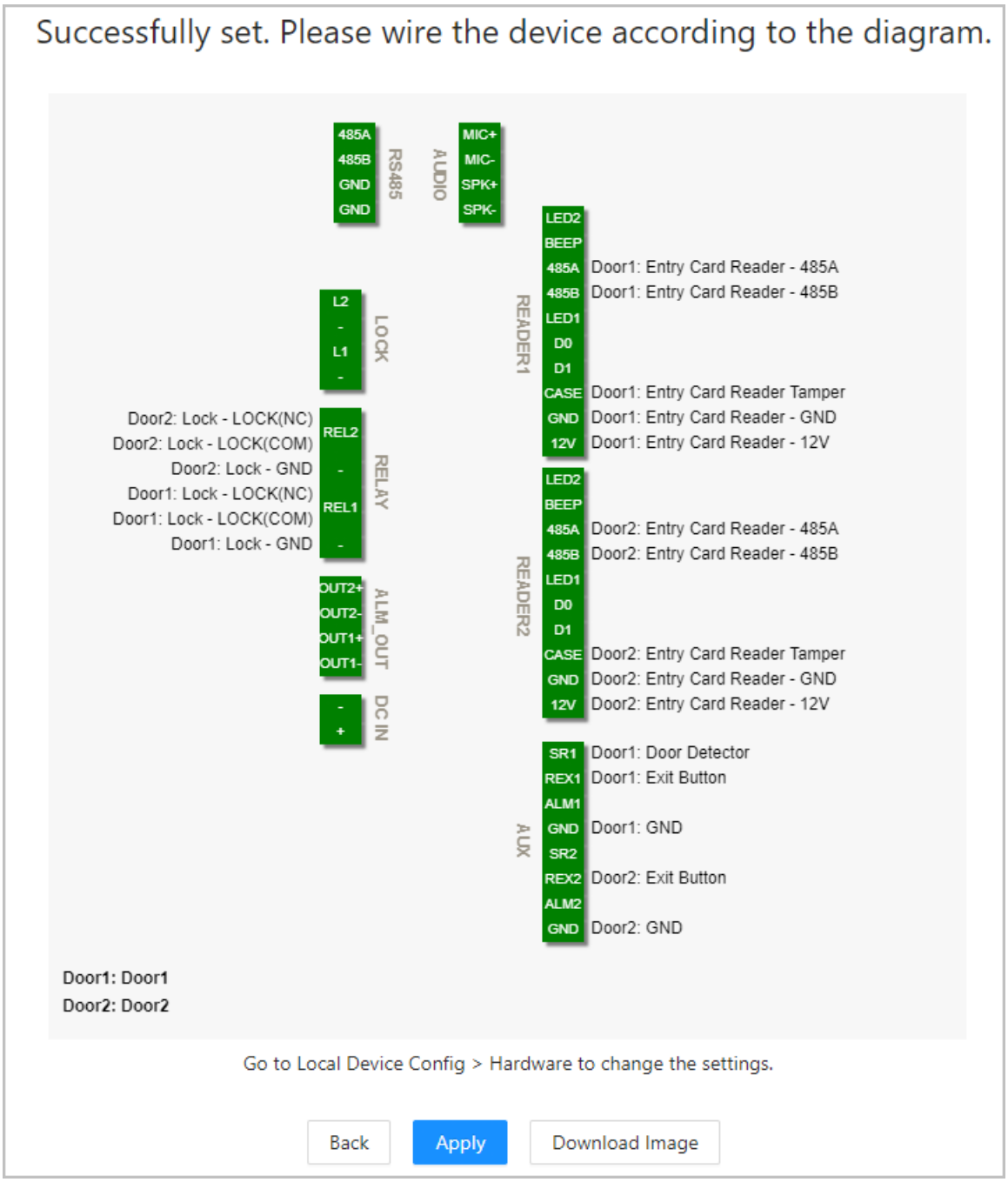
| Parámetro | Descripción |
|---|---|
| Alarma de coacción | Se activará una alarma cuando se utilice una tarjeta de coacción, una contraseña de coacción o una huella digital de coacción para desbloquear la puerta. |
| Detector de puerta | Seleccione el tipo de detector de puerta. |
| Alarma de intrusión | ● Cuando el detector de puerta está habilitado, se activará una alarma de intrusión si la puerta se abre de manera anormal.<br>● Se activará una alarma de tiempo de espera cuando la puerta permanezca desbloqueada durante más tiempo que el tiempo de desbloqueo definido.<br>● Cuando**El lector de tarjetas emite un pitido**está habilitado, el lector de tarjetas emite un pitido cuando se activa la alarma de intrusión o la alarma de tiempo de espera. |
| Desbloquear alarma de tiempo de espera | |

Paso 9 Hacer clic**Próximo**.

Se genera un diagrama de cableado en función de sus configuraciones. Puede cablear el dispositivo según el diagrama.

La imagen a continuación es solo como referencia.

Figura 2-8 Diagrama de cableado




Paso 10 Hacer clic**Aplicar**.

- Puedes ir a**Configuración del dispositivo local**>**Hardware**para cambiar la configuración después de iniciar sesión correctamente en la plataforma.
- Hacer clic**Descargar imagen**para descargar el diagrama a su computadora.

Operaciones relacionadas

Si desea cambiar la configuración del hardware, vaya a**Configuración del dispositivo local**>**Hardware**.

## 2.2.4 Panel de control

Después de iniciar sesión correctamente, se muestra la página del panel de la plataforma. Se muestra el panel que muestra los datos visualizados.

Figura 2-9 Panel de control

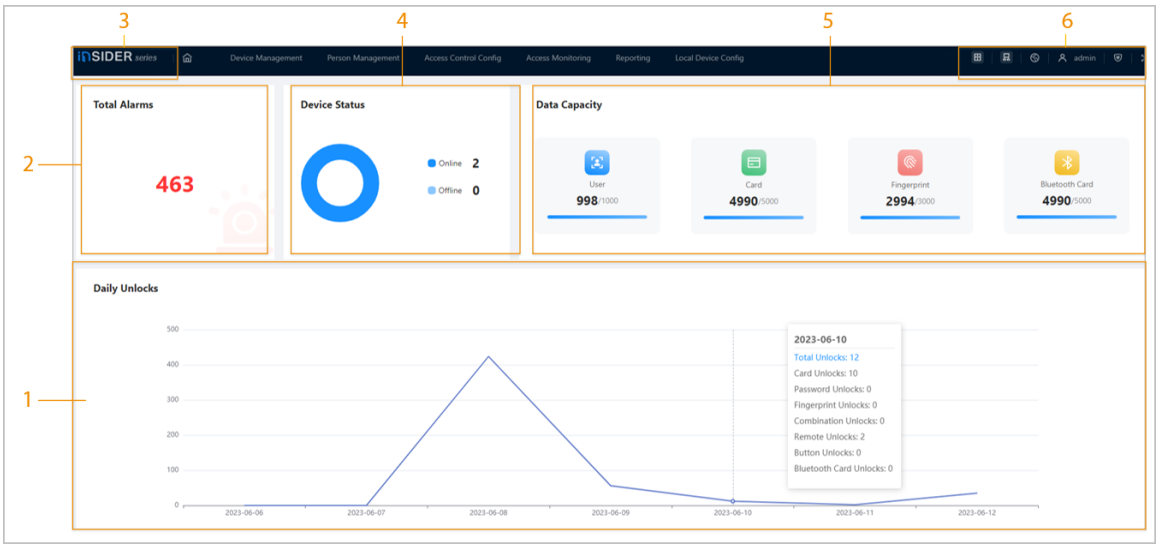



Tabla 2-4 Descripción de la página de inicio

| No. | Descripción |
|---|---|
| 1 | Muestra los métodos de desbloqueo utilizados durante el día. Pase el cursor sobre un día para ver el tipo de desbloqueos utilizados ese día. |
| 2 | Muestra el número total de alarmas. |
| 3 | • Haga clic para ir a la página del panel.<br>• Hacer clic para ir a la página del panel. para ir a<br>• Hacer clic la página de inicio de la plataforma. |
| 4 | Muestra el estado de los dispositivos, incluidos los dispositivos fuera de línea y en línea. |
| 5 | Muestra la capacidad de datos de tarjetas, huellas dactilares y tarjetas Bluetooth. |

| No. | Descripción |
|---|---|
| 6 | • El número de puertas del controlador.<br>◇ : Puerta doble<br>◇ : Puerta sencilla<br>• El tipo de controlador.<br>◇ : Controlador principal.<br>◇ : Subcontrolador.<br>• : Seleccione el idioma de la plataforma.<br>• : Ve a la**Seguridad**página directamente.<br>• : Reinicie o cierre sesión en la plataforma.<br>• : muestra la página web en pantalla completa. |

## 2.2.5 Página de inicio

Después de iniciar sesión correctamente, se muestra la página de inicio del controlador principal.

Figura 2-10 Página de inicio

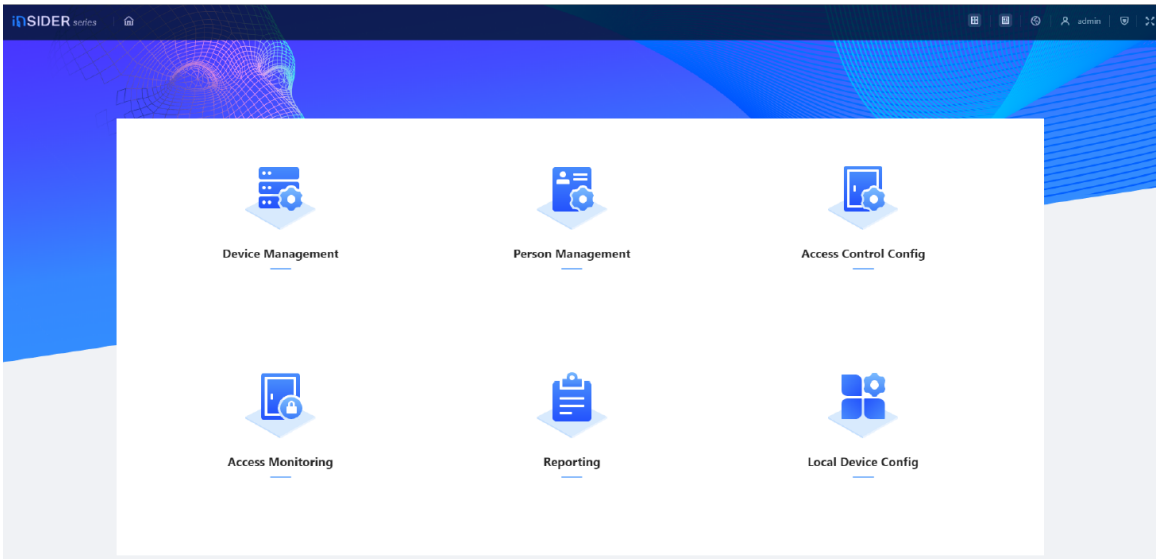



Tabla 2-5 Descripción de la página de inicio

| Menú | Descripción |
|---|---|
| Gestión de dispositivos | Agregue dispositivos a la plataforma del controlador principal. |
| Gestión de personas | Agregue personal y asígneles permisos de área. |
| Configuración de control de acceso | Agregue plantillas de tiempo, cree y asigne permisos de área, configure parámetros de puertas y vínculos de alarmas globales y vea el progreso de la autorización de permisos. |
| Monitoreo de acceso | Controle remotamente las puertas y vea los registros de eventos. |
| Informes | Ver y exportar registros de alarma y desbloquear registros. |

| Menú | Descripción |
|---|---|
| Configuración del dispositivo local | Configure los parámetros para el dispositivo local, como la red y el enlace de alarma local. |

## 2.2.6 Agregar dispositivos

Puede agregar dispositivos a la plataforma de gestión del controlador principal en lotes o uno por uno. Si el controlador se configuró como controlador principal mientras realizaba el asistente de inicio de sesión, puede agregar y administrar subcontroladores a través de la Plataforma.

Sólo el controlador principal viene con una plataforma de gestión.

### 2.2.6.1 Agregar dispositivos uno por uno

Puede agregar subcontroladores al controlador principal uno por uno.

Procedimiento

Paso 1 En la página de inicio, haga clic en**Gestión de dispositivos**,y luego haga clic**Agregar**.

Paso 2 Ingrese la información del dispositivo.

Figura 2-11 Información del dispositivo

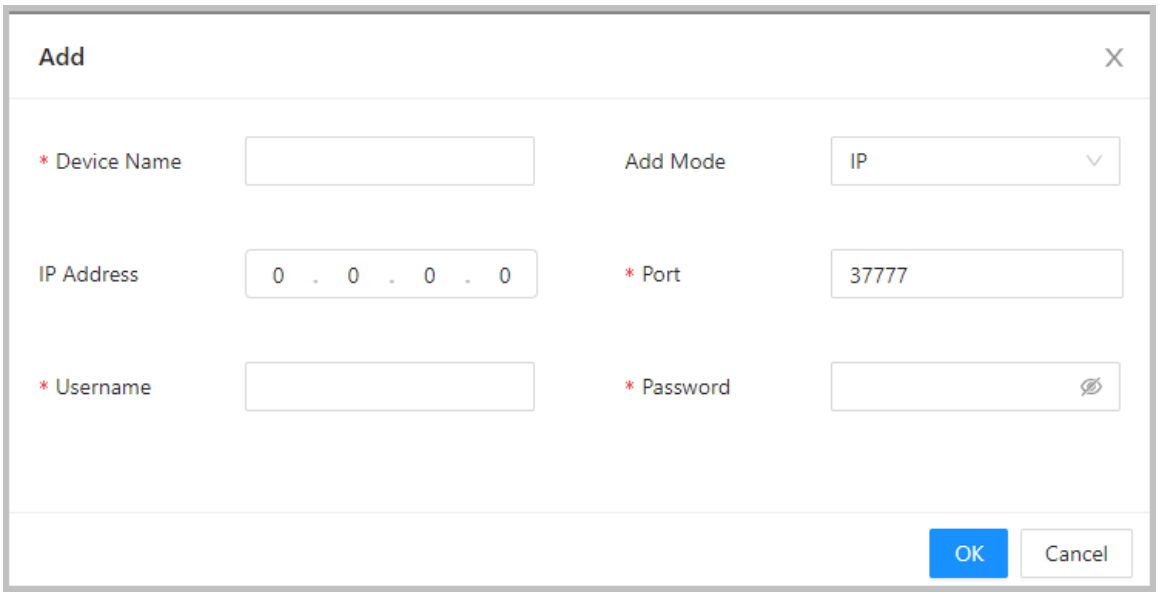



Tabla 2-6 Parámetros del dispositivo Descripción

| Parámetro | Descripción |
|---|---|
| Nombre del dispositivo | Ingrese el nombre del Controlador. Le recomendamos que le ponga el nombre de su área de instalación. |
| Agregar modo | Seleccionar**IP**para agregar el controlador de acceso ingresando su dirección IP. |
| Dirección IP | Introduzca la dirección IP del controlador. |
| Puerto | El número de puerto es 37777 de forma predeterminada. |
| Usuario Contraseña | Ingrese el nombre de usuario y contraseña del Controlador. |

Paso 3 Hacer clicDE ACUERDO.

Los controladores agregados se muestran en la**Gestión de dispositivos**página.

Figura 2-12 Agregar dispositivos exitosamente


Si el controlador se configuró como controlador principal mientras realizaba el asistente de inicio de sesión, el controlador se agregará a la plataforma de administración automáticamente y funcionará como controlador principal y subcontrolador.

Operaciones relacionadas

- : edita la información del dispositivo.

  Sólo los subcontroladores admiten las siguientes operaciones.
- : Vaya a la página web del subcontrolador.
- : cierre sesión en el dispositivo. :
- elimina el dispositivo.

## 2.2.6.2 Agregar dispositivos en lotes

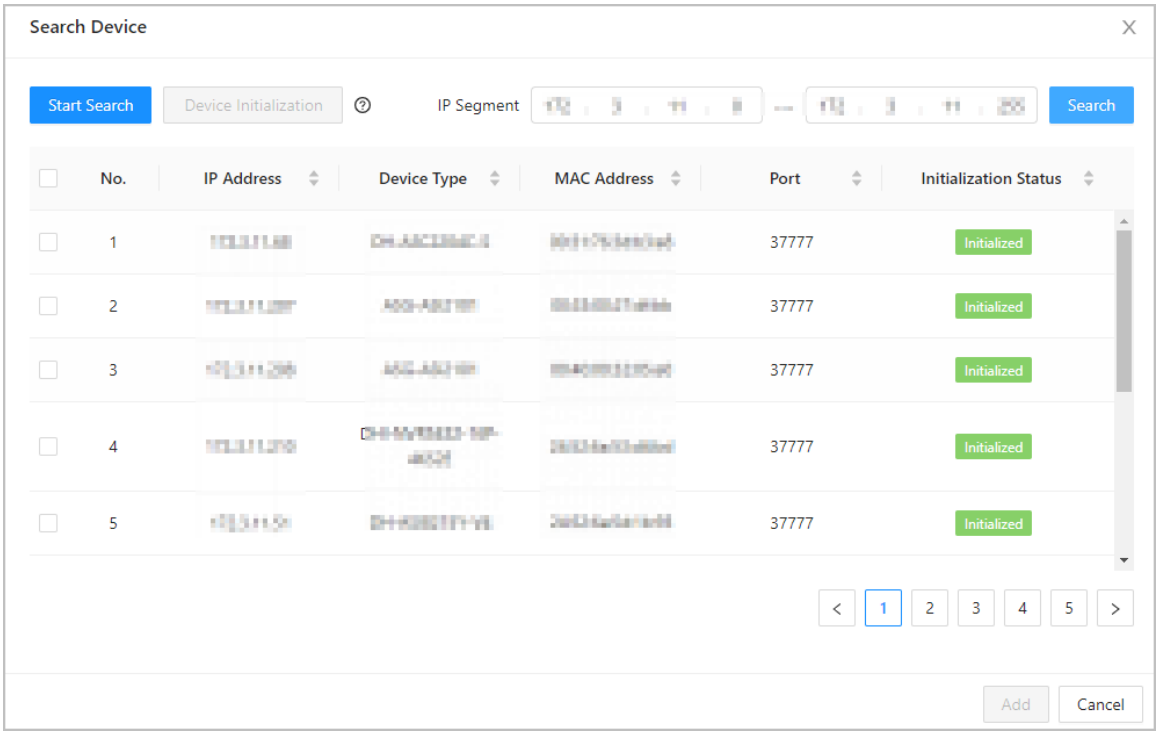
Le recomendamos que utilice la función de búsqueda automática cuando agregue subcontroladores en lotes. Asegúrese de que los subcontroladores que desea agregar estén en el mismo segmento de red.

Procedimiento

Paso 1 En la página de inicio, haga clic en**Gestión de dispositivos**,y luego haga clic**Dispositivo de búsqueda**.

- Hacer clic**Iniciar busqueda**para buscar dispositivos en la misma LAN.
- Introduzca un rango para el segmento de red y luego haga clic en**Buscar**.

Figura 2-13 Búsqueda automática




Se mostrarán todos los dispositivos que se buscaron.

Puede seleccionar dispositivos de la lista y hacer clic en**Inicialización del dispositivo**para inicializarlos en lotes.

Para garantizar la seguridad de los dispositivos, la inicialización no es compatible con dispositivos en diferentes segmentos.

Paso 2 Seleccione los controladores que desea agregar a la plataforma y luego haga clic en**Agregar**. Ingrese el

Paso 3 nombre de usuario y la contraseña del subcontrolador y luego haga clic en**DE ACUERDO**.

Los subcontroladores agregados se muestran en la**Gestión de dispositivos**página.

Operaciones relacionadas

- Modificar IP: seleccione los dispositivos agregados y luego haga clic en**Modificar IP**para cambiar sus direcciones IP.
- Hora de sincronización: seleccione los dispositivos agregados y luego haga clic en**Hora de sincronización**para sincronizar la hora de los dispositivos con el servidor NTP.
- Eliminar: seleccione los dispositivos y luego haga clic en**Borrar**para eliminarlos.

## 2.2.7 Agregar usuarios

Agregar usuarios a departamentos. Ingrese información básica para los usuarios y establezca métodos de verificación para verificar sus identidades.

Operaciones relacionadas

- Exportar todos los usuarios a Excel: En el**Gestión de personas**página, haga clic**Exportar**para exportar a todos los usuarios. También puede importar la información del usuario exportada a otros controladores.

Para evitar la pérdida de datos causada por daños de fuerza mayor al equipo, se recomienda exportar periódicamente los datos del usuario con fines de copia de seguridad.

- Importar usuarios: en el**Gestión de personas**página, haga clic**Descargar plantilla**, ingrese la información del usuario en la plantilla y luego haga clic en**Importar**para importar todos los usuarios.
- Extraiga todos los usuarios: en el**Gestión de personas**página, haga clic**Más**>**Extraer información de la persona**y seleccione un dispositivo para extraer todos los usuarios del subcontrolador y enviarles el Plataforma del controlador principal.

### 2.2.7.1 Agregar departamentos

Procedimiento

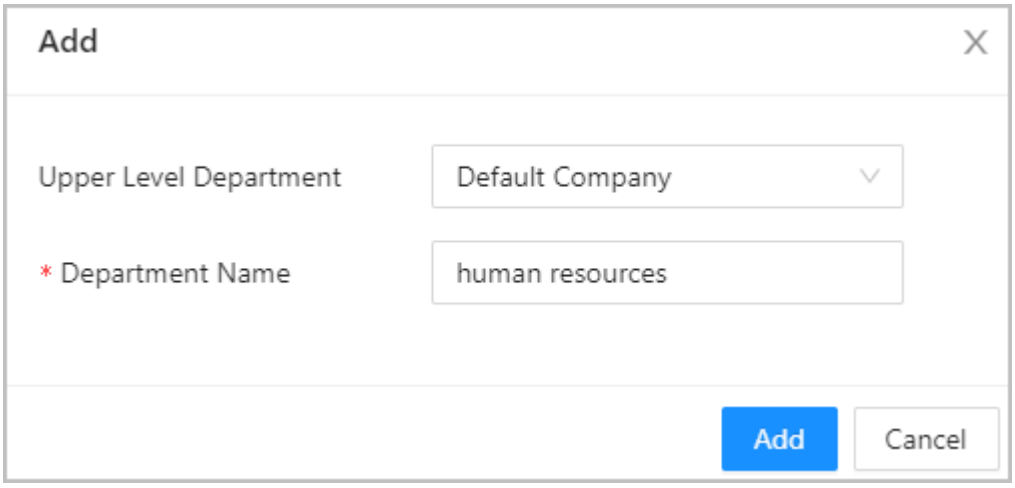
Paso 1 En la página de inicio, seleccione**Gestión de personas**.

Paso 2 Crea un departamento.

1. Haga clic en .
2. Ingrese el nombre del departamento y luego haga clic en**Agregar**.

El departamento predeterminado no se puede eliminar.

Figura 2-14 Agregar departamento




Paso 3 Hacer clic**DE ACUERDO**.

### 2.2.7.2 Agregar roles

Procedimiento

Paso 1 En la página de inicio, seleccione**Gestión de personas**.

Paso 2 Crea roles.

- Los siguientes roles ya existen y no se pueden modificar ni eliminar: Predeterminado, Gerente, Administrador, Visitante y Empleado.
- El único tipo de usuario general con rol de administrador tiene la máxima autoridad y no está limitado por reglas de acceso avanzadas, como desbloqueo con la primera tarjeta, desbloqueo para varias personas, antipassback, puerta siempre cerrada y métodos de desbloqueo.

1. Haga clic en .
2. Ingrese el nombre del rol y luego haga clic en**Agregar**.

### 2.2.7.3 Configuración de la información básica del usuario

Procedimiento

Paso 1 En la página de inicio, seleccione**Gestión de personas**. Agregar

Paso 2 usuarios.

- Agregue usuarios uno por uno.

  1. Haga clic**Agregar**y luego ingrese la información básica del usuario.

Figura 2-15 Información básica del usuario

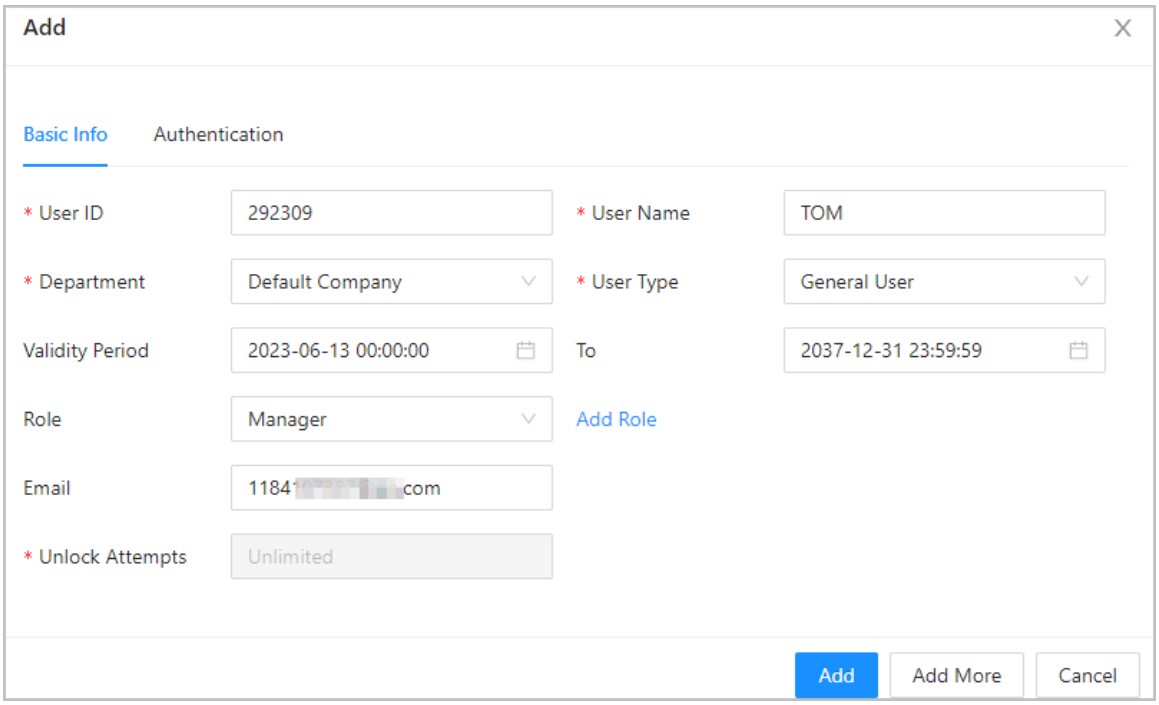



Tabla 2-7 Descripción de los parámetros

| Parámetro | Descripción |
|---|---|
| ID de usuario | La identificación del usuario. |
| Departamento | El departamento al que pertenece el usuario. Para obtener detalles sobre cómo crear departamentos, consulte "2.2.7.1 Agregar departamentos". |
| Período de validez | Establecer una fecha en la que los permisos de acceso de la persona se harán efectivos. |
| Role | Asigne un rol existente al usuario. También puedes hacer clic**Agregar rol**para crear un nuevo rol. |
| Correo electrónico | La dirección de correo electrónico debe ser la misma que se utilizó para registrarse en DMSS. |
| A | Establezca una fecha en la que expirarán los permisos de acceso de la persona. |
| Nombre de usuario | El nombre del usuario. |

| Parámetro | Descripción |
| --- | --- |
| Tipo de usuario | El tipo de usuario.<br>◇ **Usuario general**:Los usuarios generales pueden desbloquear la puerta.<br>◇ **Usuario VIP**:Cuando el VIP abra la puerta, el personal de servicio recibirá un aviso.<br>◇ **Usuario invitado**:Los huéspedes pueden desbloquear la puerta dentro de un período definido o durante un número determinado de veces. Una vez que expire el período definido o se agote el número de veces para desbloquear, no podrán desbloquear la puerta.<br>◇ **Usuario de patrulla**:Se realizará un seguimiento de la asistencia de los usuarios de la patrulla, pero no tendrán permiso para desbloquear la puerta.<br>◇ **Usuario de la lista de bloqueo**:Cuando los usuarios en la lista de bloqueo desbloquean la puerta, el personal de servicio recibirá una notificación.<br>◇ **Otro usuario**:Cuando desbloqueen la puerta, la puerta permanecerá desbloqueada durante 5 segundos más. |
| Intentos de desbloqueo | La cantidad de veces que un usuario invitado puede desbloquear la puerta. |

2. Haga clic**Agregar**.

Puedes hacer clic**Añadir más**para agregar más usuarios.

- Agregue usuarios importando la plantilla.

1. Haga clic**Importar**>**Descargar plantilla**para descargar la plantilla de usuario.
2. Ingrese la información del usuario en la plantilla y luego guárdela.
3. Haga clic**Importar**y suba la plantilla a la Plataforma.

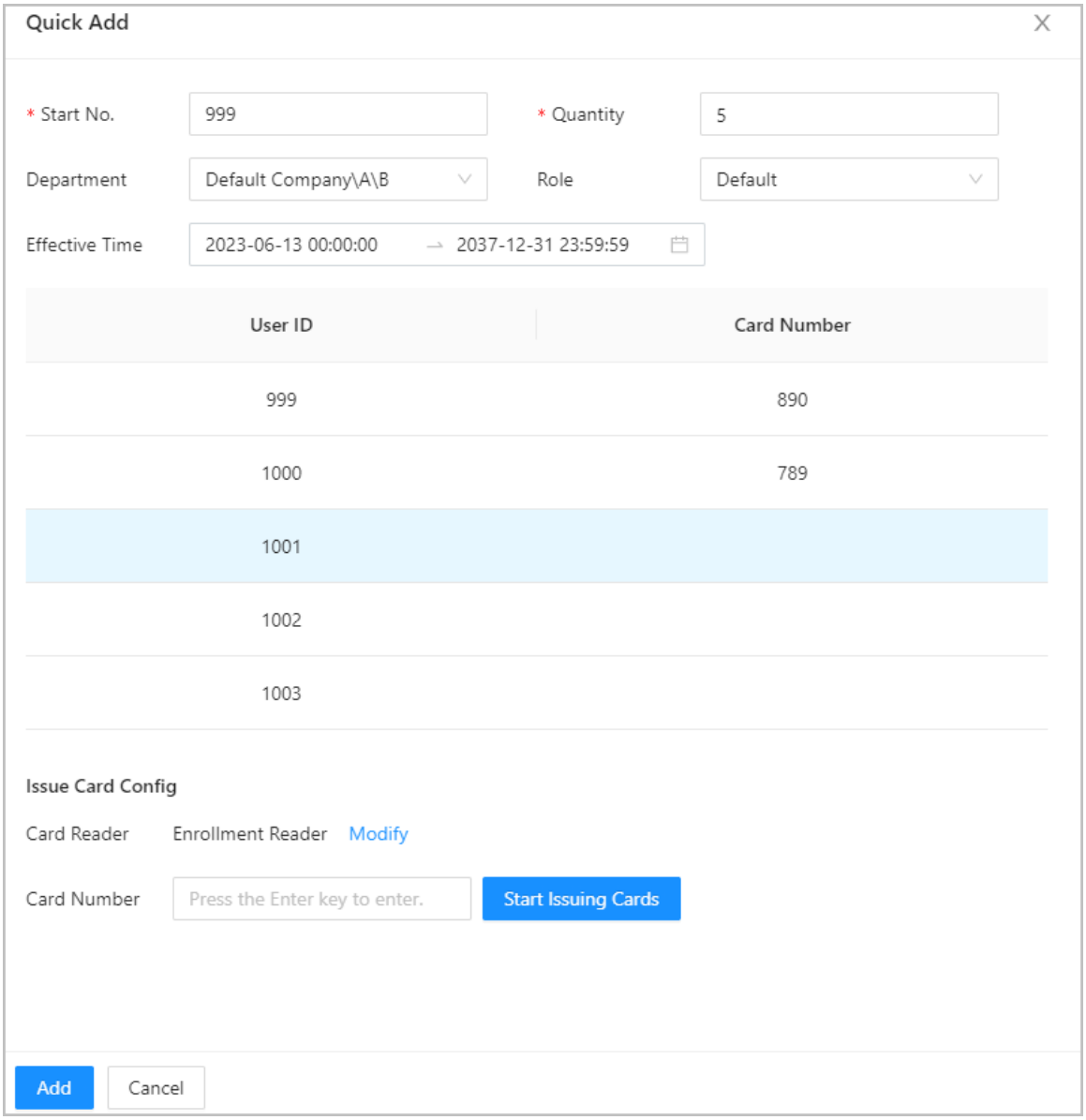
Los usuarios se agregan a la Plataforma automáticamente.

