Acceso independiente

Manual del usuario

Versión 1.0.1

Prefacio

General

Este manual presenta las funciones y operaciones del Access Standalone (en adelante, el Dispositivo). Léalo detenidamente antes de usarlo y consérvelo para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de señal	Significado
DANGER	Indica un peligro potencial alto 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.

Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
Versión 1.0.1	Se agregó inicialización descripción.	Diciembre de 2024
Versión 1.0.0	Primer lanzamiento.	Agosto de 2024

Aviso de protección de la privacidad

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

Acerca del manual

- Este manual es solo de referencia. Podrían existir ligeras diferencias entre el manual y el producto.
- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas que no cumplan con el manual.

- El manual se actualizará según las últimas leyes y regulaciones de las jurisdicciones pertinentes. Para obtener información detallada, consulte el manual de usuario impreso, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. Este manual es solo de referencia. Podrían existir ligeras diferencias entre la versión electrónica y la versión impresa.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto podrían generar diferencias entre el producto real y el manual. Para obtener el programa más reciente y la documentación complementaria, póngase en contacto con el servicio de atención al cliente.
- Podría haber errores de impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. En caso de duda o controversia, nos reservamos el derecho de ofrecer una explicación definitiva.
- 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 registradas y nombres de empresas en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o 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 explicación final.

Tabla de contenido

1 Descripción general

Este producto es un equipo de control de acceso que integra lectura, configuración y ejecución de tarjetas. Su diseño es sencillo y moderno, ideal para edificios de oficinas, escuelas, parques, comunidades, fábricas, espacios públicos, centros comerciales, edificios gubernamentales y otras aplicaciones.

2 Operaciones locales

2.1 Inicialización

Tras encender el dispositivo por primera vez, deberá configurar la contraseña de administrador. Esta contraseña se utiliza para acceder al menú principal.

Procedimiento

Paso 1 Encienda el dispositivo y la luz indicadora parpadeará lentamente en rojo.

Paso 2 Presione**#**, ingrese la contraseña de administrador y luego presione**#**.

La contraseña debe tener entre 1 y 8 caracteres.

Si la luz indicadora está en azul fijo, significa que el dispositivo está inicializado.

Tras la inicialización, solo podrá usar las funciones del dispositivo. Si desea acceder a la página web del dispositivo, inicialícelo en su página web o mediante ConfigTool.

Operaciones relacionadas

- Solo puedes establecer números como contraseña de la cuenta de administrador cuando la inicializas a través del dispositivo.
- Puede establecer números, letras y otros caracteres como contraseña de la cuenta de administrador cuando la inicialice a través de la plataforma de ConfigTool.

Tras completar la inicialización del dispositivo, solo podrá realizar operaciones en él. Si necesita conectarlo a la red, utilice ConfigTool o la plataforma para inicializarlo.

Al usar ConfigTool o la plataforma para inicializar el dispositivo, tras configurar la cuenta de red y la contraseña, el dispositivo se inicializará automáticamente y entrará en modo de espera. La contraseña de administrador local se convierte a partir de la contraseña de red. Si la contraseña supera los 8 caracteres, solo se conservan los primeros 8. Las letras se convierten en dígitos según el estándar E.161. La conversión de contraseñas no distingue entre mayúsculas y minúsculas, y todos los demás símbolos se convierten a 0.

- Después de la inicialización, si modifica la contraseña de red, la contraseña de administrador local no se verá afectada.
- Si inicializa primero a través del dispositivo y luego a través de ConfigTool o la plataforma, la contraseña de administrador local no se verá afectada.

Figura 2-1 E.161 (Teclado T9)

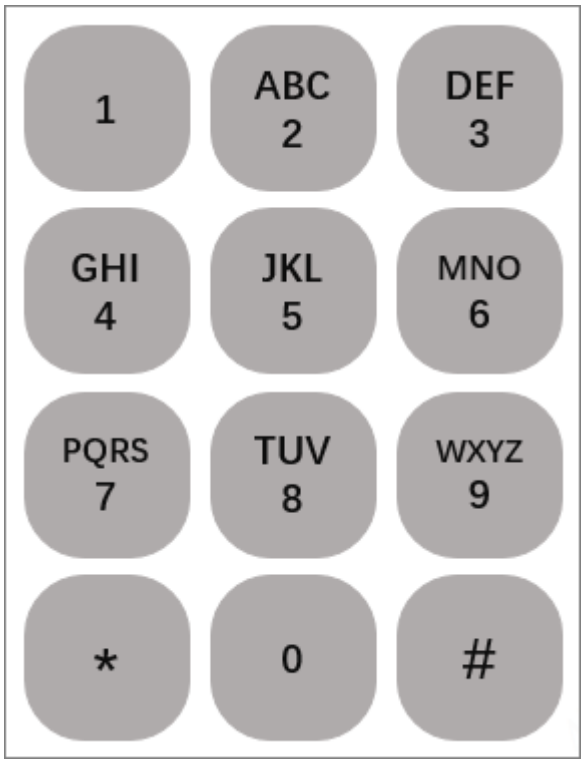


Tabla 2-1 Ejemplo de conversión

Contraseña de red	Contraseña de administrador local
ABC12345	22212345
administrador123	23646123
¡admin12!	23646120
administrador123456	23646123

2.2 Menú principal

Entrar al menú principal

Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

- El indicador parpadea en azul y significa que has ingresado al menú principal.
- El indicador parpadea en rojo una vez, el zumbador suena 3 veces y luego el indicador se vuelve azul fijo, lo que significa que la contraseña es incorrecta.

Indicaciones relacionadas

- El indicador parpadea en verde una vez y el zumbador emite un pitido, lo que significa que la operación o la verificación del control de acceso es exitosa.
- El indicador parpadea en rojo una vez y el zumbador suena 3 veces, lo que significa que la operación o la verificación del control de acceso falló.
- Si el indicador parpadea en rojo lentamente significa que el dispositivo no está inicializado.

- Si el indicador está en azul fijo, significa que el dispositivo está en estado de espera.
- El indicador parpadea en azul, significa que el dispositivo ingresa al menú principal.
- El teclado es blanco al operar el dispositivo. Si no se realiza ninguna operación en 10 segundos, la luz se apaga y el dispositivo sale de la pantalla actual.

2.3 Gestión de usuarios

2.3.1 Agregar usuario

- Solo se puede agregar una tarjeta, una contraseña o una huella digital por usuario. Se debe agregar al menos un método de tarjeta, contraseña y huella digital.
- La función de huella dactilar está disponible en modelos seleccionados.

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadeará en azul.

Paso 2 Presione**1**y**#**Para agregar usuarios, ingrese el ID de usuario y

Paso 3 presione**#**.

- Si el indicador no se enciende y el dispositivo emite un pitido, el ID de usuario se agregó correctamente.
- Si el indicador parpadea en rojo y el dispositivo emite un pitido, significa que no se ha podido agregar el ID de usuario. La posible razón es que ya existe. Intente con el otro ID.

Sólo puedes ingresar números para la identificación en el dispositivo.

Paso 4 Después de pasar la tarjeta, presione**#**para agregar la tarjeta.

Si no necesita agregar la tarjeta, presione**#**Para omitirlo, ingrese

Paso 5 la contraseña de usuario y luego presione**#**.

Si no necesita configurar la contraseña de usuario, presione**#**Para saltártelo.

La contraseña puede tener entre 1 y 8 caracteres.

Paso 6 Añade la huella dactilar y luego presiona**#**.

Si no necesita configurar la huella digital, presione**#**Para saltártelo.

Esta función está disponible en modelos seleccionados.

Paso 7 RepetirPaso 2 aPaso 6 para agregar más usuarios.

Después de agregar el usuario, presione*****para volver al menú principal y luego presione*****para volver al estado de espera.

2.3.2 Eliminación de usuario

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadeará en azul.

Paso 2 Presione**2**y**#**.

Paso 3 Eliminar un usuario.

- Pase la tarjeta y luego presione**#**.

  Si pasa una tarjeta que no ha sido agregada, la eliminación fallará.

- Ingrese el ID de usuario y luego presione**#**.

  Si ingresa un ID que no fue agregado, la eliminación fallará.

- Ingrese 0000 y luego presione**#**para eliminar todos los usuarios.

Después de eliminar, presione*****para volver al menú principal y luego presione*****para salir del menú principal.

2.4 Configuración del modo de desbloqueo de puerta

Información de fondo

La función de huella digital está disponible en modelos seleccionados.

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione**3**y**#**.

Paso 3 Seleccione el modo de desbloqueo.

- Prensa**0**y**#**para configurar el desbloqueo con tarjeta, contraseña o huella dactilar.

  Deslice la tarjeta, introduzca la contraseña o use la huella dactilar para abrir la puerta. La contraseña se puede abrir mediante los siguientes métodos.

  - ◇ En la pantalla de espera, ingrese el ID de usuario, presione**#**, y el dispositivo emite un pitido. Ingrese la contraseña y luego presione**#**para verificar la identidad.
  - ◇ En la pantalla de espera, ingrese la contraseña pública y luego presione**#**para verificar la identidad.
  - ◇ Cuando el**Autenticación de código PIN**está habilitado en la página web del Dispositivo, las personas pueden verificar la identidad simplemente ingresando la contraseña.
  - ◇ Cuando el dispositivo se utiliza con la aplicación DMSS, se admite la contraseña temporal y se puede configurar en la aplicación.

- Prensa**1**y**#**para configurar el desbloqueo mediante tarjeta y contraseña de usuario.

  Primero, pase la tarjeta. Después de que el dispositivo emita un pitido, ingrese la contraseña y presione **#** para verificar la identidad.

- Prensa**2**y**#**para configurar el desbloqueo mediante tarjeta y contraseña de usuario.

Primero, pase la tarjeta. Después de que el dispositivo emita un pitido, presione la huella dactilar para verificar la identidad.

- Prensa**3**y**#**para configurar el desbloqueo con tarjeta, contraseña y huella dactilar.

  Primero, pase la tarjeta. Después de que el dispositivo emita un pitido, presione la huella dactilar. El dispositivo emitirá otro pitido. Ingrese la contraseña y presione**#**para verificar la identidad.

Paso 4 Prensa*****para salir del menú principal.

2.5 Configuración de la duración del desbloqueo

La puerta permanece abierta después de un tiempo definido después de desbloquearse, lo que permite el paso de personas.

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione**4**y**#**.

Paso 3 Introduzca la hora y luego presione**#**.

El valor varía de 1 segundo a 600 segundos. El valor predeterminado es 3 segundos. Pulse*****

Paso 4 para salir del menú principal.

2.6 Configuración del sensor de puerta

Tras activar el sensor de puerta, la alarma de tiempo de espera se activa simultáneamente de forma predeterminada. Si la puerta permanece abierta después del tiempo de espera establecido, el zumbador del dispositivo genera alarmas.

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione**5**y**#**.

Paso 3 Encender o apagar el sensor de la puerta.

El sensor de puerta está desactivado de forma predeterminada.

- Prensa**0**y**#**para apagar el sensor de la puerta.
- Prensa**1**y**#**para encender el sensor de la puerta.

Paso 4 Prensa*****para salir del menú principal.

2.7 Gestión de contraseñas

- Contraseña de administrador: Se utiliza para ingresar al menú principal del Dispositivo.
- Contraseña pública: Se utiliza para verificar la autenticación para desbloquear la puerta.

2.7.1 Cambiar la contraseña del administrador

Para garantizar la seguridad del dispositivo, le recomendamos que cambie la contraseña de administrador de vez en cuando.

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Prensa**0**y**#**.

Paso 3 Ingrese la nueva contraseña y luego presione**#**Ingrese

Paso 4 nuevamente la nueva contraseña y luego presione**#**.

- El color verde intermitente significa que la contraseña se modificó correctamente.
- El color rojo intermitente significa que no se pudo modificar la contraseña.
- Tras la modificación, el dispositivo sale automáticamente del menú principal y el indicador se vuelve azul fijo. Acceda al menú principal con la nueva contraseña si la modificó correctamente. Acceda al menú principal con la contraseña original si no la modificó.

2.7.2 Agregar contraseña pública

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione**6**y**#**.

Paso 3 Ingrese la contraseña pública y luego presione**#**.

La contraseña puede tener entre 1 y 8 caracteres.

Solo se puede agregar una contraseña pública. Si se repiten las operaciones, la nueva contraseña reemplazará a la original.

Paso 4 Prensa*****para salir del menú principal.

2.7.3 Eliminación de la contraseña pública

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione**7**y**#**.

Paso 3 Ingrese la contraseña pública y presione**#**.

Paso 4 Prensa*****para salir del menú principal.

2.8 Gestión de la tarjeta principal

2.8.1 Agregar tarjeta principal

Después de agregar la tarjeta principal, puede agregar y eliminar rápidamente otras tarjetas de usuario a través de la tarjeta principal.

Información de fondo

La tarjeta principal no se puede utilizar para desbloquear la puerta.

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione**8**y**#**.

Paso 3 Pase la tarjeta y luego presione**#**.

- Si el indicador parpadea en verde y el dispositivo emite un pitido, significa que la tarjeta se agregó como tarjeta principal.
- Si el indicador parpadea en rojo y el dispositivo emite un pitido, significa que no se pudo agregar la tarjeta como tarjeta principal.

- Las tarjetas de usuario que se hayan agregado también se pueden configurar como tarjeta principal.
- Si una tarjeta de usuario está configurada como tarjeta principal, no podrá desbloquear la puerta.
- Solo admite una tarjeta principal. Si se añade una nueva, se sobrescribirá la anterior.

Paso 4 Prensa*****para salir del menú principal.

2.8.2 Eliminación de la tarjeta principal

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadeará en azul.

Paso 2 Presione**9**y**#**.

Paso 3 Pase la tarjeta y presione**#**. Prensa

Paso 4 *****para salir del menú principal.

2.8.3 Gestión de tarjetas de usuario a través de la tarjeta principal

Si no se realiza ninguna operación durante 3 segundos después de pasar la tarjeta principal, el dispositivo entra en modo de tarjeta principal y determinará la función correspondiente según las veces que se haya pasado. En modo de tarjeta principal, el indicador parpadea en rojo y azul alternativamente. Si no se realiza ninguna operación durante 10 segundos o se vuelve a pasar la tarjeta principal una vez, vuelve al modo de espera.

- Añadir tarjeta de usuario: Deslice la tarjeta principal una vez y, a continuación, la tarjeta de usuario para añadirla. Se pueden añadir tarjetas de usuario continuamente.
- Eliminar la tarjeta de usuario: Deslice la tarjeta principal dos veces y, a continuación, deslice la tarjeta de usuario para eliminarla. Las tarjetas de usuario se pueden eliminar continuamente.
- Borrar todas las tarjetas de usuario: Pase la tarjeta principal 5 veces seguidas.

2.9 Configuración del período de tiempo de espera de la puerta

Una vez habilitado el sensor de puerta, si la puerta permanece abierta después del tiempo establecido, el zumbador del dispositivo emitirá una alarma.

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione**10**y**#**.

Paso 3 Ingrese el período de tiempo de espera de la puerta y luego presione**#**.

El rango de valores va de 1 segundo a 9999 segundos. El valor predeterminado es 60 segundos. Pulse

Paso 4 *****para salir del menú principal.

2.10 Restaurar la configuración de fábrica

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadeará en azul.

Paso 2 Presione**11**y**#**.

Paso 3 Restaurar el dispositivo a la configuración de fábrica.

- Prensa**00**y**#**para restaurar la configuración de fábrica (conservar la información del usuario).
- Prensa**000**y**#**para restaurar la configuración de fábrica (restaurar toda la información).

Operaciones relacionadas

Puede utilizar el botón de reinicio para restaurar el dispositivo a la configuración de fábrica.

3 Operaciones de página web

En la página web también puede configurar y actualizar el dispositivo.

Las configuraciones web varían según los modelos del dispositivo.

3.1 Inicialización

Inicialice el dispositivo cuando inicie sesión en la página web por primera vez o después de que el dispositivo se restaure a los valores predeterminados de fábrica.

Prerrequisitos

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

Procedimiento

Paso 1 Abra un navegador, vaya a la dirección IP (la dirección predeterminada es 192.168.1.108) del dispositivo.

Le recomendamos que utilice la última versión de Chrome o Firefox.

Paso 2 Seleccione un idioma para el dispositivo.

Paso 3 Establezca la contraseña y la dirección de correo electrónico de acuerdo con las instrucciones en pantalla.

- La contraseña debe tener entre 8 y 32 caracteres (no espacios en blanco) y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excepto ' " ; : &). Establezca una contraseña de alta seguridad siguiendo las instrucciones de seguridad.
- Mantenga la contraseña segura después de la inicialización y cámbiela periódicamente para mejorar la seguridad.

Operaciones relacionadas

- Solo puedes establecer números como contraseña de la cuenta de administrador cuando la inicializas a través del dispositivo.
- Puede establecer números, letras y otros caracteres como contraseña de la cuenta de administrador cuando la inicialice a través de la plataforma de ConfigTool.

Tras completar la inicialización del dispositivo, solo podrá realizar operaciones en él. Si necesita conectarlo a la red, utilice ConfigTool o la plataforma para inicializarlo.

Al usar ConfigTool o la plataforma para inicializar el dispositivo, tras configurar la cuenta de red y la contraseña, el dispositivo se inicializará automáticamente y entrará en modo de espera. La contraseña de administrador local se convierte a partir de la contraseña de red. Si la contraseña supera los 8 caracteres, solo se conservan los primeros 8. Las letras se convierten en dígitos según el estándar E.161. La conversión de contraseñas no distingue entre mayúsculas y minúsculas, y todos los demás símbolos se convierten a 0.

- Después de la inicialización, si modifica la contraseña de red, la contraseña de administrador local no se verá afectada.
- Si inicializa primero a través del dispositivo y luego a través de ConfigTool o la plataforma, la contraseña de administrador local no se verá afectada.

Figura 3-1 E.161 (Teclado T9)

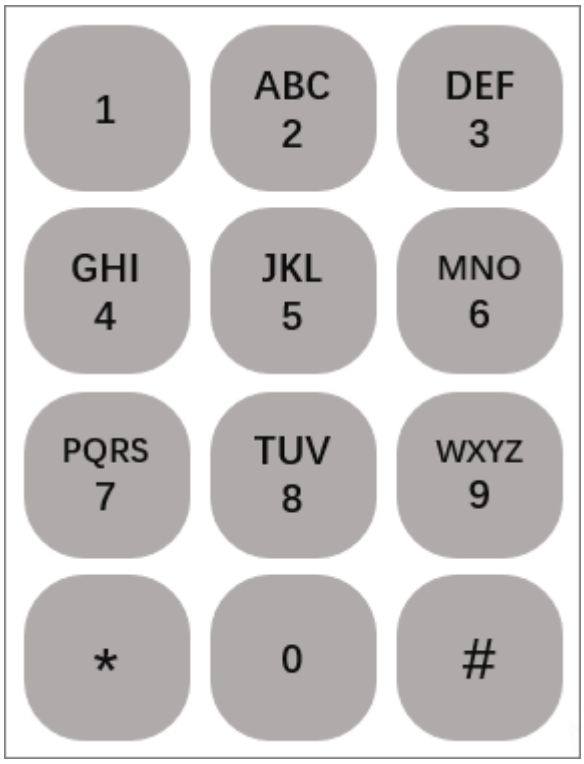


Tabla 3-1 Ejemplo de conversión

Contraseña de red	**Contraseña de administrador local**
ABC12345	22212345
administrador123	23646123
¡admin12!	23646120
administrador123456	23646123

3.2 Restablecimiento de la contraseña

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

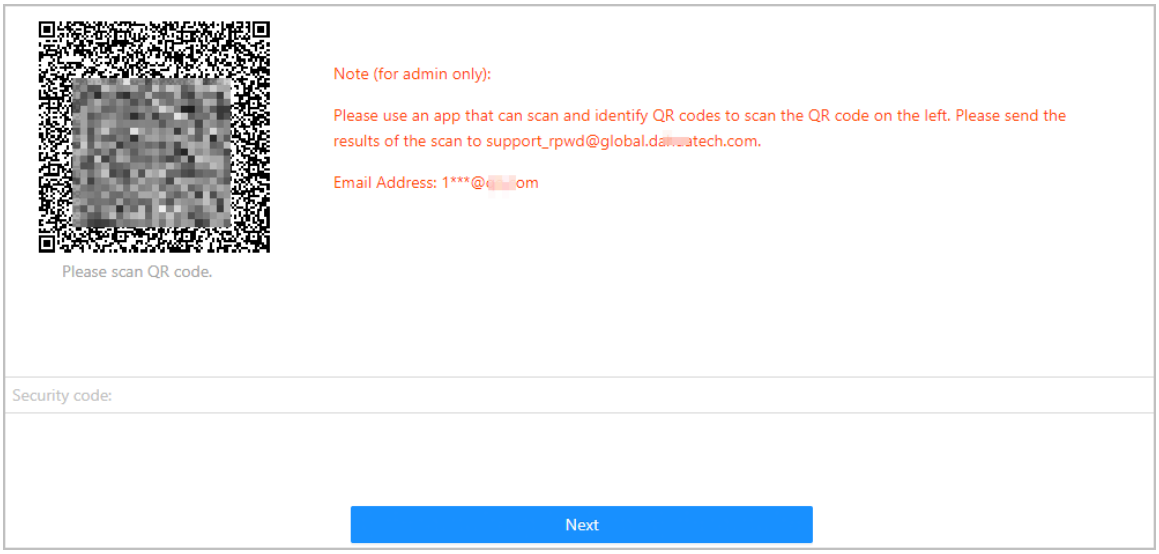
Procedimiento

Paso 1 En la página de inicio de sesión, haga clic en**Has olvidado tu contraseña**.

Paso 2 Lea atentamente las instrucciones en pantalla y luego haga clic**DE**

Paso 3 **ACUERDO**Escanea el código QR y recibirás un código de seguridad.