- Usar**Agregar rápido**para agregar usuarios fácilmente.

1. Haga clic**Agregar rápido**.
2. Ingrese el número inicial de la ID de usuario y la cantidad.

La plataforma generará una secuencia de números a partir del número inicial definido. Por ejemplo, si el número inicial es 999 y la cantidad es 5, el sistema generará una secuencia de números del 999 al 1003.

Figura 2-16 Agregar rápido



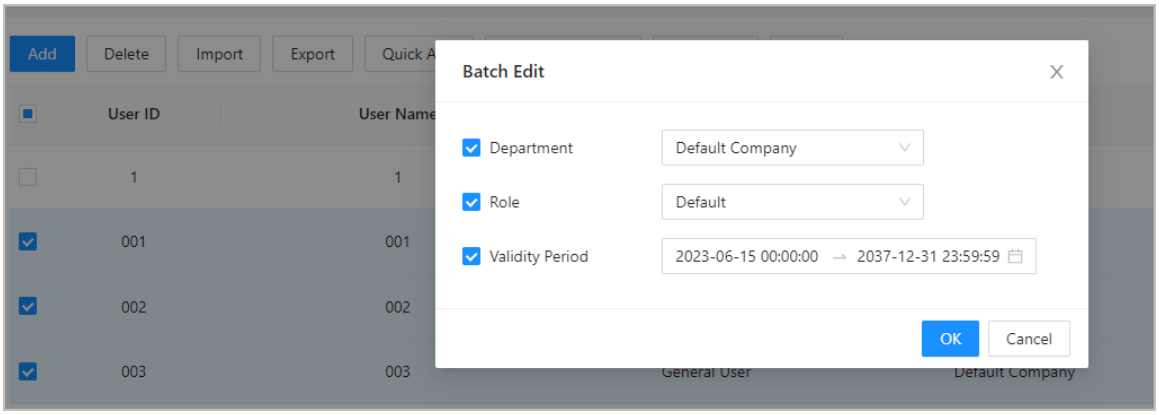

3. Seleccione el departamento, rol y tiempo de vigencia.
4. Emitir tarjetas a los usuarios en lotes.

   Puede ingresar manualmente el número de tarjeta o usar el lector de inscripción o el lector de tarjetas para leer el número de tarjeta. Para obtener más información, consulte "2.2.7.4.2 Agregar tarjetas".

Operaciones relacionadas

Edición por lotes: edite información personal en lotes.

Figura 2-17 Edición por lotes




## 2.2.7.4 Agregar métodos de autenticación

Agregue contraseñas, tarjetas, huellas dactilares o tarjetas Bluetooth a los usuarios, para que los usuarios puedan desbloquear la puerta mediante autenticación. Cada usuario puede tener hasta 1 contraseña, 5 tarjetas IC/ID, 3 huellas digitales y 5 tarjetas Bluetooth.

### 2.2.7.4.1 Agregar contraseñas

Agregue contraseñas a los usuarios para que puedan acceder ingresando su contraseña.

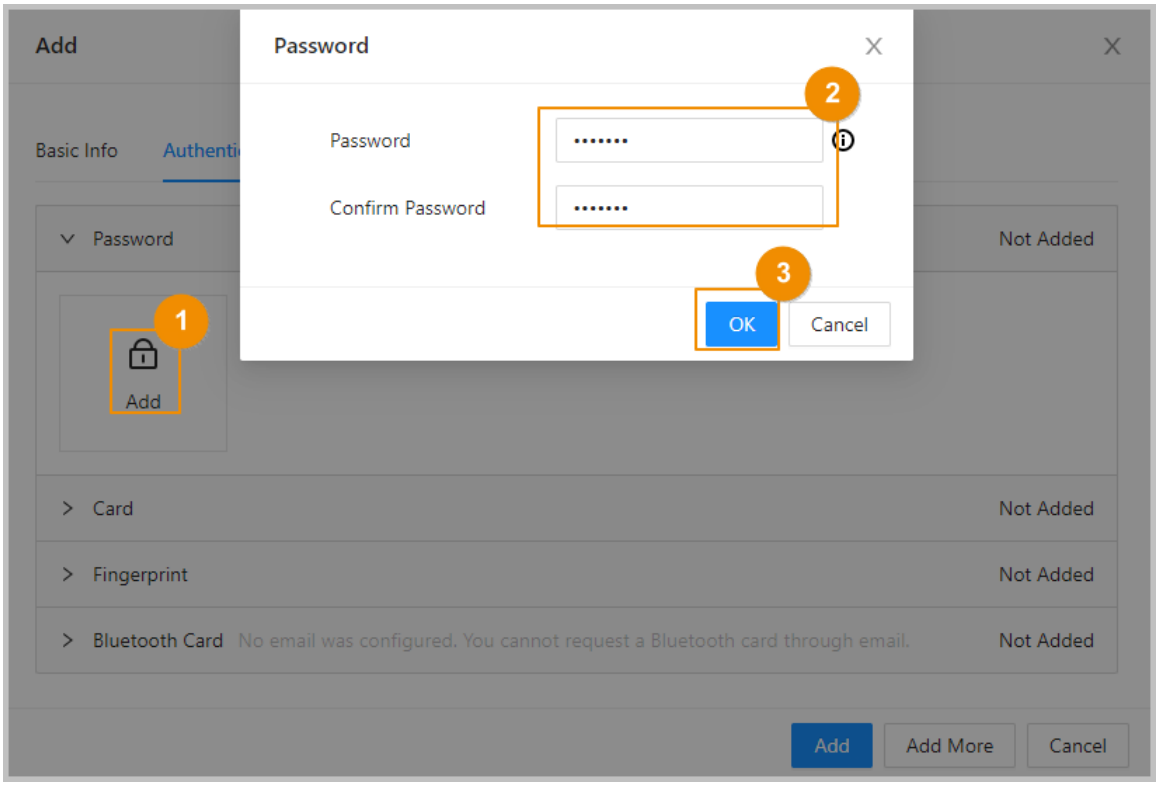
Procedimiento

Paso 1 Sobre el**Autenticación**pestaña, haga clic**Agregar**

Paso 2 Ingrese y confirme la contraseña. Hacer clic**DE**

Paso 3 **ACUERDO**.

Figura 2-18 Agregar la contraseña




- Si la autenticación con código PIN no está habilitada, puede desbloquear la puerta ingresando la contraseña de desbloqueo en el formato de**contraseña del usuario#**.Por ejemplo, si el ID de usuario es 123 y la contraseña que estableció es 12345, entonces debe ingresar**123#12345#**para desbloquear la puerta.
- Si la autenticación con código PIN está habilitada, puede desbloquear la puerta ingresando la contraseña de desbloqueo en el formato de**contraseña#**.Por ejemplo, si el ID de usuario es 123 y la contraseña que estableció es 12345, entonces debe ingresar**12345#**para desbloquear la puerta.

### 2.2.7.4.2 Agregar tarjetas

Agregue tarjetas IC o tarjetas de identificación a los usuarios para que puedan acceder deslizando sus tarjetas

Procedimiento

Paso 1 (Opcional) Antes de asignar tarjetas a los usuarios, configure el tipo de tarjeta y el tipo de número de tarjeta.

1. Sobre el**Gestión de personas**página, seleccione**Más**>**Tipo de tarjeta**.
2. Si planea emitir tarjetas mediante el uso del lector de inscripción, seleccione un tipo de tarjeta y luego haga clic en**DE ACUERDO**.

Asegúrese de que el tipo de tarjeta sea el mismo que el tipo de tarjeta que se emitirá cuando planee emitir tarjetas mediante el uso del lector de inscripción. Para obtener más información, consulte Haga clic en Agregar. Haga clic en Modificar y luego seleccione Lector de inscripción. Asegúrese de que el lector de inscripción de tarjetas esté conectado a su computadora. Siga las instrucciones que aparecen en pantalla para descargar e instalar el complemento. Haga clic en Leer tarjeta y luego pase las tarjetas por el lector de inscripción. Se muestra una cuenta atrás de 60 segundos para recordarle que pase la tarjeta y el sistema

leerá el número de tarjeta automáticamente. Si la cuenta regresiva de 60 segundos expira, haga clic en Leer tarjeta nuevamente para iniciar una nueva cuenta regresiva. Haga clic en Agregar. .

3. Seleccione**Más**>**Sistema de número de tarjeta**.

4. Seleccione el formato decimal o hexadecimal para el número de tarjeta.

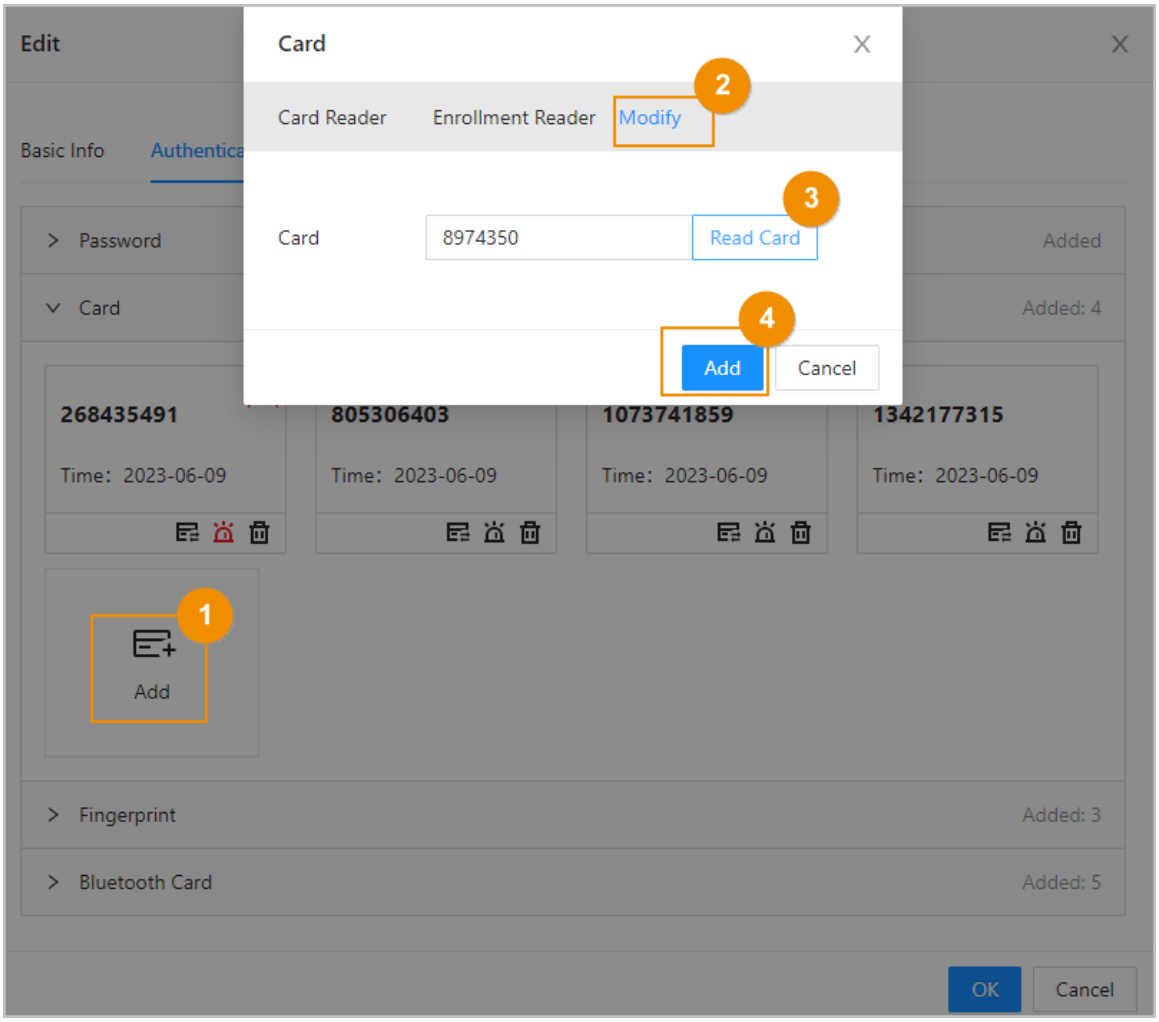
Paso 2 Sobre el**Autenticación**pestaña, haga clic**Tarjeta**para agregar tarjetas. Hay 4 métodos disponibles para agregar tarjetas.

- Ingrese el número de tarjeta manualmente.

  1. Haga clic**Agregar**.
  2. Ingrese el número de tarjeta y luego haga clic en**Agregar**.

- Utilice el lector de inscripción para leer el número de tarjeta.

Figura 2-19 Utilice el lector de inscripción para leer el número de tarjeta




1. Haga clic**Agregar**.
2. Haga clic**Modificar**,y luego seleccione**Lector de inscripción**.

   Asegúrese de que el lector de inscripción de tarjetas esté conectado a su computadora.

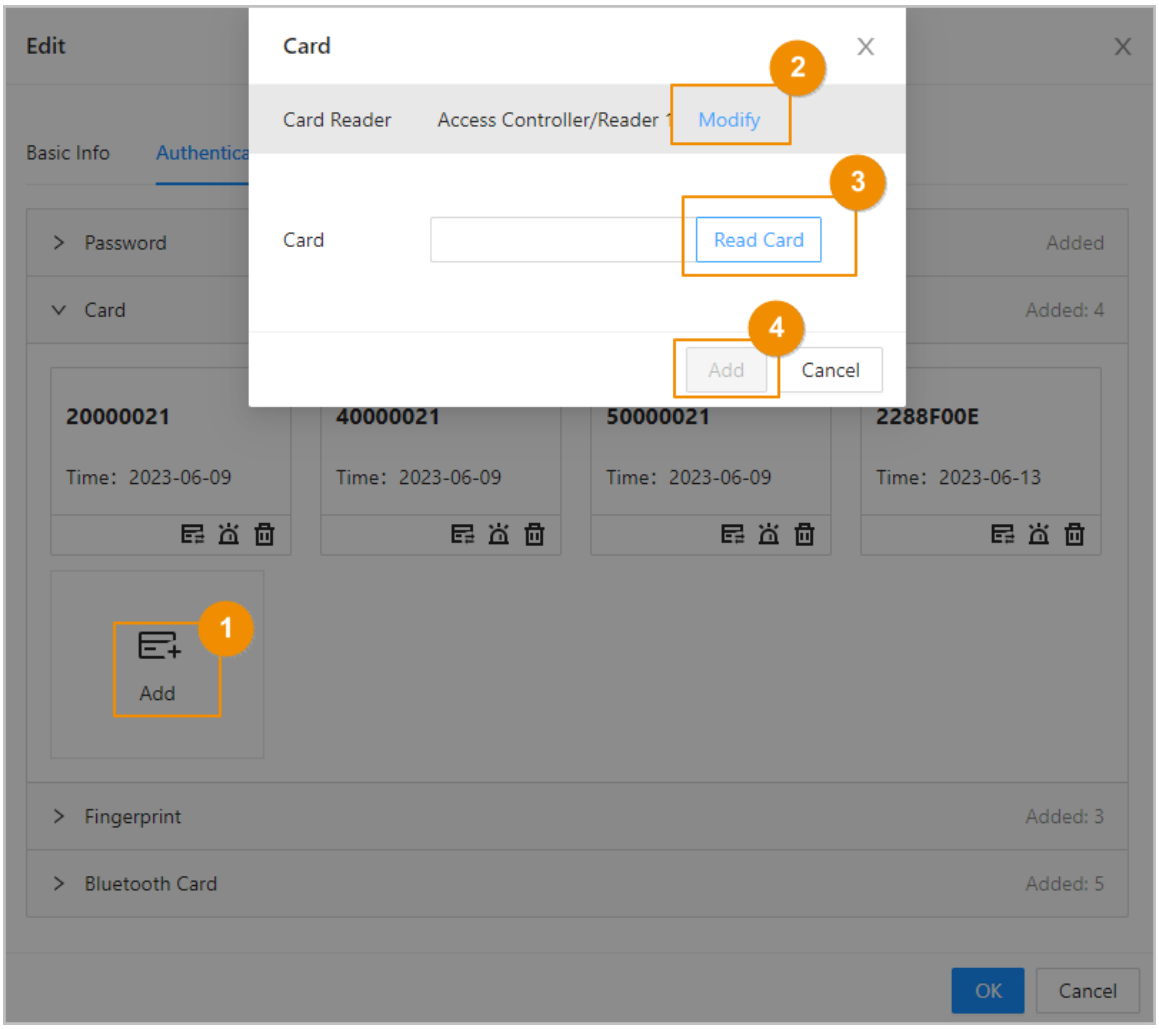
3. Siga las instrucciones que aparecen en pantalla para descargar e instalar el complemento.
4. Haga clic**Leer tarjeta**y luego pase las tarjetas por el lector de inscripción.

   Se muestra una cuenta atrás de 60 segundos para recordarle que pase la tarjeta y el sistema leerá el número de la tarjeta automáticamente. Si la cuenta regresiva de 60 segundos expira, haga clic en**Leer tarjeta**nuevamente para iniciar una nueva cuenta regresiva.

5. Haga clic**Agregar**.

- Utilice el lector de tarjetas para leer el número de tarjeta.

Figura 2-20 Utilice el lector de tarjetas para leer el número de tarjeta




1. Haga clic**Modificar**y luego seleccione un lector de tarjetas.

   Asegúrese de que el lector de tarjetas esté conectado al controlador de acceso.

2. Haga clic**Leer tarjeta**y luego pase las tarjetas por el lector de tarjetas.

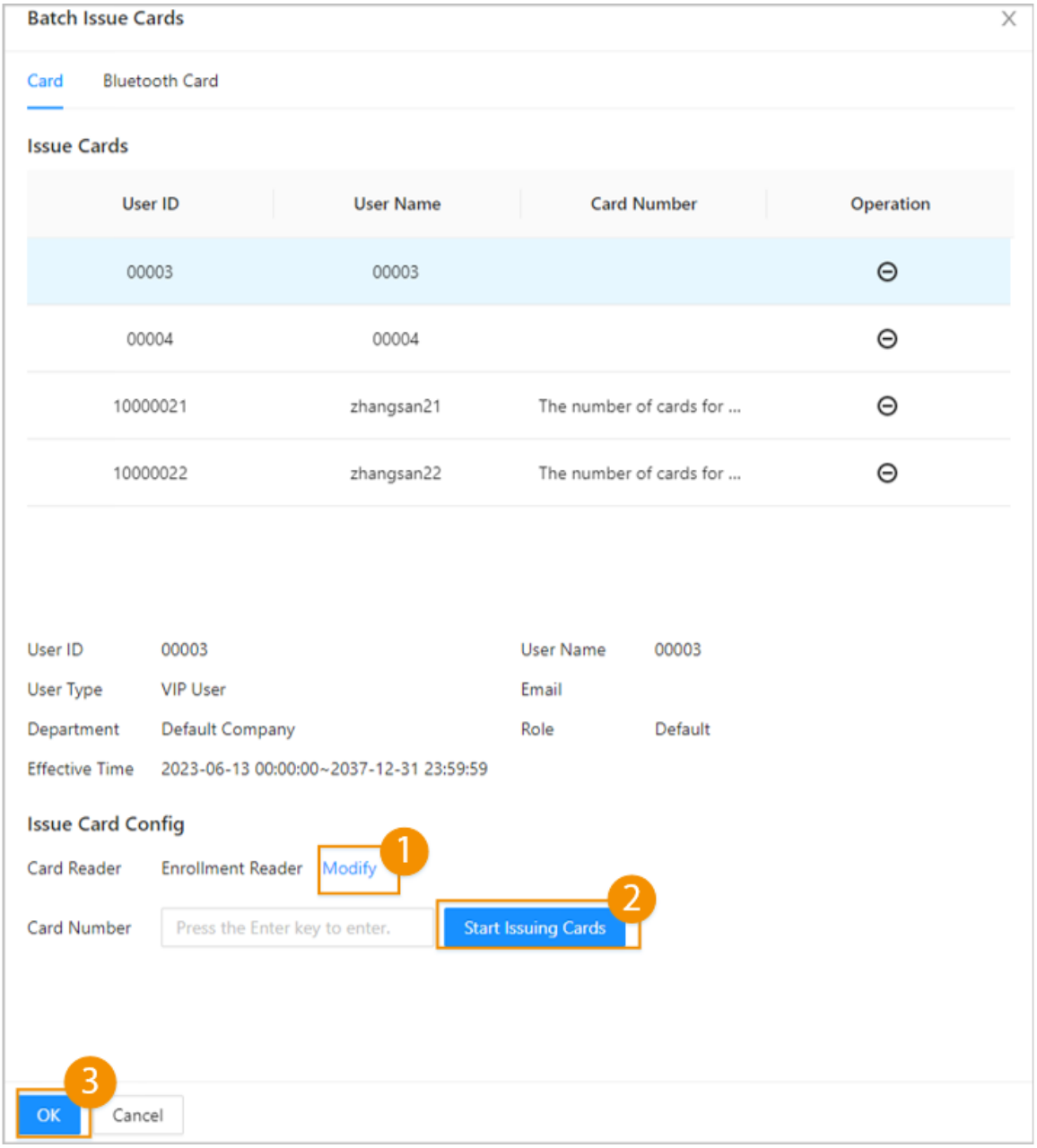
   Se muestra una cuenta atrás de 60 segundos para recordarle que pase la tarjeta y el sistema leerá el número de la tarjeta automáticamente. Si la cuenta regresiva de 60 segundos expira, haga clic en**Leer tarjeta**nuevamente para iniciar una nueva cuenta regresiva.

3. Haga clic**Agregar**.

- Agregar tarjetas en lotes: Emita tarjetas a los usuarios en lotes.

1. Haga clic**Tarjetas de emisión por lotes**,y luego seleccione**Emitir tarjetas a usuarios seleccionados**o**Emitir tarjetas a todos los usuarios**.
2. Puede ingresar manualmente el número de tarjeta o hacer clic en**Modificar**para emitir tarjetas a través del lector de matrícula o lector de tarjetas.

Figura 2-21 Emitir tarjetas a través del lector de inscripción o lector de tarjetas




Operaciones relacionadas

- : Cambia el número de la tarjeta. : configura
- la tarjeta como tarjeta de coacción.

  Se activa una alarma cuando las personas usan la tarjeta de coacción para desbloquear la puerta.
- : elimina la tarjeta.

### 2.2.7.4.3 Agregar huellas digitales

Agregue huellas digitales a los usuarios para que puedan usar su huella digital para desbloquear puertas.

Procedimiento

Paso 1 Sobre el**Autenticación**pestaña, haga clic**Huella dactilar**.

Paso 2 Conecte un escáner de huellas digitales a la computadora y siga las instrucciones que aparecen en pantalla para registrar la huella digital.

Paso 3 Hacer clic**Agregar**.

### 2.2.7.4.4 Agregar tarjetas Bluetooth

Agregue tarjetas Bluetooth a los usuarios para que puedan acceder a través de tarjetas Bluetooth.

Requisitos previos

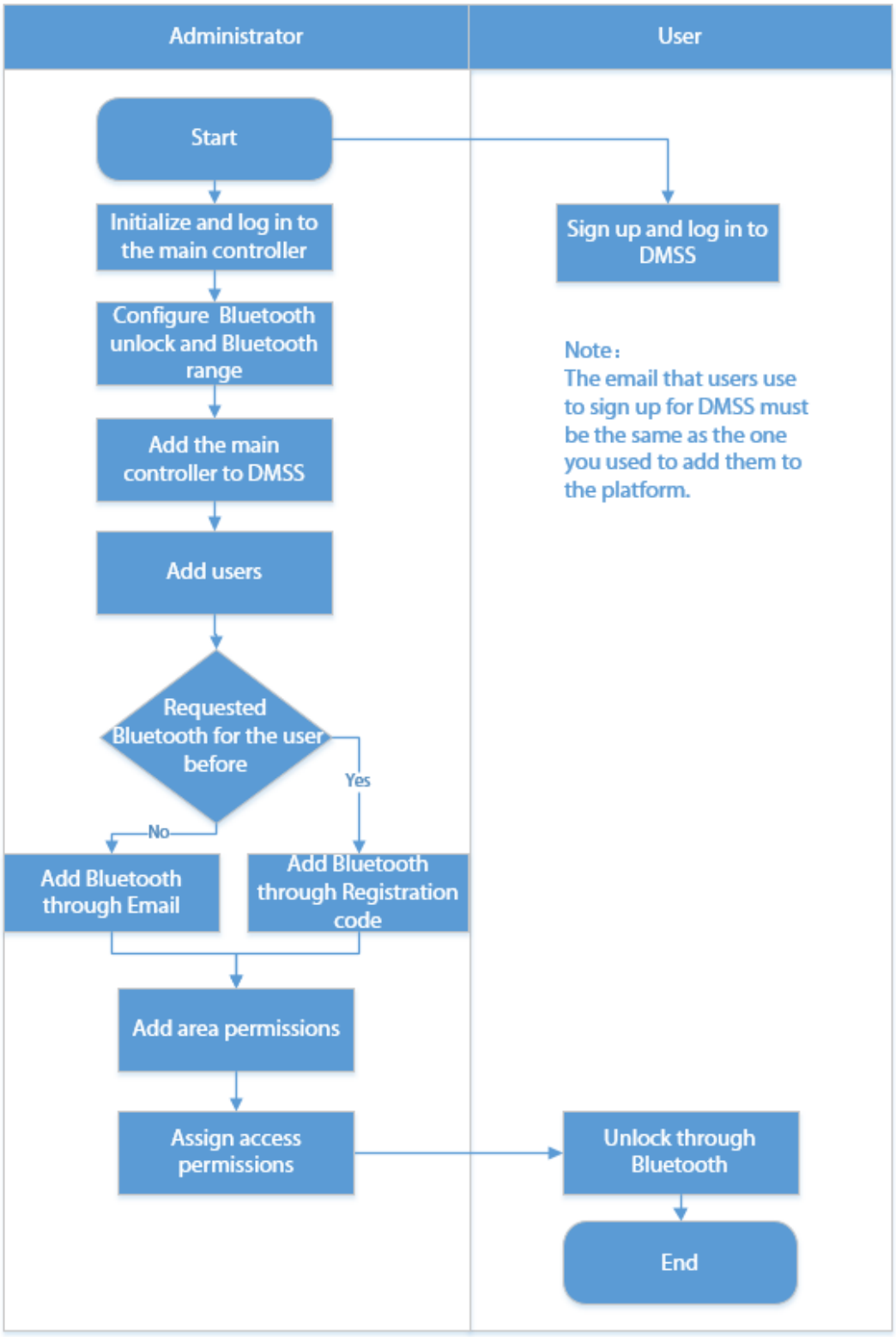
- La función de desbloqueo de Bluetooth se ha activado.
- El controlador principal se ha agregado a DMSS. Para obtener más información, consulte "2.2.21.4.3 Configuración del servicio en la nube".
- Los usuarios han sido agregados a la Plataforma del Controlador de Acceso. Para obtener más información, consulte "2.2.7.3 Configuración de la información básica del usuario".
- Los usuarios generales, como los empleados de la empresa, han instalado y registrado DMSS con su correo electrónico.

  El correo electrónico que los usuarios utilizan para registrarse en DMSS debe ser el mismo que utilizó para agregarlos al controlador de acceso.

## Información de contexto

Consulte el diagrama de flujo para configurar el desbloqueo de Bluetooth. Los administradores y los usuarios generales deben realizar diferentes operaciones para completar el proceso. Los usuarios generales, como los empleados de la empresa, sólo necesitan registrarse e iniciar sesión en DMSS con su correo electrónico para desbloquear las puertas utilizando las tarjetas Bluetooth que se les entregaron.

Figura 2-22 Diagrama de flujo para configurar el desbloqueo de Bluetooth




Procedimiento

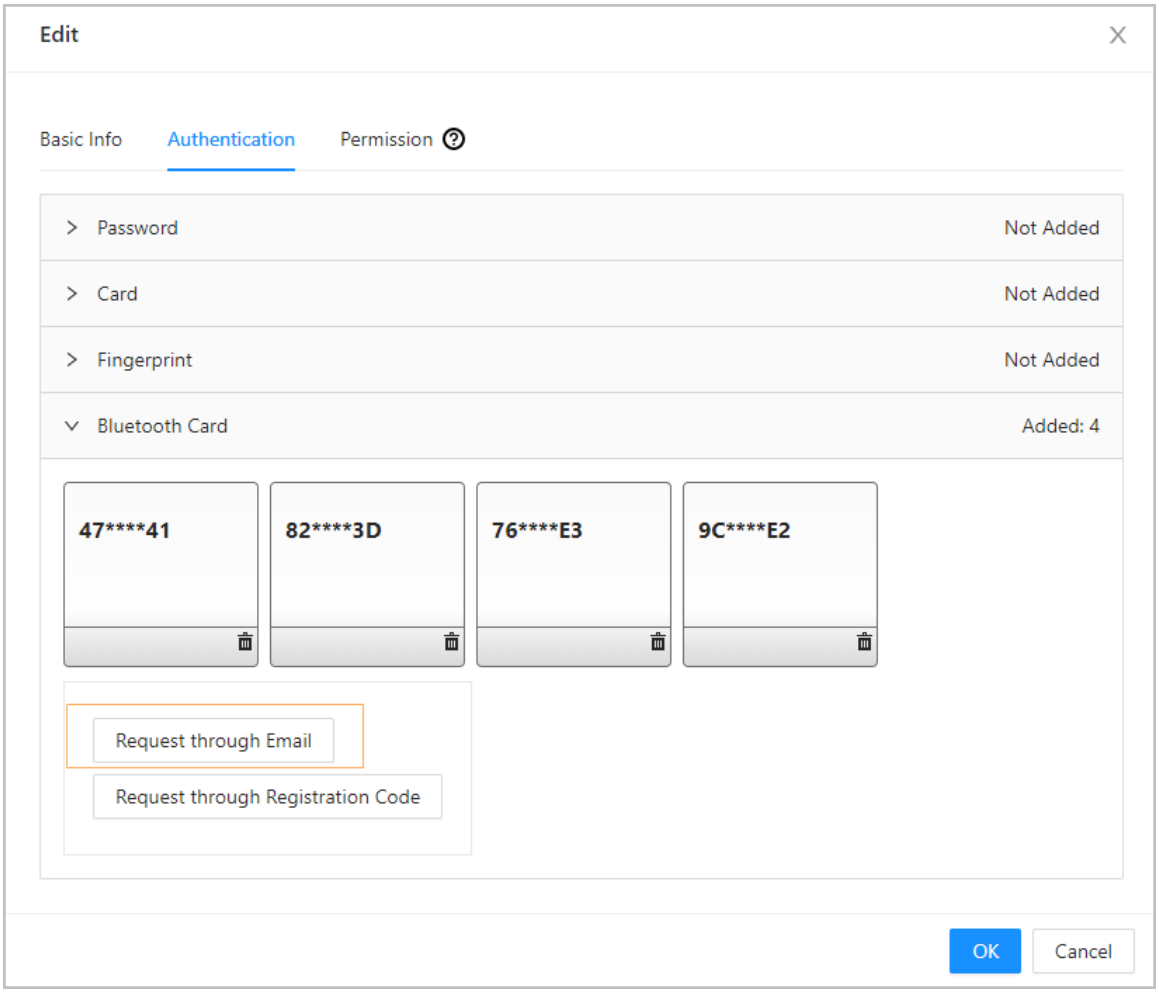
Paso 1 En la pestaña, haga clic en**Tarjeta Bluetooth**.

Hay 3 métodos disponibles para agregar tarjetas Bluetooth.