Figura 3-2 Restablecer contraseña



- Se generarán hasta dos códigos de seguridad al escanear el mismo código QR. Si el código de seguridad deja de ser válido, actualícelo y vuelva a escanearlo.
- Tras escanear el código QR, recibirá un código de seguridad en su dirección de correo electrónico asociada. Úselo dentro de las 24 horas posteriores a su recepción. De lo contrario, perderá su validez.
- Si se ingresa un código de seguridad incorrecto 5 veces seguidas, la cuenta de administrador se congelará durante 5 minutos.

Paso 4 Introduzca el código de seguridad.

Paso 5 Haga clic.**Próximo**.

Paso 6 Restablecer y confirmar la contraseña.

La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos dos de los siguientes tipos de caracteres: mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &).

Paso 7 Hacer clic**DE ACUERDO**.

3.3 Página de inicio

La página de inicio se muestra después de iniciar sesión correctamente.

Figura 3-3 Página de inicio

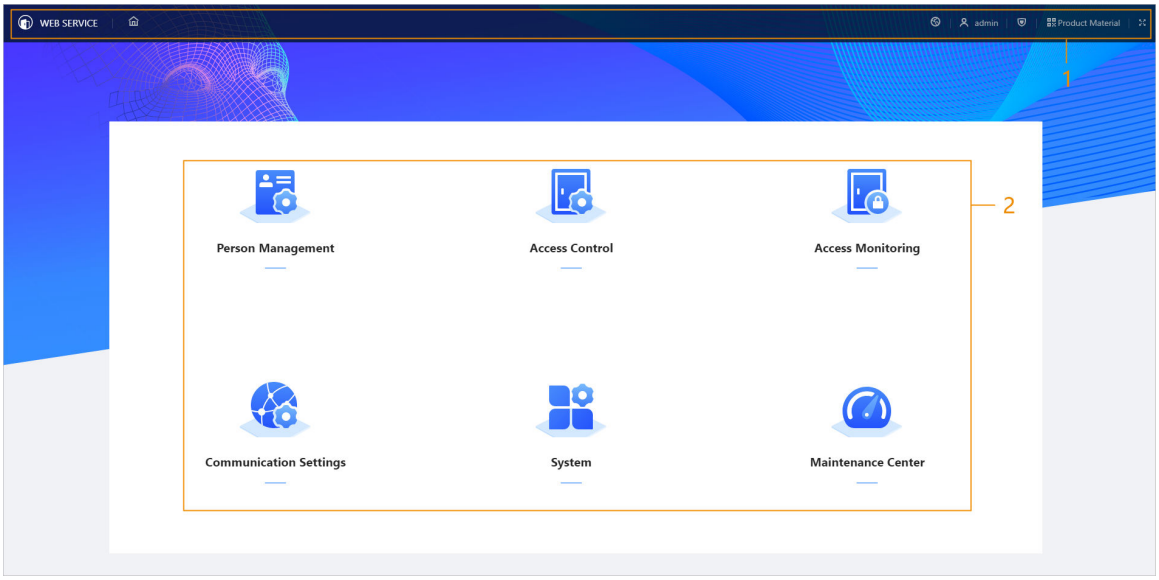


Tabla 3-2 Descripción de la página de inicio

No.	Descripción
1	• :Ingresa a la página de inicio. • :Seleccione un idioma en el dispositivo. • admin:Cierre la sesión o reinicie el dispositivo. • :Ingrese el**Seguridad**página. • **Material del producto**:Escanee el código QR para ver el material del producto. Esta función está disponible en modelos seleccionados. • :Mostrar en pantalla completa.
2	Menú principal.

3.4 Gestión de personas

Procedimiento

Paso 1 En la página de inicio, seleccione**Gestión de personas**,y luego haga clic**Agregar**. Configurar

Paso 2 la información del usuario.

Figura 3-4 Agregar usuarios

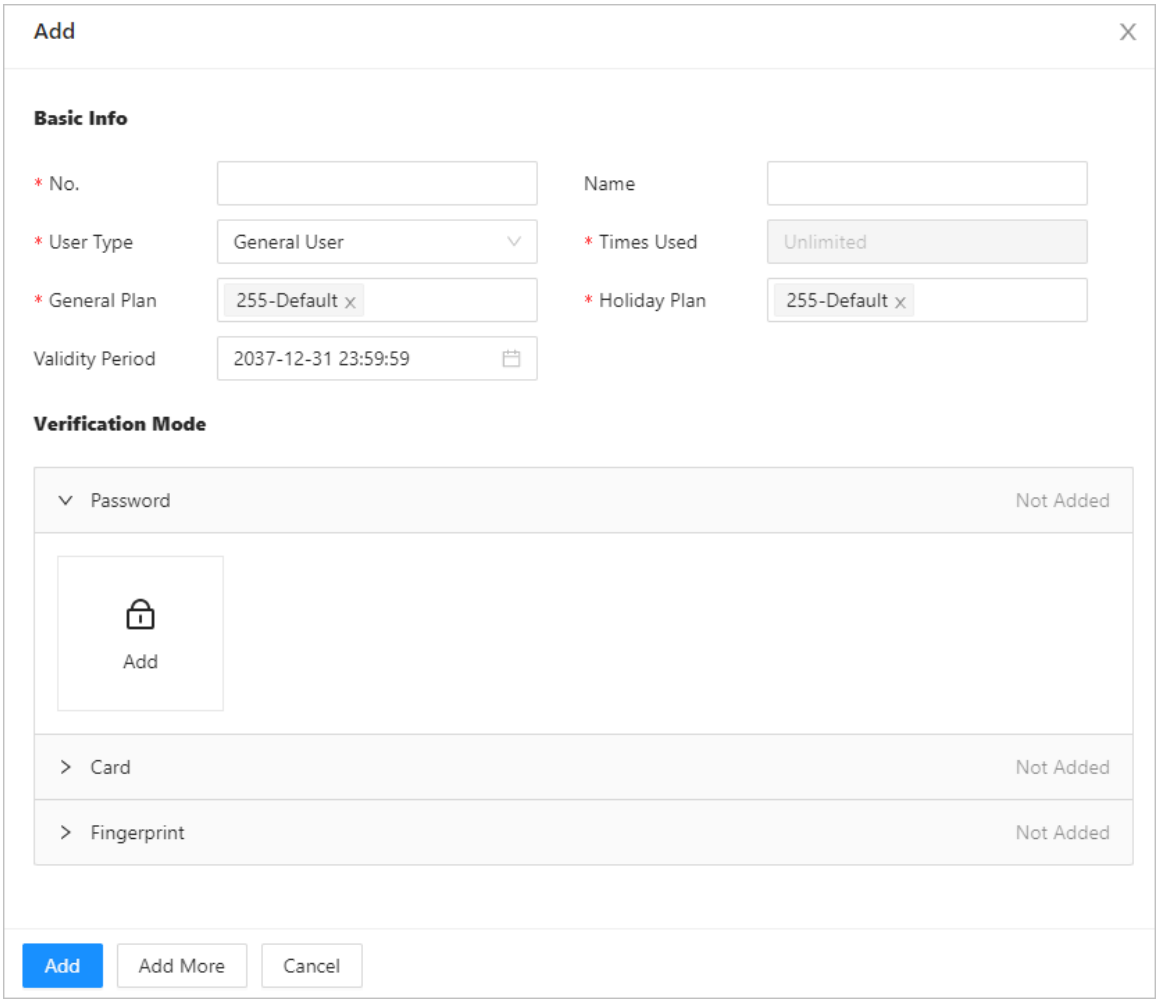


Tabla 3-3 Descripción de parámetros

Parámetro	Descripción
No.	El número es como el ID del empleado, que puede ser números, letras y sus combinaciones, y la longitud máxima del número es de 30 caracteres.
Nombre	El nombre puede tener hasta 32 caracteres (incluidos números, símbolos y letras).

Parámetro	Descripción
Tipo de usuario	• **Usuario general**:Los usuarios generales pueden desbloquear la puerta. • **Usuario de la lista negra**:Cuando los usuarios de la lista de bloqueo desbloquean la puerta, el personal de servicio recibirá una notificación. • **Usuario invitado**:Los huéspedes pueden desbloquear la puerta dentro de un periodo definido o por un número determinado de veces. Una vez transcurrido el periodo definido o el tiempo de desbloqueo, no podrán desbloquear la puerta. • **Usuario de patrulla**:Los usuarios de patrulla pueden tomar asistencia en el dispositivo, pero no tienen permisos de puerta. • **Usuario VIP**:Cuando el VIP desbloquee la puerta, el personal de servicio recibirá un aviso. • **Otro usuario**:Cuando desbloqueen la puerta, ésta permanecerá desbloqueada durante 5 segundos más. • Usuario personalizado 1/Usuario personalizado 2: Igual que los usuarios generales.
Veces utilizadas	Establezca un límite de desbloqueo para los usuarios invitados. Una vez transcurrido el tiempo de desbloqueo, no podrán abrir la puerta.
Plan General	Las personas pueden desbloquear la puerta o tomar asistencia durante el período definido. Puede seleccionar más de un plan.
Plan de vacaciones	Las personas pueden desbloquear la puerta o tomar asistencia durante el día festivo definido. Puede seleccionar más de un día festivo.
Periodo de validez	Establecer una fecha en la que expirarán los permisos de acceso a la puerta y asistencia de la persona.
Contraseña	Ingrese la contraseña de usuario. La contraseña tiene una longitud máxima de 8 dígitos. La contraseña de coacción es la contraseña de desbloqueo + 1. Por ejemplo, si la contraseña de usuario es 12345, la contraseña de coacción será 12346. Se activará una alarma de coacción cuando se use una contraseña de coacción para desbloquear la puerta.

Parámetro	Descripción
Tarjeta	• Introduzca el número de tarjeta manualmente. 1. Haga clic**Agregar**. 2. Ingrese el número de tarjeta y luego haga clic en**Agregar**. • Lea el número automáticamente a través del lector de inscripción o del Dispositivo. 1. Haga clic**Agregar**,y luego haga clic**Modificar**para seleccionar un lector de inscripción o el Dispositivo. 2. Haga clic**Leer tarjeta**y luego pase las tarjetas por el lector de tarjetas. Se muestra una cuenta regresiva 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**de nuevo para iniciar una nueva cuenta regresiva. 3. Haga clic**Agregar**. Un usuario puede registrar hasta 5 tarjetas. Ingrese su número de tarjeta o deslícela, y el dispositivo leerá la información. Puedes habilitar el**Tarjeta de coacción**Función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta. • :Establecer tarjeta de coacción. • :Cambiar número de tarjeta. Un usuario sólo puede configurar una tarjeta de coacción.
Huella dactilar	Registrar huellas dactilares. Un usuario puede registrar hasta tres huellas dactilares, y se puede configurar una como huella de coacción. Se activará una alarma cuando se use la huella de coacción para abrir la puerta. Inscriba huellas dactilares a través de un lector de inscripción o del Dispositivo. 1. Haga clic**Agregar**,y luego haga clic**Modificar**para seleccionar un lector de inscripción o el Dispositivo. 2. Presione el dedo sobre el escáner de acuerdo con las instrucciones en pantalla. 3. Haga clic**Agregar**. • La función de huella dactilar solo está disponible en modelos seleccionados. • No recomendamos que establezca la primera huella dactilar como huella dactilar de coacción. • Un usuario solo puede configurar una huella digital de coacción. • La función de huella dactilar está disponible si el dispositivo admite la conexión de un módulo de huella dactilar.

Paso 3 Hacer clic**DE ACUERDO**.

Operaciones relacionadas

- Importar información del usuario: Haga clic en**Exportar**,Descargue la plantilla e ingrese la información del usuario. Haga clic en**Importar**para importar la carpeta.

  Se pueden importar hasta 10.000 usuarios a la vez.
- Borrar: Borrar todos los usuarios.
- Actualizar: actualiza la lista de usuarios.
- Hacer clic para editar la información de la persona.
- Seleccione personas y luego haga clic**Borrar**para eliminar usuarios.
- Buscar: Busque por nombre de usuario o ID de usuario.

3.5 Configuración del control de acceso

3.5.1 Configuración de parámetros de control de acceso

3.5.1.1 Configuración de parámetros básicos

Procedimiento

Paso 1 Seleccionar**Control de acceso**>**Parámetros de control de acceso**.

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

Figura 3-5 Parámetros básicos

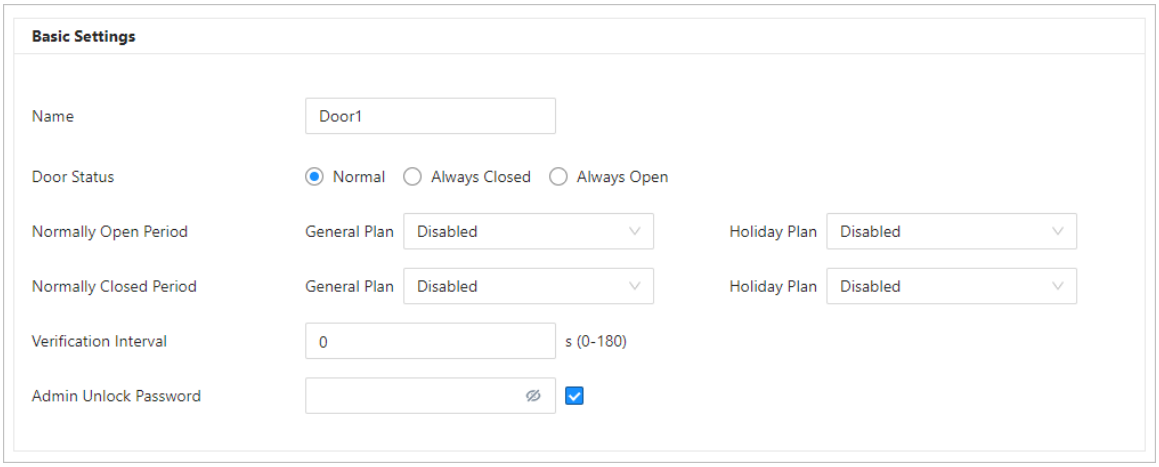


Tabla 3-4 Descripción de los parámetros básicos

Parámetro	Descripción
Nombre	El nombre de la puerta.
Estado de la puerta	Establecer el estado de la puerta. ● Normal: La puerta se desbloqueará y bloqueará según su configuración. ● Siempre abierto: la puerta permanece desbloqueada todo el tiempo. ● Siempre cerrado: la puerta permanece bloqueada todo el tiempo.

Parámetro	Descripción
Período normalmente abierto	Cuando seleccionas**Normal**Puede seleccionar una plantilla de tiempo en la lista desplegable. La puerta permanece abierta o cerrada durante el tiempo definido. ● Cuando el período normalmente abierto entra en conflicto con el período normalmente cerrado, El período normalmente abierto tiene prioridad sobre el período normalmente cerrado. ● Cuando el período entra en conflicto con el plan de vacaciones, los planes de vacaciones tienen prioridad sobre los períodos.
Período normalmente cerrado	
Intervalo de verificación	Si verifica su identidad varias veces dentro de un período establecido, solo se considerará válida la verificación más antigua y la puerta no se abrirá después de la segunda o posteriores. Si la puerta no se abre, deberá esperar el tiempo de verificación configurado antes de volver a intentar verificar su identidad.
Contraseña de desbloqueo de administrador	Puede configurar una contraseña de administrador para abrir la puerta. La contraseña debe contener entre 1 y 8 dígitos.

Paso 3 Hacer clic**Aplicar**.

3.5.1.2 Configuración de métodos de desbloqueo

Puedes usar varios métodos de desbloqueo, como huella dactilar, tarjeta y contraseña. También puedes combinarlos para crear tu propio método de desbloqueo.

Procedimiento

Paso 1 Seleccionar**Control de acceso**>**Parámetros de control de acceso**. En

Paso 2 **Desbloquear configuraciones**, seleccione un método de desbloqueo.

- Desbloqueo de combinación

  1. Seleccionar**Desbloqueo de combinación**desde**Método de desbloqueo**lista.
  2. Seleccionar**O**o**Y**.
     - ◇ O bien: Utilice uno de los métodos de desbloqueo seleccionados para abrir la puerta. Y
     - ◇ bien: Utilice todos los métodos de desbloqueo seleccionados para abrir la puerta.
  3. Seleccione los métodos de desbloqueo y luego configure otros parámetros.

Figura 3-6 Configuración de desbloqueo

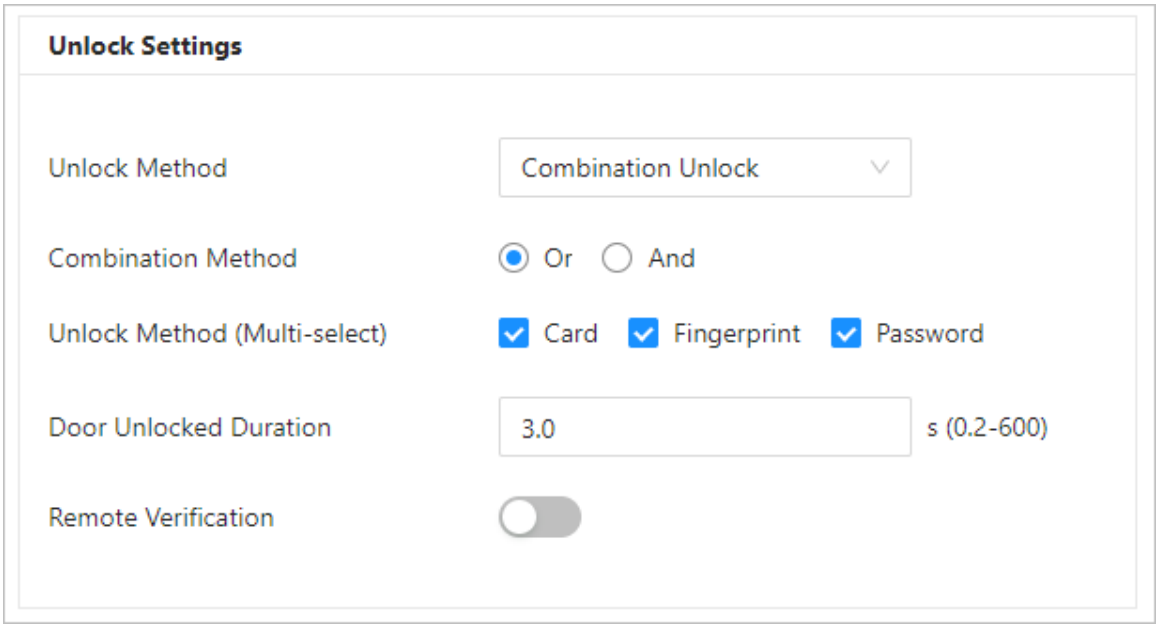


Tabla 3-5 Descripción de la configuración de desbloqueo

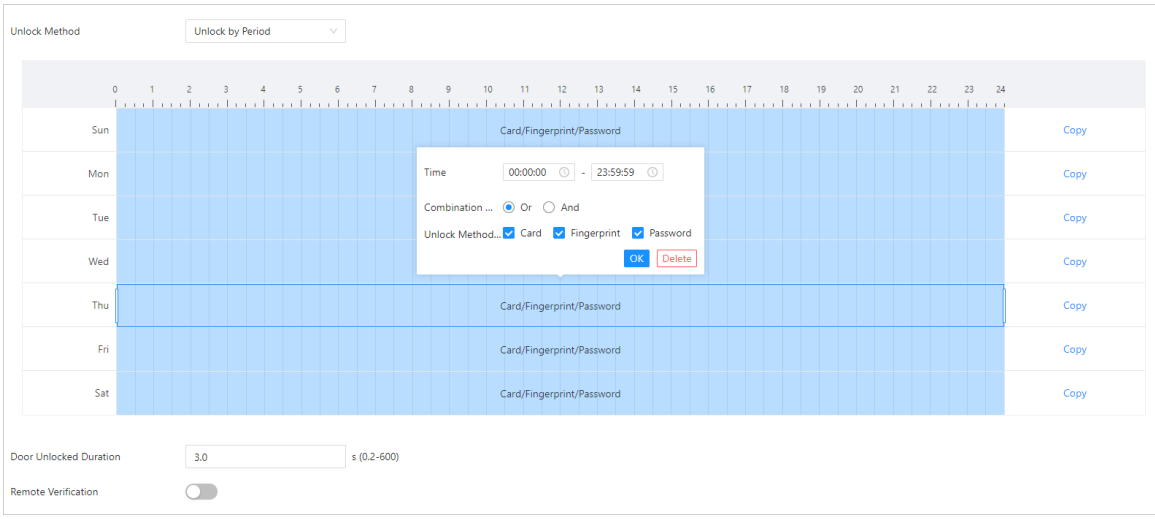
Parámetro	Descripción
Método de desbloqueo (selección múltiple)	Los métodos de desbloqueo pueden variar según los modelos de producto.
Duración del desbloqueo de la puerta	Tras conceder el acceso a una persona, la puerta permanecerá desbloqueada durante un tiempo definido para que pueda pasar. Este tiempo varía entre 0,2 y 600 segundos.
Verificación remota	Si esta función está habilitada, puede controlar la puerta en la plataforma correspondiente.

- Desbloqueo por periodo

  1. En el**Método de desbloqueo**lista, seleccionar**Desbloqueo por período**.
  2. Arrastre el control deslizante para ajustar el período de tiempo para cada día.

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

Figura 3-7 Desbloqueo por período



- Desbloqueo por múltiples usuarios.

  1. En el**Método de desbloqueo**lista, seleccionar**Desbloqueo por múltiples usuarios**.
  2. Haga clic**Agregar**para agregar grupos.
  3. Seleccione el método de desbloqueo, el número válido y los usuarios.

  ◇ El número válido indica la cantidad de personas que necesitan verificar sus identidades en el dispositivo antes de que se desbloquee la puerta.

Paso 3 Hacer clic**Aplicar**.