- Solicite por correo electrónico uno por uno: haga clic**Solicitar por correo electrónico**.

  Se genera automáticamente una tarjeta Bluetooth. Puedes generar hasta 5 tarjetas para cada usuario.

Figura 2-23 Solicitud por correo electrónico




- Solicite por correo electrónico en lotes.

  1. Sobre el**Gestión de personas**página, haga clic**Tarjetas de emisión por lotes**.

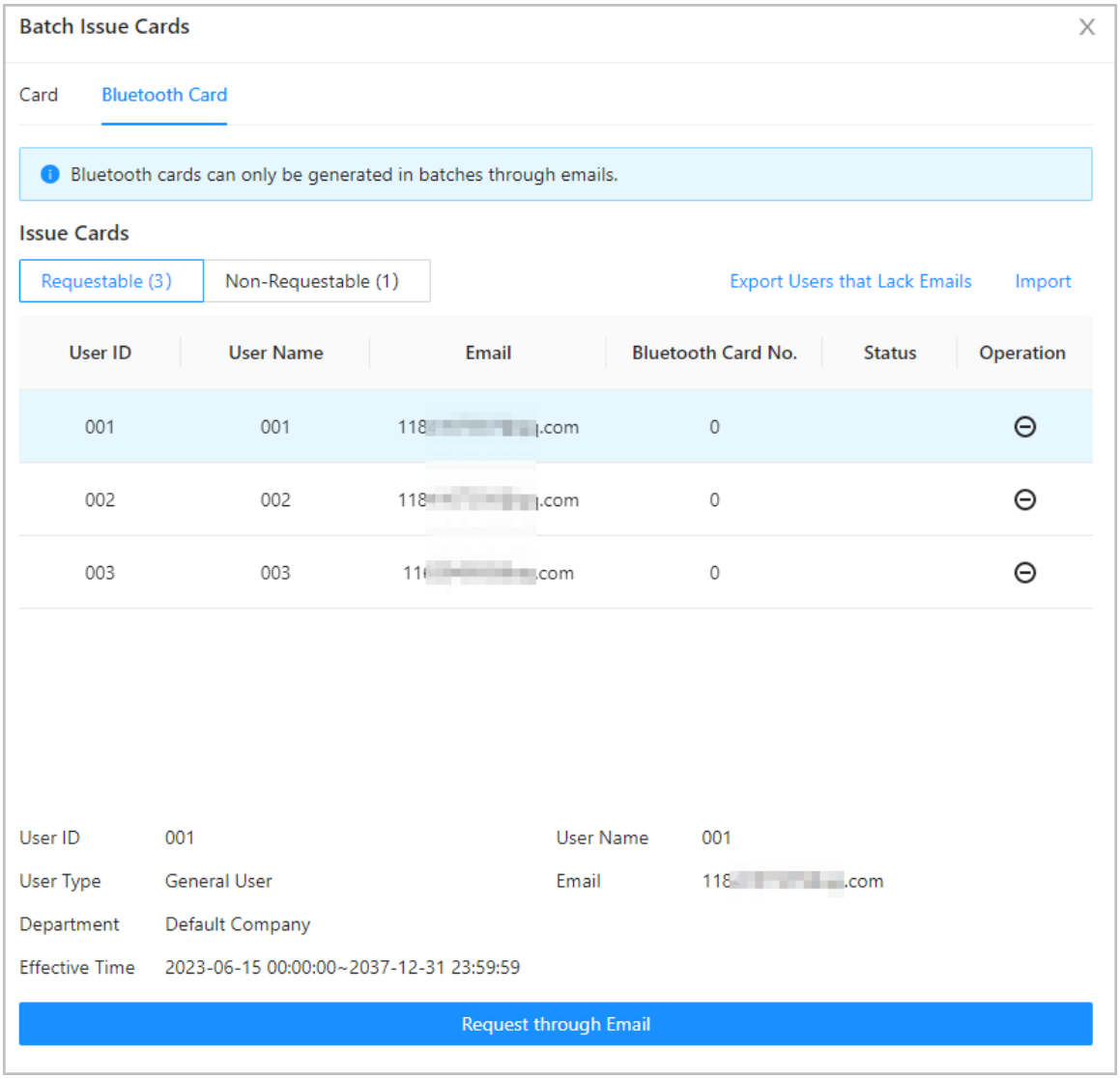
     Las tarjetas de emisión por lotes solo admiten solicitudes por correo electrónico.

     - Emitir tarjetas Bluetooth a todos los usuarios de la lista: haga clic en**Emitir tarjetas a todos los usuarios**.
     - Emitir tarjetas Bluetooth a usuarios seleccionados: seleccione usuarios y luego haga clic en**Emitir tarjetas a usuarios seleccionados**.

  2. Haga clic**Tarjeta Bluetooth**.
  3. Haga clic**Solicitar por correo electrónico**.

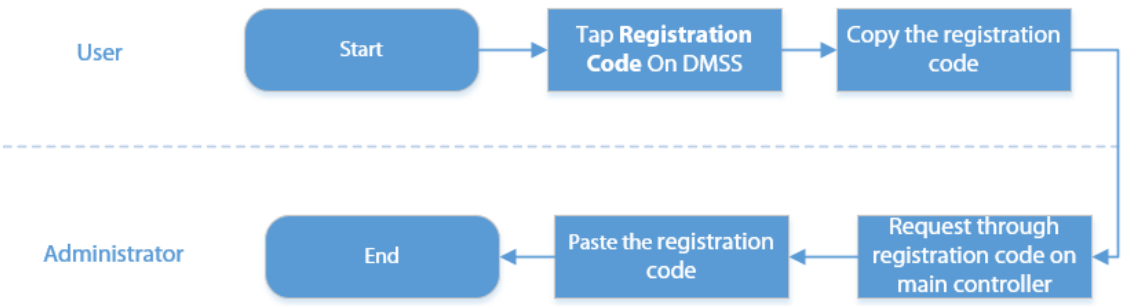
     - Los usuarios que no tengan un correo electrónico o que ya tengan 5 tarjetas Bluetooth aparecerán en la lista de no solicitables.
     - Exportar usuarios que carecen de correos electrónicos: Haga clic**Exportar**,ingrese los correos electrónicos en el formato correcto y luego haga clic en**Importar**. Serán trasladados a la lista de solicitudes.

Figura 2-24 Tarjetas de emisión de lotes




- Si ha solicitado tarjetas Bluetooth para el usuario anteriormente, puede agregar las tarjetas Bluetooth mediante el código de registro. utilizando códigos de registro.

Figura 2-25 Diagrama de flujo para solicitar a través del código de registro

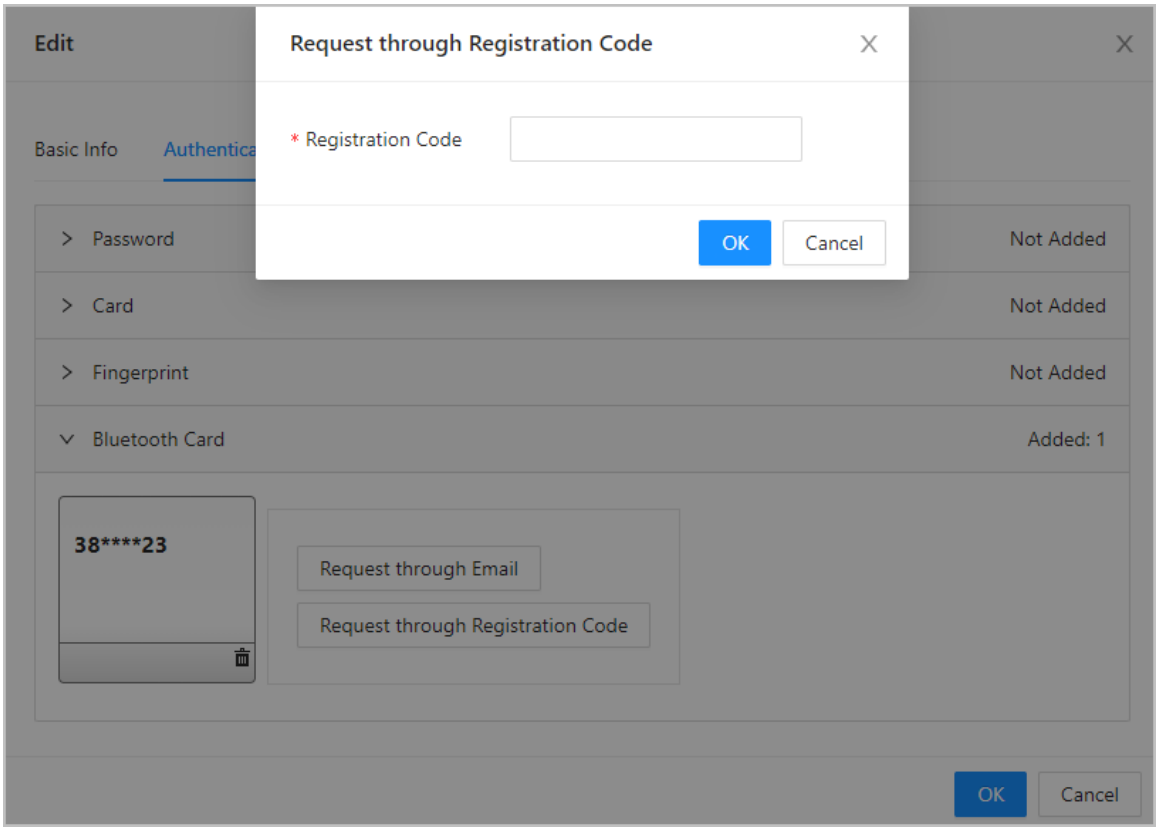



1. En DMSS, toque**Código de registro**de una tarjeta Bluetooth.

   El código de registro lo genera automáticamente DMSS.
2. Copie el código de registro.

3. En el**Tarjeta Bluetooth**pestaña, haga clic**Solicitar a través del Código de Registro**, pegue el código de registro y luego haga clic en**DE ACUERDO**.

Figura 2-26 Solicitud mediante código de registro




4. Haga clic**DE ACUERDO**.

Se agrega la tarjeta Bluetooth. Hacer clic**DE**

Paso 2 **ACUERDO**.

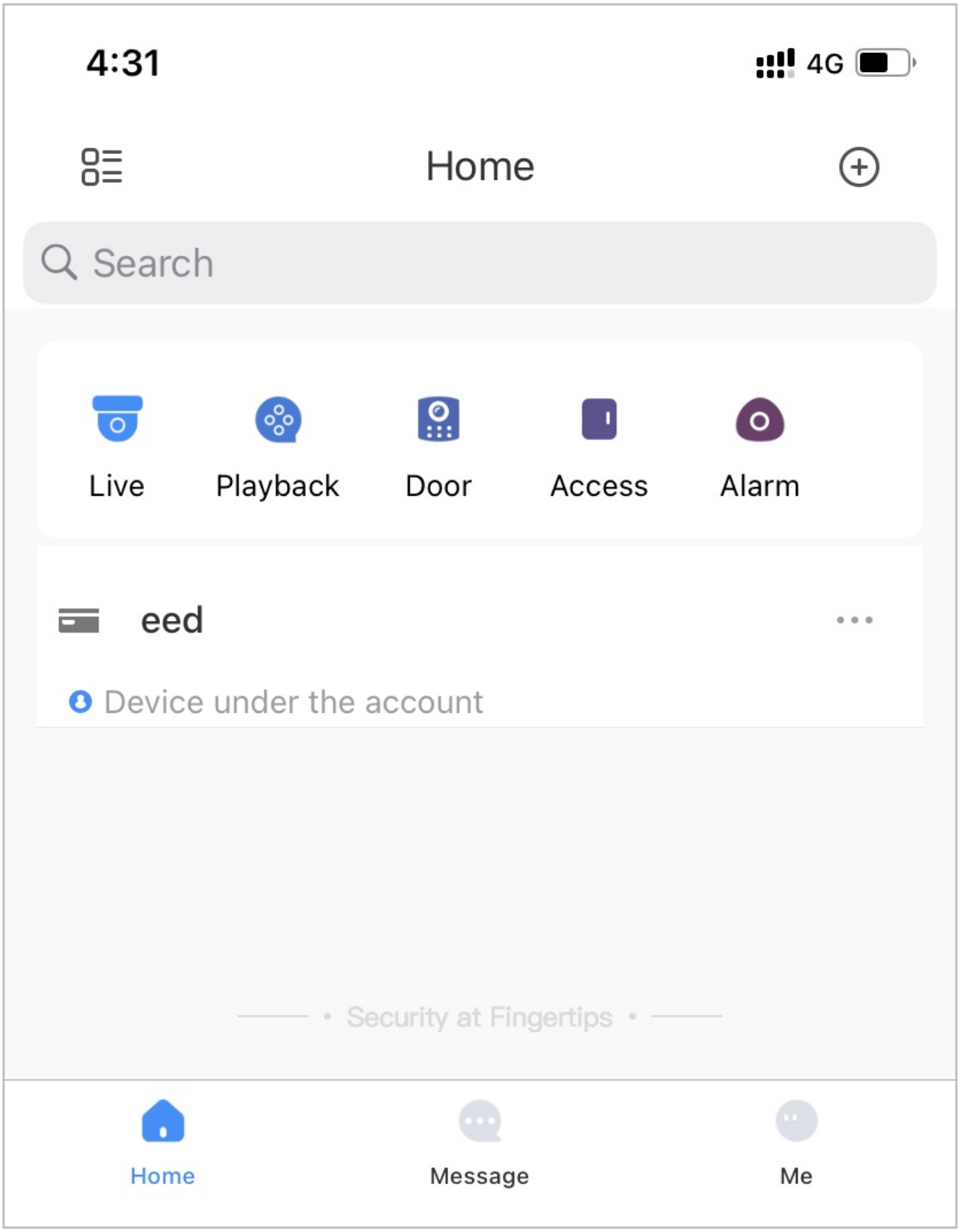
Resultados

Después de que los usuarios se registren e inicien sesión en DMSS con la dirección de correo electrónico, pueden abrir DMSS para desbloquear la puerta mediante tarjetas Bluetooth. Para obtener más información, consulte el manual del usuario de DMSS.

- Desbloqueo automático: la puerta se desbloquea automáticamente cuando se encuentra dentro del rango de Bluetooth definido, lo que permite que la tarjeta Bluetooth transmita señales al lector de tarjetas.

  En el modo de desbloqueo automático, la tarjeta Bluetooth puede desbloquear continuamente la puerta cuando se encuentre dentro del alcance de Bluetooth durante un período prolongado hasta que se produzca una falla. Apague el Bluetooth en el teléfono y luego vuelva a encenderlo.
- Agite para desbloquear: la puerta se desbloquea cuando agita su teléfono para permitir que la tarjeta Bluetooth transmita señales al lector de tarjetas.

Figura 2-27 Desbloqueo de la puerta mediante tarjetas Bluetooth

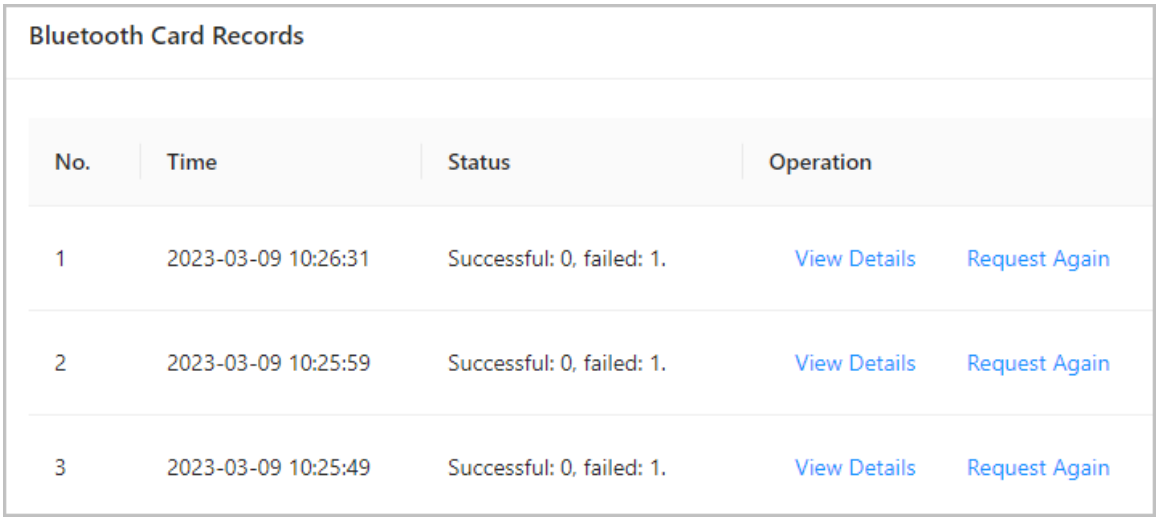



Operaciones relacionadas

- Los usuarios pueden administrar tarjetas Bluetooth en DMSS.
  - ◇ Mover a la parte superior: si se agregaron varias tarjetas Bluetooth, puede mover las tarjetas que están actualmente en uso a la parte superior.
  - ◇ Cambiar nombre: cambia el nombre de la tarjeta
  - ◇ Bluetooth. Eliminar: elimina la tarjeta Bluetooth.
- Exportar usuarios que carecen de correos electrónicos: Haga clic**Exportar**, ingrese los correos electrónicos en el formato correcto y luego haga clic en Importar. Serán trasladados a la lista de solicitudes.

- Ver los registros de solicitud: en el**Gestión de personas**página, haga clic**Más**>**Registros de tarjeta Bluetooth**para ver el estado de la solicitud.

Figura 2-28 Estado de la solicitud




  - ◇ Ver detalles: vea los detalles de la solicitud, incluida la información del usuario, los motivos de las solicitudes fallidas y más. También puede solicitar nuevamente para los usuarios fallidos.
  - ◇ Solicitar nuevamente: Solicitar nuevamente para usuarios fallidos.

## 2.2.8 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.

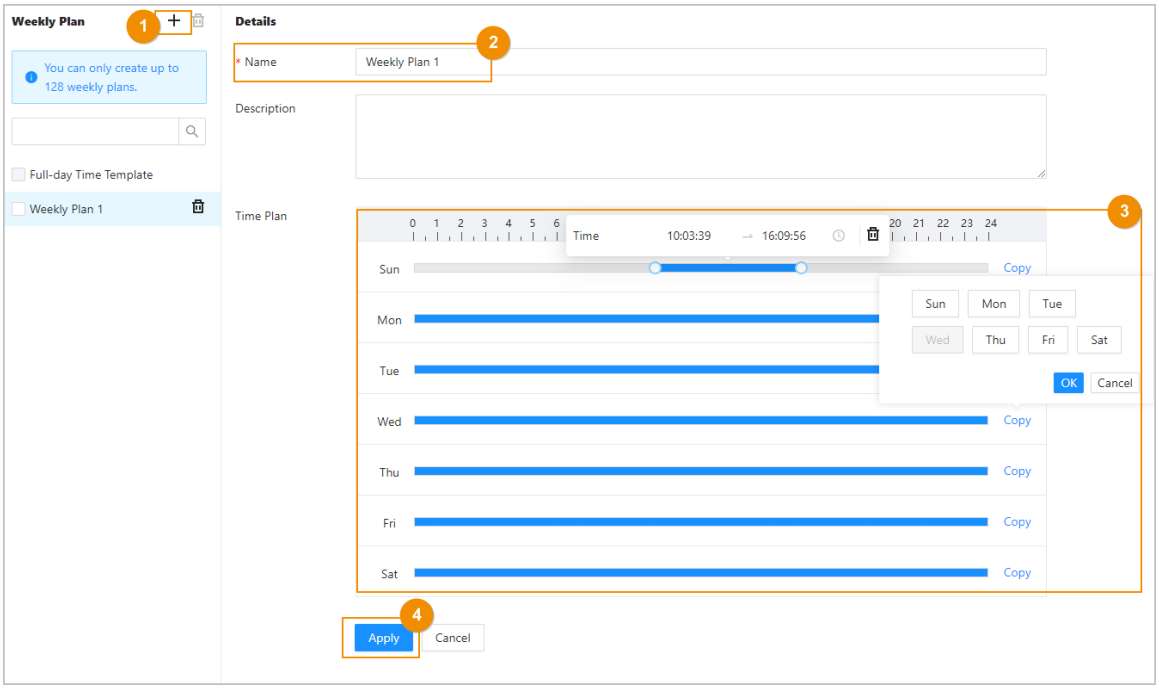
Procedimiento

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 2-29 Crear el plan semanal




Paso 3 Arrastre el control deslizante para ajustar el período de tiempo de cada día.

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

Sólo puedes configurar hasta 4 tramos horarios para cada día.

Etapa 4 Hacer clic**Aplicar**.

## 2.2.9 Agregar planes de vacaciones (opcional)

El plan de vacaciones se utiliza para establecer el calendario 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.

Paso 2 Introduzca el nombre del plan de vacaciones.

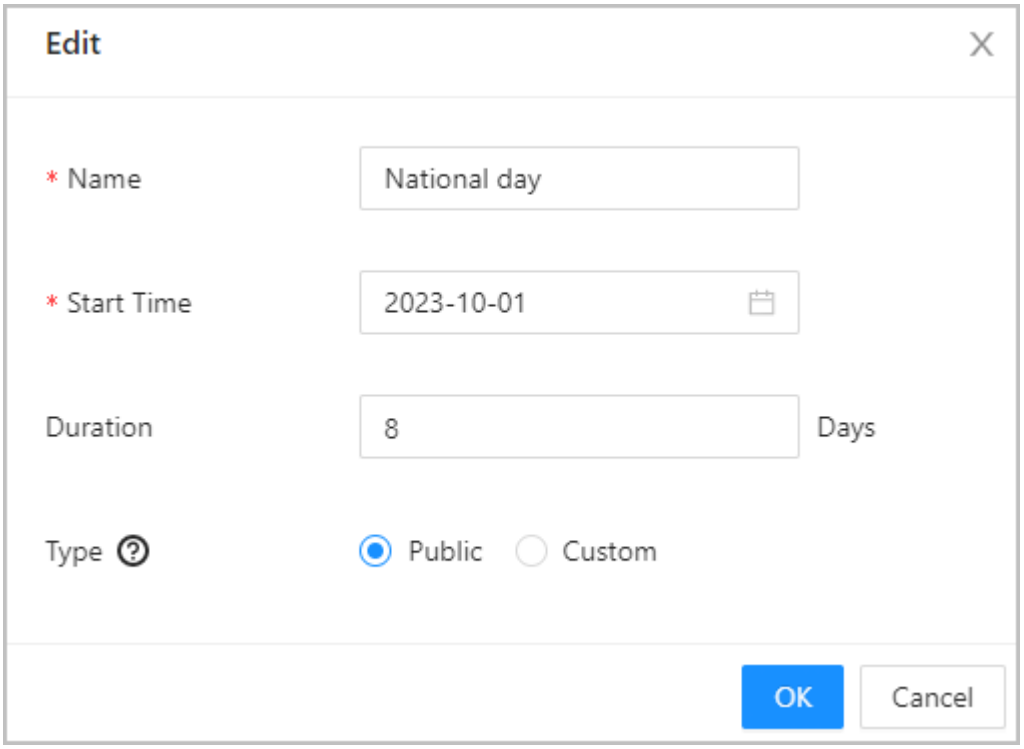
Paso 3 Arrastre el control deslizante para ajustar el período de tiempo de cada día.

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.

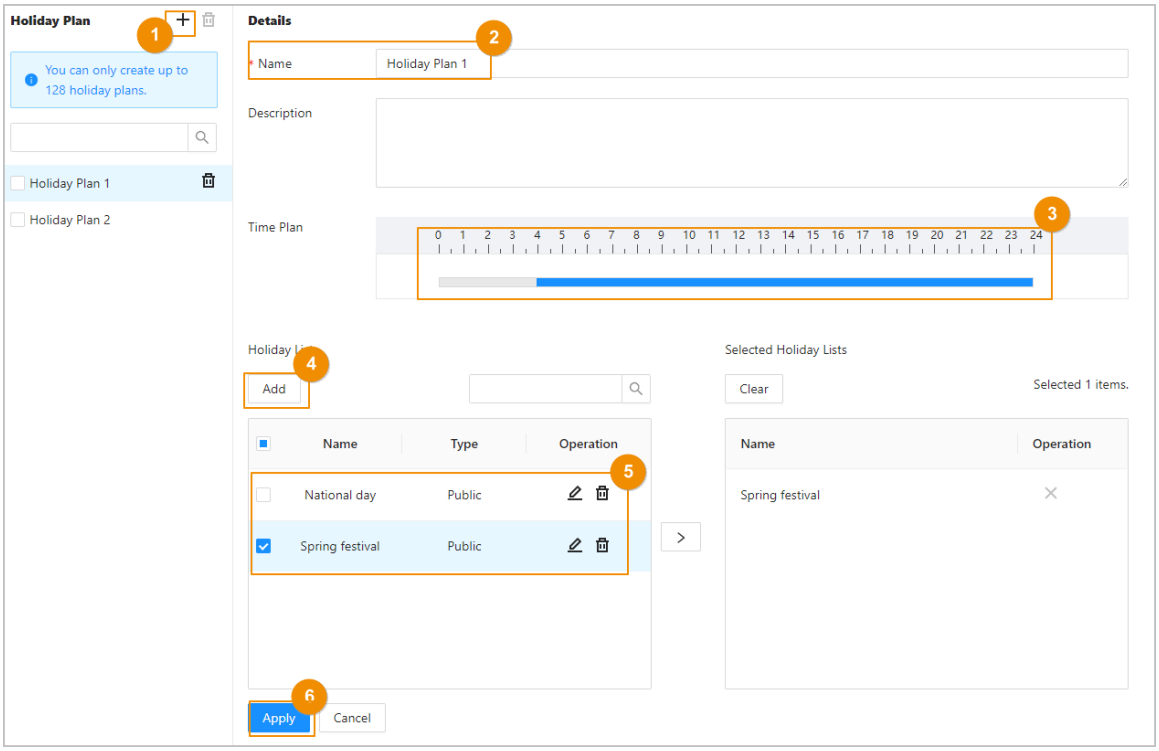
Figura 2-30 Agregar días festivos




Paso 5 Seleccione días festivos.

Paso 6 Hacer clic**Aplicar**.

Figura 2-31 Crear plan de vacaciones



# 2.2.10 Agregar áreas

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.

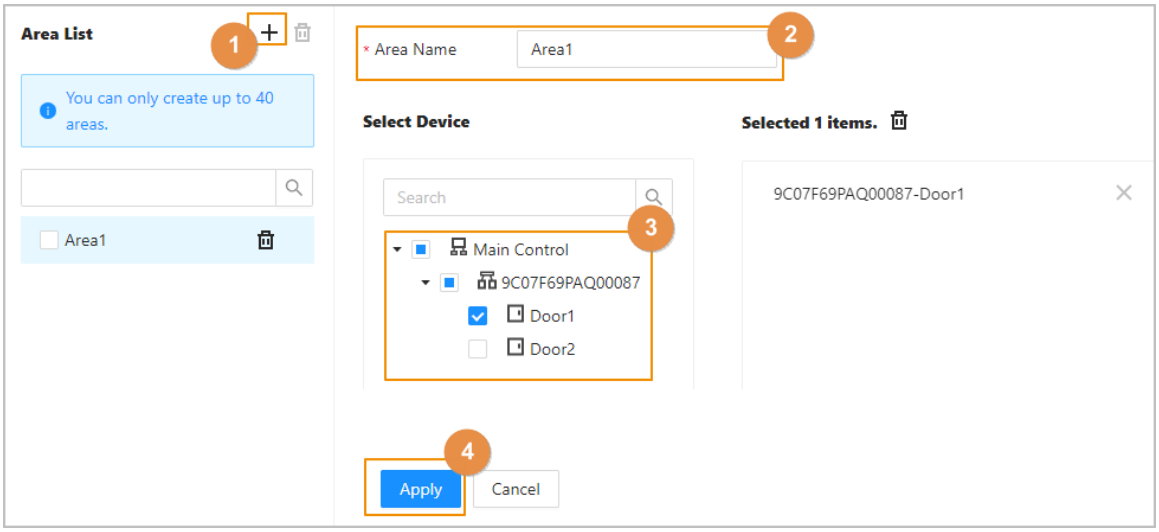
Procedimiento

Paso 1 Hacer clic**Configuración de control de acceso**>**Configuración de área**.

Paso 2 Haga clic para agregar áreas.

Puede agregar hasta 40 permisos de área.

Figura 2-32 Agregar áreas




Paso 3 Introduzca el nombre del área.

Etapa 4 Seleccione puertas.

Paso 5 Hacer clic**Aplicar**.

# 2.2.11 Agregar reglas de permiso

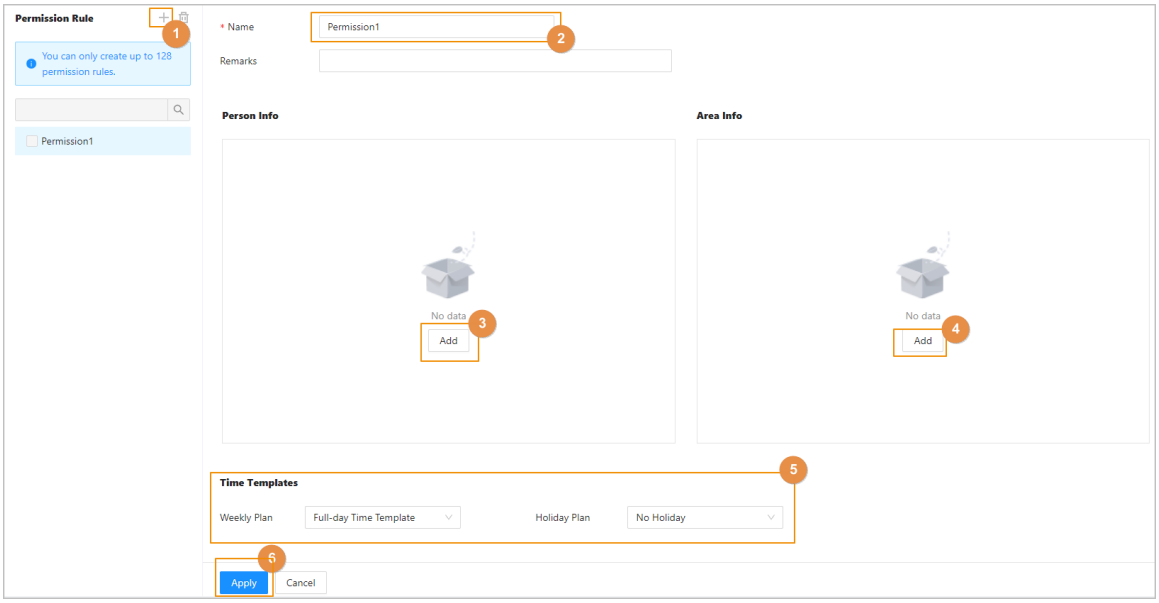
Al crear reglas de permisos, puede asignar permisos de acceso a los usuarios vinculándolos a las áreas. Esto permitirá que el personal autorizado tenga acceso a áreas seguras.

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración de control de acceso**>**Configuración de permisos**. Haga

Paso 2 clic para agregar una regla de permiso.

Figura 2-33 Asignar permisos en lotes




Paso 3 Ingrese el nombre de la regla de permiso.