3.5.2 Configuración de alarmas

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

Procedimiento

Paso 1 Seleccionar**Control de acceso**>**Alarma**>**Alarma**.

Paso 2 Configurar parámetros de alarma.

Figura 3-8 Alarma

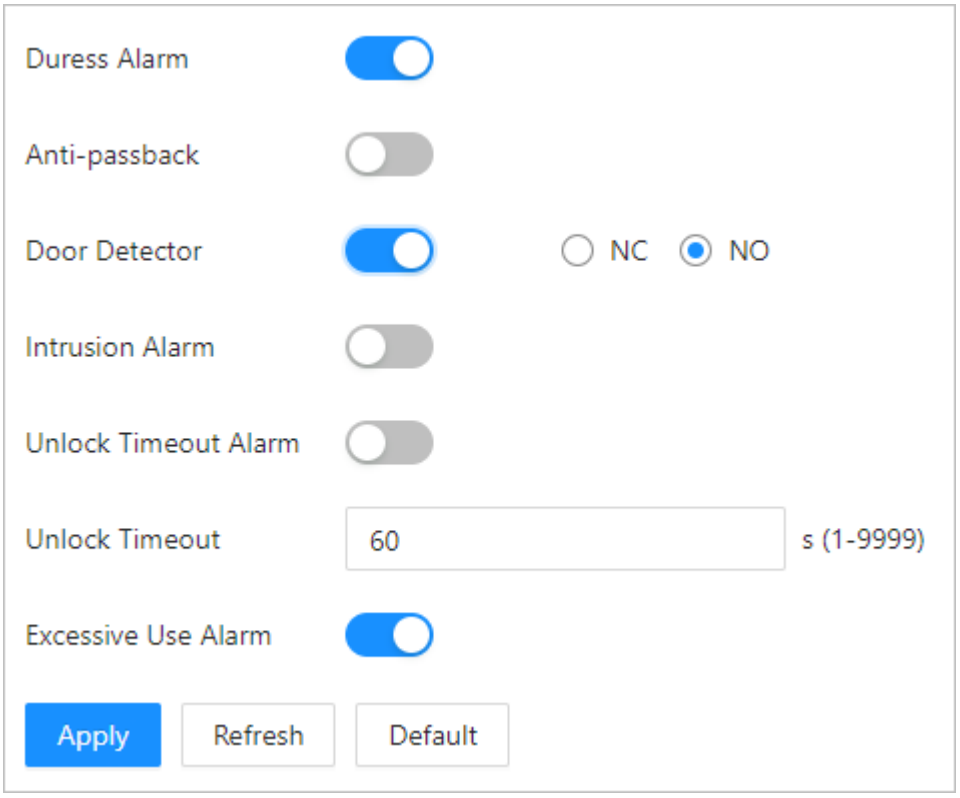


Tabla 3-6 Descripción de los parámetros de alarma

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.
Anti-passback	Los usuarios deben verificar su identidad tanto al entrar como al salir; de lo contrario, se activará una alarma. Esto ayuda a evitar que el titular de la tarjeta la entregue a otra persona para acceder. Cuando la función antirretorno está activada, el titular de la tarjeta debe salir del área protegida a través de un lector de salida antes de que el sistema le permita entrar de nuevo. ● Si una persona ingresa después de una autorización y sale sin autorización, se activará una alarma cuando la persona intente ingresar nuevamente y se le negará el acceso al mismo tiempo. ● Si una persona ingresa sin autorización y sale después de la autorización, se activará una alarma cuando la persona intente ingresar nuevamente y se le negará el acceso al mismo tiempo. Si el dispositivo solo puede conectar una cerradura, la verificación en el dispositivo indica la dirección de entrada y la verificación en el lector de tarjetas externo indica la dirección de salida por defecto. Puede modificar la configuración en la plataforma de administración.

Parámetro	Descripción
Detector de puerta	Con el detector de puerta conectado a su dispositivo, se puede activar una alarma si las puertas se abren o cierran de forma anormal. El detector de puerta incluye dos tipos: detector NC y detector NO. ● NC: El sensor está en una posición de cortocircuito cuando la puerta o ventana está cerrada. ● NO: Se crea un circuito abierto cuando la ventana o puerta está realmente cerrada.
Alarma de intrusión	Si la puerta se abre de forma anormal, se activará una alarma de intrusión que durará un tiempo definido. El detector de puerta y la intrusión deben habilitarse al mismo tiempo.
Alarma de tiempo de espera de desbloqueo	Cuando la puerta permanece desbloqueada durante más tiempo que el tiempo de espera definido, se activará la alarma de tiempo de espera de la puerta y durará el tiempo definido. El detector de puerta y la función de tiempo de espera de la puerta deben habilitarse al mismo tiempo.
Desbloquear tiempo de espera	
Alarma de uso excesivo	Si se utiliza una contraseña o tarjeta incorrecta 5 veces seguidas en 60 segundos, se activará la alarma por uso excesivo de tarjeta ilegal y durará un tiempo definido.

Paso 3 Hacer clic**Aplicar**.

3.5.3 Configuración de vínculos de alarma (opcional)

Puede configurar vínculos de alarma.

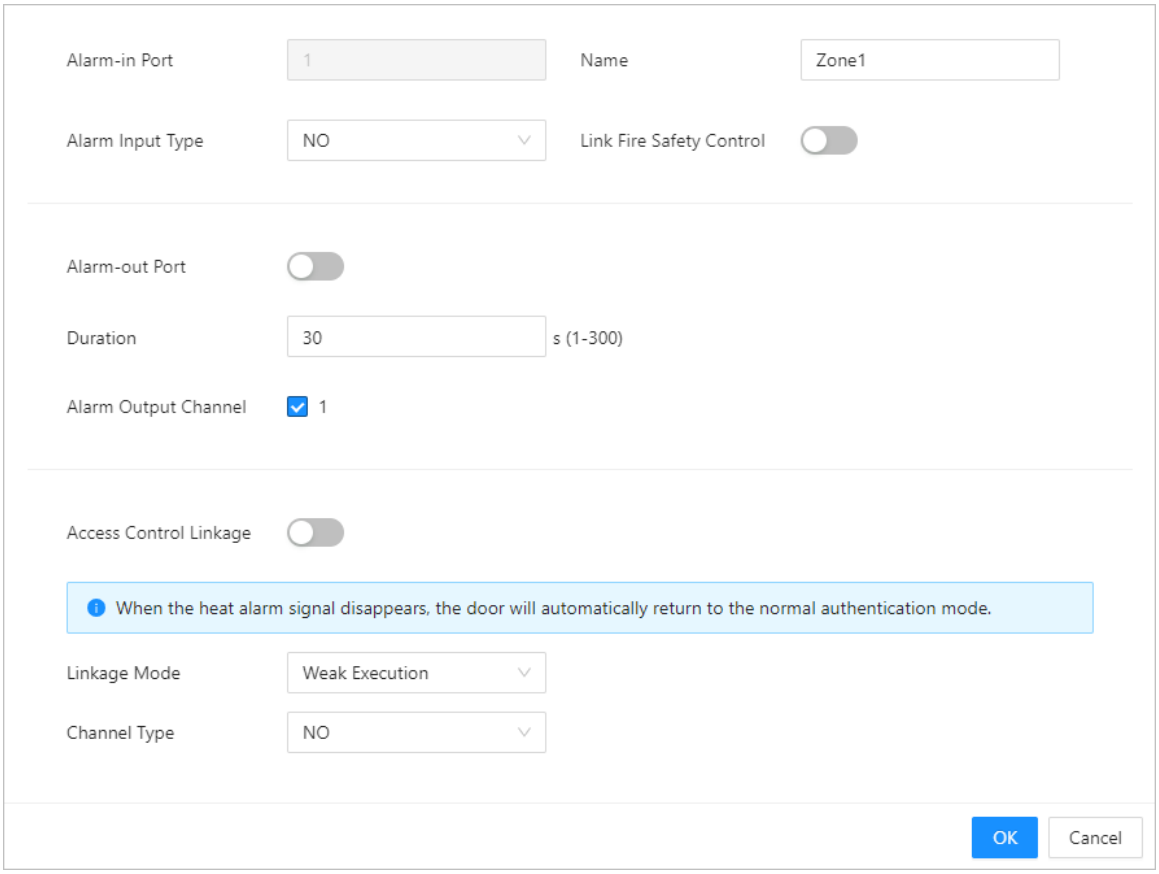
Procedimiento

Paso 1 Seleccionar**Control de acceso**>**Alarma**>**Configuración de vinculación de alarma**.

- Si el dispositivo se agrega a una plataforma de administración, la configuración de la alarma se sincronizará con la plataforma.
- Esta función solo está disponible en modelos que tienen puertos de entrada y salida de alarma.
- La cantidad de puertos de entrada y salida de alarma varía según los modelos del producto.

Paso 2 Hacer clic Para configurar la alarma.

Figura 3-9 Vinculación de alarmas



Paso 3 Crea un nombre para la zona de alarma.

Paso 4 Permitir**Enlace de control de seguridad contra incendios**y seleccione un tipo para el dispositivo de entrada de alarma.

- Normalmente Cerrado: La entrada de alarma se encuentra en estado de circuito normalmente cerrado (NC) cuando la alarma no se ha disparado. Abrir un circuito normalmente cerrado activa la alarma.
- Normalmente abierto: El dispositivo de entrada de alarma se encuentra en estado de circuito normalmente abierto (NO) cuando la alarma no se ha disparado. Al cerrar el circuito, se activa la alarma.

Paso 5 Si desea vincular el control de acceso cuando se activa la alarma de incendio, habilite**Vinculación de control de acceso**.

Esta función surte efecto sólo después**Enlace de control de seguridad contra incendios**está habilitado.

Paso 6 Seleccione un modo de vinculación.

- Ejecución robusta: Cuando desaparece la señal de alarma de incendio, la puerta conserva su estado actual. Si lo desea, puede cambiar manualmente a la configuración anterior.
- Ejecución débil: cuando la señal de alarma de incendio desaparece, la puerta vuelve automáticamente a su estado anterior.

Paso 7 Seleccione un tipo de canal.

- NO: La puerta se abre automáticamente cuando se activa la alarma de incendio.
- NC: La puerta se cierra automáticamente cuando se activa la alarma de incendio.

Paso 8 Hacer clic**DE ACUERDO**.

3.5.4 Configuración de la vinculación de eventos de alarma

Procedimiento

Paso 1 En el**Menú principal**, seleccionar**Control de acceso**>**Alarma**>**Vinculación de eventos de alarma**.

Paso 2 Configurar vínculos de eventos de alarma.

Figura 3-10 Vinculación de eventos de alarma

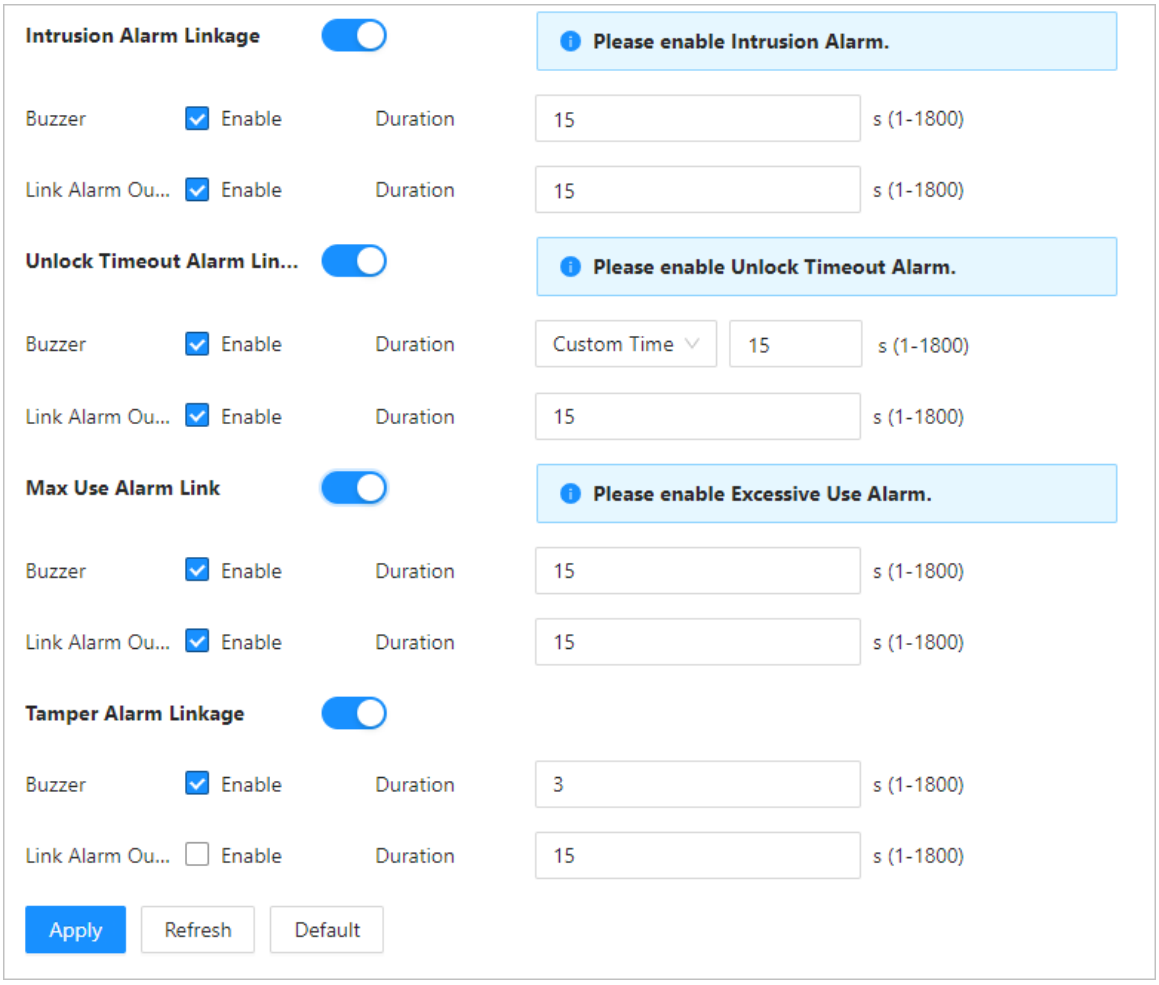


Tabla 3-7 Vinculación de eventos de alarma

Parámetro	Descripción
Vinculación de alarma de intrusión	Si la puerta se abre de forma anormal, se activará una alarma de intrusión. ● Zumbador: El zumbador suena cuando se activa una alarma de intrusión. Puede configurar la duración de la alarma. ● Salida de alarma de enlace: El dispositivo de alarma externo genera alarmas cuando se activa la alarma de intrusión. Puede configurar la duración de la alarma.

Parámetro	Descripción
Alarma de tiempo de espera de desbloqueo Enlace	Cuando la puerta permanece desbloqueada durante más tiempo que el tiempo de espera definido, se activará la alarma de tiempo de espera de la puerta y durará el tiempo definido. ● Zumbador: El zumbador suena cuando se activa la alarma de tiempo de desbloqueo. Puede configurar la duración de la alarma. ● Salida de alarma local: El dispositivo de alarma externo genera alarmas cuando se activa la alarma de tiempo de desbloqueo. Puede configurar la duración de la alarma.
Enlace de alarma de uso máximo	Si se utiliza una contraseña o tarjeta incorrecta 5 veces seguidas en 60 segundos, se activará la alarma por uso excesivo de tarjeta ilegal y durará un tiempo definido. ● Timbre: El timbre suena cuando se activa la alarma de uso excesivo. Puede configurar su duración. ● Salida de alarma local: El dispositivo de alarma externo genera alarmas cuando se activa la alarma de tiempo de desbloqueo. Puede configurar la duración de la alarma.
Conexión de alarma antimanipulación	La alarma de manipulación se activa cuando alguien intenta dañar físicamente el dispositivo. ● Zumbador: El zumbador suena cuando se activa la alarma antimanipulación. Puede configurar su duración. ● Salida de alarma local: El dispositivo de alarma externo genera alarmas cuando se activa la alarma antimanipulación. Puede configurar la duración de la alarma.

Paso 3 Hacer clic**Aplicar**.

3.5.5 Configuración de los ajustes de la tarjeta

Información de fondo

Esta función sólo está disponible en modelos seleccionados.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Control de acceso**>**Configuración de la**

Paso 3 **tarjeta**. Configure los parámetros de la tarjeta.

Figura 3-11 Parámetros de la tarjeta

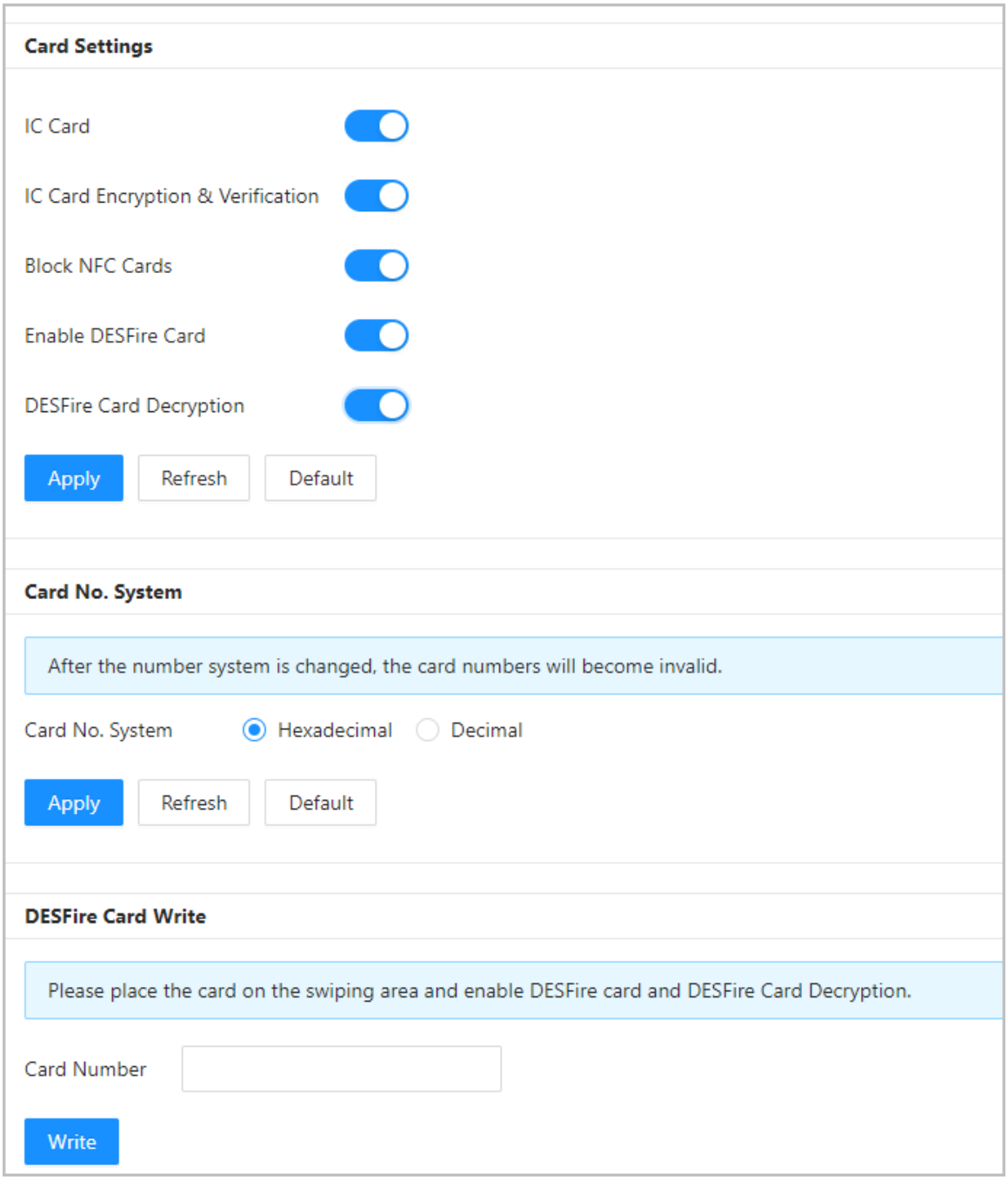


Tabla 3-8 Descripción de los parámetros de la tarjeta

Artículo	Parámetro	Descripción
Configuración de la tarjeta	Tarjeta IC	La tarjeta IC se puede leer cuando esta función está habilitada. Esta función sólo está disponible en modelos seleccionados.

Artículo	Parámetro	Descripción
	Cifrado y verificación de tarjetas IC	La tarjeta cifrada se puede leer cuando esta función está habilitada.  Cerciorarse**Tarjeta IC**está habilitado.
	Bloquear tarjetas NFC	Evitar el desbloqueo mediante tarjeta NFC duplicada después de habilitar esta función.  ● Esta función sólo está disponible en modelos que admiten tarjetas IC. ● Cerciorarse**Tarjeta IC**está habilitado. ● La función NFC solo está disponible en algunos modelos de teléfonos.
	Habilitar tarjeta Desfire	El dispositivo puede leer el número de tarjeta de la tarjeta Desfire cuando esta función y**Tarjeta IC** se habilitan al mismo tiempo.  ● Esta función sólo está disponible en modelos que admiten tarjetas IC. ● Sólo admite formato hexadecimal.
	Descifrado de la tarjeta Desfire	La información de la tarjeta Desfire se puede leer cuando**Tarjeta IC**,**Habilitar tarjeta Desfire**y **Descifrado de la tarjeta Desfire**se habilitan al mismo tiempo.  ● Esta función sólo está disponible en modelos que admiten tarjetas IC. ● Asegúrese de que la tarjeta Desfire esté habilitada.
Sistema de N.º de Tarjeta	Sistema de N.º de Tarjeta	Seleccione el formato decimal o hexadecimal para el número de tarjeta al conectar un lector de tarjetas Wiegand. El sistema de numeración de tarjeta es el mismo para la entrada y la salida de números de tarjeta.
Escritura de tarjeta DESFire	Número de tarjeta	Coloque la tarjeta en el lector, ingrese el número de tarjeta y luego haga clic**Escribir**para escribir el número de tarjeta en la tarjeta.  ● La función de tarjeta Desfire debe estar habilitada. ● Sólo admite formato hexadecimal. ● Admite hasta 8 caracteres.