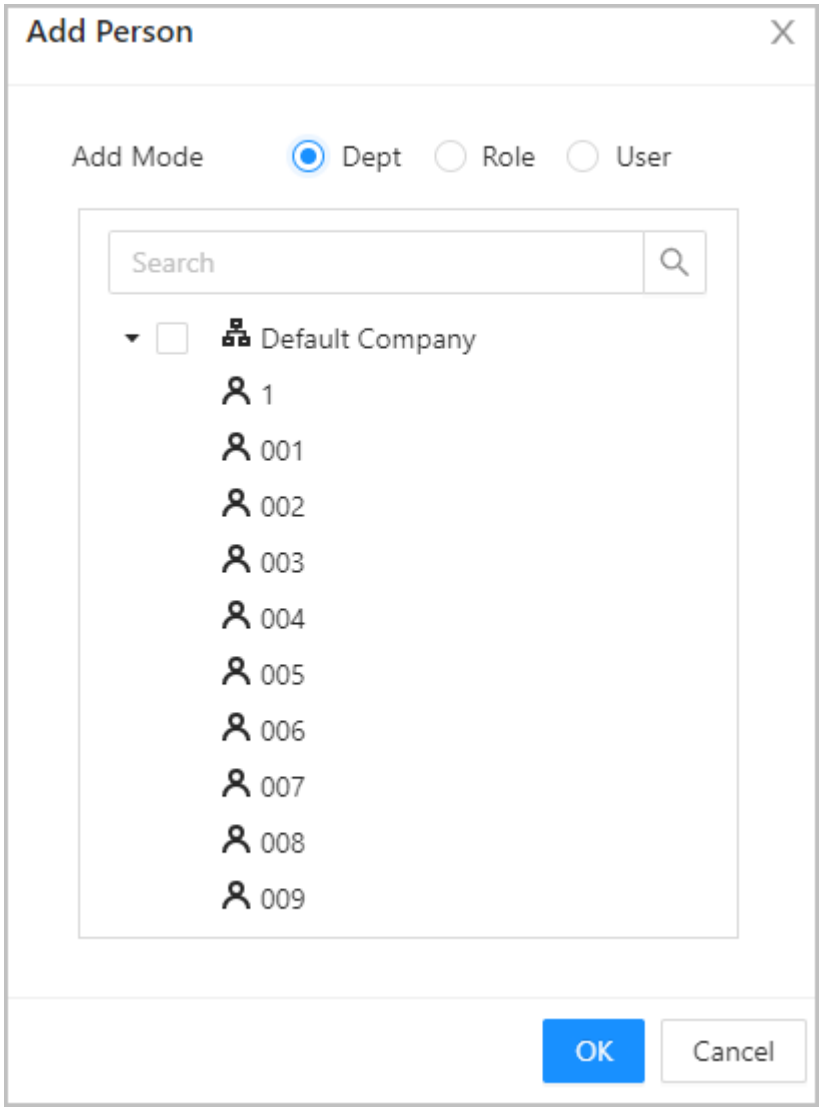
Etapa 4 En el**Información de la persona**área, haga clic**Agregar**para seleccionar personal y luego haga clic en**DE ACUERDO**.

Puede seleccionar personal por departamento, rol o usuarios individuales.

- Departamento: A todo el personal del departamento se le asignarán permisos de acceso.
- Rol: A todo el personal con estos roles 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. .

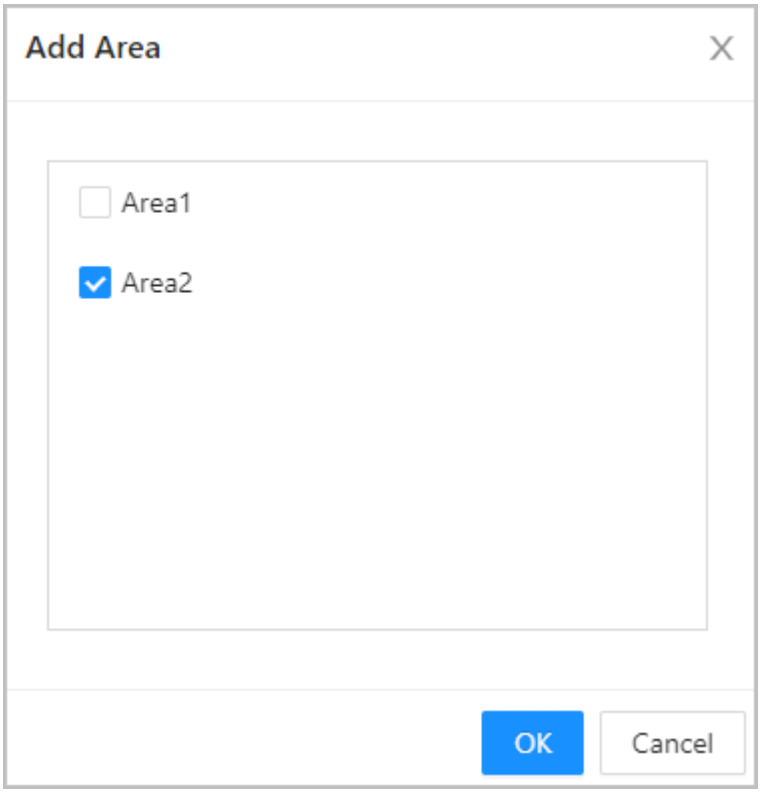
Figura 2-34 Agregar personal




Puedes hacer clic + para crear nuevos grupos de permisos. Para obtener detalles sobre la creación de permisos grupos, consulte "2.2.10 Agregar áreas".

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

Figura 2-35 Agregar área




Paso 6 En el**Plantillas de tiempo**área, seleccione el plan semanal y el plan de vacaciones. Hacer

Paso 7 clic**Aplicar**.

Operaciones relacionadas

# 2.2.12 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.

- Sincronizar persona de subcontrol: sincroniza el personal del controlador principal con el subcontrolador.
- Sincronizar persona local: sincroniza el personal de la plataforma de gestión del controlador principal con su servidor.
- Sincronizar hora local: sincroniza las plantillas de hora en los permisos del área con el subcontrolador.

Figura 2-36 Progreso de la autorización

| Area Permission | Device Name | Type | Progress | Results | Time | Operation |
|---|---|---|---|---|---|---|
| | [redacted] | Sync SubControl Person | | Succeed: 1, Failed: 0 | 2022-08-12 20:01:59 | |
| | [redacted] | Sync SubControl Person | | Succeed: 0, Failed: 1 | 2022-08-12 20:01:23 | |
| | 186 | Sync Local Person | | Succeed: 1, Failed: 0 | 2022-08-12 20:01:23 | |

Paso 3 (Opcional) Si la autorización falló, haga clic para intentarlo nuevamente.

Puede hacer clic para ver detalles sobre la tarea de autorización fallida.

# 2.2.13 Configuración del control de acceso (opcional)

## 2.2.13.1 Configuración de parámetros básicos

Procedimiento

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

Paso 2 En**Ajustes básicos**, configurar parámetros básicos para el control de acceso.

Figura 2-37 Parámetros básicos

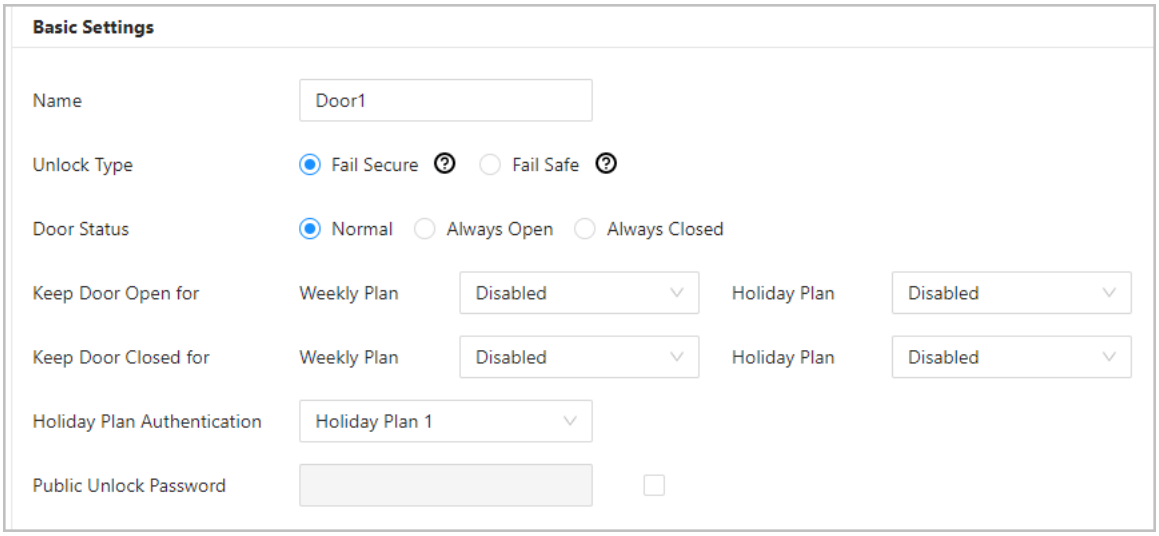



Tabla 2-8 Descripción de los parámetros básicos

| Parámetro | Descripción |
|---|---|
| Nombre | El nombre de la puerta. |
| Tipo de desbloqueo | ● Si seleccionó**12 voltios**Para suministrar energía a la cerradura a través del controlador durante el asistente de inicio de sesión, puede configurar a prueba de fallas o a prueba de fallas.<br>◇ A prueba de fallos: cuando se interrumpe o falla la energía, la puerta permanece bloqueada.<br>◇ A prueba de fallos: cuando se interrumpe o falla la energía, la puerta se desbloquea automáticamente para permitir que las personas salgan.<br>● Si seleccionó**Relé**Para suministrar energía a la cerradura a través del relé durante el asistente de inicio de sesión, puede configurar el relé abierto o cerrado.<br>◇ Relé abierto=bloqueado: configura el bloqueo para que permanezca bloqueado cuando el relé está abierto.<br>◇ Relé abierto = desbloqueado: configure el bloqueo para que se desbloquee cuando el relé esté abierto. |
| Estado de la puerta | Establecer el estado de la puerta.<br>● **Normal**:La puerta se desbloqueará y bloqueará según su configuración.<br>● **Siempre abierto**:La puerta permanece abierta todo el tiempo.<br>● **Siempre cerrado**:La puerta permanece cerrada todo el tiempo. |

| Parámetro | Descripción |
|---|---|
| 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. |
| Plan de vacaciones<br>Autenticación | Se permite el acceso autorizado a puerta siempre cerrada en el plan vacacional definido. |
| Periodo normalmente cerrado | Cuando seleccionas**Normal**, puede seleccionar una plantilla de tiempo de la lista desplegable. La puerta permanece abierta o cerrada durante el tiempo definido. |
| Contraseña de desbloqueo público | Active esta función y luego ingrese una contraseña, y luego podrá desbloquear la puerta ingresando solo la contraseña pública. |

### 2.2.13.2 Configuración de métodos de desbloqueo

Puede utilizar varios métodos de desbloqueo para desbloquear la puerta, como desbloqueo con tarjeta Bluetooth, huella digital, tarjeta y contraseña. También puedes combinarlos para crear tu propio método de desbloqueo personal.

Procedimiento

Paso 1 Seleccionar**Configuración de control de acceso**>**Parámetros de la puerta**. En

Paso 2 **Configuración de desbloqueo**, selecciona un modo de desbloqueo.

- Desbloqueo combinado

  1. Seleccione**Desbloqueo combinado**desde el**Modo de desbloqueo**lista.
  2. Seleccione**O**o**Y**.
     - ◇ O: utilice uno de los métodos de desbloqueo seleccionados para abrir la puerta. Y:
     - ◇ utilice todos los métodos de desbloqueo seleccionados para abrir la puerta.

     La tarjeta Bluetooth no se puede seleccionar cuando configura el método de combinación en **Y**.
  3. Seleccione los métodos de desbloqueo y luego configure otros parámetros.

Figura 2-38 Configuración de desbloqueo

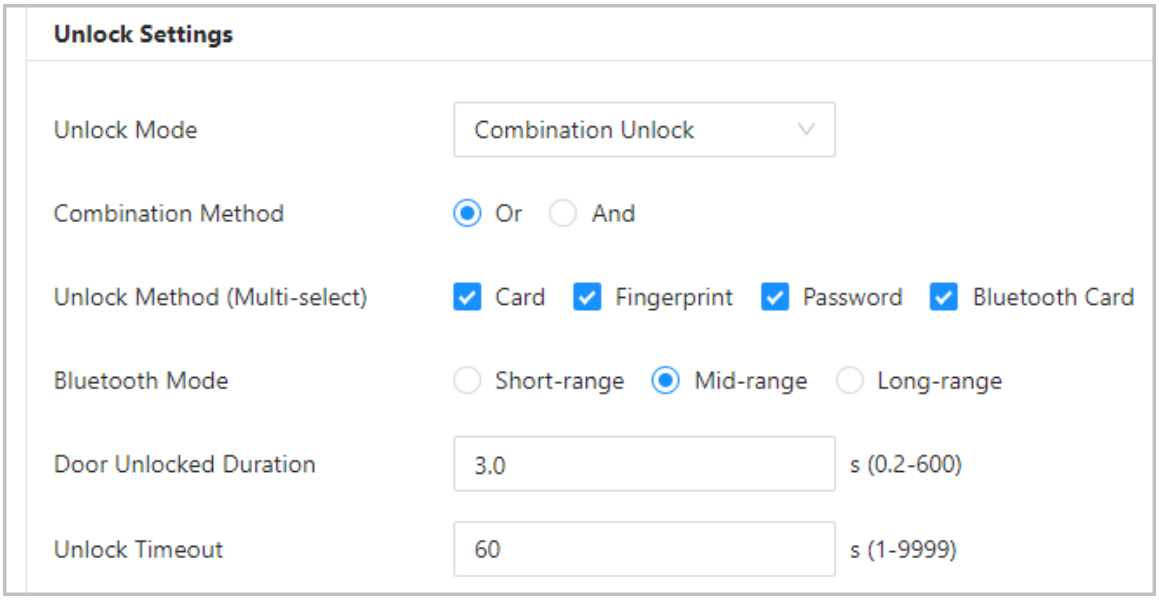



Tabla 2-9 Descripción de la configuración de desbloqueo

| Parámetro | Descripción |
|---|---|
| Método de desbloqueo (selección múltiple) | Admite desbloqueo mediante tarjeta, huella digital, contraseña o tarjeta Bluetooth. La función de tarjeta Bluetooth está desactivada de forma predeterminada. |
| Modo Bluetooth | La tarjeta Bluetooth debe estar a cierta distancia del dispositivo de control de acceso para intercambiar datos y desbloquear la puerta. A continuación se detallan las gamas más adecuadas para ello.<br>● Corto alcance: el alcance de desbloqueo de Bluetooth es inferior a 0,2 m.<br>● Alcance medio: El alcance de desbloqueo de Bluetooth es inferior a 2 m.<br>● Largo alcance: el alcance de desbloqueo de Bluetooth es inferior a 10 m.<br>El rango de desbloqueo de Bluetooth puede variar según los modelos de su teléfono y el entorno. |
| Duración del desbloqueo 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. |

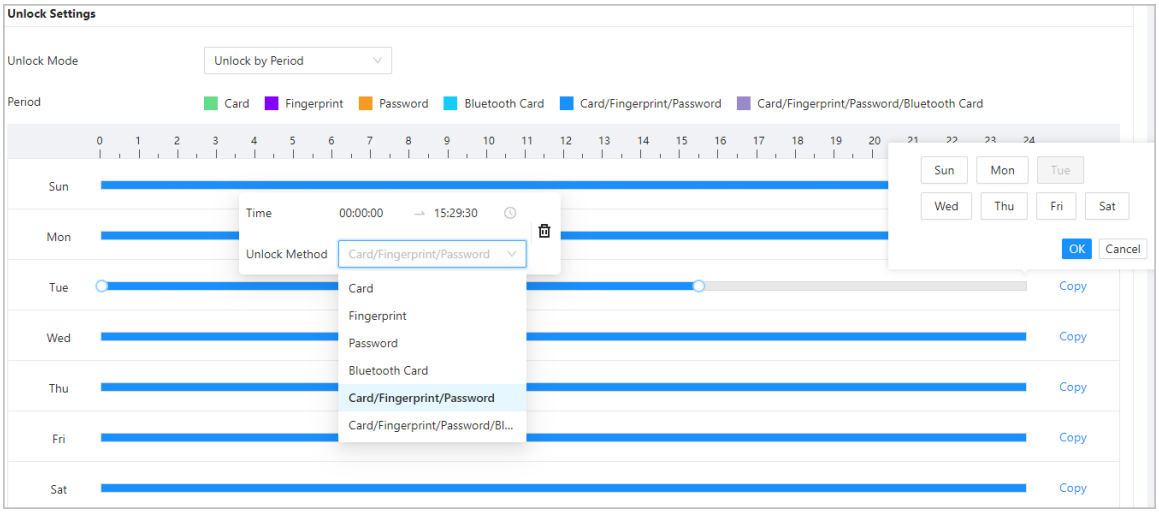
- Desbloquear por período

1. En el**Modo de desbloqueo**lista, seleccione**Desbloquear por período**.
2. Arrastre el control deslizante para ajustar el período de tiempo para cada día.

   También puedes hacer clic**Copiar**para aplicar el periodo de tiempo configurado a otros días.
3. Seleccione un método de desbloqueo para el período de tiempo y luego configure otros parámetros.

Sólo puedes configurar hasta 4 tramos horarios para cada día.

Figura 2-39 Desbloqueo por período




Paso 3 Hacer clic**Aplicar**.

## 2.2.13.3 Configuración de alarmas

Se activará una alarma cuando ocurra un evento de acceso anormal.

Procedimiento

Paso 1 Seleccionar**Configuración de control de acceso**>**Parámetros de la puerta**>**Configuración de alarma**.

Paso 2 Configurar los parámetros de alarma.

Figura 2-40 Alarma

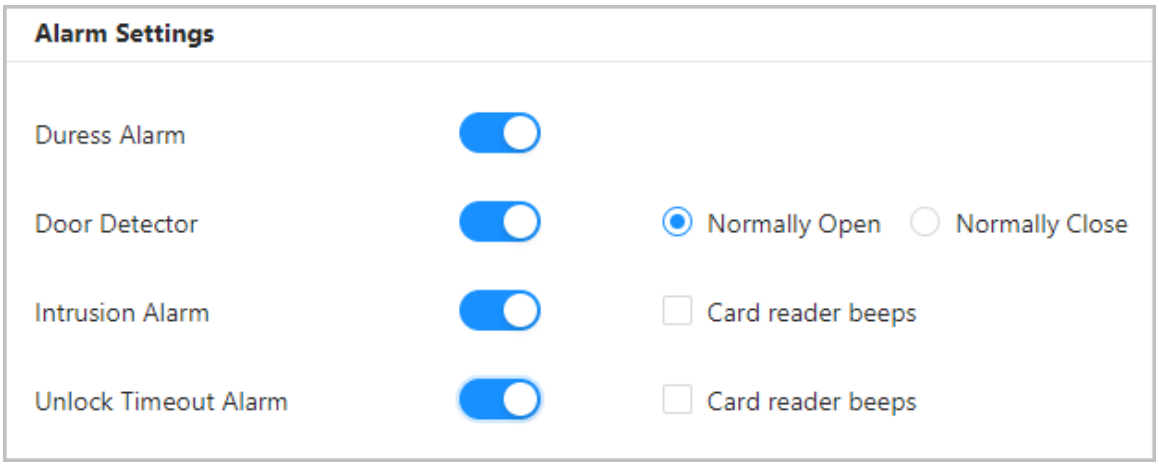



Tabla 2-10 Descripción de los parámetros de alarma

| Parámetro | Descripción |
|---|---|
| Alarma de 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. |
| Detector de puerta | Seleccione el tipo de detector de puerta. |

| Parámetro | Descripción |
| --- | --- |
| Alarma de intrusión | ● Cuando el detector de puerta está habilitado, se activará una alarma de intrusión si la puerta se abre de manera anormal.<br>● Se activará una alarma de tiempo de espera si la puerta permanece desbloqueada por más tiempo que el tiempo de desbloqueo definido.<br>● Cuando**El lector de tarjetas emite un pitido**está habilitado, el lector de tarjetas emite un pitido cuando se activa la alarma de intrusión o la alarma de tiempo de espera. |
| Desbloquear alarma de tiempo de espera | |

Paso 3 Hacer clic**Aplicar**.

## 2.2.14 Configurar el desbloqueo de contraseña

Cuando la autenticación con código PIN está habilitada, las personas pueden desbloquear la puerta simplemente ingresando la contraseña.

### Información de contexto

- Si la autenticación con código PIN no está habilitada, puede desbloquear la puerta ingresando la contraseña de desbloqueo en el formato de**contraseña del usuario#**.Por ejemplo, si el ID de usuario es 123 y la contraseña que estableció es 12345, entonces debe ingresar**123#12345#**para desbloquear la puerta.
- Si la autenticación con código PIN está habilitada, puede desbloquear la puerta ingresando la contraseña de desbloqueo en el formato de**contraseña#**.Por ejemplo, si el ID de usuario es 123 y la contraseña que estableció es 12345, entonces debe ingresar**12345#**para desbloquear la puerta.

### Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración de control de acceso**>**Configuración del método de**

Paso 2 **desbloqueo**. Encender**Autenticación de código PIN**,y luego haga clic**Aplicar**.

Existen algunos riesgos de seguridad al habilitar la autenticación con código PIN. Cuando está activado, los tipos y roles de usuario se vuelven ineficaces y se producen las siguientes situaciones.

- Los titulares de la primera tarjeta y los usuarios de grupos de desbloqueo de varias personas deben verificar sus identidades mediante los métodos de desbloqueo definidos, excepto la contraseña. Si verifican mediante contraseña, la función de desbloqueo de la primera tarjeta o de desbloqueo de varias personas dejará de ser efectiva.
- Los usuarios deben verificar sus métodos de desbloqueo definidos, excepto la contraseña. Si obtienen acceso mediante contraseña, la función anti-passback dejará de ser efectiva.
- Los usuarios de patrulla y los usuarios de la lista bloqueada pueden simplemente ingresar su contraseña para desbloquear la puerta.
- Las cuentas congeladas y vencidas aún pueden desbloquear puertas simplemente ingresando su contraseña.
- Cuando el método de desbloqueo con contraseña está desactivado al mismo tiempo, todos los tipos de usuarios no pueden desbloquear la puerta con su contraseña.

## 2.2.15 Configuración de enlaces de alarma global (opcional)

Puede configurar enlaces de alarma globales entre diferentes controladores de acceso.

### Procedimiento

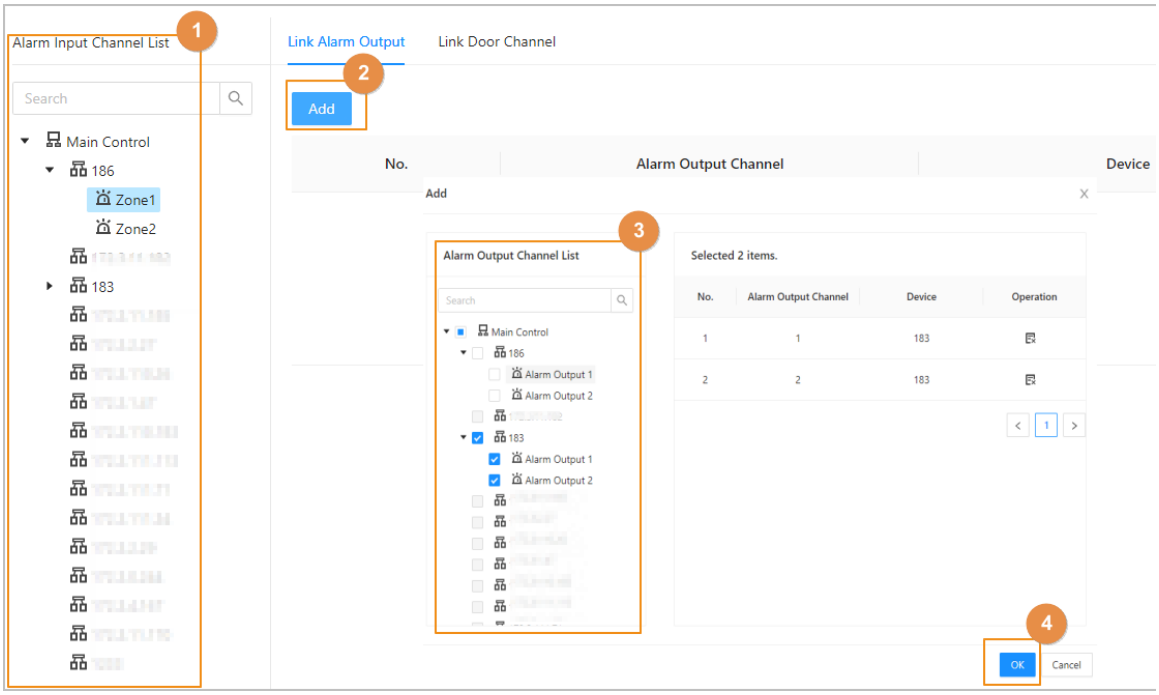
Paso 1 Seleccionar**Configuración de control de acceso**>**Enlace de alarma global**.

- Cuando haya configurado tanto los vínculos de alarma globales como los vínculos de alarma locales, y si los vínculos de alarma globales entran en conflicto con los vínculos de alarma locales, los últimos vínculos de alarma que haya configurado entrarán en vigor.
- Cuando haya configurado enlaces de alarma para subcontroladores a través del controlador principal, si el controlador principal ha sido restaurado a los valores predeterminados de fábrica, le recomendamos restaurar el subcontrolador a los valores predeterminados de fábrica al mismo tiempo.

Paso 2 Configure la salida de alarma.

1. Seleccione una entrada de alarma de la lista de canales de entrada de alarma y luego haga clic en**Enlace de salida de alarma**.
2. Haga clic**Agregar**,seleccione un canal de salida de alarma y luego haga clic en**DE ACUERDO**.

Figura 2-41 Salida de alarma



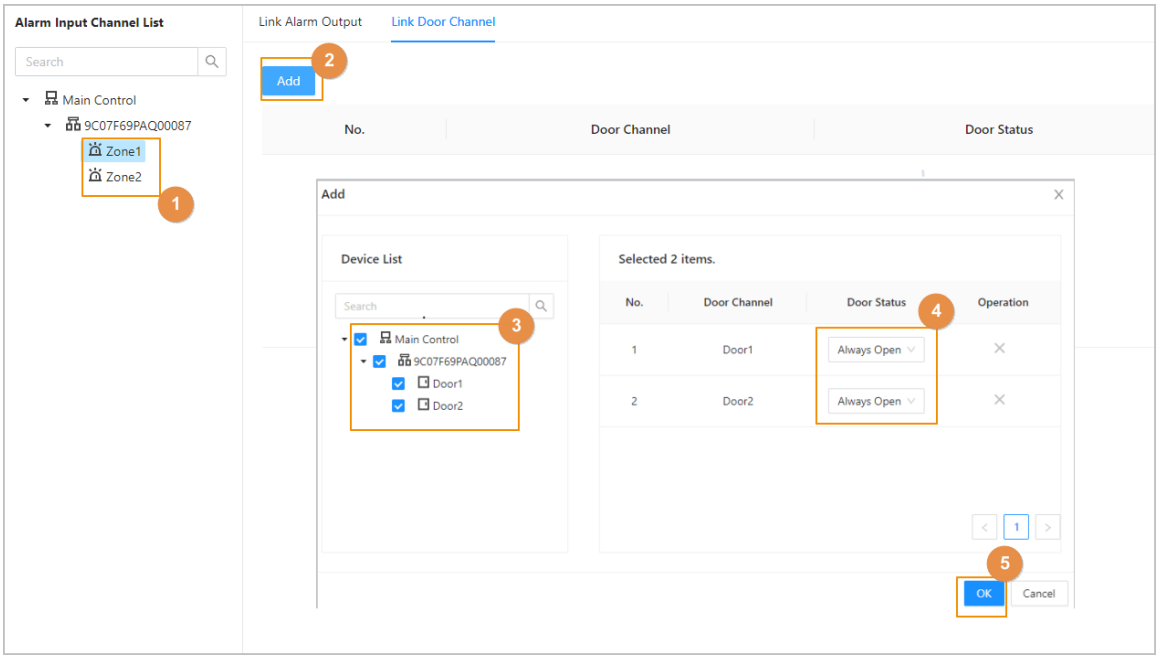

3. Active la función de salida de alarma y luego ingrese la duración de la alarma.
4. Haga clic**Aplicar**.

Paso 3 Configurar el enlace de la puerta.

1. Seleccione una entrada de alarma de la lista de canales y luego haga clic en**Agregar**.
2. Seleccione la puerta de enlace, seleccione el estado de la puerta y luego haga clic en**DE ACUERDO**.

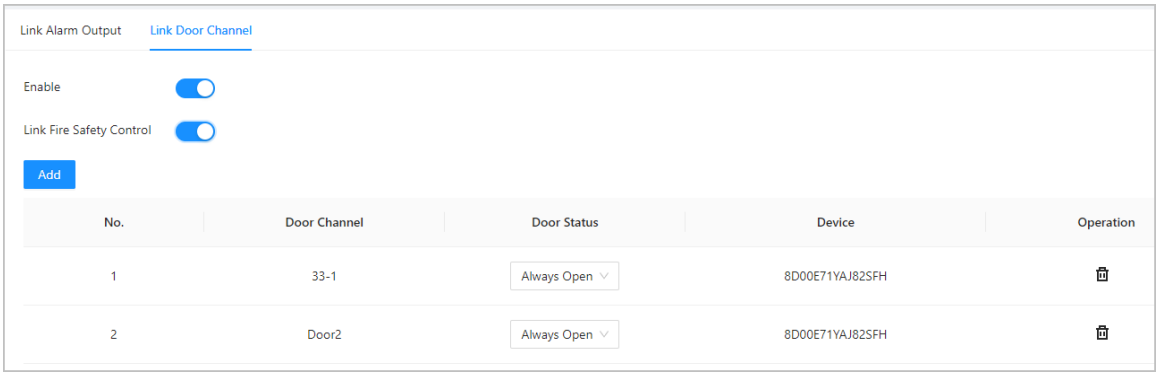
- Siempre cerrada: la puerta se bloquea automáticamente cuando se activa una alarma.
- Siempre abierta: la puerta se desbloquea automáticamente cuando se activa una alarma.

Figura 2-42 Enlace de puerta




3. Haga clic**Permitir**para activar la función de enlace de la puerta.

Figura 2-43 Enlace de puerta




Si activa el control de seguridad contra incendios del enlace, todos los enlaces de la puerta cambiarán automáticamente al **Siempre abierto**estado, y todas las puertas se abrirán cuando se active la alarma de incendio.

4. Haga clic**Aplicar**.

Puedes hacer clic**Copiar a**para aplicar los enlaces de alarma preconfigurados a otros canales de entrada de alarma.

## 2.2.16 Configurar el desbloqueo de la primera tarjeta

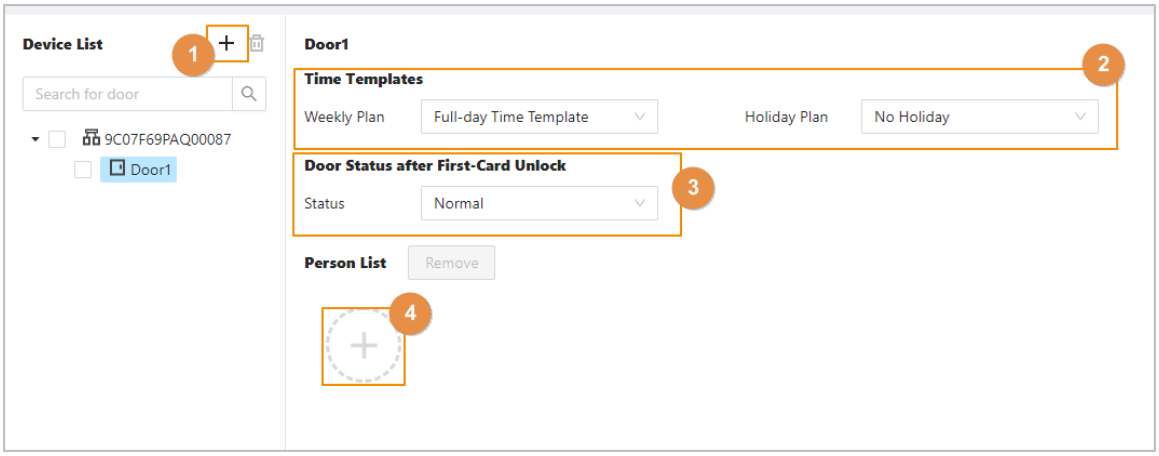
Defina a ciertas personas como los primeros titulares de la tarjeta; otros usuarios pueden verificar sus identidades para desbloquear la puerta solo después de que los primeros titulares de la tarjeta verifiquen sus identidades primero.