Paso 4 Hacer clic**Aplicar**.

3.5.6 Configuración de períodos

Configure planes generales y planes de vacaciones, y luego podrá definir cuándo un usuario tiene permisos para desbloquear puertas.

3.5.6.1 Configuración del plan general

Puede configurar hasta 128 periodos (del 0 al 127) de planes generales. En cada periodo, debe configurar horarios de acceso para una semana completa. Solo se puede desbloquear la puerta durante el horario programado.

Procedimiento

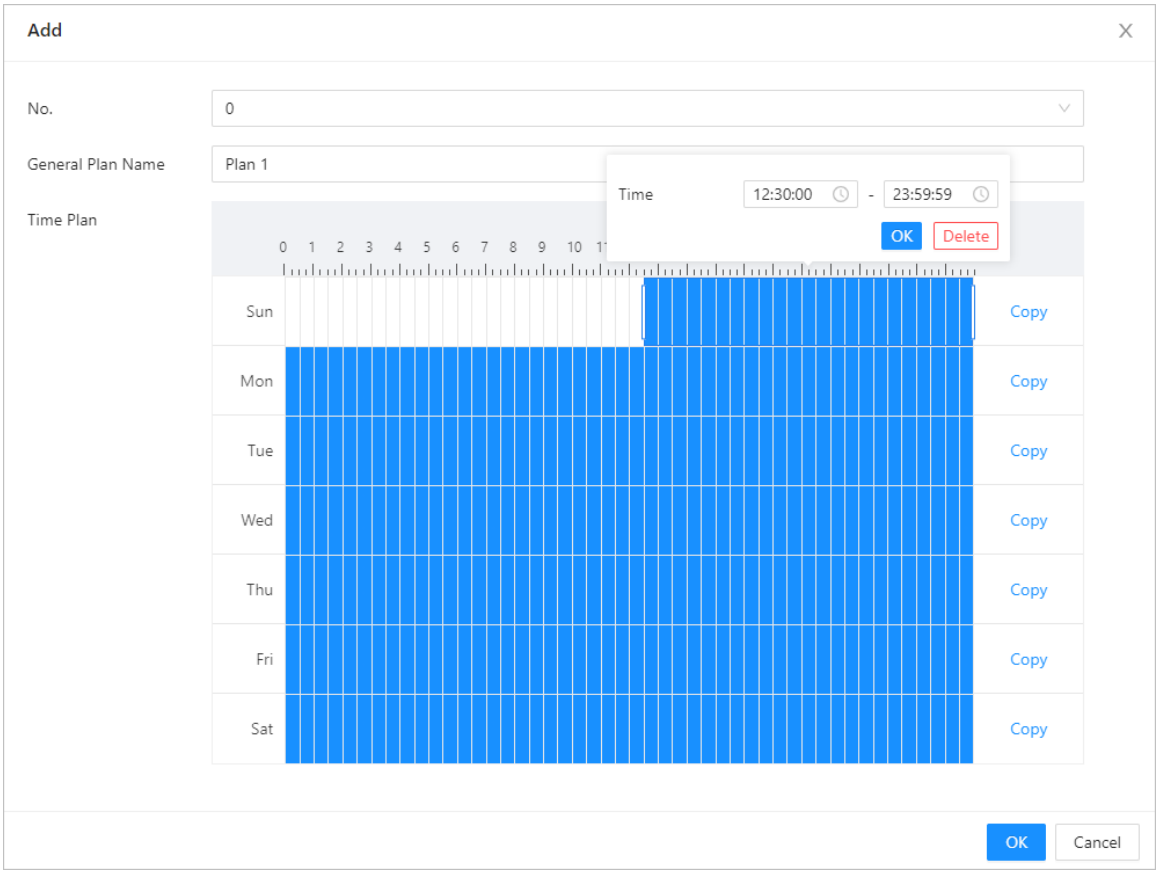
Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Control de acceso**>**Configuración del período**>**Plan General**. Haga

Paso 3 clic**Agregar**.

1. Configure el número del plan y el nombre del plan.
2. Arrastre el control deslizante de tiempo para configurar la hora de cada día.
3. (Opcional) Haga clic en**Copiar**para copiar la configuración al resto de días.

Figura 3-12 Configurar el plan general



Paso 4 Hacer clic**DE ACUERDO**.

3.5.6.2 Configuración del plan de vacaciones

Puede configurar hasta 128 grupos de vacaciones (del 0 al 127) y, para cada grupo, puede añadir hasta 16 días festivos. Posteriormente, puede asignar los grupos configurados al plan de vacaciones. Los usuarios solo pueden desbloquear la puerta durante el horario definido en el plan de vacaciones.

Procedimiento

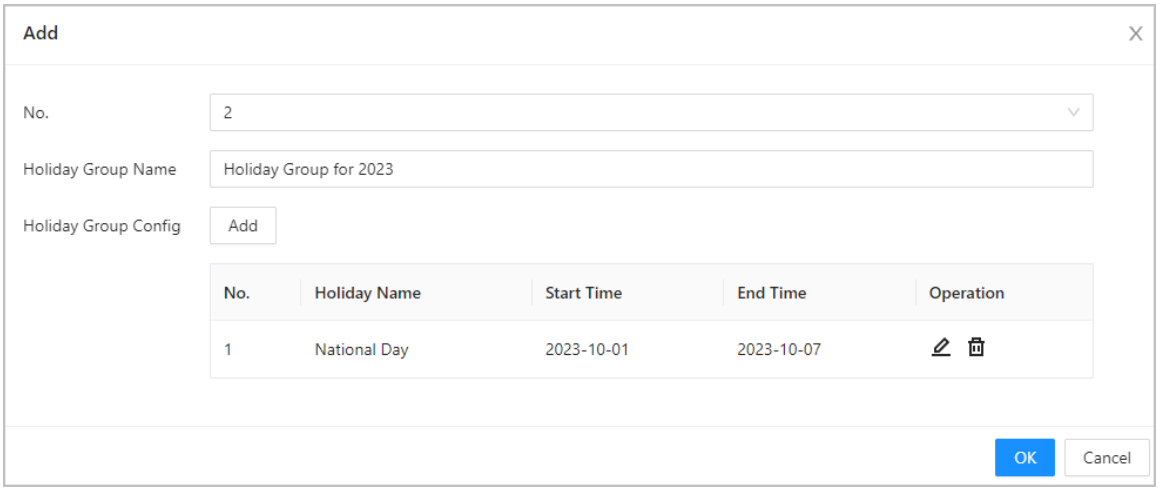
Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Control de acceso**>**Configuración del período**>**Plan de vacaciones**.

Paso 3 Haga clic**Gestión de vacaciones**,y luego haga clic**Agregar**.

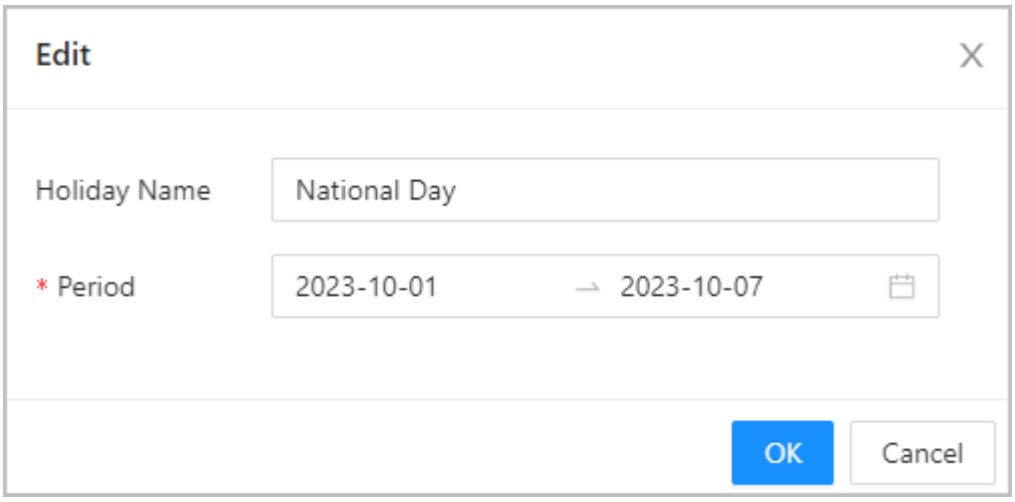
1. Seleccione un número para el grupo de vacaciones y luego ingrese un nombre para el grupo.

Figura 3-13 Agregar un grupo de vacaciones



2. Haga clic**Agregar**,Agregue un día festivo a un grupo de días festivos y luego haga clic en**DE ACUERDO**.

Figura 3-14 Agregar un día festivo a un grupo de días festivos



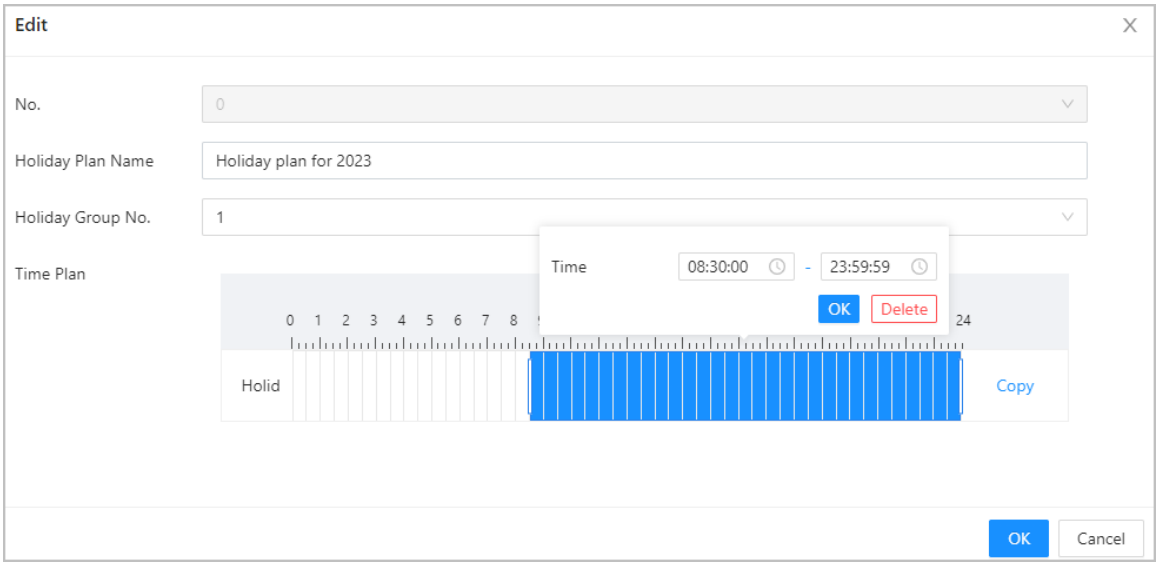
Paso 4 Hacer clic**DE ACUERDO**.

Paso 5 Hacer clic**Gestión de planes**,y luego haga clic**Agregar**.

1. Seleccione un número para el plan de vacaciones y luego ingrese un nombre para el mismo.
2. Seleccione un grupo de vacaciones y luego arrastre el control deslizante para configurar la hora de cada día.

Admite agregar hasta 4 secciones de tiempo en un día.

Figura 3-15 Agregar plan de vacaciones



Paso 6 Hacer clic**DE ACUERDO**.

3.5.7 Configuración de funciones del puerto

Algunos puertos pueden funcionar como puertos diferentes, puedes configurarlos como puertos diferentes según las necesidades reales.

Información de fondo

- Esta función sólo está disponible en modelos seleccionados.
- Los puertos pueden variar según los modelos del producto.

Procedimiento

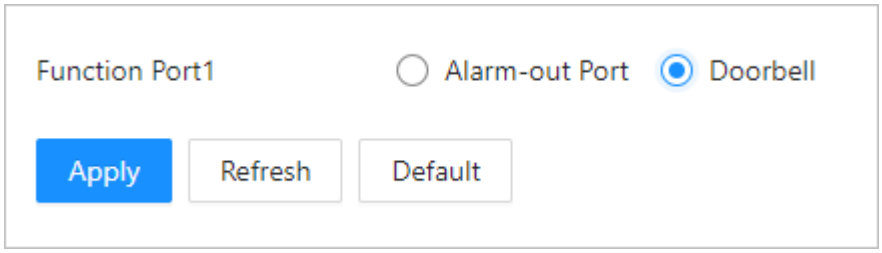
Paso 1 En la página web, seleccione**Control de acceso**>**Configuración del**

Paso 2 **puerto**. Seleccione el tipo de puerto.

Es**Timbre de la puerta**Por defecto.

Paso 3 Haga clic en**Aplicar**.

Figura 3-16 Configurar puertos



3.5.8 Configuración del desbloqueo de contraseña

Cuando el**Autenticación de código PIN**está habilitado, las personas pueden desbloquear la puerta simplemente ingresando la contraseña.

Información de fondo

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

Procedimiento

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

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

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

- Los titulares de la primera tarjeta y los usuarios de grupos de desbloqueo multipersonal deben verificar su identidad mediante los métodos de desbloqueo definidos, excepto la contraseña. Si verifican con contraseña, la función de desbloqueo de la primera tarjeta o multipersonal dejará de estar disponible.
- Los usuarios deben verificar su identidad mediante los métodos de desbloqueo definidos, excepto la contraseña. Si acceden con contraseña, la función antirretorno dejará de funcionar.
- Los usuarios de patrulla y los usuarios bloqueados pueden simplemente ingresar su contraseña para desbloquear la puerta.
- Las cuentas congeladas o 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 usando su contraseña.

3.5.9 Configuración del desbloqueo en primera persona

Cualquier persona solo podrá acceder a las puertas después de que las personas que especifique hayan pasado. Si especifica varias personas, otras podrán acceder a las puertas después de que cualquiera de ellas haya pasado.

Prerrequisitos

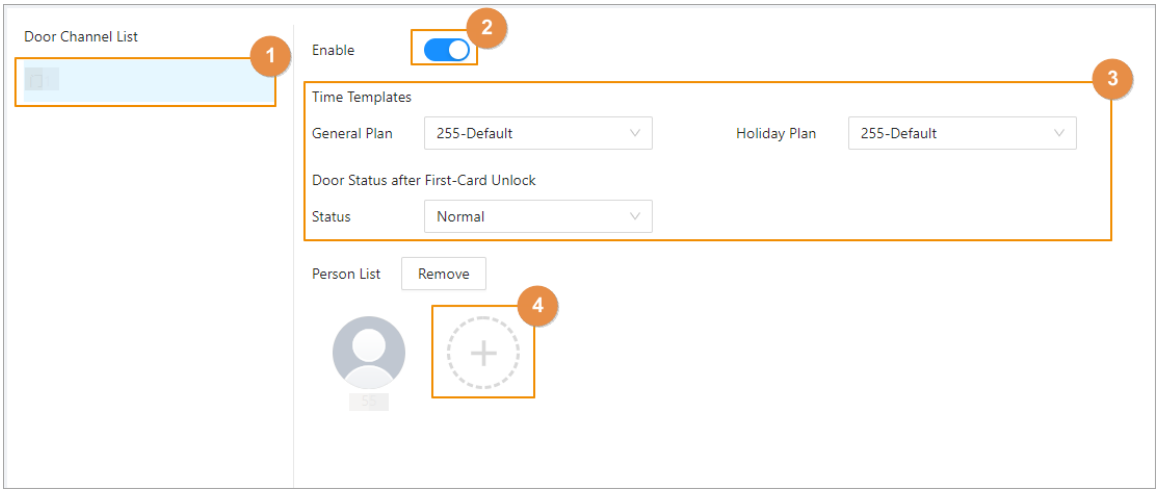
Las personas solo pueden configurarse como primeras personas cuando tienen permisos para acceder a las puertas.

Procedimiento

Paso 1 En la página de inicio, seleccione**Control de acceso**>**Desbloqueo en primera**

Paso 2 **persona**. Seleccione el canal de la puerta y luego habilite la función.

Figura 3-17 Desbloqueo en primera persona



Paso 3 Configurar los parámetros.

Tabla 3-9 Descripción de parámetros

Parámetro	Descripción
Plantillas de tiempo	Seleccione cuándo es efectiva esta regla.
Estado de la puerta después del desbloqueo con la primera tarjeta	• **Normal**:Las demás personas deberán verificar su identificación para pasar. • **Siempre abierto**:Todas las personas pueden pasar sin verificar sus identificaciones.
Lista de personas	Hacer clic+para seleccionar una o más personas, y tendrán permisos para acceder a las puertas.

Paso 4 Hacer clic**Aplicar**.

3.5.10 Configuración de Anti-Passback

Los usuarios deben verificar su identidad tanto al entrar como al salir; de lo contrario, se activará una alarma antirretorno. Esta alarma impide que el titular de la tarjeta devuelva la tarjeta de acceso a otra persona para que esta pueda acceder. Cuando la función antirretorno está activada, el titular de la tarjeta debe abandonar el área segura para que el sistema le permita entrar de nuevo.

- Si una persona ingresa después de haber sido autorizada y sale sin haber sido autorizada, se activará una alarma cuando intente ingresar nuevamente y se le negará el acceso al mismo tiempo.
- Si una persona no está autorizada y sale después de haber sido autorizada, se activará una alarma cuando intente entrar de nuevo y se le negará el acceso al mismo tiempo.

- 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 la identidad, pero podría activarse una alarma de tiempo de espera en el lector de tarjetas. Asegúrese de que la red sea estable.

Procedimiento

Paso 1 En la página de inicio, seleccione**Control de acceso**>**Configuración del grupo anti-passback**

Paso 2 Active esta función y luego configure un tiempo de reinicio.

Especifique la hora a la que se restablecerá el estado antirretorno de todo el personal.

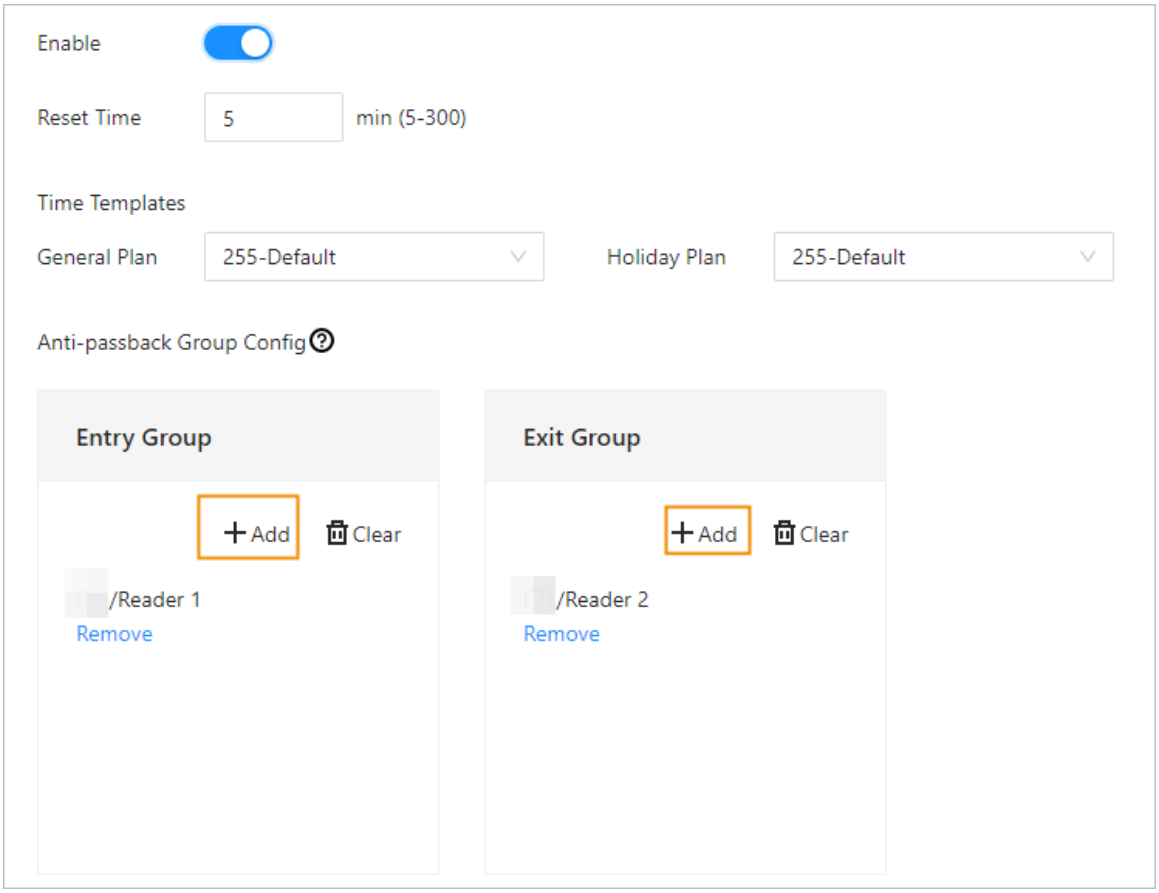
Paso 3 Seleccione el plan general y el plan de vacaciones.

El anti-passback es efectivo durante el tiempo definido.

Paso 4 En el grupo de entrada, haga clic en**Agregar**y luego seleccione el lector de tarjetas. En el

Paso 5 grupo de salida, haga clic en**Agregar**y luego seleccione el lector de tarjetas.