Procedimiento

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

Paso 2 **tarjeta**. En la lista de dispositivos, haga clic en y luego seleccione la puerta.

Figura 2-44 Asignar permiso de primera tarjeta a los usuarios




Paso 3 Selecciona el plan semanal y el plan vacacional.

La primera tarjeta es válida sólo durante el tiempo definido.

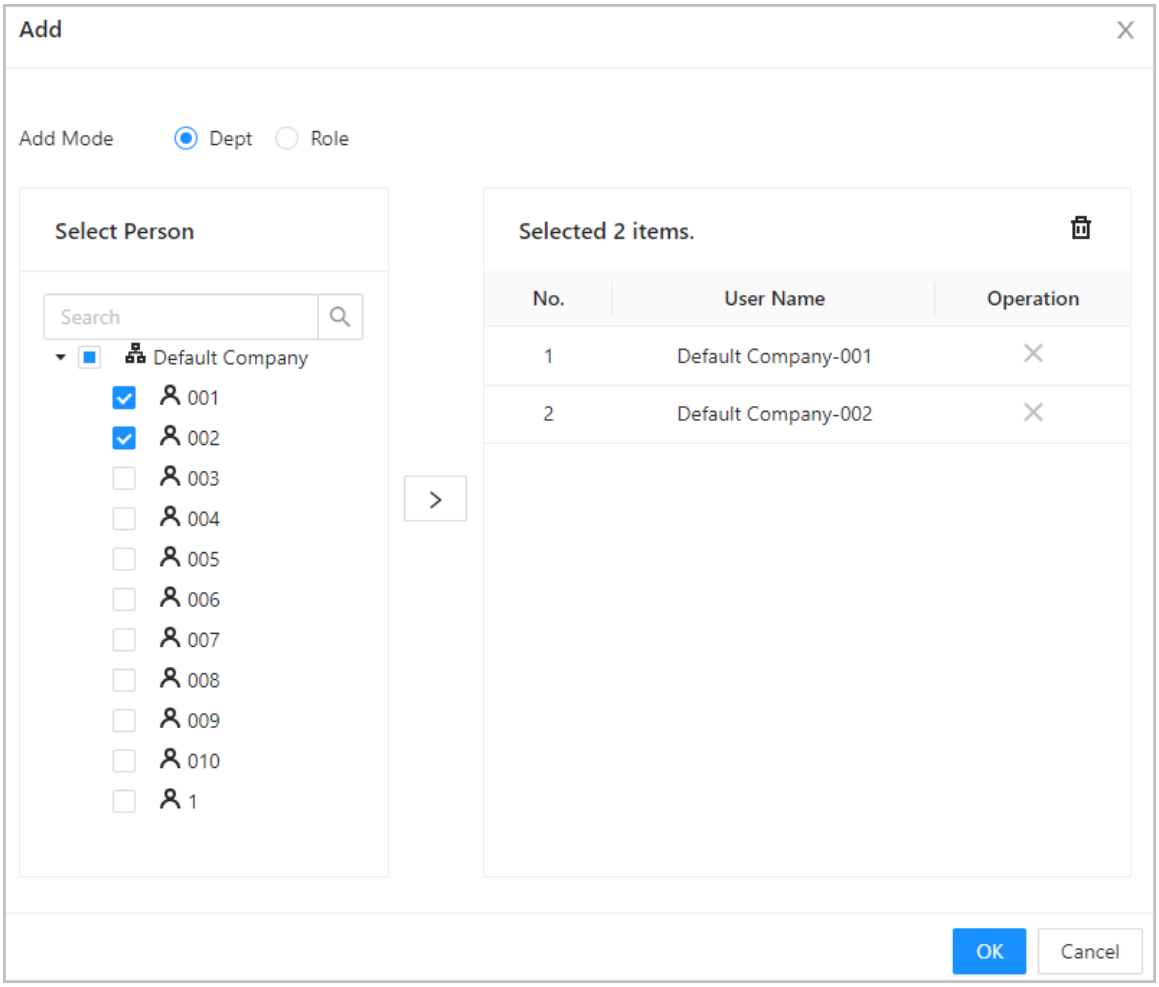
Etapa 4 Seleccione el estado de la puerta.

- 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.
- Siempre abierta: la puerta permanece abierta después de que los usuarios con la primera tarjeta otorgan acceso al controlador de acceso.

Paso 5 Haga clic para agregar usuarios de primera tarjeta y luego haga clic en**DE**

**ACUERDO**. Puede seleccionar usuarios de departamentos o roles.

Figura 2-45 Agregar usuarios de primera tarjeta




## 2.2.17 Configuración del desbloqueo para varias personas

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

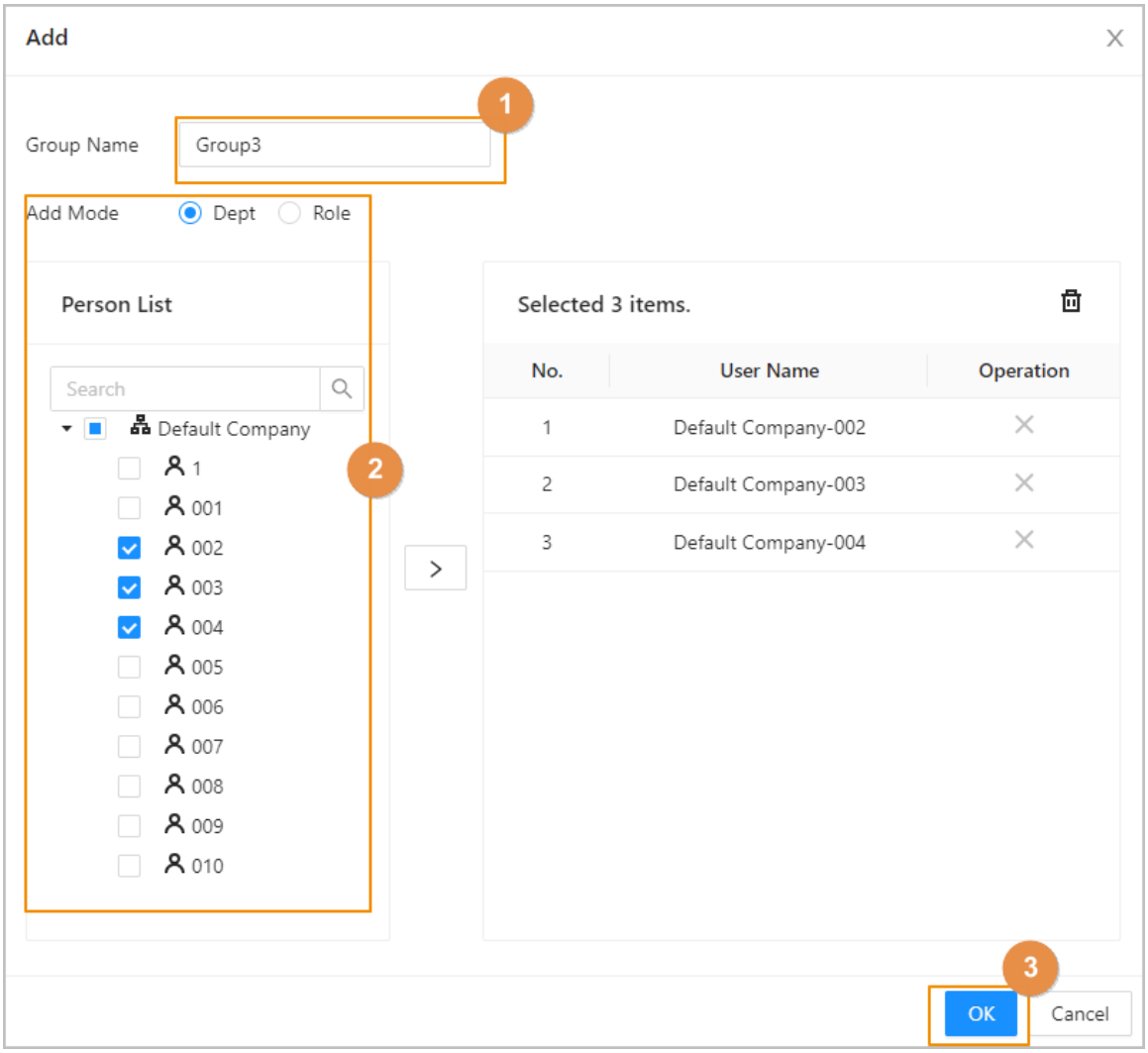
Paso 1 Seleccionar**Configuración de control de acceso**>**Desbloqueo multipersona**.

Paso 2 Haga clic para agregar puertas a la lista de dispositivos.

Paso 3 Hacer clic**Gestión de grupos 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 2-46 Agregar grupos




Etapa 4 Seleccione una puerta y luego haga clic**Agregar grupos de personas**.

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.

Paso 6 Configure los parámetros de desbloqueo multipersona. 1.

Ingrese el número válido.

El número válido indica la cantidad de personas en cada grupo que necesitan verificar sus identidades en el controlador de acceso antes de que se desbloquee la puerta. Por ejemplo, si el número 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.

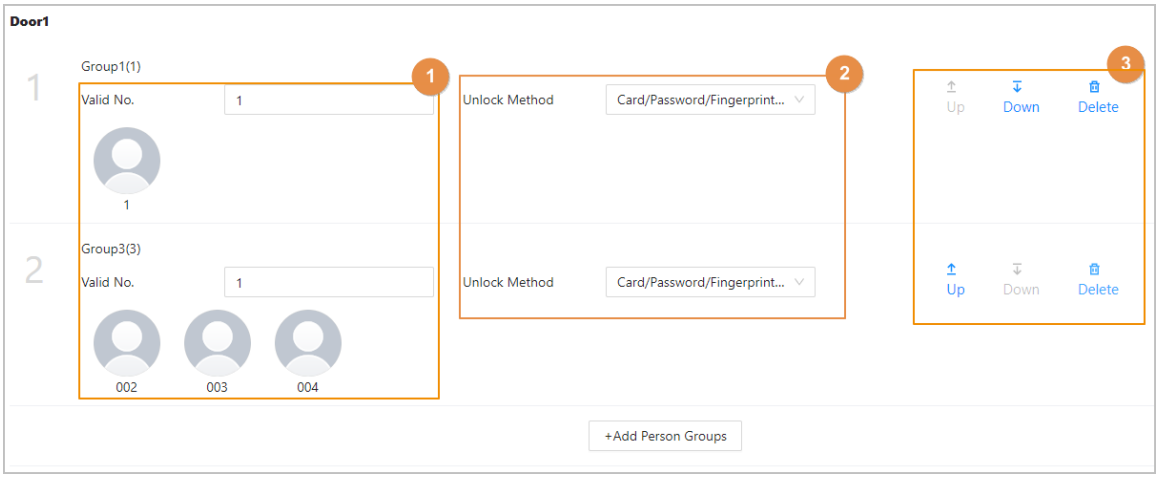
2. Seleccione el método de desbloqueo.

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

3. (Opcional) Haga clic**Arriba**o**Abajo**para cambiar la secuencia de grupos.

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

Figura 2-47 Configurar el desbloqueo para varias personas




Paso 7 Hacer clic**Aplicar**.

# 2.2.18 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 le pase una tarjeta de acceso a otra persona para que pueda entrar. 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 autorización, 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.

- Cuando haya configurado el anti-passback para los subcontroladores a través del controlador principal y planee restaurar el controlador principal a sus valores predeterminados de fábrica, le recomendamos que también restaure el subcontrolador a sus valores predeterminados de fábrica al mismo tiempo.
- Si se utiliza la regla anti-passback cuando la red no es estable, la puerta podría abrirse después de verificar una identidad, pero podría activarse una alarma de tiempo de espera en el lector de tarjetas. Asegúrese de que su red sea estable.

Procedimiento

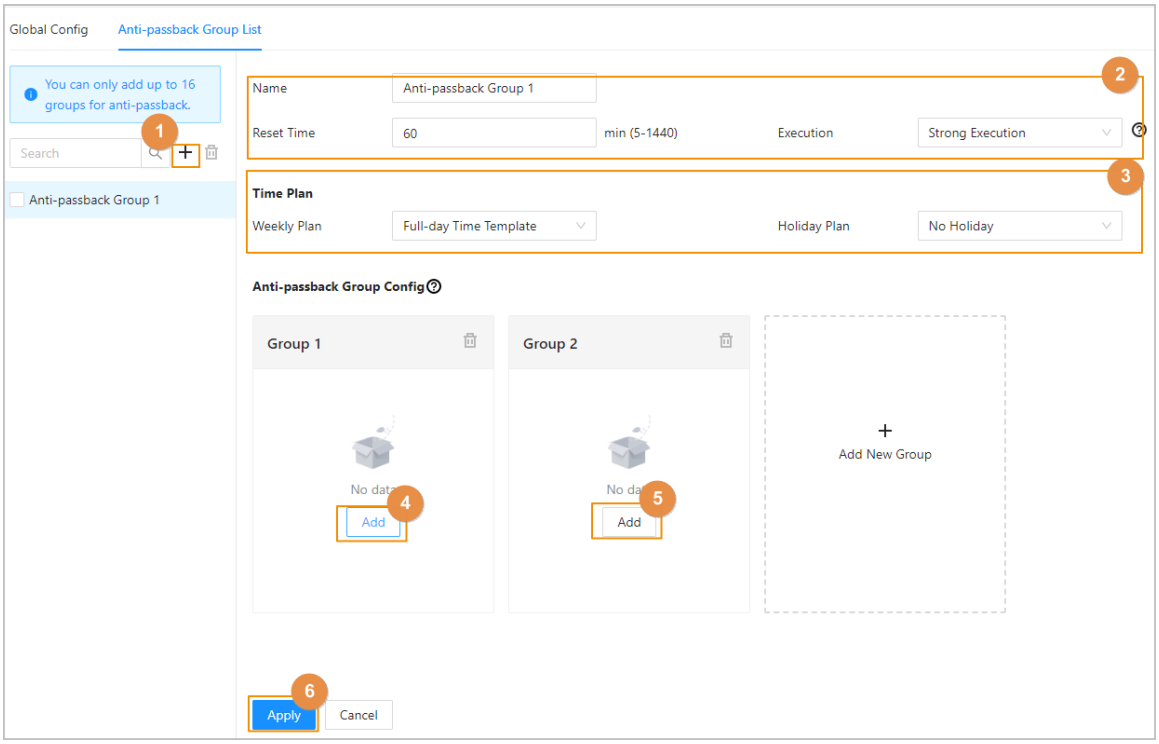
Paso 1 Seleccionar**Configuración de control de acceso**>**Anti-passback global**.

Paso 2 Enciende el**Restablecer Anti-Passback**y luego seleccione un tiempo de reinicio.

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

Paso 3 clic**Lista de grupos anti-passback**y luego haga clic para agregar un grupo anti-passback.

Figura 2-48 Configurar anti-passback




Etapa 4 Cree un nombre para el grupo anti-passback, ingrese un tiempo de reinicio y luego seleccione el modo de ejecución.

Establezca un período de tiempo en el que se activará la alarma anti-passback. 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.

- Ejecución sólida: el controlador secundario y el controlador principal realizan la función anti-passback incluso cuando se desconectan.
- Ejecución débil: el controlador secundario y el controlador principal no realizan la función antipassback cuando se desconectan.

Paso 5 Selecciona el plan semanal y el plan vacacional.

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

Paso 6 1, haga clic**Agregar**y luego seleccione lectores de tarjetas. En el

Paso 7 grupo 2, haga clic**Agregar**y luego seleccione lectores de tarjetas.

Se deben agregar al menos 2 grupos.

Paso 8 (Opcional) Puedes hacer clic**Agregar nuevo grupo**para agregar más grupos.

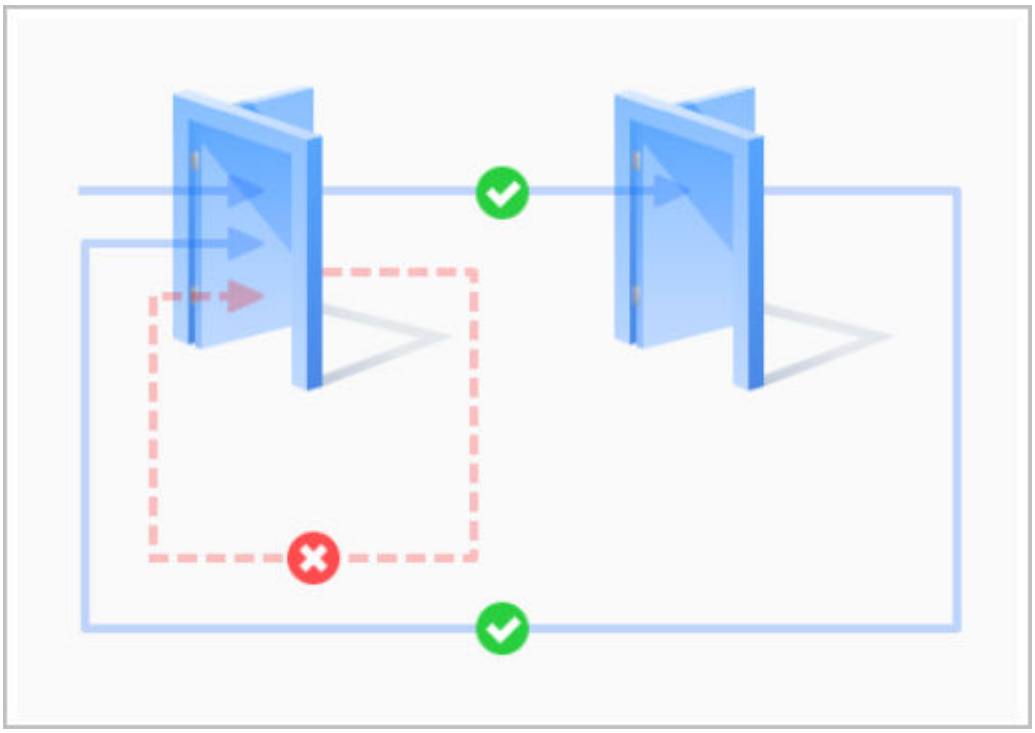
Puede agregar más de un lector a un grupo y los usuarios pueden deslizar el dedo hacia cualquiera de los lectores para obtener acceso.

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 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 2-49 Función anti-passback



## 2.2.19 Configuración del bloqueo de puertas múltiples

El enclavamiento de puertas múltiples controla el bloqueo de dos o más puertas. Si una puerta está desbloqueada, se prohibirá el acceso al resto de puertas.

### Información de contexto

- Cuando haya configurado el enclavamiento de puertas múltiples para los subcontroladores a través del controlador principal y planee restaurar el controlador principal a sus valores predeterminados de fábrica, le recomendamos que también restaure el subcontrolador a sus valores predeterminados de fábrica al mismo tiempo.
- Si se utiliza la regla de enclavamiento de puertas múltiples cuando la red no es estable, la puerta podría abrirse después de verificar una identidad, pero podría activarse una alarma de tiempo de espera en el lector de tarjetas. Asegúrese de que su red sea estable.

### 2.2.19.1 Configurar el enclavamiento dentro de un grupo

Si se abre alguna puerta de un grupo, las demás puertas del grupo no se podrán desbloquear.

Procedimiento

Paso 1 Seleccionar**Configuración de control de acceso**>**Enclavamiento global de puertas múltiples**y luego haga clic en**Interbloqueo dentro del grupo**.

Paso 2 Haga clic en y luego agregue un grupo de interbloqueo.

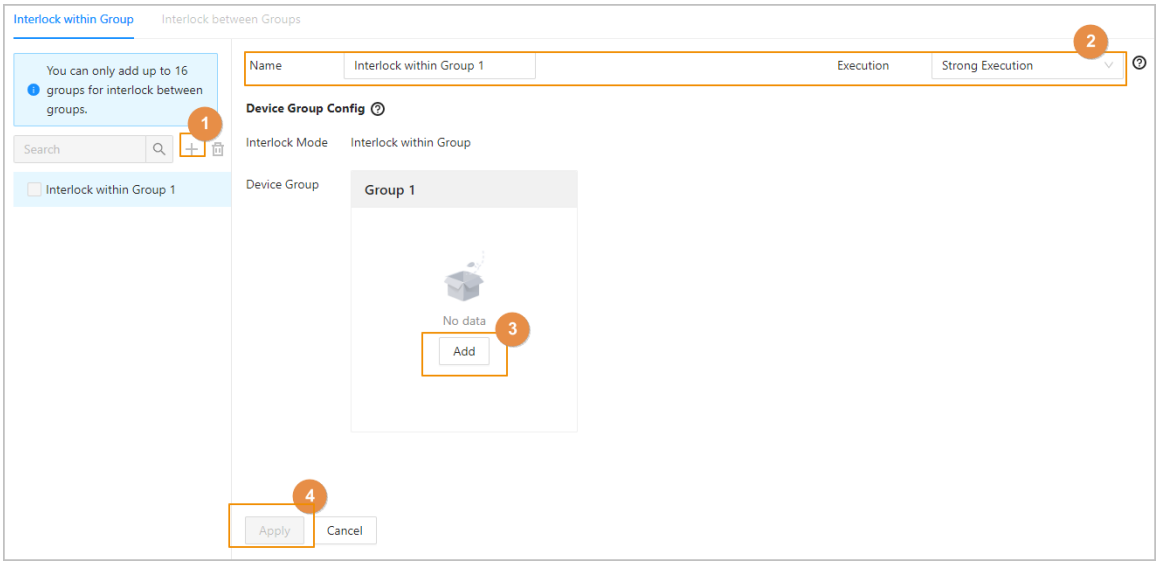
Paso 3 Cree un nombre para el grupo de enclavamiento y luego seleccione el modo de ejecución.

- Ejecución sólida: el controlador secundario y el controlador principal realizan la función de enclavamiento incluso cuando se desconectan.
- Ejecución débil: el controlador secundario y el controlador principal no realizan la función de enclavamiento cuando se desconectan.

Etapa 4 Hacer clic**Agregar**para agregar puertas en un grupo de dispositivos.

Se deben agregar al menos 2 puertas a un grupo.

Figura 2-50 Interbloqueo dentro de un grupo




Paso 5 Hacer clic**Aplicar**.

Resultados

Una vez que se ha verificado la identidad de una persona y ha abierto la puerta, primero debe cerrar la puerta detrás de ella antes de poder abrir la siguiente.

## 2.2.19.2 Configurar el interbloqueo entre grupos

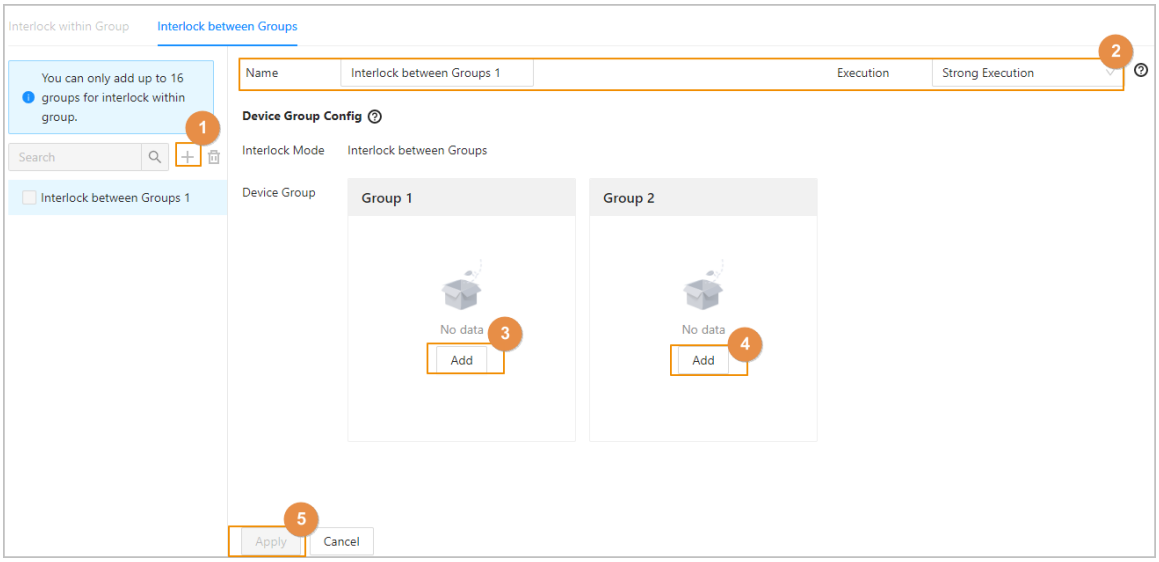
Si alguna puerta de un grupo está desbloqueada, las puertas de los otros grupos no se pueden abrir.

Procedimiento

Paso 1 Seleccionar**Configuración de control de acceso**>**Enclavamiento global de puertas múltiples**y luego haga clic en **Interbloqueo entre grupos**.

Paso 2 Haga clic en y luego agregue un grupo de interbloqueo.

Figura 2-51 Interbloqueo entre grupos




Paso 3 Cree un nombre para el grupo de enclavamiento y luego seleccione el modo de ejecución.

- Ejecución sólida: el controlador secundario y el controlador principal realizan la función de enclavamiento incluso cuando se desconectan.
- Ejecución débil: el controlador secundario y el controlador principal no realizan la función de enclavamiento cuando se desconectan.

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

Paso 5 grupo 2, haga clic**Agregar**para agregar puertas al grupo. Hacer clic

Paso 6 **Aplicar**.

Resultados

Si alguna puerta de un grupo está desbloqueada, las puertas del otro grupo no se pueden abrir.

# 2.2.20 Monitoreo de acceso (opcional)

## 2.2.20.1 Apertura y cierre de puertas de forma remota

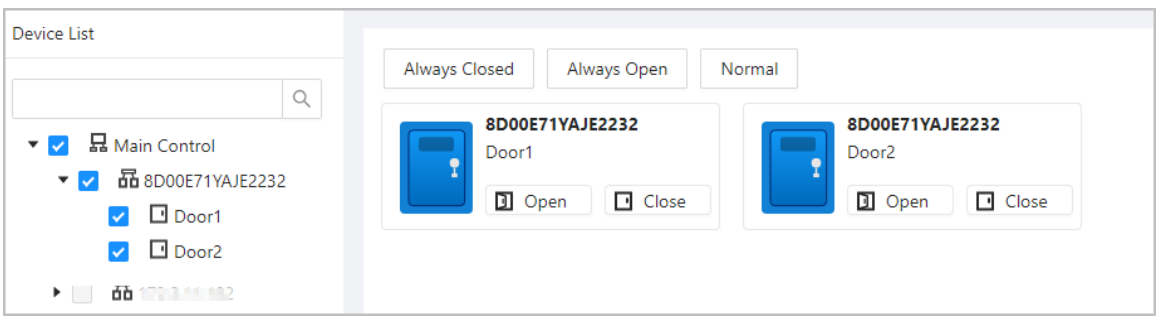
Puede monitorear y controlar remotamente la puerta a través de la plataforma. Por ejemplo, puede abrir o cerrar la puerta de forma remota.

Procedimiento

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

Paso 2 Seleccione la puerta y luego haga clic**Abierto**o**Cerca**para controlar remotamente la puerta.

Figura 2-52 Control remoto de la puerta



Operaciones relacionadas

- Filtrado de eventos: seleccione el tipo de evento en**Información del evento**y la lista de eventos muestra los tipos de eventos seleccionados, como eventos de alarma y eventos anormales.
- Eliminación de eventos: haga clic para borrar todos los eventos de la lista de eventos.

### 2.2.20.2 Configuración de Siempre abierto y Siempre cerrado

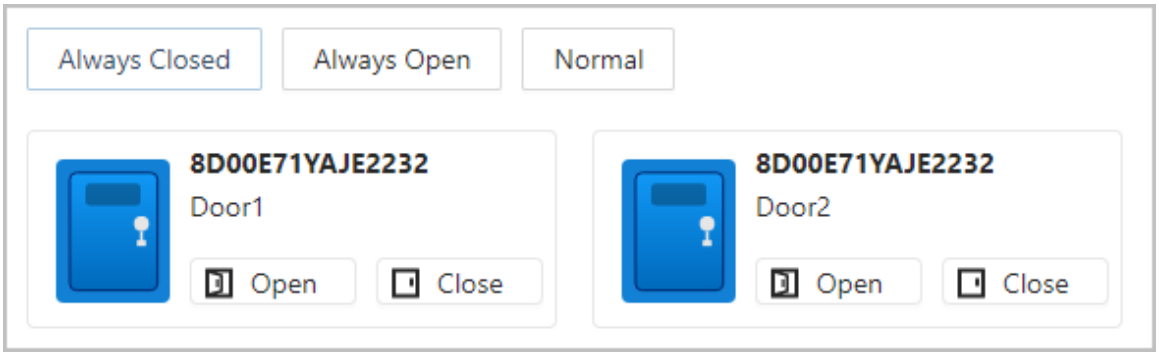
Después de configurar siempre abierta o siempre cerrada, la puerta permanece abierta o cerrada todo el tiempo.

Procedimiento

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

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

Figura 2-53 Siempre abierto o cerrado




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

## 2.2.21 Configuraciones de dispositivos locales (opcional)

Las configuraciones de dispositivos locales solo se pueden aplicar a los controladores de acceso locales.

### 2.2.21.1 Configurar enlaces de alarma locales

Solo puede configurar enlaces de alarma locales en el mismo controlador de acceso. Cada controlador tiene 2 entradas de alarma y 2 salidas de alarma.

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración del dispositivo local**>**Enlace de alarma local**.

Paso 2 Haga clic para configurar el enlace de alarma local.

Figura 2-54 Conexión de alarma local

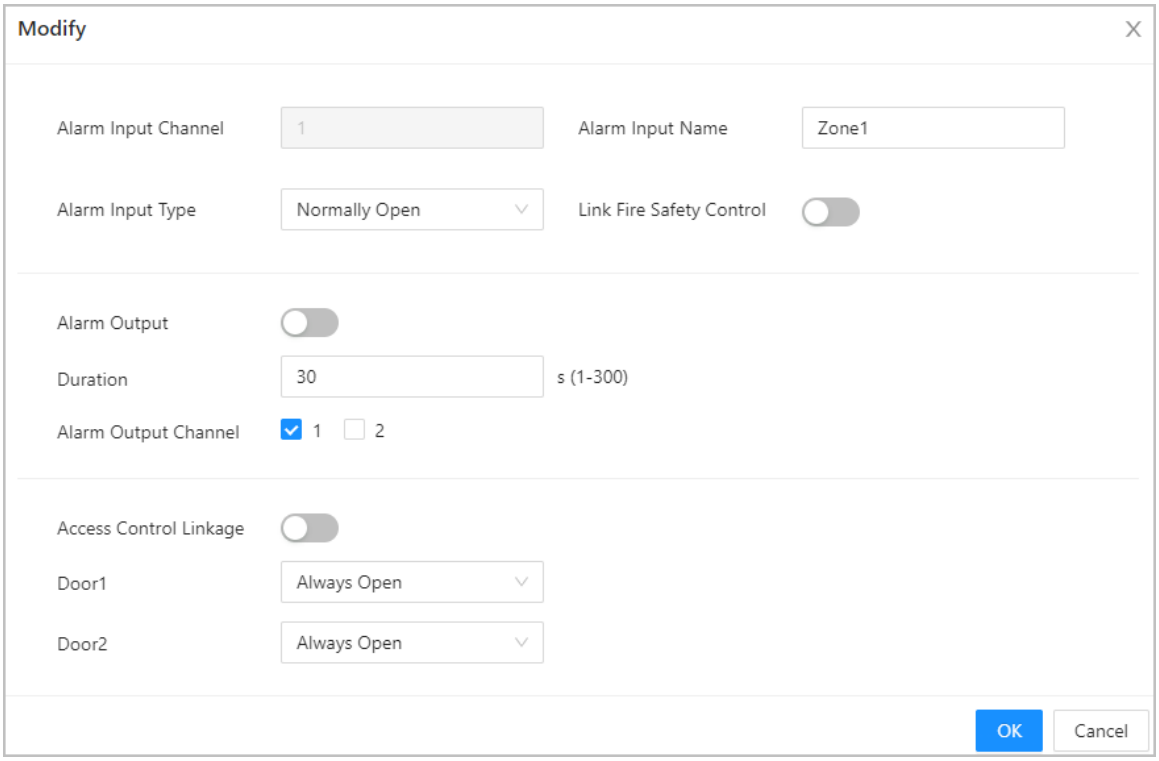



Tabla 2-11 Vinculación de alarma local

| Parámetro | Descripción |
|---|---|
| Canal de entrada de alarma | El número del canal de entrada de alarma.<br>Cada controlador tiene 2 entradas de alarma y 2 salidas de alarma. |
| Nombre de entrada de alarma | El nombre de la entrada de alarma. |
| Tipo de entrada de alarma | El tipo de entrada de alarma.<br>● Normalmente abierto<br>● Normalmente cerrado |
| Enlace de control de seguridad contra incendios | Si activa el control de seguridad contra incendios del enlace, todas las puertas se abrirán cuando se active la alarma contra incendios. |
| Salida de alarma | Puede activar la función de salida de alarma. |
| Duración | Cuando se activa una alarma, la alarma permanece encendida durante un tiempo definido. |
| Canal de salida de alarma | Seleccione el canal de salida de alarma.<br>Cada controlador tiene 2 entradas de alarma y 2 salidas de alarma. |
| Enlace de control de acceso | Active esta función para configurar el enlace de la puerta. |
| Puerta1/Puerta2 | Configure la puerta para que esté siempre abierta o siempre cerrada. Cuando se activa una alarma, la puerta se abrirá o cerrará automáticamente. |

Paso 3 Hacer clicDE ACUERDO.