Figura 3-18 Anti-passback

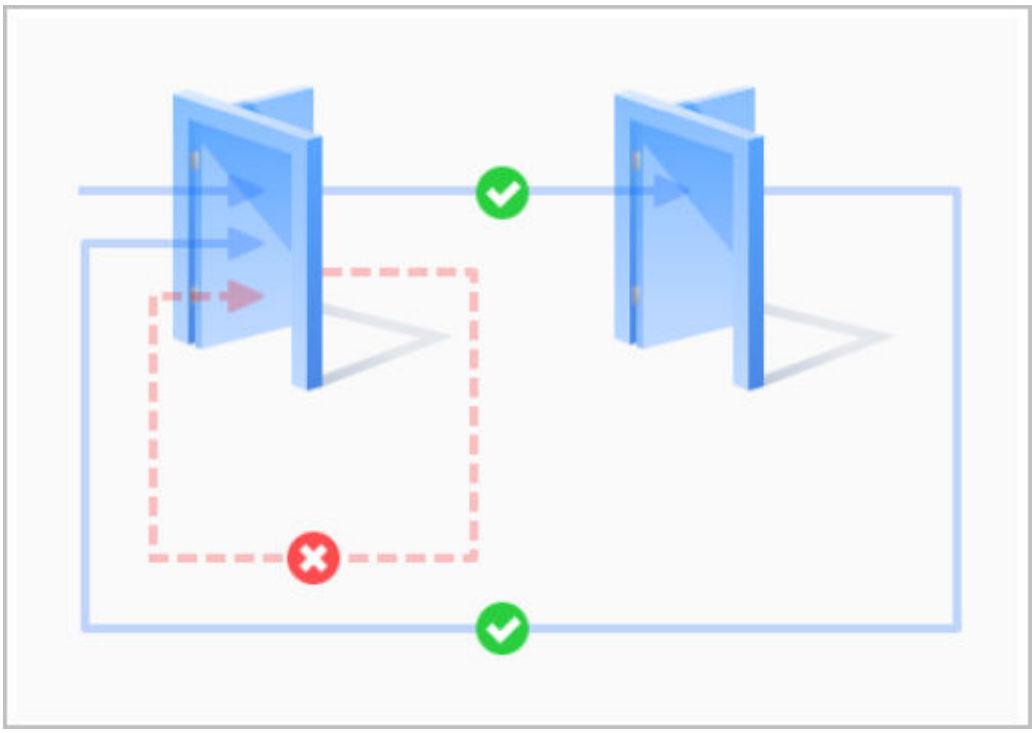


Paso 6 Hacer clic**Aplicar**.

Resultados

El número de grupo indica la secuencia de tarjetas. La tarjeta debe usarse siguiendo la secuencia específica de grupos. Por ejemplo, debe pasar la tarjeta por el lector del grupo de entrada y luego por el del grupo de salida. Siempre que pase la tarjeta siguiendo la secuencia establecida, el sistema funcionará correctamente.

Figura 3-19 Función anti-passback



3.6 Monitoreo de acceso

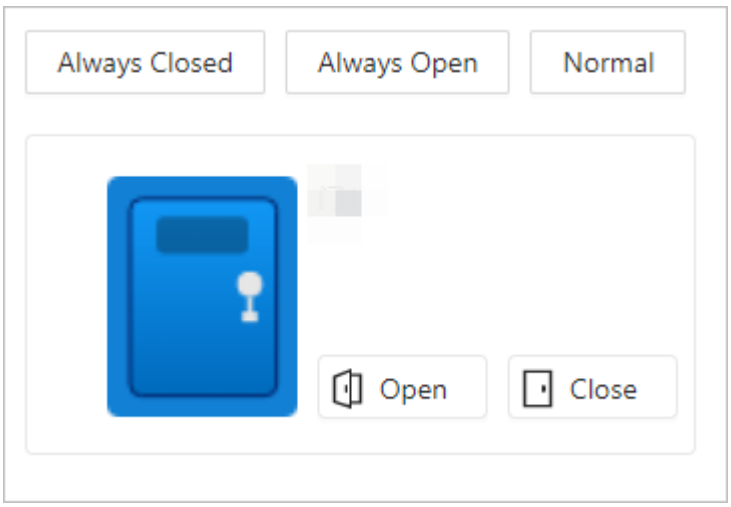
Inicie sesión en la página web, seleccione**Monitoreo de acceso**y se muestran todas las puertas conectadas.

Operaciones para controlar la puerta

- Hacer clic**Abierto**o**Cerca**para controlar la puerta de forma remota.
- Hacer clic**Siempre abierto**o**Siempre cerrado**para controlar la puerta de forma remota.

  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.

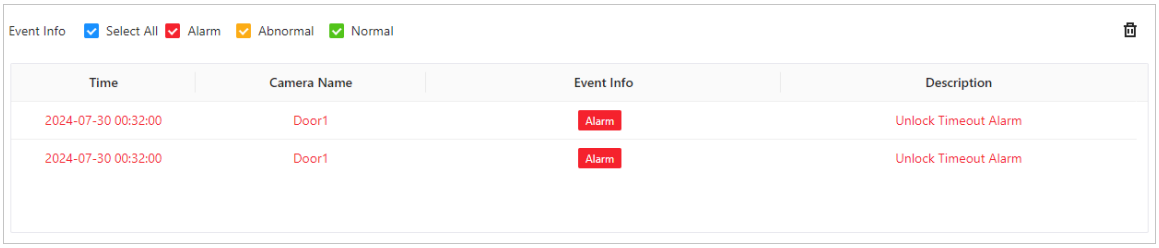
Figura 3-20 Operaciones para controlar la puerta



Información del evento

En el**Información del evento**En el área, seleccione el tipo de evento para verlos. Haga clic en para borrar todos los eventos.

Figura 3-21 Información del evento



Detalles

Se muestran los detalles del dispositivo. Aquí puede ver la dirección IP, el tipo y el modelo del dispositivo.

3.7 Configuración de comunicación

3.7.1 Configuración de red

3.7.1.1 Configuración de TCP/IP

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

Procedimiento

Paso 1 Seleccionar**Configuración de comunicación**>**Configuración de red**>**TCP/IP**.

Paso 2 Configure los parámetros.

Figura 3-22 TCP/IP

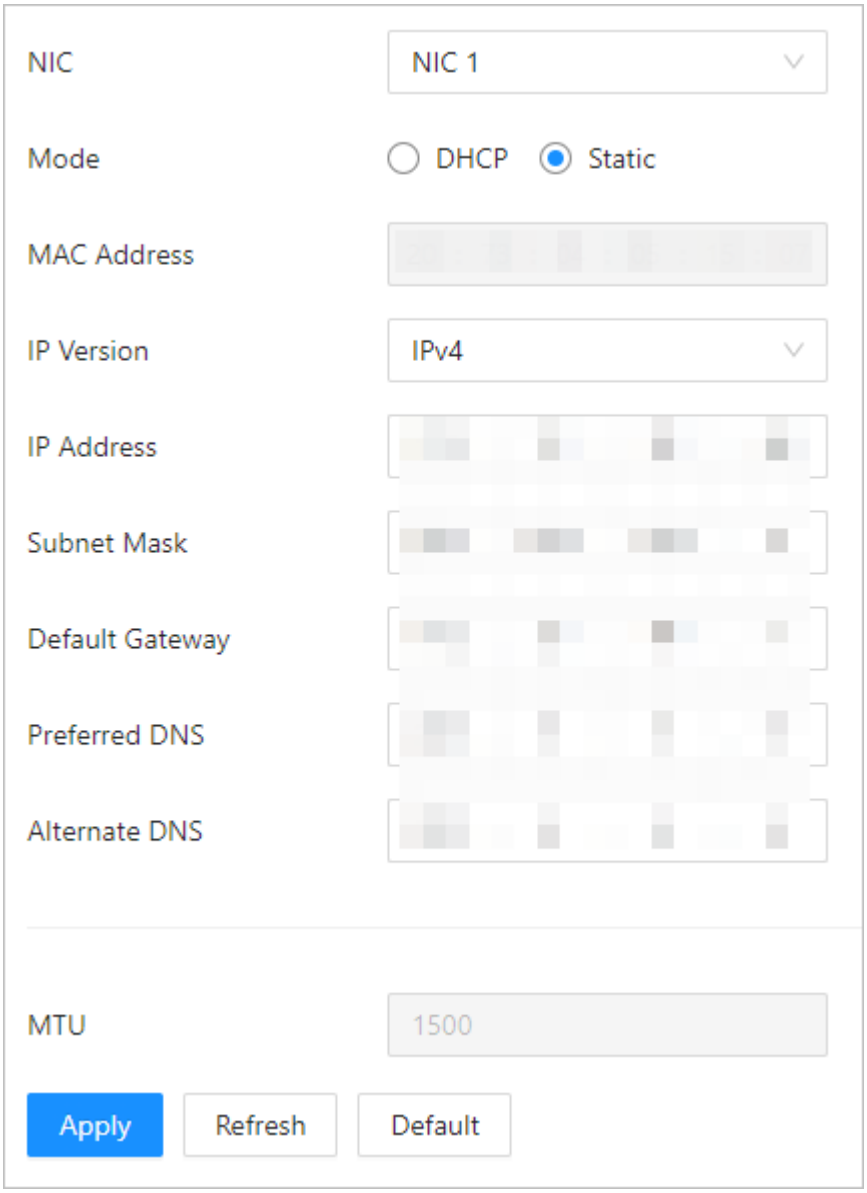


Tabla 3-10 Descripción de TCP/IP

Parámetro	Descripción
Modo	• Estático: ingrese manualmente la dirección IP, la máscara de subred y la puerta de enlace. • DHCP: Protocolo de Configuración Dinámica de Host. Al activar DHCP, se le asignará automáticamente al dispositivo una dirección IP, una máscara de subred y una puerta de enlace.
Dirección MAC	Dirección MAC del dispositivo.
Versión IP	IPv4 o IPv6.

Parámetro	Descripción
Dirección IP	Si configura el modo en**Estático**, configure la dirección IP, la máscara de subred y la puerta de enlace. ● La dirección IPv6 se representa en hexadecimal. ● La versión IPv6 no requiere configurar máscaras de subred. ● La dirección IP y la puerta de enlace predeterminada deben estar en el mismo segmento de red.
Máscara de subred	
Puerta de enlace predeterminada	
DNS preferido	Establecer la dirección IP del servidor DNS preferido.
DNS alternativo	Establecer la dirección IP del servidor DNS alternativo.
Unidad de tratamiento de datos móviles (MTU)	La MTU (Unidad Máxima de Transmisión) se refiere al tamaño máximo de datos que se puede transmitir en un solo paquete de red en redes informáticas. Un valor de MTU mayor puede mejorar la eficiencia de la transmisión de la red al reducir la cantidad de paquetes y la sobrecarga asociada. Si un dispositivo en la ruta de red no puede procesar paquetes de un tamaño específico, puede producirse fragmentación de paquetes o errores de transmisión. En redes Ethernet, el valor de MTU habitual es de 1500 bytes. Sin embargo, en ciertos casos, como al usar PPPoE o VPN, pueden requerirse valores de MTU menores para cumplir con los requisitos de protocolos o servicios de red específicos. A continuación, se recomiendan los valores de MTU: ● 1500: Valor máximo para paquetes Ethernet, también el valor predeterminado. Esta configuración es típica para conexiones de red sin PPPoE ni VPN, así como para algunos routers, adaptadores de red y switches. ● 1492: Valor óptimo para PPPoE ● 1468: Valor óptimo para DHCP. ● 1450: Valor óptimo para VPN.

Paso 3 Hacer clic**DE ACUERDO**.

3.7.1.2 Configuración de Wi-Fi

- La función Wi-Fi está disponible en modelos seleccionados.
- No se pueden habilitar Wi-Fi y Wi-Fi AP al mismo tiempo.

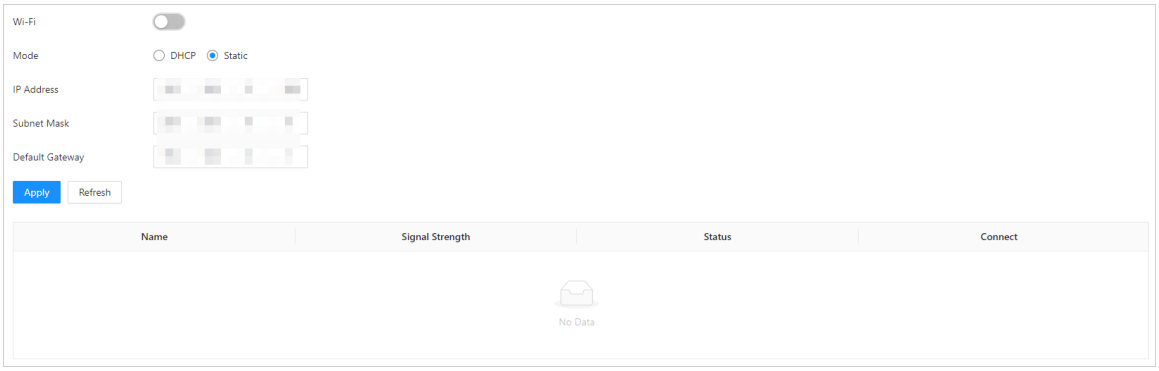
Procedimiento

Paso 1 Seleccionar**Configuración de comunicación**>**Configuración de red**>**Wi-Fi**

Paso 2 Encienda el Wi-Fi.

Se muestran todas las conexiones WiFi disponibles.

Figura 3-23 Wi-Fi



- No se pueden habilitar Wi-Fi y Wi-Fi AP al mismo tiempo.
- La función Wi-Fi solo está disponible en modelos seleccionados.

Paso 3 Hacer clic**+**, y luego ingrese la contraseña del Wi-Fi.

El wifi está conectado

Operaciones relacionadas

- DHCP: Habilite esta función y haga clic en**Aplicar**, al dispositivo se le asignará automáticamente una dirección Wi-Fi.
- Estático: habilite esta función, ingrese manualmente una dirección Wi-Fi y luego haga clic en**Aplicar**, el dispositivo se conectará al Wi-Fi.

3.7.1.3 Configuración del punto de acceso Wi-Fi

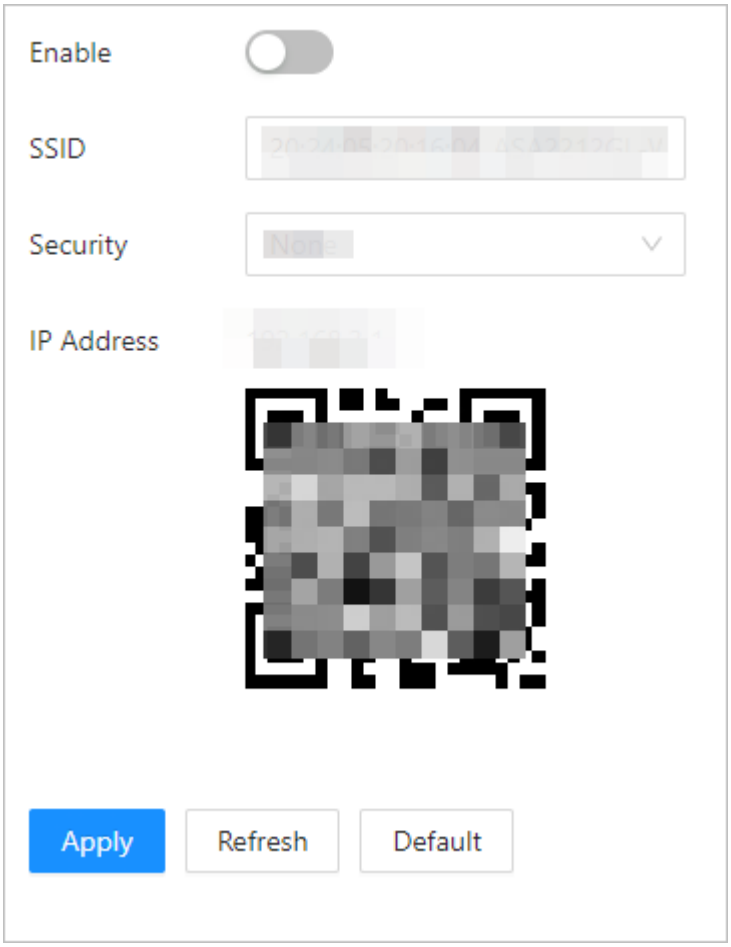
- La función Wi-Fi está disponible en modelos seleccionados.
- No se pueden habilitar Wi-Fi y Wi-Fi AP al mismo tiempo.

Procedimiento

Paso 1 Seleccionar**Configuración de comunicación**>**Configuración de red**>**Punto de acceso**

Paso 2 **Wi-Fi**Habilite la función y luego haga clic en**Aplicar**.

Figura 3-24 Punto de acceso Wi-Fi



Resultados

Una vez habilitado, puede conectarse al Wi-Fi del dispositivo a través de su teléfono e iniciar sesión en la página web del dispositivo en su teléfono.

3.7.1.4 Configuración del puerto

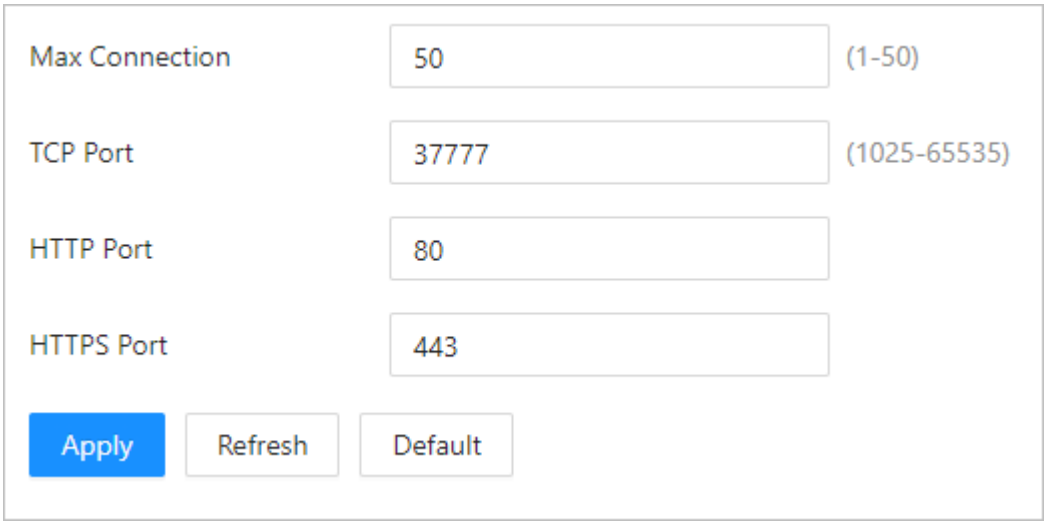
Puede limitar el acceso al dispositivo al mismo tiempo a través de la página web, el cliente de escritorio y el cliente móvil.

Procedimiento

Paso 1 Seleccionar**Configuración de comunicación**>**Configuración de red**>**Puerto**.

Paso 2 Configurar los puertos.

Figura 3-25 Configurar puertos



Es necesario reiniciar el dispositivo para que las configuraciones sean efectivas después de configurar los parámetros.

Tabla 3-11 Descripción de los puertos

Parámetro	Descripción
Conexión máxima	Puede establecer el número máximo de clientes (como página web, cliente de escritorio y cliente móvil) que pueden acceder al dispositivo al mismo tiempo.
Puerto TCP	El valor predeterminado es 37777.
Puerto HTTP	El valor predeterminado es 80. Si ha cambiado el número de puerto, agregue el número de puerto después de la dirección IP cuando acceda a la página web.
Puerto HTTPS	El valor predeterminado es 443.

Paso 3 Hacer clic**Aplicar**.

3.7.1.5 Configuración del servicio básico

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

Procedimiento

Paso 1 Seleccionar**Configuración de comunicación**>**Configuración de red**>**Servicios básicos**.

Paso 2 Configurar el servicio básico.

Figura 3-26 Servicio básico

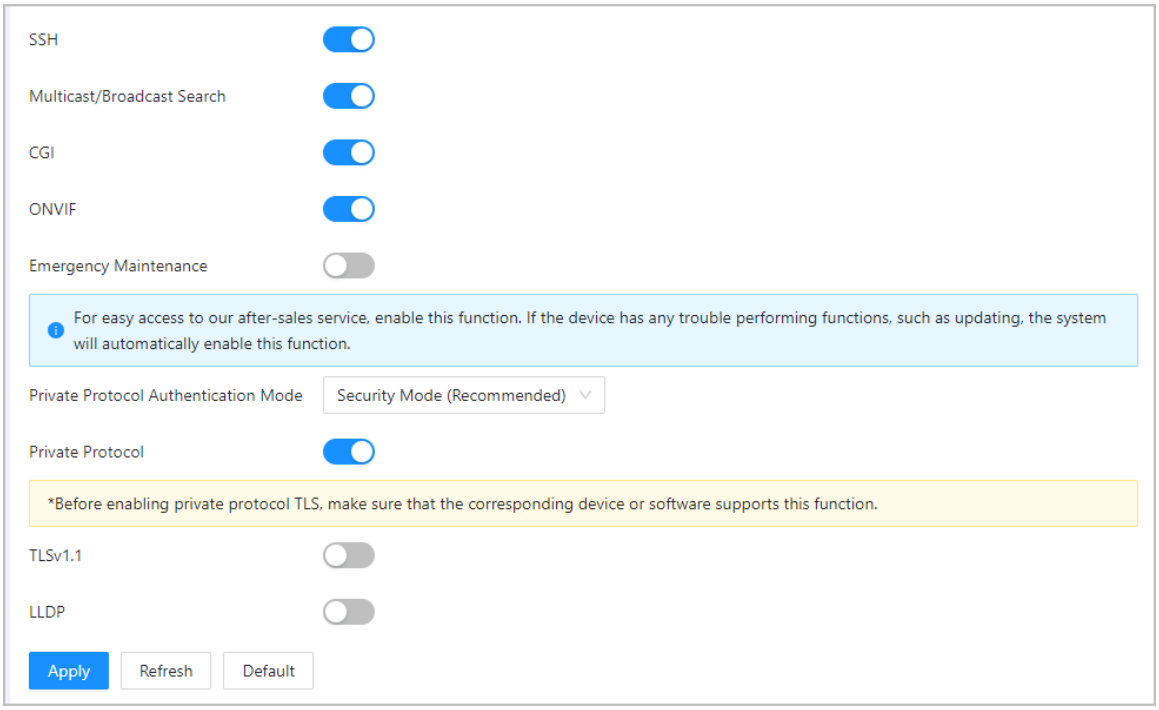


Tabla 3-12 Descripción de los parámetros básicos del servicio

Parámetro	Descripción
SSH	SSH, o Protocolo Secure Shell, es un protocolo de administración remota que permite a los usuarios acceder, controlar y modificar sus servidores remotos a través de Internet.
Búsqueda multicast/transmisión	Busque dispositivos a través del protocolo de multidifusión o difusión.
CGI	La interfaz de enlace común (CGI) es una intersección entre servidores web a través de la cual es posible el intercambio de datos estandarizado entre aplicaciones externas y servidores.
ONVIF	ONVIF significa Foro Abierto de Interfaz de Video en Red (Open Network Video Interface Forum). Su objetivo es proporcionar un estándar para la interfaz entre diferentes dispositivos de seguridad basados en IP. Estas especificaciones estandarizadas de ONVIF funcionan como un lenguaje común que todos los dispositivos pueden usar para comunicarse.
Mantenimiento de emergencia	Está activado de forma predeterminada.
Modo de autenticación de protocolo privado	Configure el modo de autenticación, incluyendo el modo seguro y el modo de compatibilidad. Se recomienda elegir**Modo de seguridad**. ● Modo de seguridad (recomendado): no admite el acceso al dispositivo a través de los métodos de autenticación Digest, DES y texto simple, lo que mejora la seguridad del dispositivo. ● Modo compatible: admite el acceso al dispositivo a través de métodos de autenticación Digest, DES y texto simple, con seguridad reducida.
Protocolo privado	La plataforma agrega dispositivos a través de protocolo privado.

Parámetro	Descripción
TLSv1.1	TLSv1.1 se refiere a la versión 1.1 de Transport Layer Security. TLS es un protocolo criptográfico diseñado para proporcionar una comunicación segura y autenticada a través de una red informática.  Pueden presentarse riesgos de seguridad al habilitar TLSv1.1. Tenga en cuenta lo siguiente.
LLDP	LLDP es la abreviatura de Protocolo de Descubrimiento de Capa de Enlace (Link Layer Discovery Protocol), un protocolo de capa de enlace de datos. Permite que dispositivos de red, como conmutadores, enrutadores o servidores, intercambien información sobre sus identidades y capacidades. El protocolo LLDP ayuda a los administradores de red a comprender mejor la topología de la red y proporciona un método estandarizado para automatizar el descubrimiento y la asignación de conexiones entre dispositivos de red. Esto facilita la configuración de la red, la resolución de problemas y la optimización del rendimiento.

Paso 3 Hacer clic**Aplicar**.

3.7.1.6 Configuración del servicio en la nube

El servicio en la nube ofrece un servicio de penetración NAT. Los usuarios pueden administrar múltiples dispositivos mediante DMSS. No es necesario solicitar un nombre de dominio dinámico, configurar la asignación de puertos ni implementar un servidor.

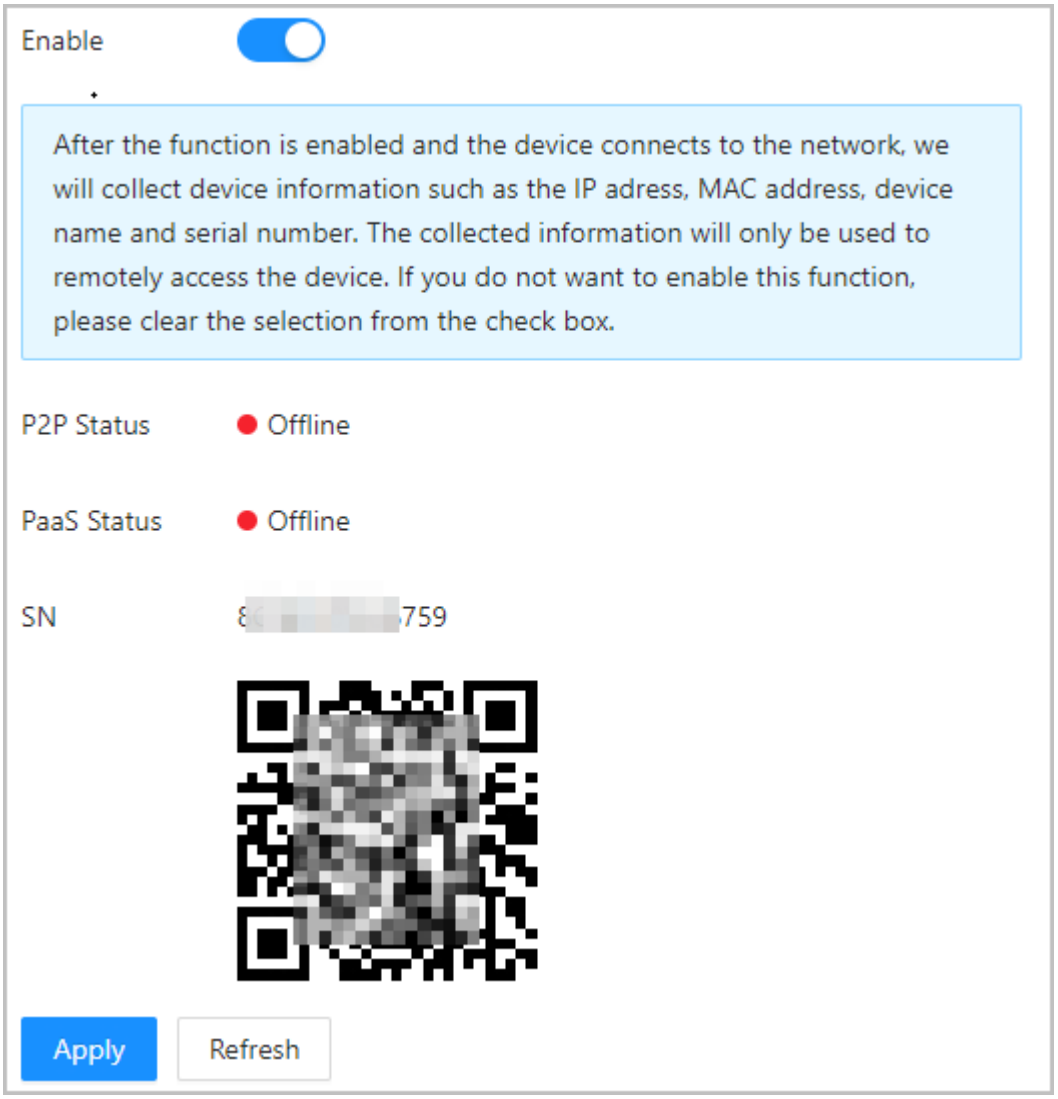
Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración de comunicación**>**Configuración de red**>**Servicio en la nube**.

Paso 2 Activar la función de servicio en la nube.

El servicio en la nube se conecta en línea si el P2P y el PaaS están en línea.

Figura 3-27 Servicio en la nube



Paso 3 Hacer clic**Aplicar**.

Paso 4 Escanee el código QR con DMSS para agregar el dispositivo.

3.7.1.7 Configuración del registro automático

El registro automático permite agregar los dispositivos a la plataforma de administración sin necesidad de ingresar manualmente información del dispositivo, como la dirección IP y el puerto.

Información de fondo

El registro automático solo es compatible con SDK.

Procedimiento

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

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

Figura 3-28 Registro automático

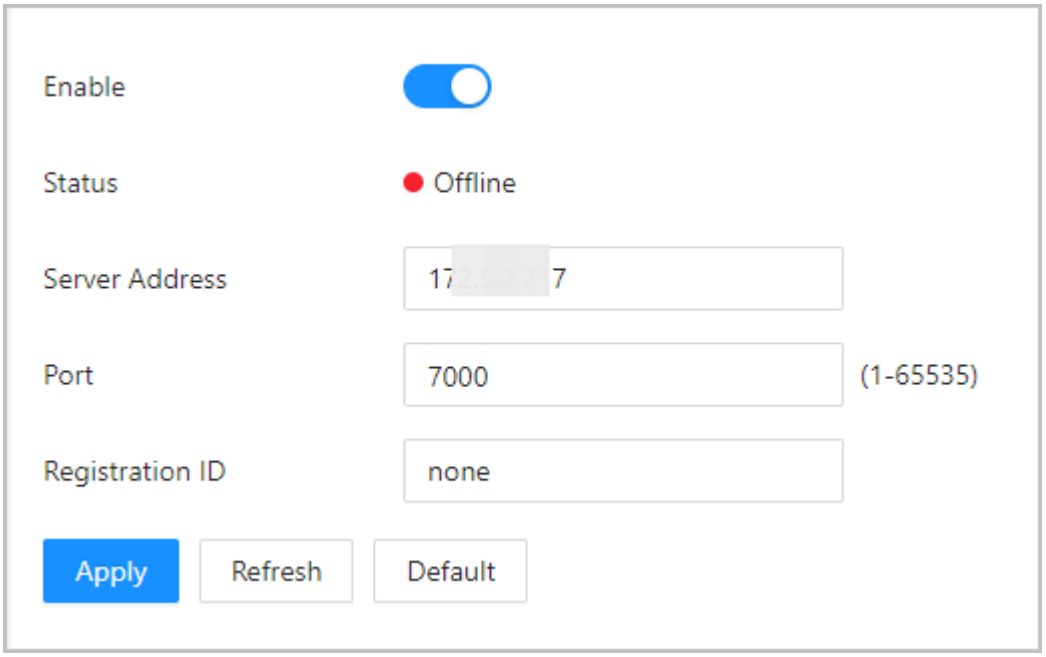


Tabla 3-13 Descripción del registro automático

Parámetro	Descripción
Estado	Muestra el estado de la conexión del registro automático.
Dirección del servidor	La dirección IP o el nombre de dominio del servidor.
Puerto	El puerto del servidor que se utiliza para el registro automático.
ID de registro	El ID de registro del dispositivo (definido por el usuario). Para añadir el dispositivo a la administración, introduzca el ID de registro en la plataforma.

Paso 3 Hacer clic**Aplicar**.

3.7.1.8 Configuración del registro automático de CGI

Conectarse a una plataforma de terceros a través del protocolo CGI.

Información de fondo

Sólo admite IPv4.

Procedimiento

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

Paso 2 Habilite esta función y luego haga clic en para configurar los parámetros.

Tabla 3-14 Descripción del registro automático

Parámetro	Descripción
ID del dispositivo	Admite hasta 32 bytes, incluidos chinos, números, letras y caracteres especiales.
Tipo de dirección	Admite 2 métodos de registro. ● IP del host: ingrese la dirección IP de la plataforma de terceros. ● Nombre de dominio: ingrese el nombre de dominio de la plataforma de terceros.
IP del host	
Nombre de dominio	
HTTPS	Acceda a la plataforma de terceros a través de HTTPS. HTTPS protege la comunicación a través de una red informática.

Paso 3 Hacer clic**DE ACUERDO**.

3.7.1.9 Configuración de la carga automática

Envía información del usuario y desbloquea registros a través de la plataforma de administración.

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración de comunicación**>**Configuración de red**>**Carga automática**.

Paso 2 (Opcional) Habilitar**Introducir información de la persona**.

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

Paso 3 Habilitar el modo de carga HTTP.

Paso 4 Hacer clic**Agregar**y luego configurar los parámetros.

Figura 3-29 Carga automática

Tabla 3-15 Descripción de parámetros

Parámetro	Descripción
Nombre de dominio/IP	La IP o nombre de dominio de la plataforma de gestión.
Puerto	El puerto de la plataforma de gestión.
HTTPS	Acceda a la plataforma de gestión a través de HTTPS. HTTPS protege la comunicación a través de una red informática.
Autenticación	Habilite la autenticación de la cuenta al acceder a la plataforma de administración. Se requieren nombre de usuario y contraseña.

Parámetro	Descripción
Tipo de evento	Seleccione el tipo de evento que se enviará a la plataforma de administración. ● Antes de utilizar esta función, habilite**Introducir información de la persona**. ● La información personal solo se puede enviar a una plataforma de administración y los registros de desbloqueo se pueden enviar a múltiples plataformas de administración.

Paso 5 Hacer clic**Aplicar**.

3.7.2 Configuración de RS-485

Configure los parámetros RS-485 si conecta un dispositivo externo al puerto RS-485.

Procedimiento

Paso 1 Seleccionar**Configuración de comunicación**>**Configuración**

Paso 2 **RS-485**. Configure los parámetros.

Figura 3-30 Configurar parámetros

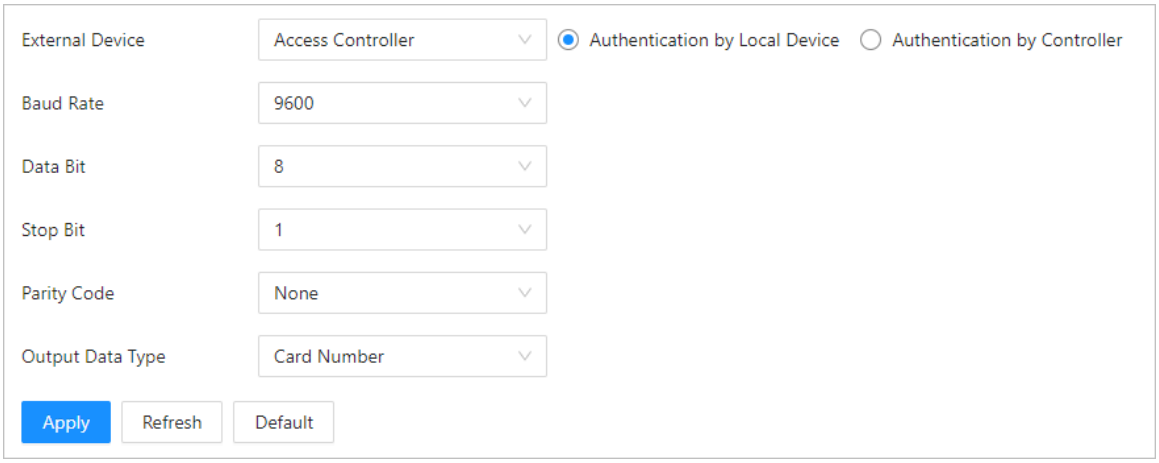


Tabla 3-16 Descripción de los parámetros RS-485

Parámetro	Descripción
Dispositivo externo	● Controlador de acceso Seleccionar**Controlador de acceso**cuando el dispositivo funciona como un lector de tarjetas y envía datos a otros controladores de acceso externos para controlar el acceso. ◇ **Autenticación por dispositivo local**:La identidad se verifica tanto en el dispositivo como en el controlador. ◇ **Autenticación por parte del controlador**:La identidad se verifica únicamente en el controlador. ● Lector de tarjetas: el dispositivo funciona como un controlador de acceso y se conecta a un lector de tarjetas externo. ● Lector (OSDP): El dispositivo está conectado a un lector de tarjetas basado en el protocolo OSDP. ● Seguridad de control de puerta: El botón de salida de la puerta, la cerradura y el enlace de incendio no son efectivos después de que se habilita el módulo de seguridad.
Tasa de Baud	Seleccione la velocidad en baudios. La velocidad predeterminada es 9600.
Bit de datos	El número de bits utilizado para transmitir los datos en una comunicación serial. Representa los dígitos binarios que contienen la información transmitida.
Bit de parada	Un bit enviado después de los datos y los bits de paridad opcionales para indicar el final de una transmisión de datos. Permite al receptor prepararse para el siguiente byte de datos y proporciona sincronización en el protocolo de comunicación.
Código de paridad	Un bit adicional que se envía después de los bits de datos para detectar errores de transmisión. Ayuda a verificar la integridad de los datos transmitidos al garantizar un número específico de bits lógicos altos o bajos.
Tipo de datos de salida	Cuando configure el dispositivo externo como**Controlador de acceso**. ● Número de tarjeta: emite datos basados en el número de tarjeta cuando los usuarios pasan la tarjeta para desbloquear la puerta; emite datos basados en el primer número de tarjeta del usuario cuando utilizan otros métodos de desbloqueo. ● No.: Genera datos basados en el ID del usuario.

Paso 3 Hacer clic**Aplicar**.

3.7.3 Configuración de Wiegand

Compatible con dispositivos Wiegand. Configure el modo y el modo de transmisión según sus dispositivos.

Procedimiento

Paso 1 Seleccionar**Configuración de comunicación**>**Wiegand**Seleccione

Paso 2 un tipo de Wiegand y luego configure los parámetros.

- Seleccionar**Entrada Wiegand**cuando conecta un lector de tarjetas externo al dispositivo.

Cuando el dispositivo se conecta a un dispositivo de terceros a través del puerto de entrada Wiegand, y el número de tarjeta que lee el dispositivo está en orden inverso al número real de la tarjeta. En este caso, puede activar**Tarjeta n.º Inversión**función.

- Seleccionar**Salida Wiegand**cuando el dispositivo funciona como lector de tarjetas y necesita conectarlo a otro controlador de acceso.

Figura 3-31 Salida Wiegand

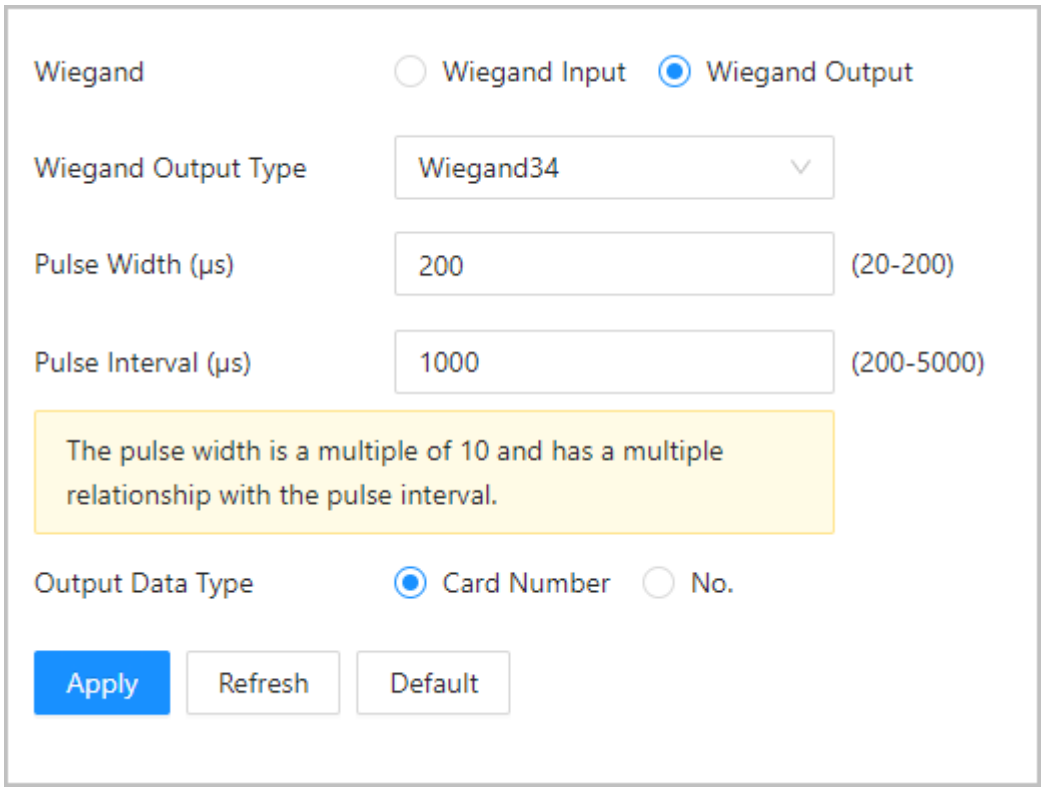


Tabla 3-17 Descripción de la salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	Seleccione un formato Wiegand para leer números de tarjeta o números de identificación. • **Wiegand26**:Lee 3 bytes o 6 dígitos. • **Wiegand34**:Lee 4 bytes u 8 dígitos. • **Wiegand66**:Lee 8 bytes o 16 dígitos.
Ancho de pulso	Introduzca el ancho de pulso y el intervalo de pulso de la salida Wiegand.
Intervalo de pulso	
Tipo de datos de salida	Seleccione el tipo de datos de salida. • **No.**:Genera datos según el ID del usuario. El formato de los datos es hexadecimal o decimal. • **Número de tarjeta**:Genera datos basados en el primer número de tarjeta del usuario.

Paso 3 Hacer clic**Aplicar**.

3.8 Configuración del sistema

3.8.1 Gestión de usuarios

Puede agregar o eliminar usuarios, cambiar contraseñas de usuarios e ingresar una dirección de correo electrónico para restablecer la contraseña cuando la olvide.

3.8.1.1 Agregar administradores

Puede agregar nuevas cuentas de administrador y luego podrán iniciar sesión en la página web del dispositivo.