## 2.2.21.2 Configurar reglas de tarjeta

La plataforma admite 5 tipos de formatos Wiegand de forma predeterminada. También puede agregar formatos Wiegand personalizados.

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración del dispositivo local**>**Configuración de regla de tarjeta de**

Paso 2 **acceso**. Hacer clic**Agregar**y luego configurar nuevos formatos Wiegand.

También puedes hacer clic**Agregar protocolo**para importar un archivo Wiegand a la plataforma.

Figura 2-55 Agregar nuevos formatos Wiegand

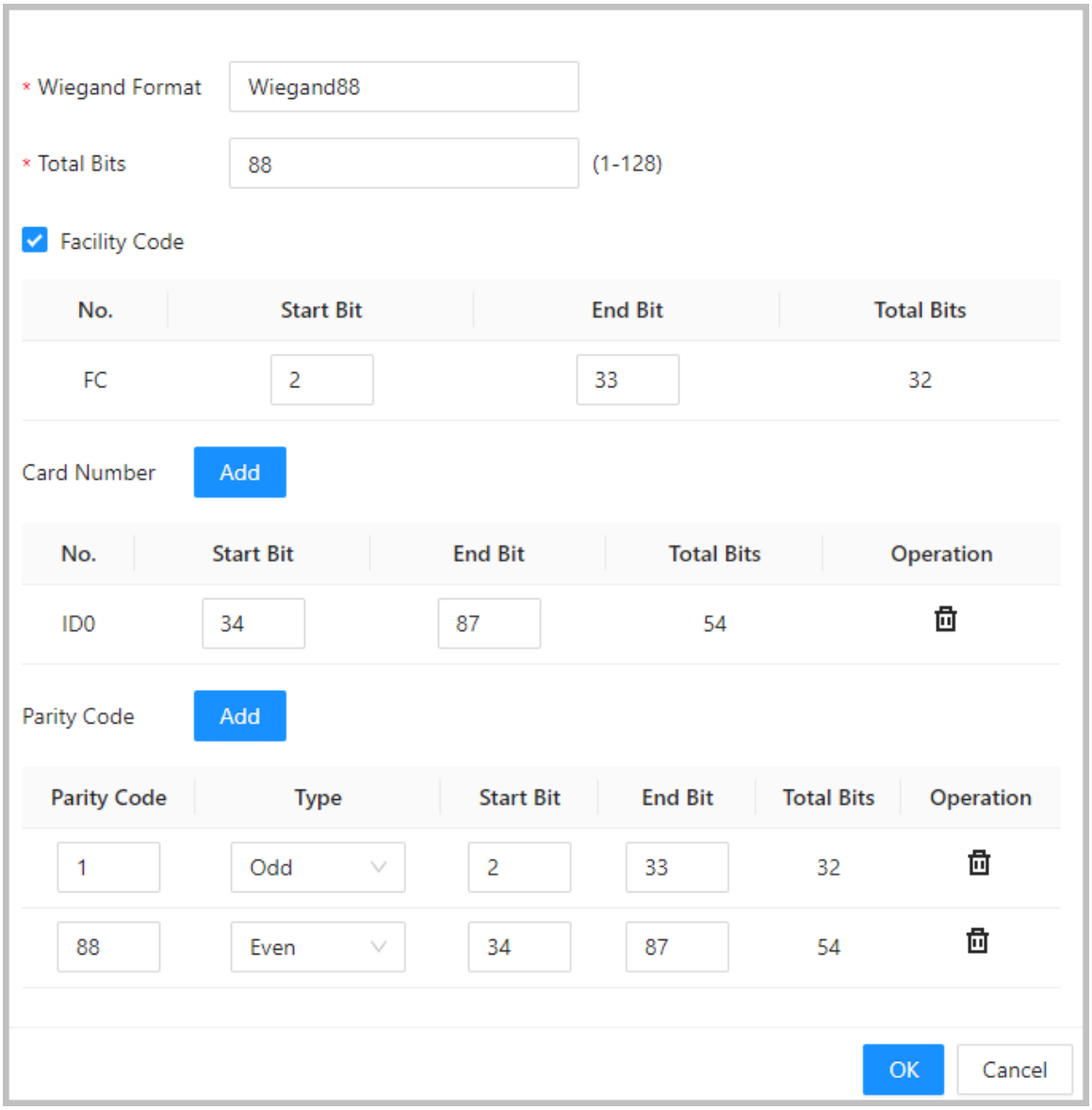



Tabla 2-12 Configurar el formato Wiegand

| Parámetro | Descripción |
|---|---|
| formato Wiegand | El nombre del formato Wiegand. |

| Parámetro | Descripción |
|---|---|
| bits totales | Introduzca el número total de bits. |
| Código de instalación | Ingrese el bit de inicio y el bit de finalización para el código de instalación. |
| Número de tarjeta | Introduzca el bit de inicio y el bit de finalización del número de tarjeta. |
| Código de paridad | 1. Introduzca el bit de inicio de paridad par y el bit de final de paridad par.<br>2. Introduzca el bit de inicio de paridad impar y el bit de fin de paridad impar. |

Paso 3 Hacer clic**DE ACUERDO**.

Operaciones relacionadas

- Código de instalación: si esta función está habilitada y configura**Sistema de número de tarjeta**al formato decimal en el **Gestión de personas**página, el código de instalación y el número de tarjeta se transforman al formato decimal por separado y luego se combinan.
- HID26: Si esta función está activada:
  - Sólo se admite Wiegand 26.
  - La plataforma sólo admite mostrar tarjetas en formato decimal.
  - El número de tarjeta debe tener 5 caracteres y el código de instalación debe tener 3 caracteres como máximo. Cuando ingresa manualmente la tarjeta, el sistema agregará automáticamente un cero inicial a la longitud fija del número. Por ejemplo, si el número de tarjeta que ingresa tiene menos de 5 caracteres, como 56, se agrega un cero inicial para fijar la longitud del número en 5 caracteres, como 00056, y se agrega otro 0 para que funcione como código de instalación. Por tanto, el nº de tarjeta final será 000056.

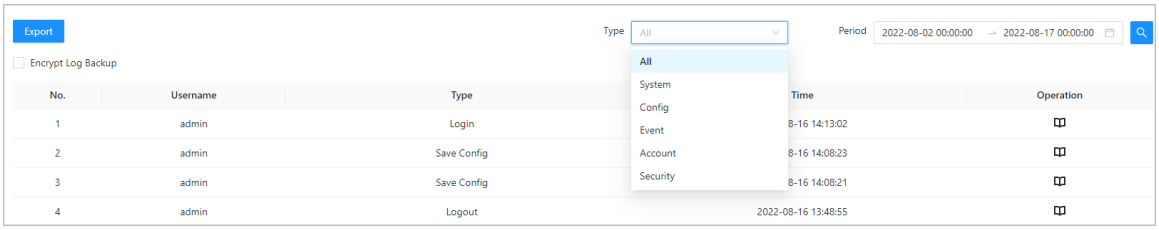
#### 2.2.21.3 Copia de seguridad de los registros del sistema

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración del dispositivo local**>**Registros del**

Paso 2 **sistema**. Seleccione el tipo de registro y luego seleccione el rango de tiempo.

Figura 2-56 Registros de copia de seguridad




Paso 3 Hacer clic**Cifrar copia de seguridad de registros**y luego ingrese la contraseña para realizar una copia de seguridad de los registros cifrados.

Etapa 4 (Opcional) También puedes hacer clic**Exportar**para exportar registros.

## 2.2.21.4 Configuración de la red

### 2.2.21.4.1 Configuración de TCP/IP

Debe configurar la dirección IP del controlador de acceso para asegurarse de que pueda comunicarse con otros dispositivos.

Procedimiento

Paso 1 Seleccionar**Configuración del dispositivo local**>**Configuración de red**>**TCP/IP**.

Paso 2 Configure los parámetros.

Figura 2-57 TCP/IP

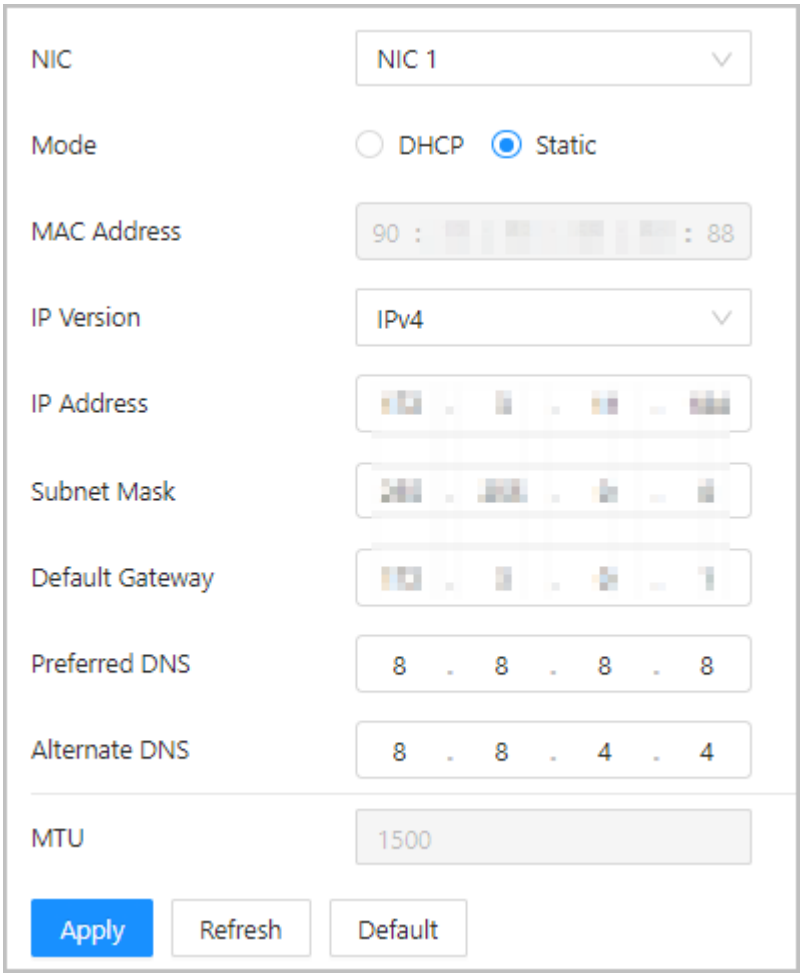



Tabla 2-13 Descripción de TCP/IP

| Parámetro | Descripción |
|---|---|
| Versión IP | IPv4. |
| Dirección MAC | Dirección MAC del controlador de acceso. |
| Modo | • **Estático**:Ingrese manualmente la dirección IP, la máscara de subred y la puerta de enlace.<br>• **DHCP**:Protocolo de configuración huésped dinámico.<br>Cuando DHCP está activado, al controlador de acceso se le asignará automáticamente la dirección IP, la máscara de subred y la puerta de enlace. |
| Dirección IP | Si selecciona el modo estático, configure la dirección IP, la máscara de subred y la puerta de enlace.<br>La dirección IP y la puerta de enlace deben estar en el mismo segmento de red. |
| Máscara de subred | |
| Puerta de enlace predeterminada | |
| DNS preferido | Configure la dirección IP del servidor DNS preferido. |
| DNS alternativo | Establezca la dirección IP del servidor DNS alternativo. |

Paso 3 Hacer clicDE ACUERDO.

#### 2.2.21.4.2 Configuración de puertos

Puede limitar el acceso al controlador de acceso al mismo tiempo a través de la web, el cliente de escritorio y el teléfono.

Procedimiento

Paso 1 Seleccionar**Configuración del dispositivo local**>**Configuración de red**>**Puerto**.

Paso 2 Configure los números de puerto.

Debe reiniciar el controlador para que las configuraciones sean efectivas para todos los parámetros excepto**Conexión máxima**y**Puerto RTSP**.

Figura 2-58 Configurar puertos

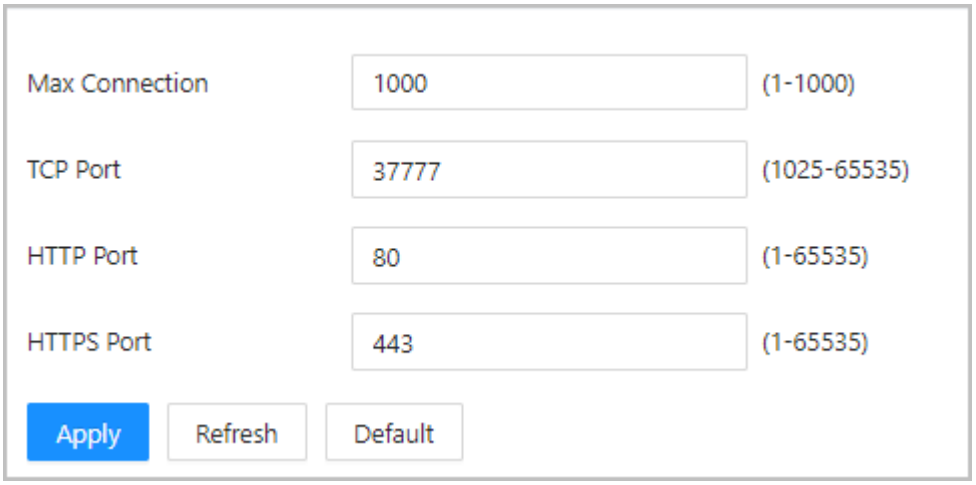



Tabla 2-14 Descripción de puertos

| Parámetro | Descripción |
|---|---|
| Conexión máxima | Puede establecer la cantidad máxima de clientes que pueden acceder al Access Controller al mismo tiempo, como el cliente web, el cliente de escritorio y el teléfono. |
| Puerto TCP | Es 37777 por defecto. |
| Puerto HTTP | Es 80 por defecto. Si desea cambiar el número de puerto, agregue el nuevo número de puerto después de la dirección IP cuando inicie sesión en la página web. |
| Puerto HTTPS | Es 443 por defecto. |

Paso 3 Hacer clicDE ACUERDO.

#### 2.2.21.4.3 Configuración del servicio en la nube

Agregue el controlador principal a DMSS antes de solicitar tarjetas Bluetooth para los usuarios. Para obtener detalles sobre el uso de DMSS, consulte el manual del usuario de DMSS.

## Información de contexto

Si cambió la contraseña del controlador principal o la restauró a los valores predeterminados de fábrica, debe eliminar el controlador en DMSS y agregarlo nuevamente a DMSS.

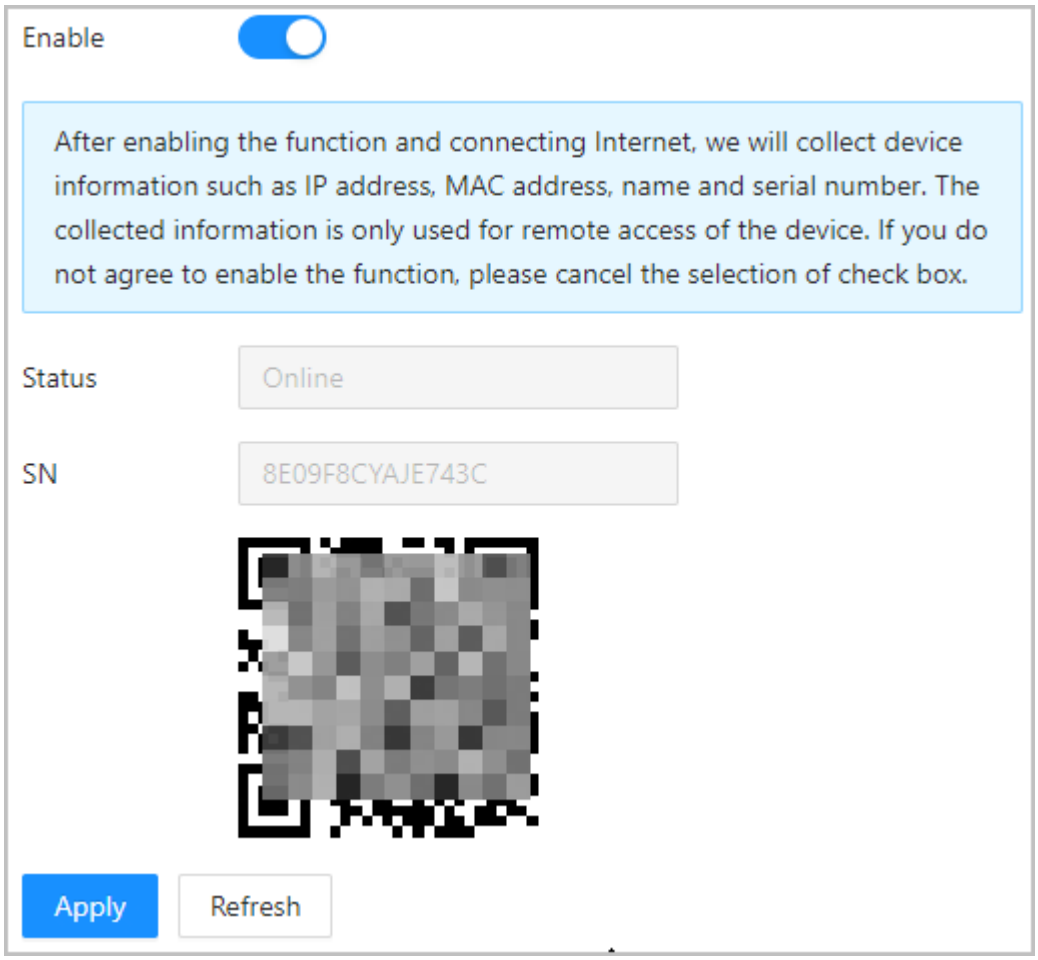
## Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración del dispositivo local**>**Configuración de red**>**Servicio de almacenamiento en la nube**.

Paso 2 Active la función del servicio en la nube.

La función del servicio en la nube está activada de forma predeterminada.

Figura 2-59 Servicio en la nube




Paso 3 Hacer clic**Aplicar**.

Etapa 4 Descargue DMSS y regístrese con correo electrónico, escanee el código QR con DMSS para agregarle el controlador de acceso.

### 2.2.21.4.4 Configurar el registro automático

El Controlador de acceso informa su dirección al servidor designado para que usted pueda obtener acceso al Controlador de acceso a través de la plataforma de administración.

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración de red**>**Registro**.

Paso 2 Habilite la función de registro automático y luego configure los parámetros.

Figura 2-60 Registro

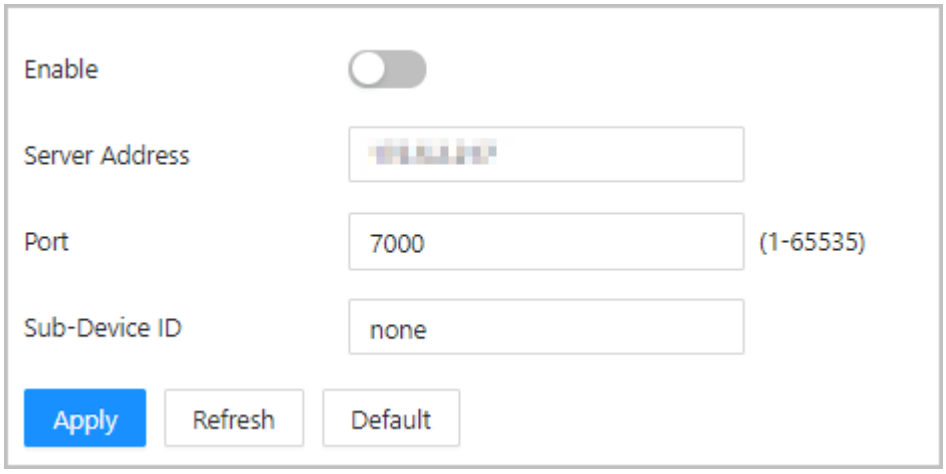



Tabla 2-15 Descripción del registro automático

| Parámetro | Descripción |
|---|---|
| Dirección del servidor | La dirección IP del servidor. |
| Puerto | El puerto del servidor utilizado para el registro automático. |
| ID de subdispositivo | Ingrese la ID del subdispositivo (definida por el usuario).<br>Cuando agrega el Controlador de acceso a la plataforma de administración, la ID del subdispositivo en la plataforma de administración debe coincidir con la ID del subdispositivo definida en el Controlador de acceso. |

Paso 3 Hacer clic**Aplicar**.

### 2.2.21.4.5 Configuración del servicio básico

Cuando desee conectar el controlador de acceso a una plataforma de terceros, active las funciones CGI y ONVIF.

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**Servicio**

Paso 2 **Básico**. Configurar el servicio básico.

Figura 2-61 Servicio básico

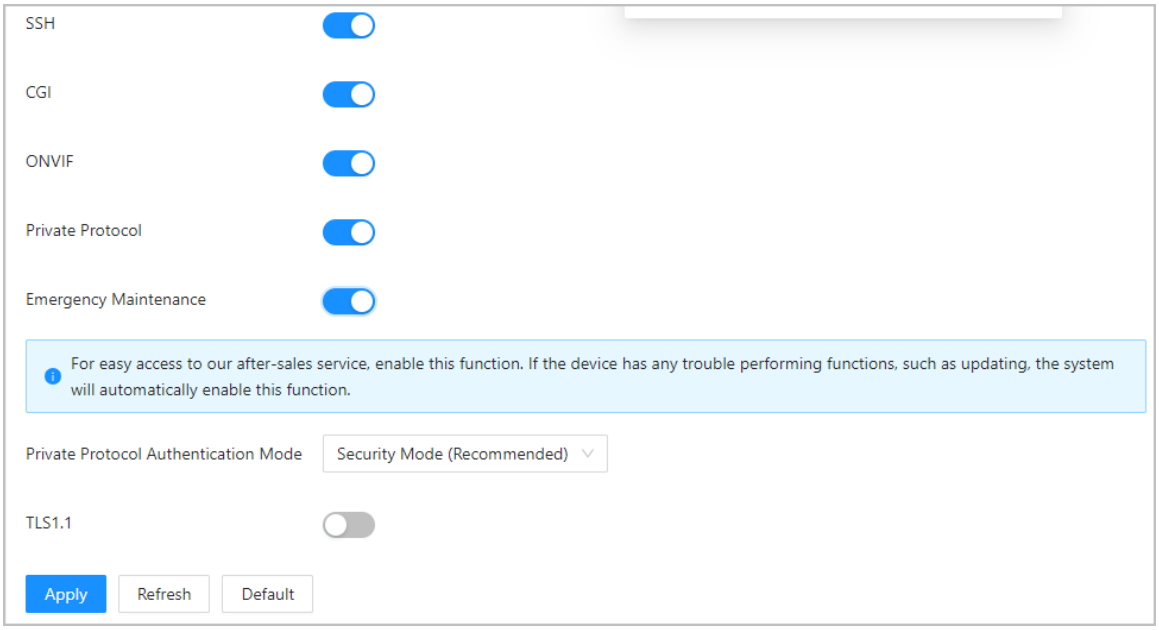



Tabla 2-16 Descripción de los parámetros del servicio básico

| Parámetro | Descripción |
|---|---|
| SSH | SSH, o Secure Shell Protocol, es un protocolo de administración remota que permite a los usuarios acceder, controlar y modificar sus servidores remotos a través de Internet. |
| CGI | La Common Gateway Interface (CGI) es una intersección entre servidores web a través de la cual es posible el intercambio de datos estandarizado entre aplicaciones y servidores externos. |
| ONVIF | ONVIF significa Foro de interfaz de vídeo en red abierta. Su objetivo es proporcionar un estándar para la interfaz entre diferentes dispositivos de seguridad basados en IP. Estas especificaciones ONVIF estandarizadas son como un lenguaje común que todos los dispositivos pueden usar para comunicarse. |
| Protocolo privado | La plataforma agrega dispositivos mediante el protocolo TLSv1.1.<br>Es posible que se presenten riesgos de seguridad cuando TLSv1.1 está habilitado. Por favor tenga en cuenta. |
| Mantenimiento de emergencia | Por defecto viene apagado. |
| Modo de autenticación de protocolo privado | Configure el modo de autenticación, incluido el modo seguro y el modo de compatibilidad. Se recomienda elegir**modo de seguridad**.<br>● Modo de seguridad (recomendado): no admite el acceso al dispositivo a través de métodos de autenticación implícita, DES y de texto sin formato, lo que mejora la seguridad del dispositivo.<br>● Modo compatible: admite el acceso al dispositivo a través de métodos de autenticación implícita, DES y de texto sin formato, con seguridad reducida. |

Paso 3 Hacer clic**Aplicar**.

## 2.2.21.5 Configurar la hora

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración del dispositivo local**>

Paso 2 **Tiempo**. Configurar la hora de la Plataforma.

Figura 2-62 Configuración de fecha

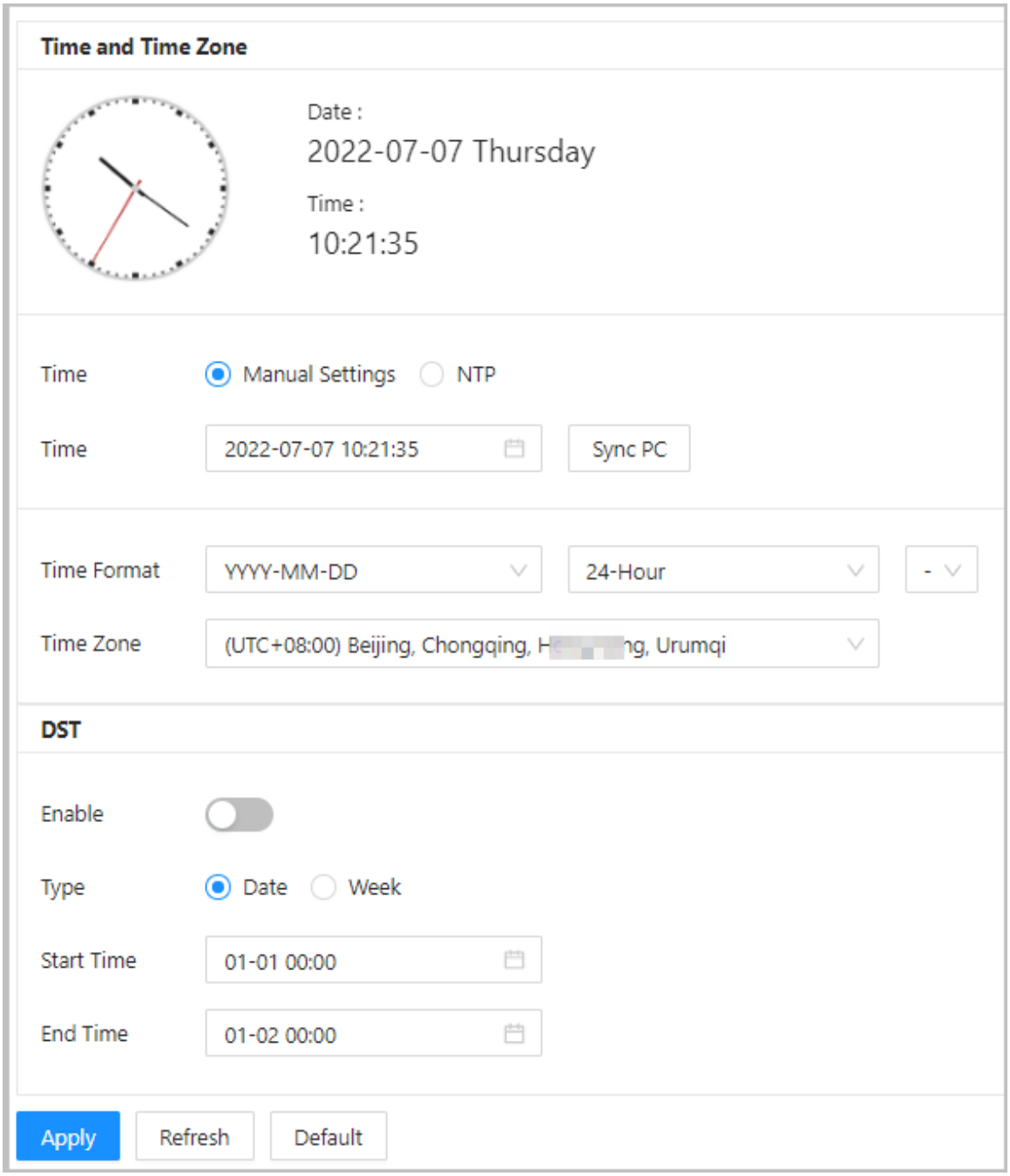


Tabla 2-17 Descripción de la configuración de hora

| Parámetro | Descripción |
|---|---|
| Tiempo | ● Configuración manual: ingrese manualmente la hora o puede hacer clic en**Sincronizar PC** para sincronizar la hora con la computadora.<br>● NTP: El controlador de acceso sincronizará automáticamente la hora con el servidor NTP.<br>◇ **Servidor**:Ingrese el dominio del servidor NTP.<br>◇ **Puerto**:Ingrese el puerto del servidor NTP.<br>◇ **Intervalo**:Ingrese su hora con el intervalo de sincronización. |
| Formato de tiempo | Seleccione el formato de hora para la Plataforma. |
| Zona horaria | Ingrese la zona horaria del controlador de acceso. |
| horario de verano | 1. (Opcional) Habilite el horario de verano.<br>2. Seleccione**Fecha**o**Semana**desde el**Tipo**.<br>3. Configure la hora de inicio y la hora de finalización. |

Paso 3 Hacer clic**Aplicar**.

# 2.2.21.6 Gestión de cuentas

Puede agregar o eliminar usuarios, cambiar la contraseña de usuario e ingresar una dirección de correo electrónico para restablecer su contraseña si la olvida.

## 2.2.21.6.1 Agregar cuentas de administrador

Agregue administradores en el controlador de acceso.