Procedimiento

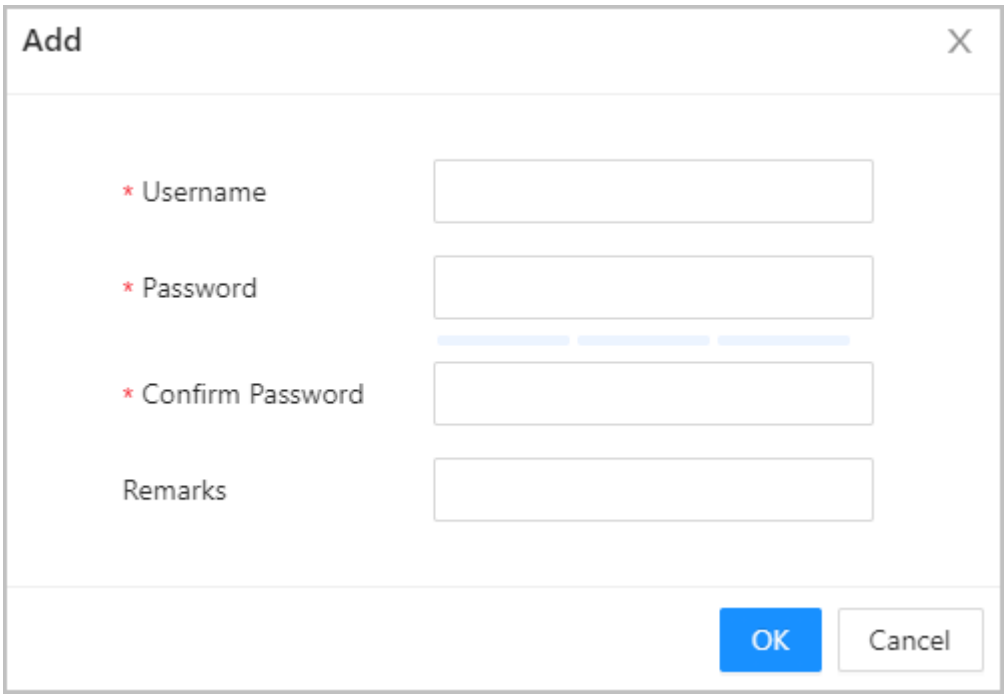
Paso 1 En la página de inicio, seleccione**Sistema**>**Cuenta**>**Cuenta**. Haga clic

Paso 2 **Agregar**, e 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 tener hasta 31 caracteres y solo admite números, letras, guiones bajos, líneas centrales, puntos o @.
- La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &).

  Establezca una contraseña de alta seguridad siguiendo las instrucciones de fortaleza de la contraseña.

Figura 3-32 Agregar administradores



Paso 3 Hacer clic**DE ACUERDO**.

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

3.8.1.2 Agregar usuarios ONVIF

Información de fondo

El Foro Abierto de Interfaz de Video en Red (ONVIF) es un foro global y abierto de la industria, creado para desarrollar un estándar abierto global para la interfaz de productos de seguridad basados en IP física, lo que permite la compatibilidad entre diferentes fabricantes. La identidad de los usuarios de ONVIF se verifica mediante el protocolo ONVIF. El usuario predeterminado de ONVIF es admin.

Procedimiento

Paso 1 En la página de inicio, seleccione**Sistema**>**Cuenta**>**Usuario de ONVIF**.

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

Figura 3-33 Agregar usuario ONVIF

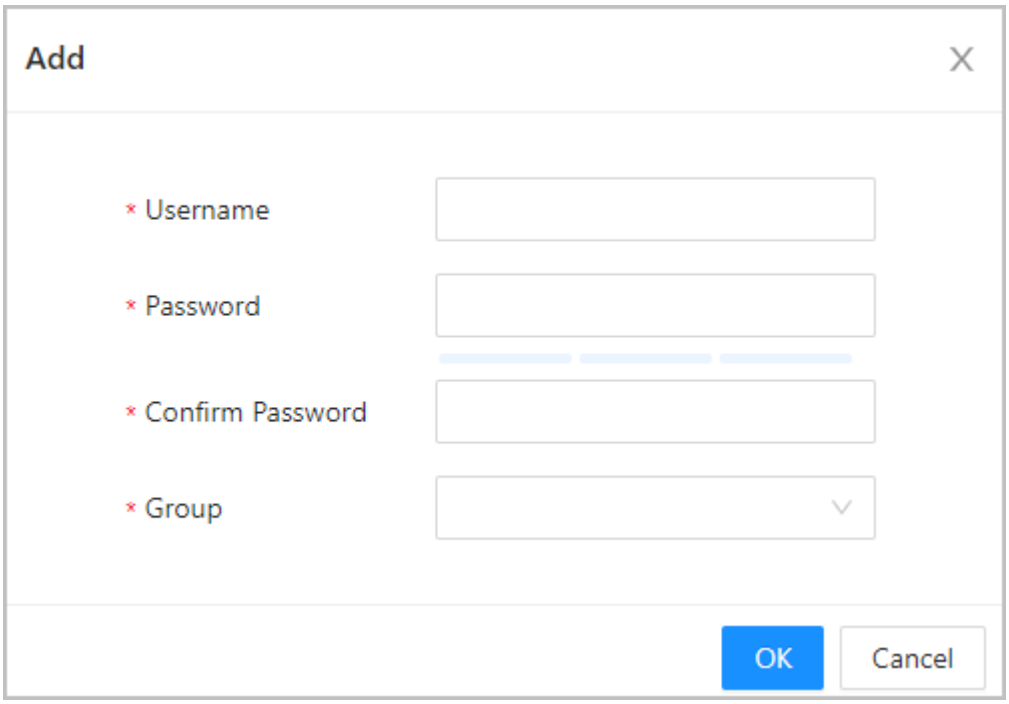


Tabla 3-18 Descripción del usuario de ONVIF

Parámetro	Descripción
Nombre de usuario	El nombre de usuario no puede ser el mismo que el de la cuenta existente. El nombre de usuario puede tener hasta 31 caracteres y solo admite números, letras, guiones bajos, líneas centrales, puntos o @.
Contraseña	La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &).

Parámetro	Descripción
Grupo	Hay tres grupos de permisos que representan diferentes niveles de permisos. ● admin: puede ver y administrar otras cuentas de usuario en el Administrador de dispositivos ONVIF. ● Operador: no puede ver ni administrar otras cuentas de usuario en el Administrador de dispositivos ONVIF. ● Usuario: no puede ver ni administrar otras cuentas de usuario ni registros del sistema en el Administrador de dispositivos ONVIF.

Paso 3 Hacer clic**DE ACUERDO**.

3.8.1.3 Restablecimiento de la contraseña

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

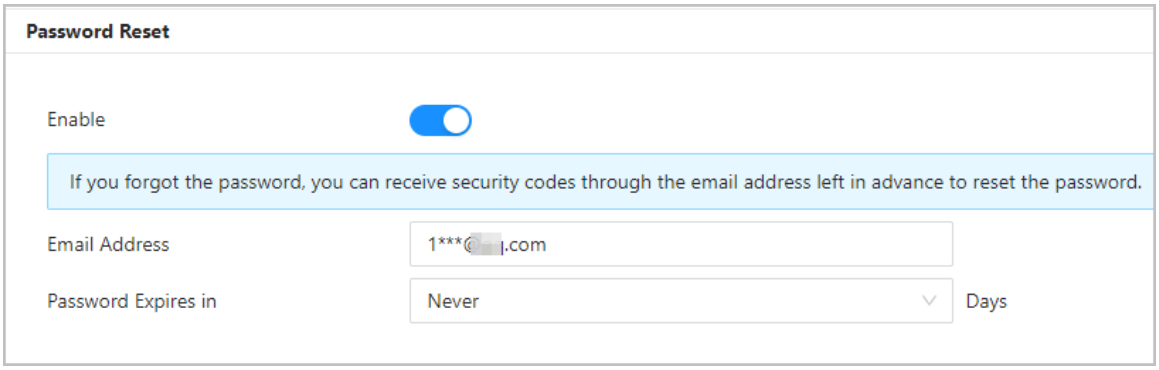
Procedimiento

Paso 1 Seleccionar**Sistema**>**Cuenta**>**Cuenta**.

Paso 2 Introduce la dirección de correo electrónico y establece el tiempo de caducidad de la

Paso 3 contraseña. Activa la función de restablecimiento de contraseña.

Figura 3-34 Restablecer contraseña



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

Paso 4 Hacer clic**Aplicar**.

3.8.2 Visualización de usuarios en línea

Puedes ver los usuarios conectados que actualmente están conectados a la página web. En la página de inicio, selecciona **Sistema**>**Usuario en línea**.

3.8.3 Configuración de la hora

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccione

Paso 2 **Sistema**>**Tiempo**. Configurar la hora de la

Paso 3 Plataforma.

Figura 3-35 Ajustes de tiempo

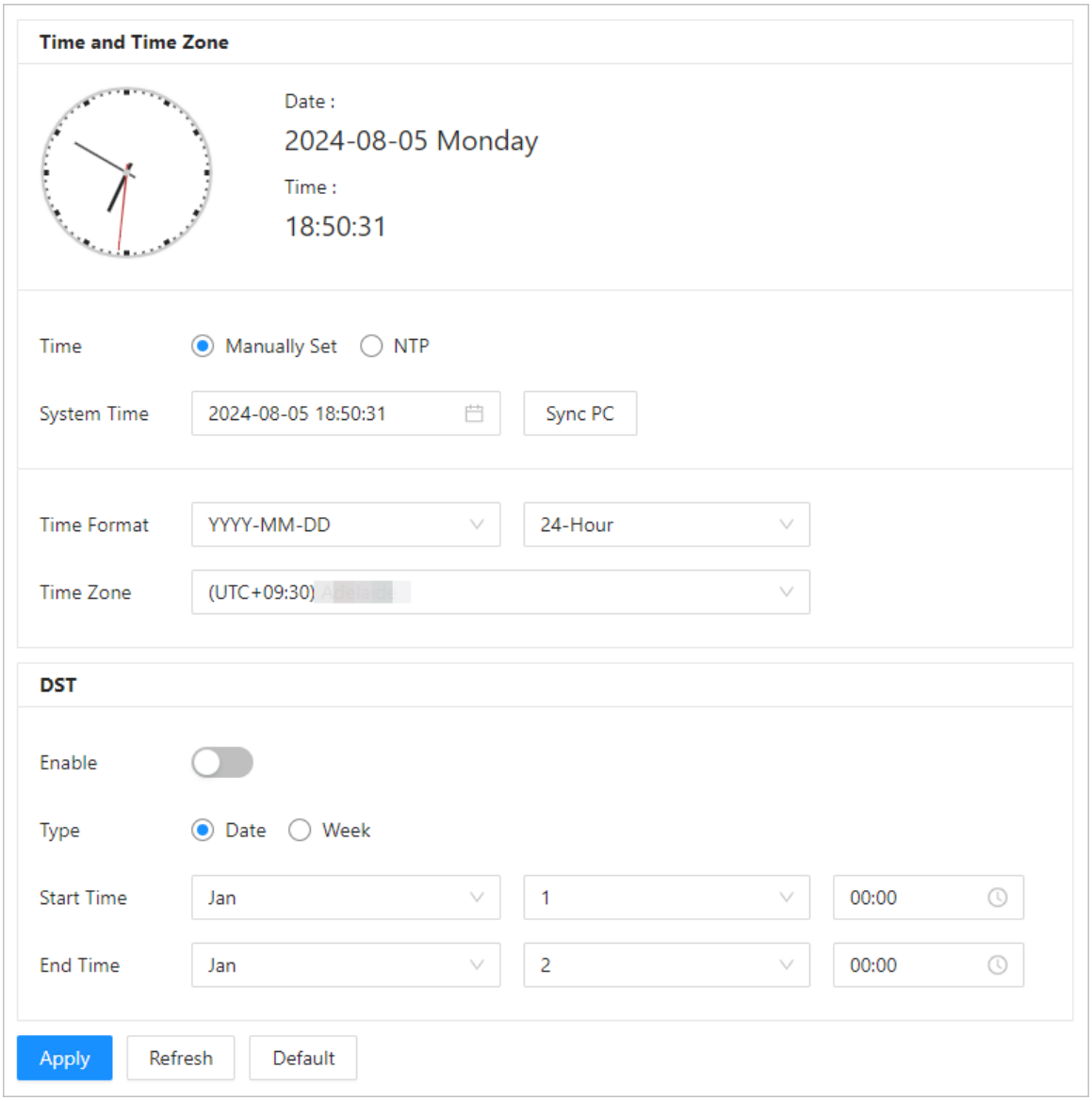


Tabla 3-19 Descripción de la configuración de tiempo

Parámetro	Descripción
Tiempo	● Configuración manual: ingrese la hora manualmente o puede hacer clic**Sincronizar PC**para sincronizar la hora con la computadora. ● NTP: El dispositivo sincronizará automáticamente la hora con el servidor NTP. ◇ **Servidor**:Introduzca el dominio del servidor NTP. ◇ **Puerto**:Introduzca el puerto del servidor NTP. ◇ **Intervalo**:Introduzca su hora con el intervalo de sincronización.
Formato de hora	Seleccione el formato de hora.
Huso horario	Seleccione la zona horaria.

Parámetro	Descripción
Horario de verano	1. (Opcional) Habilitar el horario de verano. 2. Seleccionar**Fecha**o**Semana**desde**Tipo**. 3. Configure la hora de inicio y la hora de finalización del horario de verano.

Paso 4 Hacer clic**Aplicar**.

3.9 Centro de mantenimiento

3.9.1 Diagnóstico con un solo clic

El sistema diagnostica automáticamente las configuraciones y el estado del dispositivo para mejorar su rendimiento.

Procedimiento

Paso 1 En la página de inicio, seleccione**Centro de mantenimiento**>**Diagnóstico con un solo clic**.

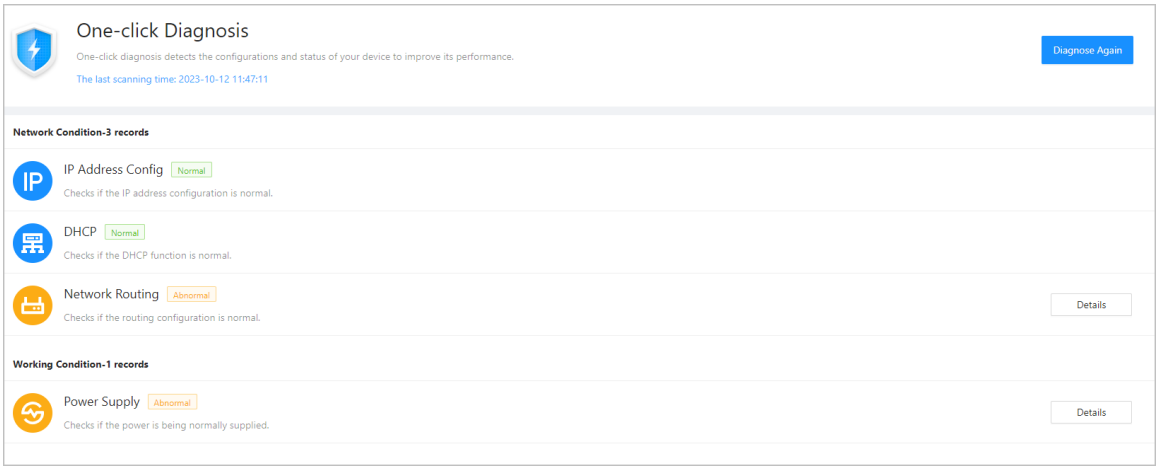
Paso 2 Haga clic**Diagnosticar**.

El sistema diagnostica automáticamente las configuraciones y el estado del dispositivo y muestra los resultados del diagnóstico una vez finalizado.

Paso 3 (Opcional) Haga clic en**Detalles**para ver detalles de artículos anormales.

Puedes ignorar la anomalía u optimizarla. También puedes hacer clic en**Diagnosticar de nuevo**para realizar nuevamente el diagnóstico automático.

Figura 3-36 Diagnóstico con un solo clic



3.9.2 Información del sistema

3.9.2.1 Visualización de la información de la versión

En la página web, seleccione**Centro de mantenimiento**>**Información del sistema**>**Versión**, y podrá ver la información de la versión del dispositivo.

3.9.2.2 Visualización de información legal

En la página de inicio, seleccione**Centro de mantenimiento**>**Información del sistema**>**Información legal**, y puede ver el acuerdo de licencia de software, la política de privacidad y el aviso de software de código abierto.

3.9.3 Capacidad de datos

Puede ver cuántos usuarios y tarjetas puede almacenar el dispositivo.

Inicie sesión en la página web y seleccione**Centro de mantenimiento**>**Capacidad de datos**.

3.9.4 Visualización de registros

Ver registros como registros del sistema, registros de administración y registros de desbloqueo.

3.9.4.1 Registros del sistema

Ver y buscar registros del sistema.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Centro de mantenimiento**>**Registro**>**Registro**.

Paso 3 Seleccione el rango de tiempo y el tipo de registro y luego haga clic en**Buscar**.

Operaciones relacionadas

- hacer clic**Exportar**para exportar los registros buscados a su computadora local.
- Hacer clic**Cifrar copia de seguridad del registro**y luego ingrese una contraseña. El archivo exportado solo se puede abrir después de ingresar la contraseña.
- Hacer clic para ver los detalles de un registro.

3.9.4.2 Desbloquear registros

Busque registros de desbloqueo y expórtelos.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Centro de mantenimiento**>**Registro**>**Desbloquear registros**

Paso 3 Seleccione el rango de tiempo y el tipo, y luego haga clic en**Buscar**.

Puedes hacer clic**Exportar**para descargar el registro.

3.9.4.3 Registros de alarmas

Ver registros de alarmas.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Centro de mantenimiento**>**Registro**>**Registros de**

Paso 3 **alarmas**. Seleccione el tipo y el rango de tiempo.

Paso 4 Ingrese el ID de administrador y luego haga clic en**Buscar**.

3.9.4.4 Registros de administración

Busque registros de administración utilizando el ID de administrador.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Centro de mantenimiento**>**Registro**>**Registros de**

Paso 3 **administración**Ingrese el ID de administrador y luego haga clic en**Buscar**.

Hacer clic**Exportar**para exportar registros de administración.

3.9.5 Gestión de mantenimiento

Cuando más de un dispositivo necesita las mismas configuraciones, puede configurar parámetros para ellos importando o exportando archivos de configuración.

3.9.5.1 Exportación e importación de archivos de configuración

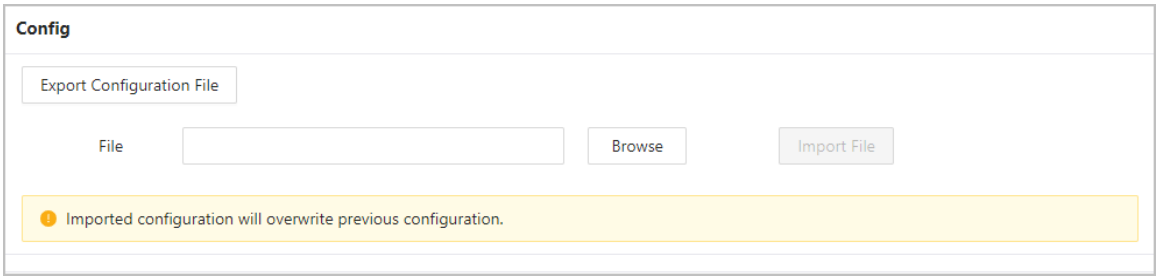
Puede importar y exportar el archivo de configuración del dispositivo. Si desea aplicar la misma configuración a varios dispositivos, puede importar el archivo de configuración.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Centro de mantenimiento**>**Gestión de mantenimiento**>**Configuración**.

Figura 3-37 Gestión de la configuración



Paso 3 Exportar o importar archivos de configuración.

- Exportar el archivo de configuración.

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

  La IP no se exportará.

- Importar 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.

3.9.5.2 Configuración del umbral de similitud de huellas dactilares

Configure el umbral de similitud de huellas dactilares. Cuanto mayor sea el valor, mayor será la precisión y menor la tasa de aprobación.

Procedimiento

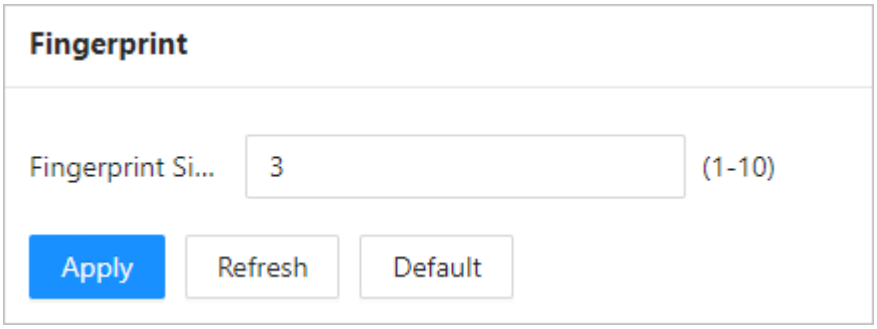
Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Centro de mantenimiento**>**Gestión de mantenimiento**>**Configuración**

Paso 3 Ingrese el umbral de similitud y luego haga clic en**Aplicar**.

- El parámetro está disponible en el controlador de acceso modular con el módulo de huellas dactilares.
- El parámetro está disponible en el controlador de acceso con función de huella dactilar.

Figura 3-38 Umbral de similitud de huellas dactilares



3.9.5.3 Restauración de la configuración predeterminada de fábrica

Procedimiento

Paso 1 Seleccionar**Centro de mantenimiento**>**Gestión de mantenimiento**>**Configuración**.

Restaurando el**Dispositivo**Restablecer la configuración predeterminada provocará la pérdida de datos. Tenga en cuenta lo siguiente.

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

- **Valores predeterminados de fábrica**:Restablece todas las configuraciones del dispositivo y borra todos los datos.
- **Restaurar a valores predeterminados (excepto información de usuario y registros)**:Restablece las configuraciones del dispositivo y borra todos los datos excepto la información del usuario y los registros.

3.9.5.4 Mantenimiento

Reinicie periódicamente el dispositivo durante su tiempo de inactividad para mejorar su rendimiento.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Centro de mantenimiento**>**Gestión de mantenimiento**>**Mantenimiento**.

Paso 3 Establezca la hora y luego haga clic en**Aplicar**.

El dispositivo se reiniciará a la hora programada, o puede hacer clic**Reanudar**para reiniciarlo inmediatamente.