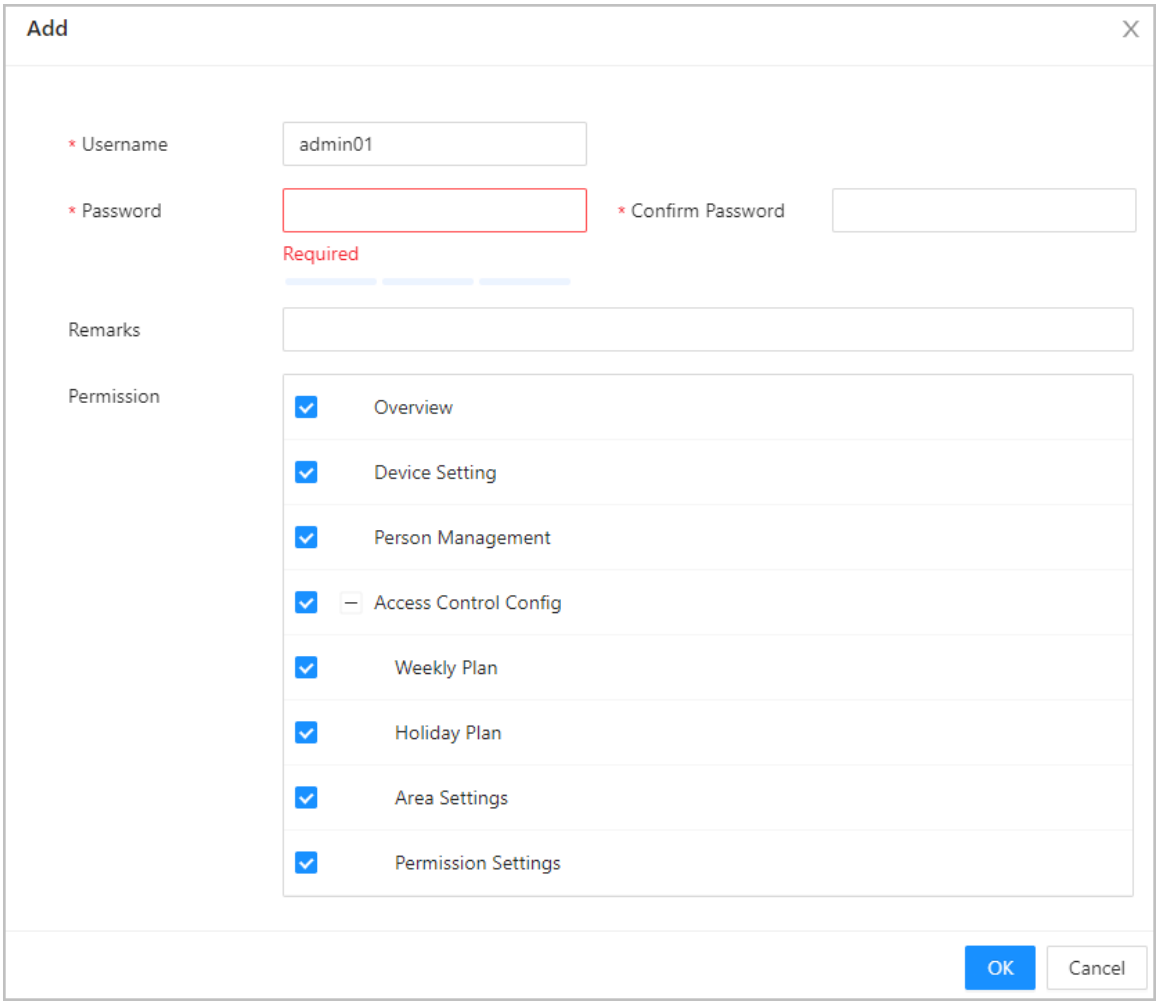
Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración del dispositivo local**>**Administración de cuentas**>**Cuenta**.

Paso 2 Hacer clic**Agregar**y luego ingrese la información del usuario.

- El nombre de usuario no puede ser el mismo que el de la cuenta existente. El nombre de usuario puede contener hasta 31 caracteres y admite números, letras, subrayados, puntos y @.
- La contraseña debe contener de 8 a 32 caracteres que no estén en blanco y contener al menos 2 tipos de los siguientes caracteres: letras mayúsculas y minúsculas, números y caracteres especiales (excluidos ' "; : &). Establezca una contraseña de alta seguridad mediante siguiendo la indicación de seguridad de la contraseña.

Figura 2-63 Agregar cuentas de administrador




Paso 3 Hacer clic**DE ACUERDO**.

Sólo la cuenta de administrador puede cambiar la contraseña y la cuenta de administrador no se puede eliminar.

## 2.2.21.6.2 Restablecer la contraseña

Restablezca la contraseña a través del correo electrónico vinculado cuando la olvide.

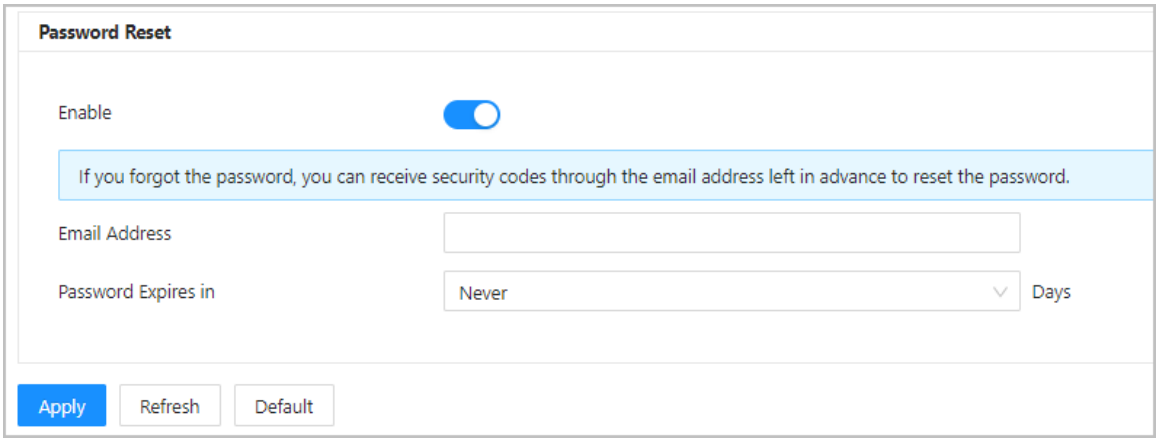
Procedimiento

Paso 1 Seleccionar**Configuración del dispositivo local**>**Administración de cuentas**>**Cuenta**. Ingrese la

Paso 2 dirección de correo electrónico y establezca el tiempo de vencimiento de la contraseña. Active la

Paso 3 función de restablecimiento de contraseña.

Figura 2-64 Restablecer contraseña




Si olvidó la contraseña, puede recibir códigos de seguridad a través de la dirección de correo electrónico vinculada para restablecer la contraseña.

Etapa 4 Hacer clic**Aplicar**.

### 2.2.21.6.3 Agregar usuarios ONVIF

Open Network Video Interface Forum (ONVIF), un foro industrial global y abierto que se estableció para el desarrollo de un estándar abierto global para la interfaz de productos de seguridad físicos basados en IP, que permite la compatibilidad de diferentes fabricantes. Los usuarios de ONVIF verifican sus identidades a través del protocolo ONVIF. El usuario ONVIF predeterminado es administrador.

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración del dispositivo local**>**Administración de cuentas**>**Cuenta ONVIF**.

Paso 2 Hacer clic**Agregar**y luego configurar los parámetros.

Figura 2-65 Agregar el usuario ONVIF

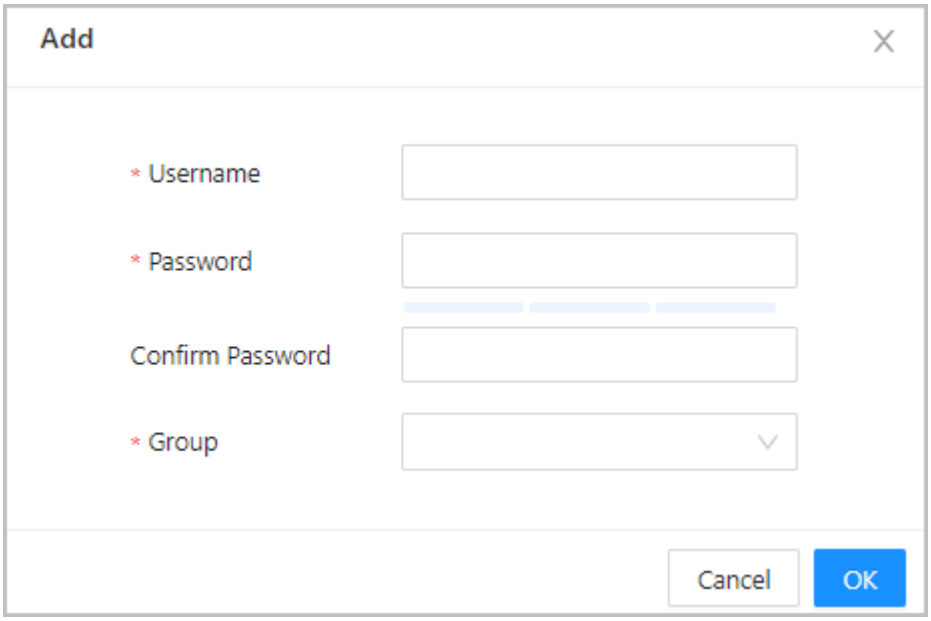


Tabla 2-18 Descripción de usuario de ONVIF

| Parámetro | Descripción |
|---|---|
| Nombre de usuario | El nombre de usuario no puede ser el mismo que el de la cuenta existente. El nombre de usuario consta de hasta 31 caracteres y sólo permite números, letras, guiones bajos, líneas medias, puntos o @. |
| Contraseña | La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de los siguientes caracteres: Mayúsculas, minúsculas, números y caracteres especiales (Excluyendo ' " ; : &). |
| Grupo | Hay tres grupos de permisos que representan diferentes niveles de permiso.<br>● admin: Puede acceder a la gestión de usuarios en ONVIF Administrador de dispositivos.<br>● Operador: No puede acceder a la gestión de usuarios en el Administrador de dispositivos ONVIF.<br>● Usuario: No puede acceder a la administración de usuarios ni a los registros del sistema. en el Administrador de dispositivos ONVIF. |

Paso 3 Hacer clic**DE ACUERDO**.

## 2.2.21.7 Mantenimiento

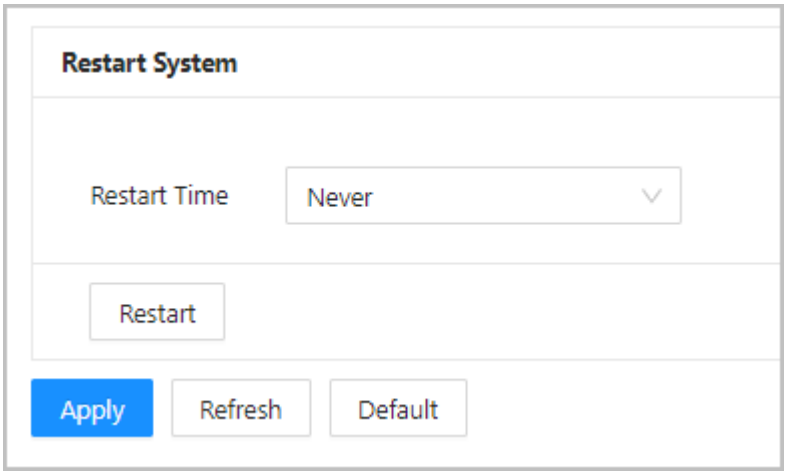
Puede reiniciar periódicamente el controlador de acceso durante su tiempo de inactividad para mejorar su rendimiento. Es **Nunca** De forma predeterminada, le recomendamos cambiarlo a un día a la semana.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Configuración del dispositivo local**>**Mantenimiento**.

Figura 2-66 Mantenimiento




Paso 3 Establezca la hora de reinicio y luego haga clic en**DE ACUERDO**.

Etapa 4 (Opcional) Haga clic**Reanudar**y el controlador de acceso se reiniciará inmediatamente.

# 2.2.21.8 Gestión Avanzada

Cuando más de un controlador de acceso requiere las mismas configuraciones, puede configurarlas rápidamente importando o exportando archivos de configuración.

### 2.2.21.8.1 Exportación e importación de archivos de configuración

Puede importar y exportar el archivo de configuración del Access Controller. Cuando desee aplicar las mismas configuraciones a varios dispositivos, puede importarles el archivo de configuración.

## Información de contexto

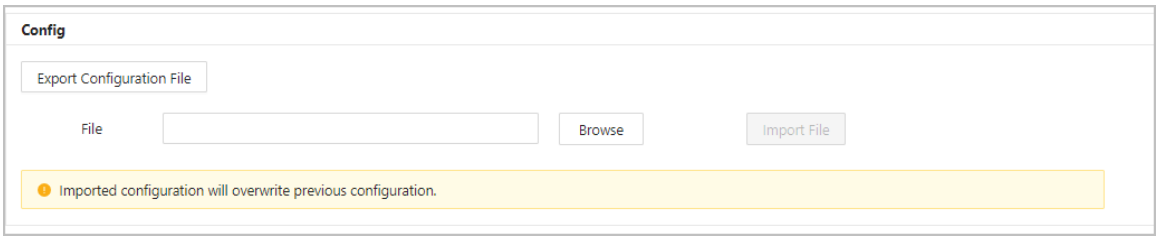
Las configuraciones de gestión de dispositivos, control de acceso avanzado, horarios y hardware no se pueden exportar.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Configuración del dispositivo local**>**Ajustes avanzados**.

Figura 2-67 Gestión de configuración




Paso 3 Exportar o importar archivos de configuración.

- Exporte el archivo de configuración.

  Hacer clic**Exportar archivo de configuración**para descargar el archivo a la computadora local.

  La IP no se exportará.

- Importe el archivo de configuración.

  1. Haga clic**Navegar**para seleccionar el archivo de configuración.
  2. Haga clic**Importar configuración**.

     Los archivos de configuración solo se pueden importar a dispositivos que tengan el mismo modelo.

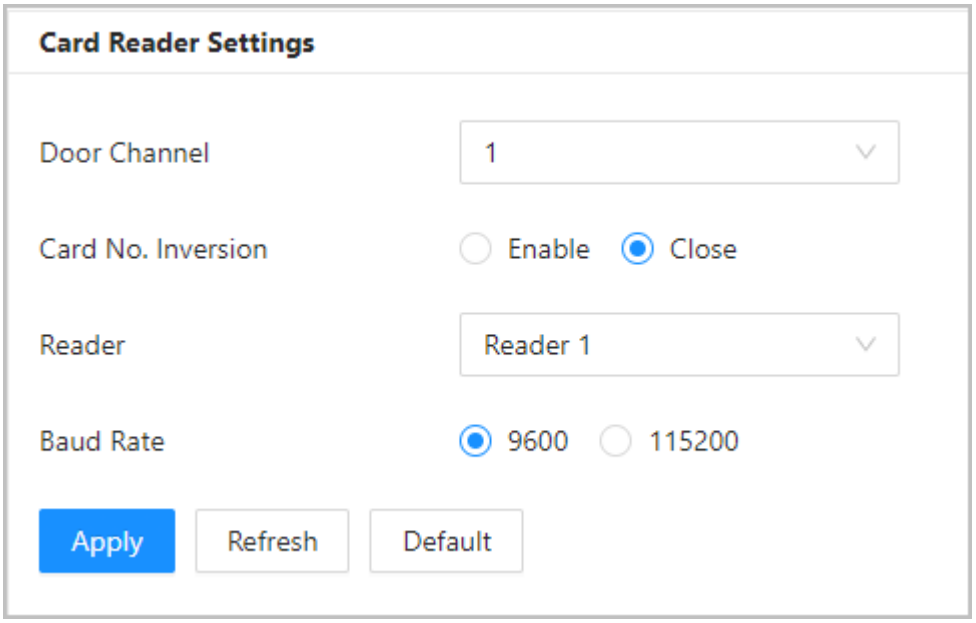
### 2.2.21.8.2 Configuración del lector de tarjetas

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración del dispositivo local**>**Ajustes avanzados**.

Paso 2 Configurar el lector de tarjetas.

Figura 2-68 Configurar el lector de tarjetas




### 2.2.21.8.3 Configurar el nivel de huella digital

En la página de inicio, seleccione**Configuración del dispositivo local**>**Ajustes avanzados**y luego ingrese el umbral de huellas digitales. El valor oscila entre 1 y 10 y un valor más alto significa una mayor precisión de reconocimiento.

Figura 2-69 Nivel de huella digital


### 2.2.21.8.4 Configuración de la expansión RS-485

Si el controlador de acceso está montado en la caja metálica del controlador de acceso, seleccione**Configuración del dispositivo local**>**Expansión RS-485**y luego seleccione**Caja metálica de control de acceso**.

#### 2.2.21.8.5 Restauración de la configuración predeterminada de fábrica

Procedimiento

Paso 1 Seleccionar**Configuración del dispositivo local**>**Ajustes avanzados**.

Restaurando el**Controlador de acceso**a sus configuraciones predeterminadas resultará en la pérdida de datos. Por favor tenga en cuenta.

Paso 2 Restaure la configuración predeterminada de fábrica si es necesario.

- **Fallas de fábrica**:Restablece todas las configuraciones del Controlador y elimina todos los datos.
- **Restaurar a los valores predeterminados (excepto la información del usuario)**:Restablece las configuraciones del Controlador de acceso y elimina todos los datos excepto la información del usuario y la información que se configuró durante el asistente de inicio de sesión).

Sólo el controlador principal admite**Restaurar a los valores predeterminados (excepto la información del usuario)**.

## 2.2.21.9 Actualización del sistema

- Utilice el archivo de actualización correcto. Asegúrese de obtener el archivo de actualización correcto del soporte técnico.
- No desconecte la fuente de alimentación ni la red, y no reinicie ni apague el controlador de acceso durante la actualización.

#### 2.2.21.9.1 Actualización de archivos

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración del dispositivo local**>**Actualizacion del sistema**. En

Paso 2 **Actualización de archivos**,hacer clic**Navegar**y luego cargue el archivo de actualización.

El archivo de actualización debe ser un archivo .bin.

Paso 3 Hacer clic**Actualizar**.

El controlador de acceso se reiniciará una vez finalizada la actualización.

#### 2.2.21.9.2 Actualización en línea

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración del dispositivo local**>**Actualizacion del sistema**. En el

Paso 2 **Actualización en línea**área, seleccione un método de actualización.

- Seleccionar**Comprobación automática de actualizaciones**y el controlador de acceso buscará automáticamente la última actualización de la versión.
- Seleccionar**Verificación manual**, y podrá comprobar inmediatamente si la última versión está disponible.

Paso 3 Hacer clic**Verificación manual**para actualizar el controlador de acceso cuando la última versión esté disponible.

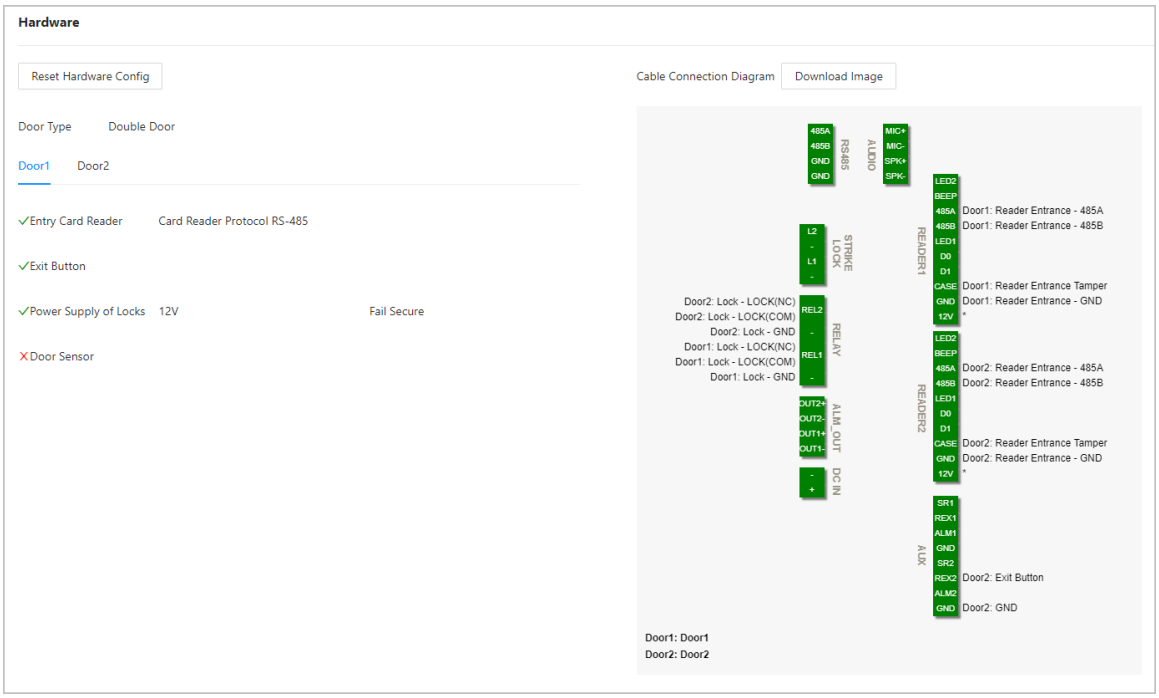
## 2.2.21.10 Configuración de hardware

En la página de inicio, seleccione**Configuración del dispositivo local**>**Hardware**. Puede ver el hardware que ha configurado cuando inicia sesión en la plataforma por primera vez. También puedes hacer clic**Restablecer configuración de hardware**para reconfigurar el hardware. Para obtener más información, consulte la Tabla 2-1.

Cuando cambia entre puerta simple y puerta doble, le recomendamos restaurar los valores predeterminados de fábrica del controlador principal.

El diagrama de cableado se genera para su referencia. Puedes descargarlo a tu computadora.

Figura 2-70 Hardware




## 2.2.21.11 Ver información de la versión

En la página de inicio, seleccione**Configuración del dispositivo local**>**Información de la versión**y podrá ver información sobre la versión, como modelo de dispositivo, número de serie, versión de hardware, información legal y más.

### 2.2.21.12 Visualización de información legal

En la página de inicio, seleccione**Configuración del dispositivo local**>**Información legal**y podrá ver el acuerdo de licencia de software, la política de privacidad y el aviso de software de código abierto.

# 2.2.22 Ver registros

Puede ver registros de alarmas y desbloquear registros.

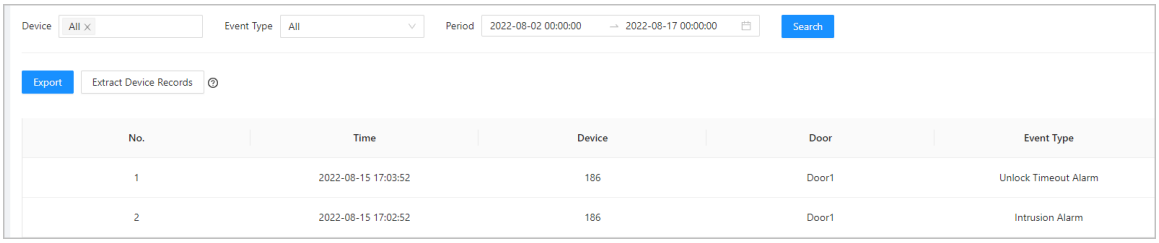
### 2.2.22.1 Visualización de registros de alarma

Procedimiento

Paso 1 En la página de inicio, seleccione**Informes**>**Registros de alarma**.

Paso 2 Seleccione el dispositivo, el departamento y el rango de tiempo, y luego haga clic en**Buscar**.

Figura 2-71 Registros de alarma




- **Exportar**:Exporta registros de desbloqueo en el controlador principal a una computadora local.
- **Extraer registros de dispositivos**:Cuando los registros para el subcontrolador se generan cuando se conectan, puede extraer registros del subcontrolador al controlador principal.

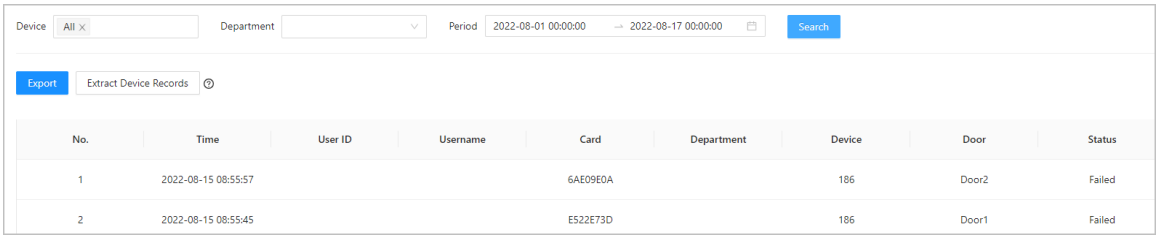
#### 2.2.22.2 Visualización de registros de desbloqueo

Procedimiento

Paso 1 En la página de inicio, seleccione**Informes**>**Desbloquear registros**

Paso 2 Seleccione el dispositivo, el departamento y el rango de tiempo, y luego haga clic en**Buscar**.

Figura 2-72 Registros de desbloqueo




- Exportar: Exporta registros de desbloqueo.
- Extraer registros del dispositivo: cuando se generan registros en el subcontrolador cuando se conectan, se extraen los registros del subcontrolador al controlador principal.

## 2.2.23 Configuración de seguridad (opcional)

### 2.2.23.1 Estado de seguridad

Escanee los módulos de usuarios, servicios y seguridad para verificar el estado de seguridad del controlador de acceso.

## Información de contexto

- Detección de usuarios y servicios: compruebe si la configuración actual cumple con la recomendación.
- Escaneo de módulos de seguridad: escanea el estado de ejecución de los módulos de seguridad, como la transmisión de audio y video, la protección confiable, la advertencia de seguridad y la defensa contra ataques, sin detectar si están habilitados.

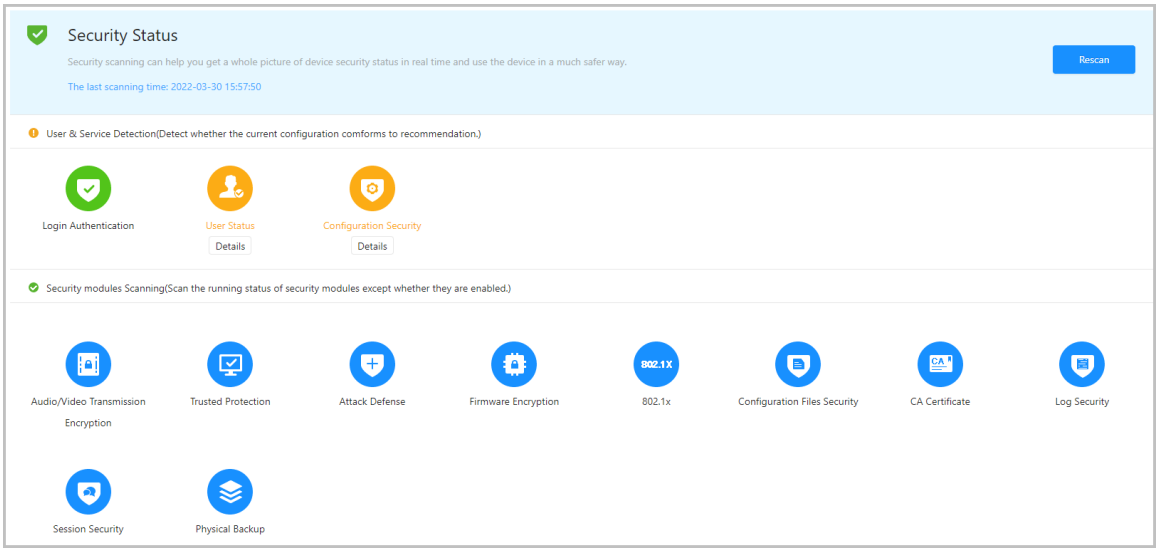
Procedimiento

Paso 1 Seleccionar**Seguridad**>**Estado de seguridad**.

Paso 2 Hacer clic**Volver a escanear**para realizar un análisis de seguridad del controlador de acceso.

Pase el cursor sobre los íconos de los módulos de seguridad para ver su estado de ejecución.

Figura 2-73 Estado de seguridad




Operaciones relacionadas

Después de realizar el escaneo, los resultados se mostrarán en diferentes colores. El amarillo indica que los módulos de seguridad son anormales y el verde indica que los módulos de seguridad son normales.

- Hacer clic**Detalles**para ver los detalles de los resultados del análisis.
- Hacer clic**Ignorar**para ignorar la anomalía y no será escaneada. La anomalía que se ignoró se resaltará en gris.

  Hacer clic**Reincorporarse a la detección**y la anomalía que se ignoró se analizará nuevamente.
- Hacer clic**Optimizar**para solucionar la anomalía.

## 2.2.23.2 Configurar HTTPS

Cree un certificado o cargue un certificado autenticado y luego podrá iniciar sesión en la página web a través de HTTPS en su computadora. HTTPS protege la comunicación a través de una red informática.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Servicio del sistema**>

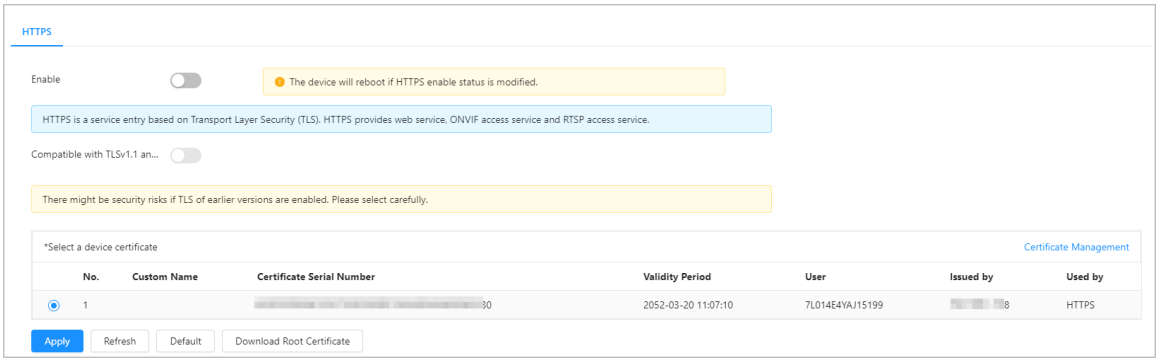
Paso 2 **HTTPS**. Active el servicio HTTPS.

Si activa la compatibilidad con TLS v1.1 y versiones anteriores, pueden ocurrir riesgos de seguridad. Por favor tenga en cuenta.

Paso 3 Seleccione el certificado.

Si no hay certificados en la lista, haga clic en**Gestión de certificados**para cargar un certificado. Para obtener más información, consulte "2.2.23.4 Instalación del certificado del dispositivo".

Figura 2-74 HTTPS




Etapa 4 Hacer clic**Aplicar**.

Ingrese “https://*dirección IP*:*httpsdeporte*" en un navegador web. Si el certificado está instalado, puede iniciar sesión en la página web correctamente. De lo contrario, la página web mostrará el certificado como incorrecto o no confiable.

## 2.2.23.3 Defensa de ataque

### 2.2.23.3.1 Configuración del cortafuegos

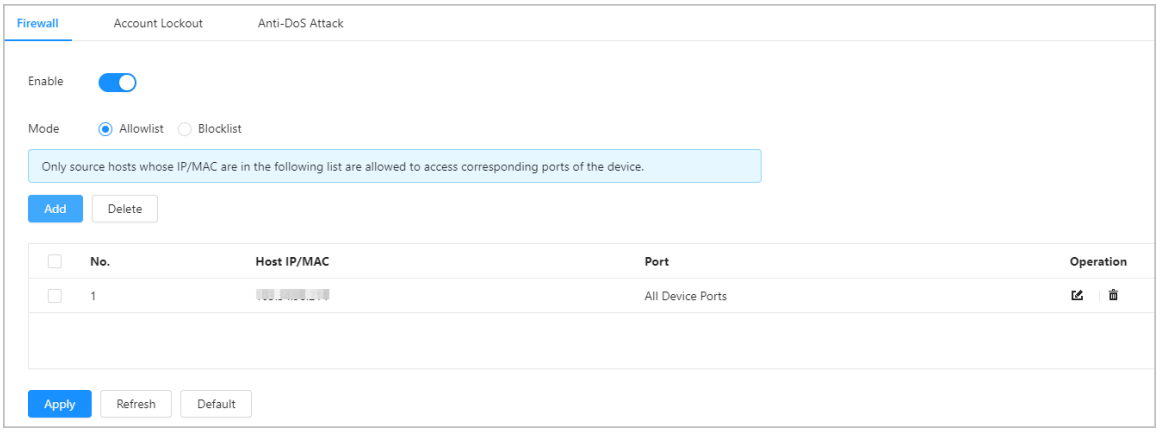
Configure el firewall para limitar el acceso al controlador de acceso.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Defensa de ataque**>**Cortafuegos**

Paso 2 . Haga clic para habilitar la función de firewall.

Figura 2-75 Cortafuegos

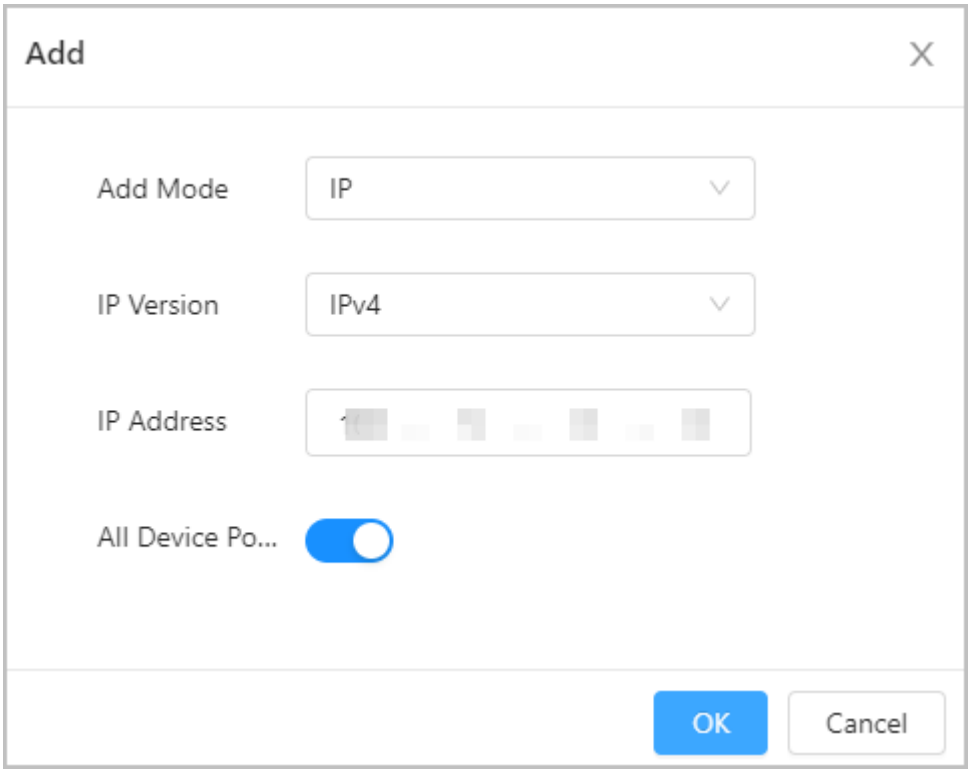



Paso 3 Seleccione el modo:**Lista de permitidos**y**Lista de bloqueos**.

- **Lista de permitidos**:Solo las direcciones IP/MAC en la lista permitida pueden acceder al Controlador de acceso.
- **Lista de bloqueos**:Las direcciones IP/MAC en la lista de bloqueo no pueden acceder al controlador de acceso.

Etapa 4 Hacer clic**Agregar**para ingresar la información de IP.

Figura 2-76 Agregar información de IP




Paso 5 Hacer clicDE ACUERDO.

Operaciones relacionadas

- Hacer clic para editar la información de IP.
- Hacer clic para eliminar la dirección IP.

### 2.2.23.3.2 Configurar el bloqueo de cuenta

Si se ingresa la contraseña incorrecta una cantidad determinada de veces, la cuenta se bloqueará.

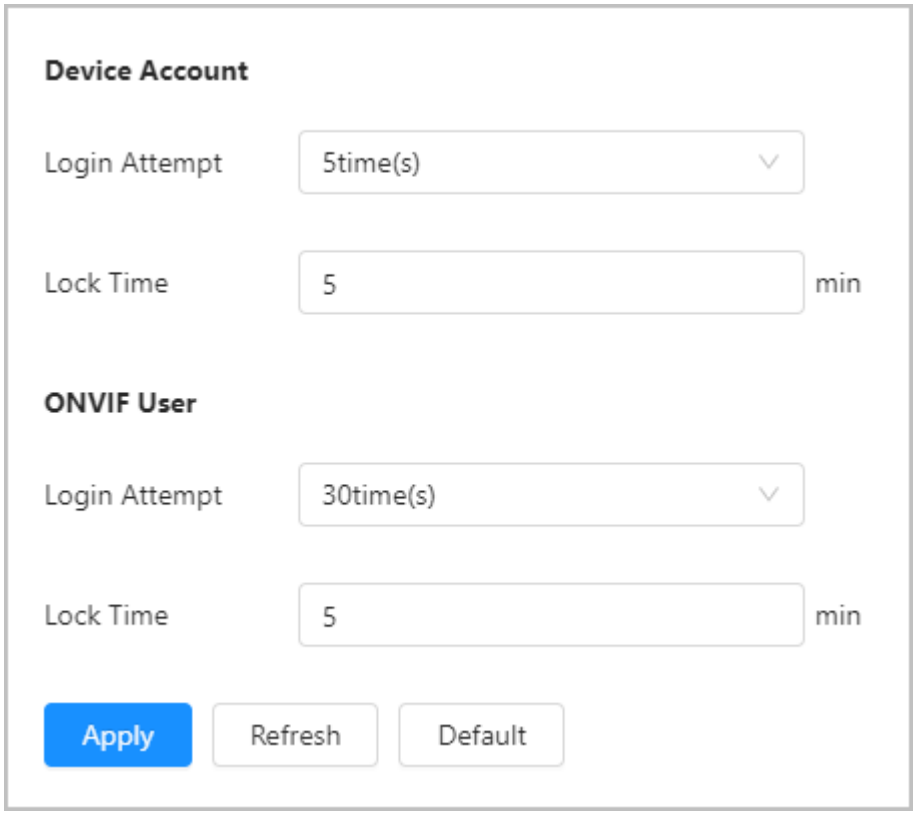
Procedimiento

Paso 1 Seleccionar**Seguridad**>**Defensa de ataque**>**Bloqueo de cuenta**.

Paso 2 Ingrese la cantidad de intentos de inicio de sesión y el tiempo durante el cual la cuenta de administrador y el usuario ONVIF estarán bloqueados.

- Intento de inicio de sesión: el límite de intentos de inicio de sesión. Si se ingresa la contraseña incorrecta una cantidad determinada de veces, la cuenta se bloqueará.
- Tiempo de bloqueo: el período durante el cual no puede iniciar sesión después de que la cuenta esté bloqueada.

Figura 2-77 Bloqueo de cuenta




Paso 3 Hacer clic**Aplicar**.

### 2.2.23.3.3 Configuración del ataque Anti-DoS

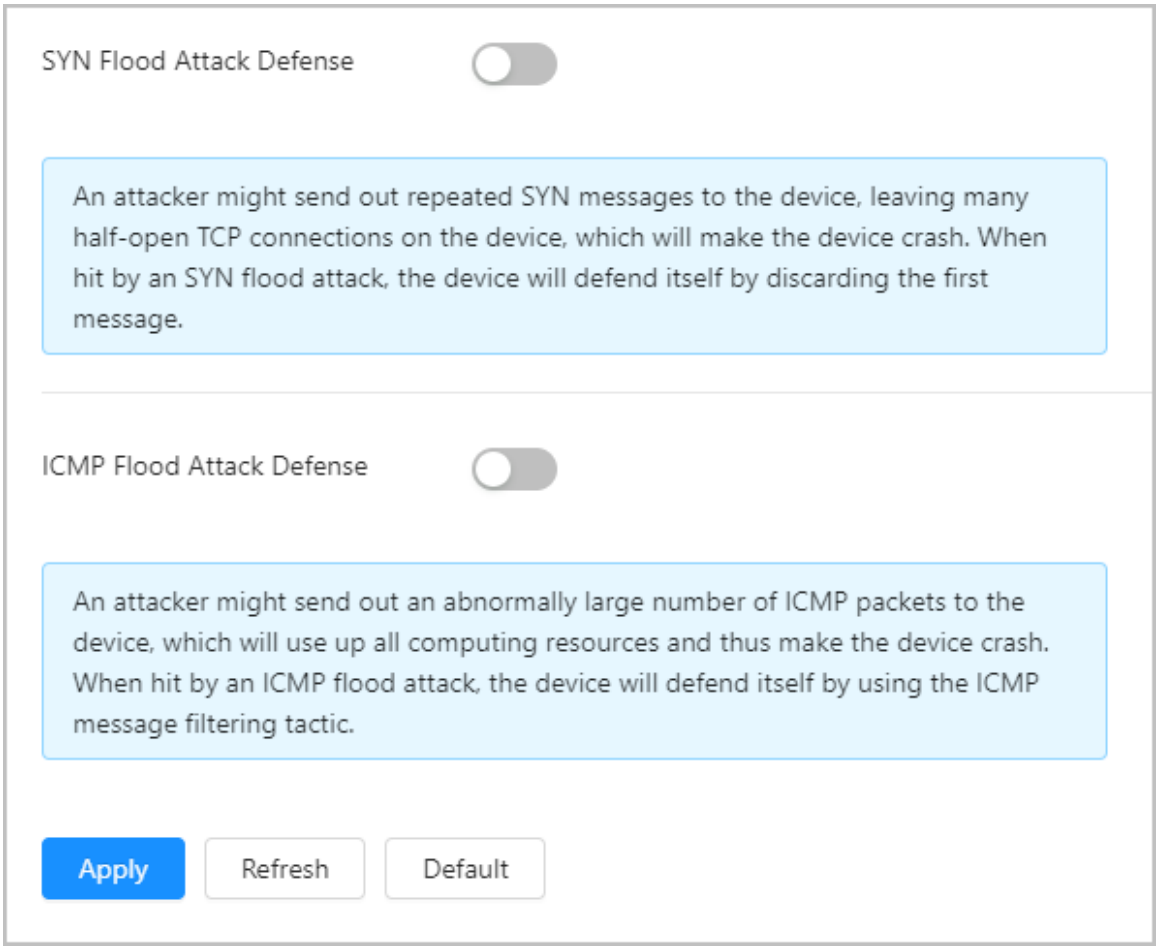
Puedes habilitar**Defensa contra ataques de inundación SYN**y**Defensa contra ataques de inundaciones ICMP**para defender el controlador de acceso contra ataques DOS.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Defensa de ataque**>**Ataque antiDoS**.

Paso 2 Encender**Defensa contra ataques de inundación SYN**o**Defensa contra ataques de inundaciones ICMP**para proteger el controlador de acceso contra ataques DOS.

Figura 2-78 Ataque Anti-DoS




Paso 3 Hacer clic**Aplicar**.

### 2.2.23.4 Instalación del certificado del dispositivo

Cree un certificado o cargue un certificado autenticado y luego podrá iniciar sesión a través de HTTPS en su computadora.

#### 2.2.23.4.1 Creación de certificado

Cree un certificado para el controlador de acceso.

Procedimiento

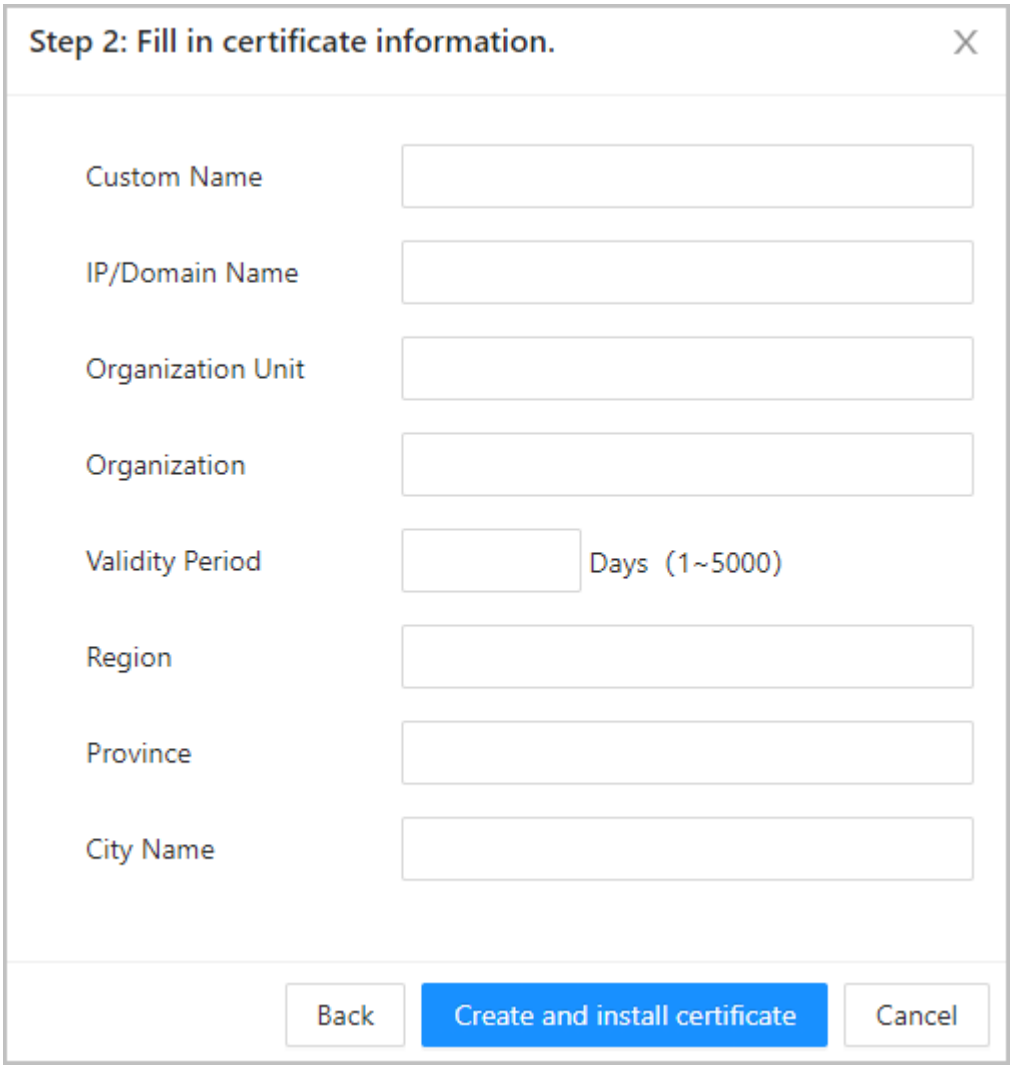
Paso 1 Seleccionar**Seguridad**>**Certificado de CA**>**Certificado de dispositivo**.

Paso 2 Seleccionar**Instalar certificado de dispositivo**. Seleccionar**Crear certificado**,y haga clic**Próximo**. Ingrese la información del certificado.

Paso 3

Etapa 4

Figura 2-79 Información del certificado




El nombre de la región no puede exceder los 2 caracteres. Recomendamos ingresar la abreviatura del nombre de la región.

Paso 5 Hacer clic**Crear e instalar certificado**.

El certificado recién instalado se muestra en la**Certificado de dispositivo**página después de que el certificado se haya instalado correctamente.

Operaciones relacionadas

- Hacer clic**Ingrese al modo de edición**sobre el**Certificado de dispositivo**página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

### 2.2.23.4.2 Solicitud e importación de certificado de CA

Importe el certificado de CA de terceros al controlador de acceso.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Certificado de CA**>**Certificado de dispositivo**. Hacer

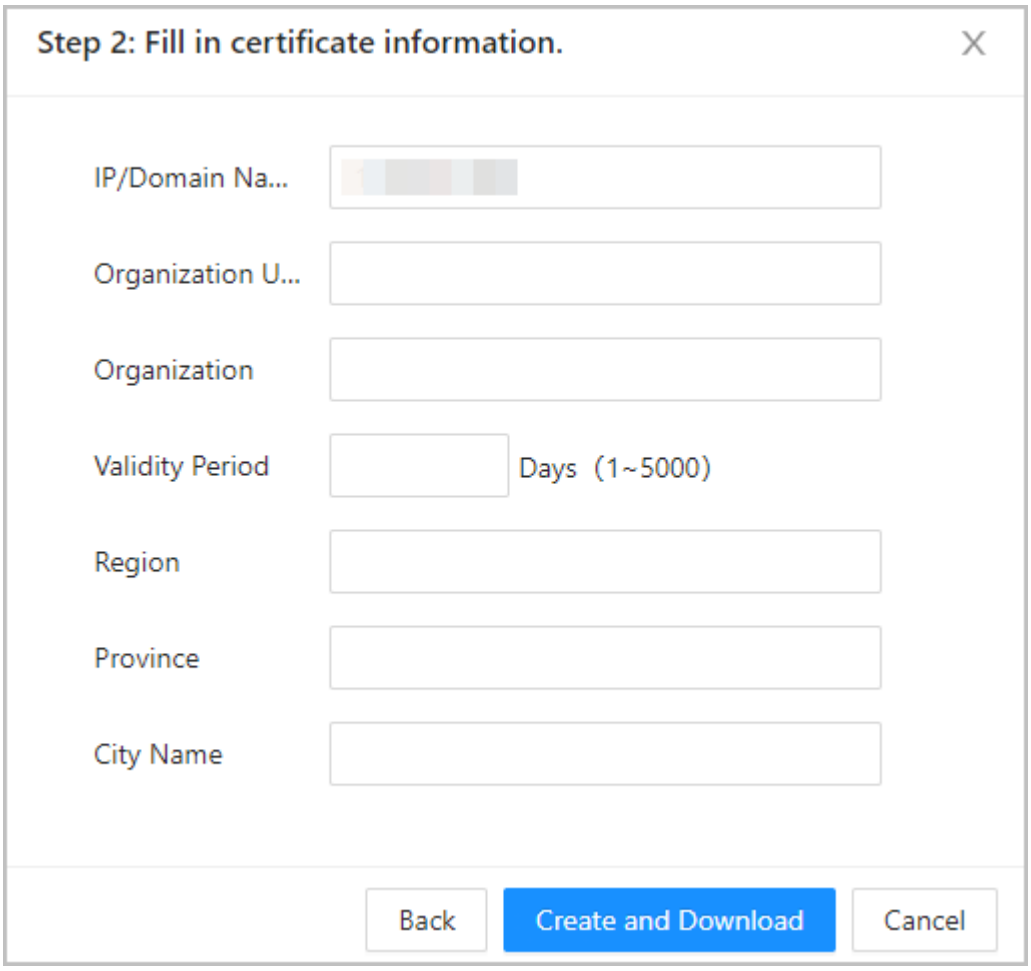
Paso 2 clic**Instalar certificado de dispositivo**.

Paso 3 Seleccionar**Solicite certificado de CA e importación (recomendado)**,y haga clic**Próximo**.

Etapa 4 Ingrese la información del certificado.

- IP/Nombre de dominio: la dirección IP o nombre de dominio del Controlador de acceso.
- Región: el nombre de la región no debe exceder los 3 caracteres. Le recomendamos ingresar la abreviatura del nombre de la región.

Figura 2-80 Información del certificado (2)




Paso 5 Hacer clic**Crear y descargar**.

Guarde el archivo de solicitud en su computadora.

Paso 6 Solicite el certificado a una autoridad de CA de terceros mediante el archivo de solicitud.

Paso 7 Importe el certificado de CA firmado.

1. Guarde el certificado de CA en su computadora.
2. Haga clic**Instalación del certificado del dispositivo**.
3. Haga clic**Navegar**para seleccionar el certificado de CA.
4. Haga clic**Importar e instalar**.

   El certificado recién instalado se muestra en la**Certificado de dispositivo**página después de que el certificado se haya instalado correctamente.

   - Hacer clic**Recrear**para crear el archivo de solicitud nuevamente.
   - Hacer clic**Importar más tarde**importar el certificado en otro momento.

Operaciones relacionadas

- Hacer clic**Ingrese al modo de edición**sobre el**Certificado de dispositivo**página para editar el nombre del certificado.

- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

### 2.2.23.4.3 Instalación del certificado existente

Si ya tiene un certificado y un archivo de clave privada, importe el certificado y el archivo de clave privada.

Procedimiento

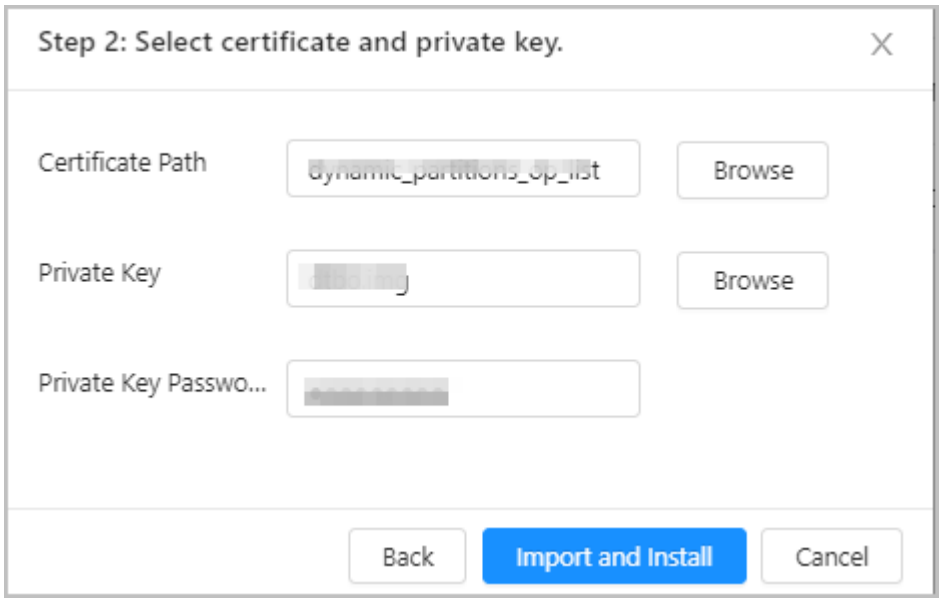
Paso 1 Seleccionar**Seguridad**>**Certificado de CA**>**Certificado de dispositivo**. Hacer

Paso 2 clic**Instalar certificado de dispositivo**.

Paso 3 Seleccionar**Instalar certificado existente**,y haga clic**Próximo**.

Etapa 4 Hacer clic**Navegar**para seleccionar el certificado y el archivo de clave privada, e ingrese la contraseña de clave privada.

Figura 2-81 Certificado y clave privada




Paso 5 Hacer clic**Importar e instalar**.

El certificado recién instalado se muestra en la**Certificado de dispositivo**página después de que el certificado se haya instalado correctamente.

Operaciones relacionadas

- Hacer clic**Ingrese al modo de edición**sobre el**Certificado de dispositivo**página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

## 2.2.23.5 Instalación del certificado de CA de confianza

Un certificado de CA confiable es un certificado digital que se utiliza para validar las identidades de sitios web y servidores. Por ejemplo, cuando se utiliza el protocolo 802.1x, se requiere el certificado de CA para los conmutadores para autenticar su identidad.

### Información de contexto

802.1X es un protocolo de autenticación de red que abre puertos para el acceso a la red cuando una organización autentica la identidad de un usuario y le autoriza el acceso a la red.

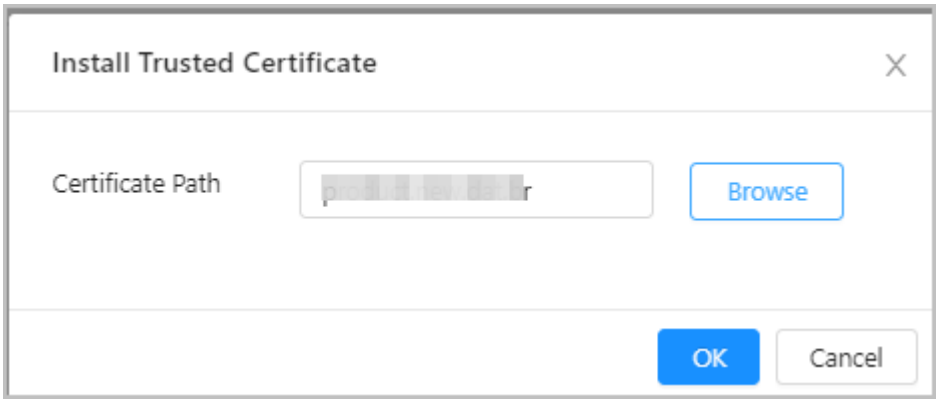
Procedimiento

Paso 1 Seleccionar**Seguridad**>**Certificado de CA**>**Certificados de CA confiables**.

Paso 2 Seleccionar**Instalar certificado de confianza**.

Paso 3 Hacer clic**Navegar**para seleccionar el certificado de confianza.

Figura 2-82 Instalar el certificado de confianza




Etapa 4 Hacer clic**DE ACUERDO**.

El certificado recién instalado se muestra en la**Certificados de CA confiables**página después de que el certificado se haya instalado correctamente.

Operaciones relacionadas

- Hacer clic**Ingrese al modo de edición**sobre el**Certificado de dispositivo**página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

### 2.2.23.6 Advertencia de seguridad

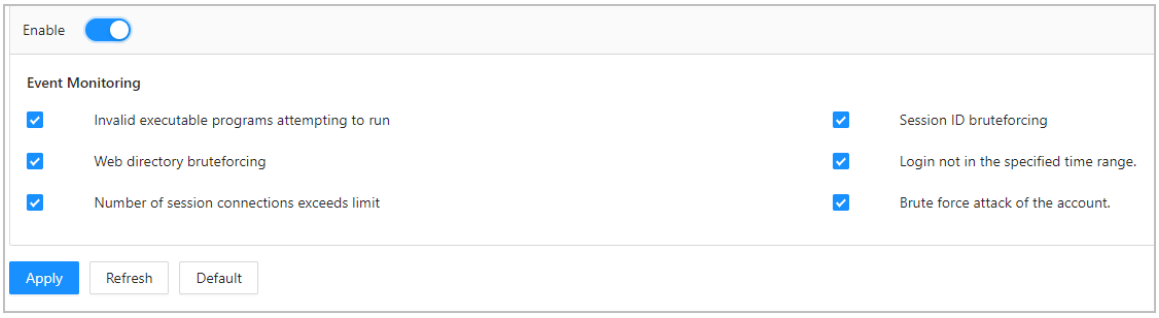
Procedimiento

Paso 1 Seleccionar**Seguridad**>**Certificado de CA**>**Advertencia de seguridad**.

Paso 2 Habilite la función de advertencia de seguridad.

Paso 3 Seleccione los elementos de seguimiento.

Figura 2-83 Advertencia de seguridad




Etapa 4 Hacer clic**Aplicar**.

# 2.3 Configuraciones del subcontrolador

Puede iniciar sesión en la página web del subcontrolador para configurarlo localmente.

## 2.3.1 Inicialización

Inicialice el subcontrolador cuando inicie sesión en la página web por primera vez o después de que el subcontrolador se restablezca a su configuración predeterminada de fábrica. Para obtener detalles sobre cómo inicializar el subcontrolador, consulte "2.2.2 Inicialización".

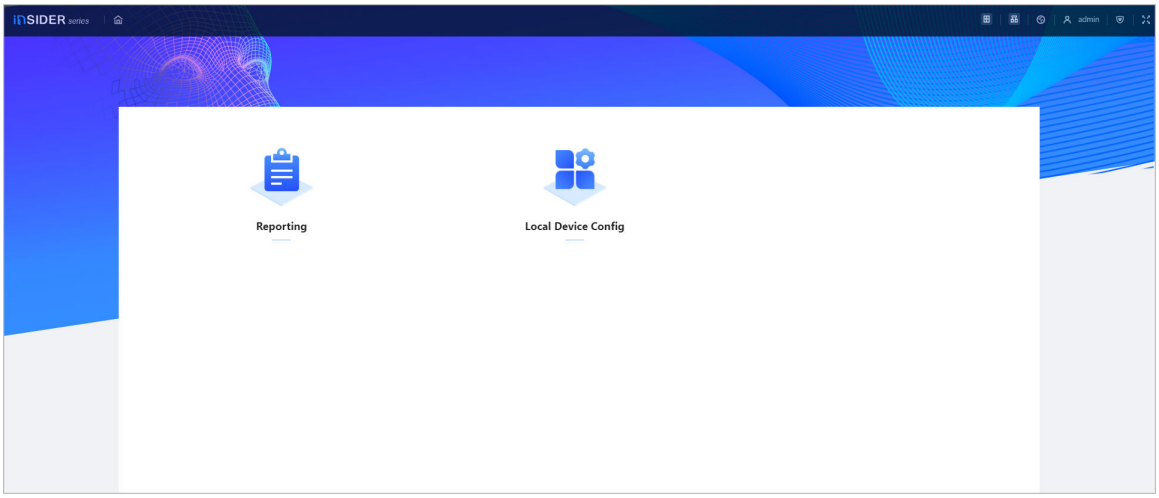
## 2.3.2 Iniciar sesión

Configure el control de acceso como subcontrolador mientras realiza el asistente de inicio de sesión. Para obtener más información, consulte "2.2.3 Iniciar sesión".

## 2.3.3 Página de inicio

La página web del subcontrolador solo incluye**Configuración del dispositivo local**y**Informes**menú. Para obtener más información, consulte "2.2.21 Configuraciones de dispositivos locales (opcional)" y "2.2.22 Visualización de registros".

Figura 2-84 Página de inicio

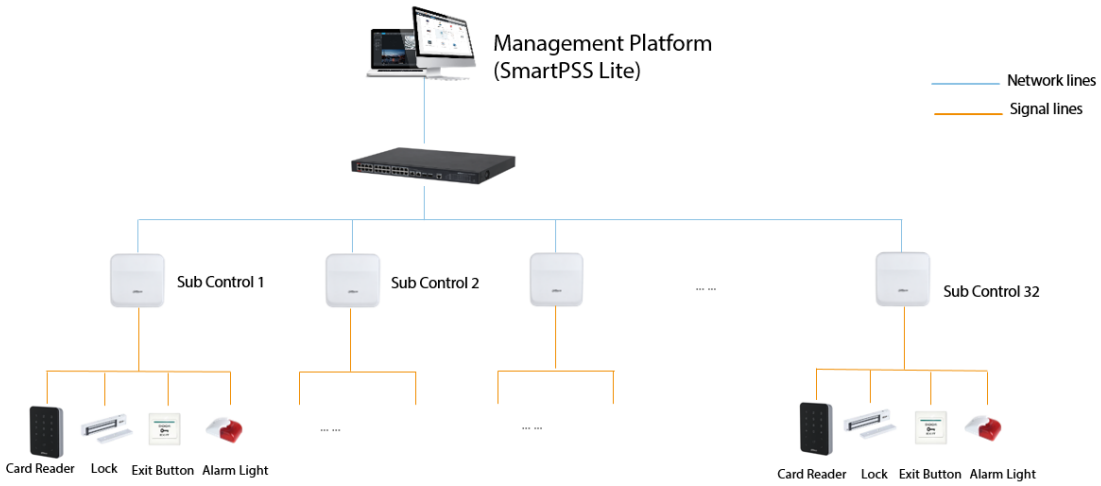


# 3 controladores inteligentes PSS Lite-Sub

## 3.1 Diagrama de red

Los subcontroladores se agregan a una plataforma de gestión independiente, como SmartPSS Lite. Puede administrar todos los subcontroladores a través de SmartPSS Lite.

Figura 3-1 Diagrama de red




## 3.2 Configuraciones en SmartPSS Lite

Agregue subcontroladores a SmartPSS Lite y configúrelos en la plataforma. Para obtener más información, consulte el manual del usuario de SmartPSS Lite.

## 3.3 Configuraciones en el subcontrolador

Para obtener más información, consulte "2.3 Configuraciones del subcontrolador".

# Apéndice 1 Recomendaciones de ciberseguridad

La ciberseguridad es más que una simple palabra de moda: es algo que pertenece a todos los dispositivos 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 conectados 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 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 “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 un dispositivo extraíble (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.

## Más información

Visite el centro de respuesta a emergencias de seguridad del sitio web oficial de Dahua para obtener anuncios de seguridad y las últimas recomendaciones de seguridad.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188