3.9.6 Actualización del sistema

- Utilice el archivo de actualización correcto. Asegúrese de obtenerlo del soporte técnico.
- No desconecte la fuente de alimentación ni la red y no reinicie ni apague el dispositivo durante la actualización.
- Actualizar a una versión anterior puede conllevar riesgos. Tenga en cuenta lo siguiente.
- Si inicia el dispositivo por primera vez o lo restaura a la configuración de fábrica, este creará automáticamente una copia de seguridad de los archivos del sistema en los primeros 10 minutos. No actualice durante este periodo.

3.9.6.1 Actualización de archivos

Procedimiento

Paso 1 En la página de inicio, seleccione**Centro de mantenimiento**>**Actualizar**. 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 dispositivo se reiniciará después de que finalice la actualización.

3.9.6.2 Actualización en línea

Procedimiento

Paso 1 En la página de inicio, seleccione**Centro de mantenimiento**>**Actualizar**. En el

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

- Seleccionar**Búsqueda automática de actualizaciones**y el dispositivo buscará automáticamente la última actualización de la versión.
- Seleccionar**Comprobación manual**y podrás comprobar inmediatamente si la última versión está disponible.

Paso 3 (Opcional) Haga clic en**Actualizar ahora**para actualizar el dispositivo inmediatamente.

3.9.7 Mantenimiento avanzado

Adquirir información del dispositivo y capturar paquetes para facilitar que el personal de mantenimiento realice la resolución de problemas.

3.9.7.1 Exportación

Procedimiento

Paso 1 En la página de inicio, seleccione**Centro de mantenimiento**>**Mantenimiento avanzado**>**Exportar**.

Paso 2 Hacer clic**Exportar**para exportar el número de serie, la versión del firmware, los registros de funcionamiento del dispositivo y la información de configuración.

3.9.7.2 Captura de paquetes

Procedimiento

Paso 1 En la página de inicio, seleccione**Centro de mantenimiento**>**Mantenimiento avanzado**>**Captura de paquetes**.

Figura 3-39 Captura de paquetes

Paso 2 Introduzca la dirección IP, haga clic en .

cambios a .

Paso 3 Una vez que haya adquirido suficientes datos, haga clic en .

Los paquetes capturados se descargan automáticamente a su computadora local.

3.10 Configuración de seguridad (opcional)

3.10.1 Estado de seguridad

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

Información de fondo

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

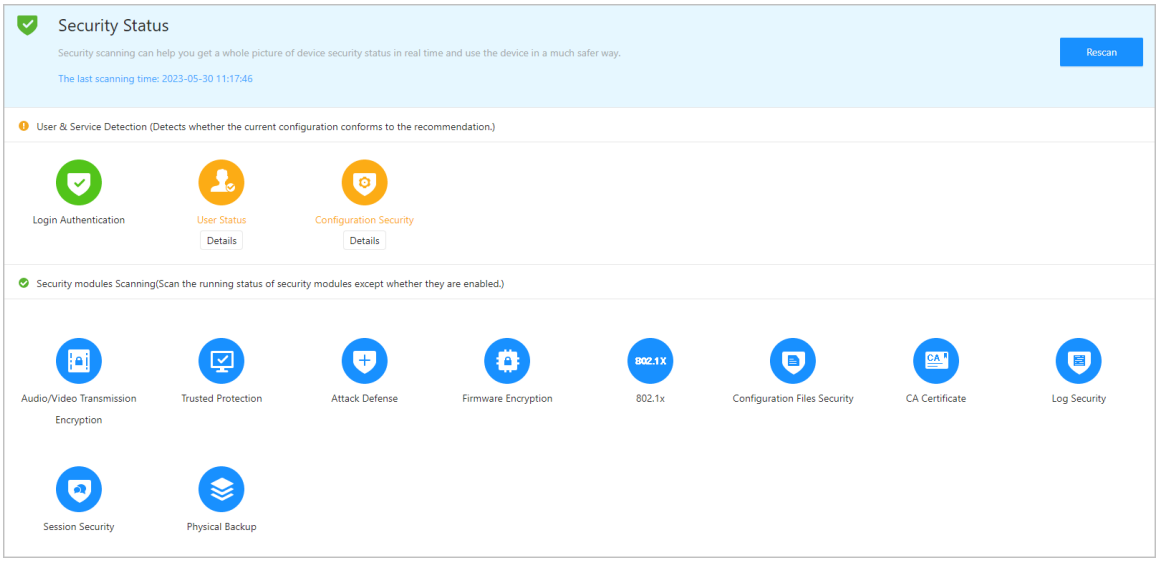
Procedimiento

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

Paso 2 Hacer clic**Volver a escanear**para realizar un escaneo de seguridad del dispositivo.

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

Figura 3-40 Estado de seguridad



Operaciones relacionadas

Tras realizar el análisis, los resultados se mostrarán en diferentes colores. El amarillo indica que los módulos de seguridad presentan anomalías y el verde, que están normales.

- Hacer clic**Detalles**para ver los detalles de los resultados del escaneo.
- Hacer clic**Ignorar**Para ignorar la anomalía, no se escaneará. La anomalía ignorada se resaltará en gris.
- Hacer clic**Optimizar**para solucionar la anomalía.

3.10.2 Configuración del servicio del sistema

Cree un certificado o cargue uno autenticado y podrá iniciar sesión en la página web mediante HTTPS en su computadora. HTTPS protege la comunicación en una red informática.

Procedimiento

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

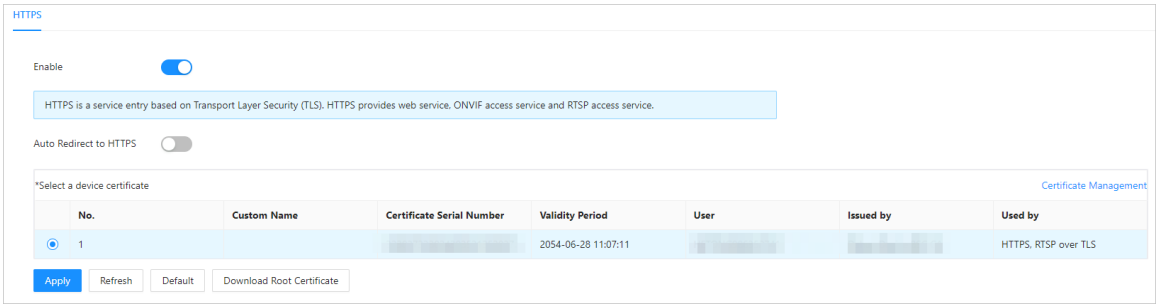
Paso 2 Activar el servicio HTTPS.

Si activa la compatibilidad con TLS v1.1 y versiones anteriores, podrían producirse riesgos de seguridad. Tenga en cuenta lo siguiente.

Paso 3 Seleccione el certificado.

Si no hay certificados en la lista, haga clic en**Gestión de certificados**para cargar un certificado.

Figura 3-41 Servicio del sistema



Paso 4 Hacer clic**Aplicar**.

Introduzca "https://*Dirección IP*:*httpsport*" en un navegador web. Si el certificado está instalado, podrá iniciar sesión en la página web correctamente. De lo contrario, la página web mostrará el certificado como incorrecto o no confiable.

3.10.3 Defensa de ataque

3.10.3.1 Configuración del firewall

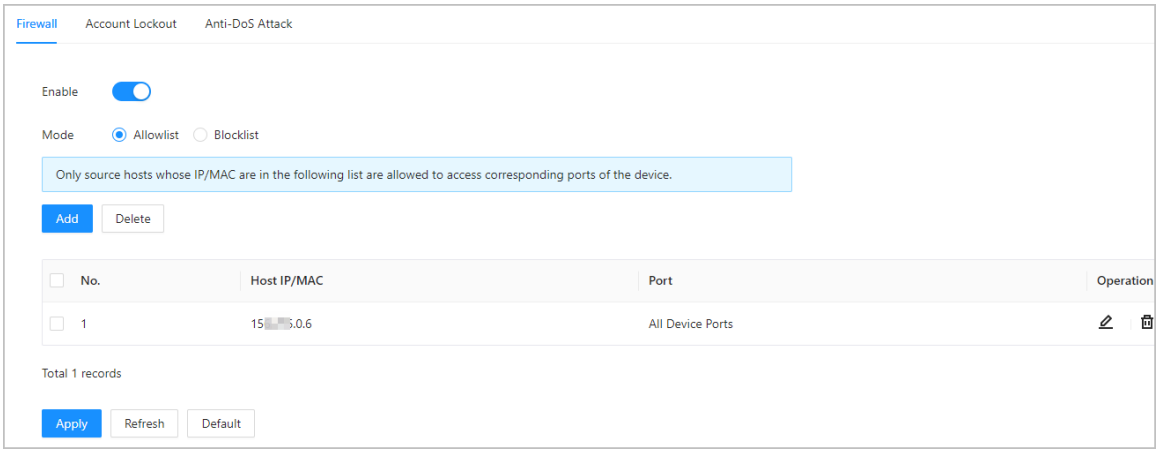
Configurar el firewall para limitar el acceso al dispositivo.

Procedimiento

Paso 1 Seleccionar > **Ataque Defensa**>**Cortafuegos**.

Paso 2 Hacer clic para habilitar la función de firewall.

Figura 3-42 Cortafuegos

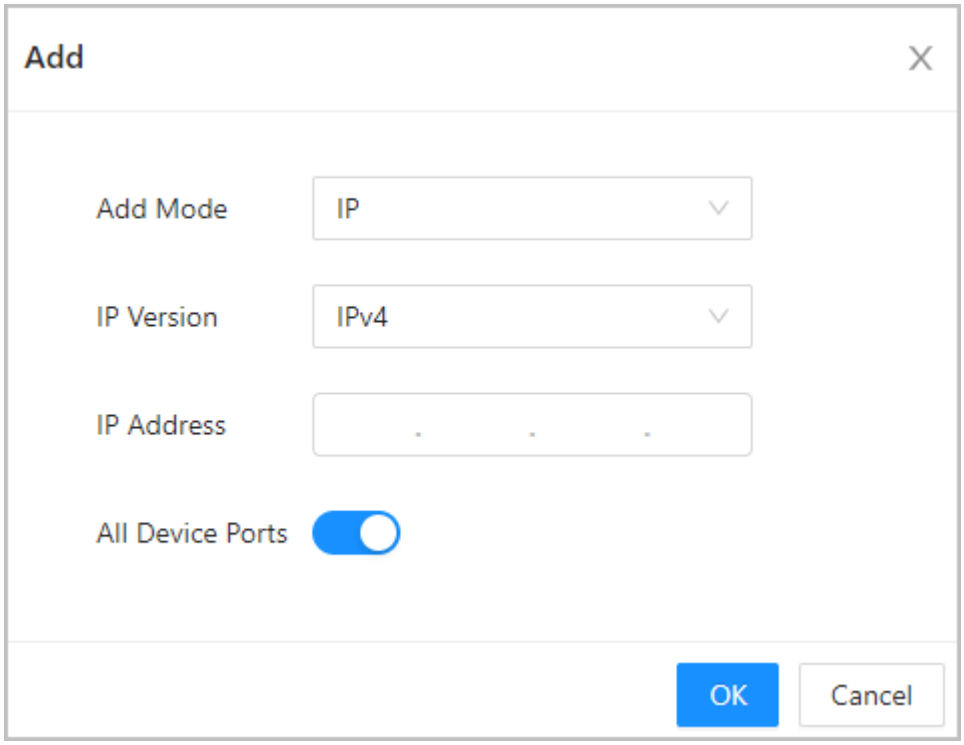


Paso 3 Seleccione el modo:**Lista de permitidos**y**Lista de bloqueo**.

- **Lista de permitidos**:Sólo las direcciones IP/MAC en la lista blanca pueden acceder al dispositivo.
- **Lista de bloqueo**:Las direcciones IP/MAC en la lista de bloqueo no pueden acceder al dispositivo.

Paso 4 Hacer clic**Agregar**para ingresar la información IP.

Figura 3-43 Agregar información de IP



Paso 5 Hacer clicDE ACUERDO.

Operaciones relacionadas

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

3.10.3.2 Configuración del bloqueo de cuenta

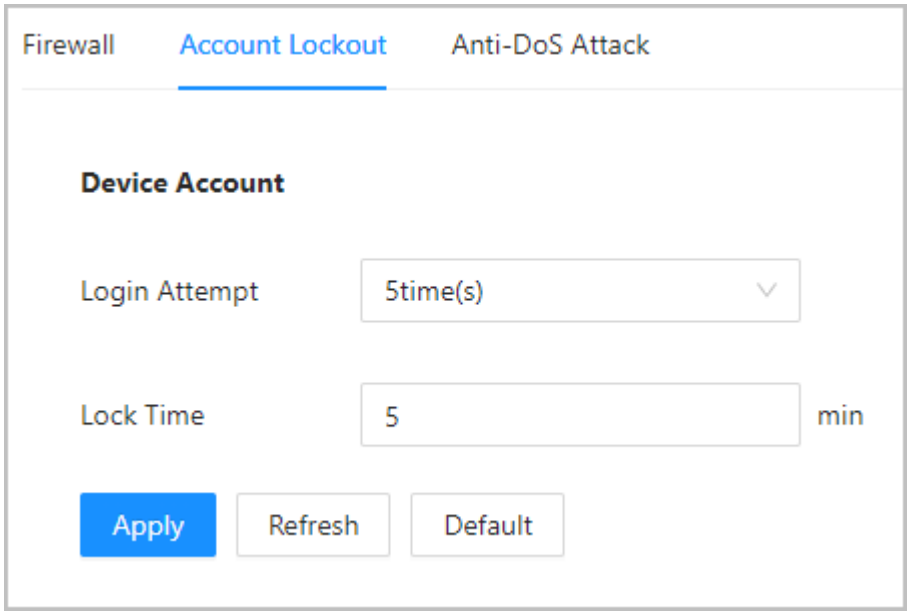
Si se ingresa una contraseña incorrecta una cantidad definida de veces, la cuenta se bloqueará.

Procedimiento

Paso 1 Seleccionar > **Ataque Defensa**>**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 permanecerán bloqueados.

Figura 3-44 Bloqueo de cuenta



- Intento de inicio de sesión: El límite de intentos de inicio de sesión. Si se ingresa una contraseña incorrecta un número determinado de veces, la cuenta se bloqueará.
- Tiempo de bloqueo: El tiempo durante el cual no podrá iniciar sesión después de que la cuenta esté bloqueada. Haga

Paso 3 clic en**Aplicar**.

3.10.3.3 Configuración de ataques anti-DoS

Puedes habilitar**Defensa contra ataques de inundación SYN**y**Defensa contra ataques de inundación ICMP**para defender el dispositivo contra ataques DoS.

Procedimiento

Paso 1 Seleccionar > **Ataque Defensa**>**Ataque anti-DoS**.

Paso 2 Encender**Defensa contra ataques de inundación SYN**o**Defensa contra ataques de inundación ICMP**para proteger el dispositivo contra ataques DoS.

Figura 3-45 Ataque anti-DoS

Paso 3 Hacer clic**Aplicar**.

3.10.4 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.

3.10.4.1 Creación de certificado

Crear un certificado para el dispositivo.

Procedimiento

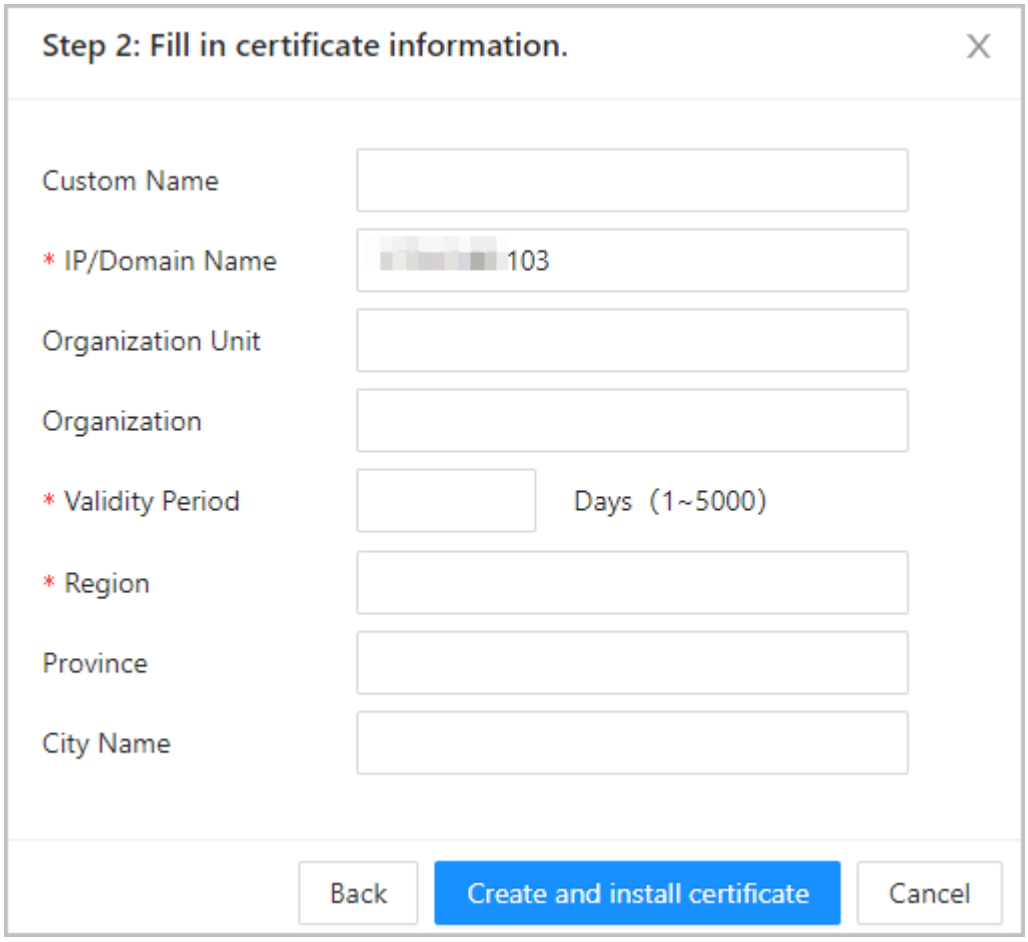
Paso 1 Seleccionar > **Certificado CA**>**Certificado del dispositivo**.

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

Paso 3 Seleccionar**Crear certificado**,y haga clic**Próximo**.

Paso 4 Ingrese la información del certificado.

Figura 3-46 Información del certificado



El nombre de la región no puede tener más de dos caracteres. Recomendamos introducir la abreviatura del nombre de la región.

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

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

Operaciones relacionadas

- Hacer clic**Entrar al modo de edición**en el**Certificado del dispositivo**Página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

3.10.4.2 Solicitud e importación de un certificado de CA

Importe el certificado CA de terceros al dispositivo.

Procedimiento

Paso 1 Seleccionar > **Certificado CA**>**Certificado del dispositivo**.

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

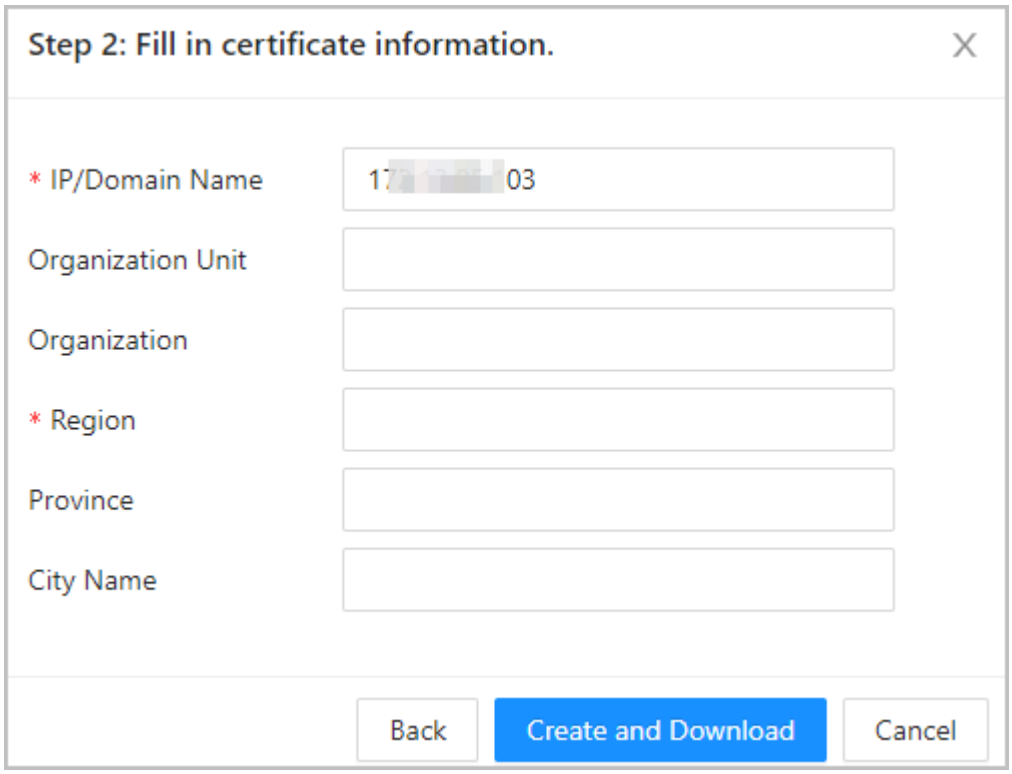
Paso 3 Seleccionar**Solicitar certificado CA e importación (recomendado)**,y haga clic**Próximo**.

Paso 4 Ingrese la información del certificado.

- IP/Nombre de dominio: la dirección IP o el nombre de dominio del dispositivo.

- Región: El nombre de la región no debe exceder los 3 caracteres. Recomendamos introducir la abreviatura del nombre de la región.

Figura 3-47 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 certificación externa mediante el archivo de solicitud. Importe

Paso 7 el certificado de la 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 CA.
4. Haga clic**Importar e instalar**.

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

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

Operaciones relacionadas

- Hacer clic**Entrar al modo de edición**en el**Certificado del dispositivo**Página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

3.10.4.3 Instalación de un certificado existente

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

Procedimiento

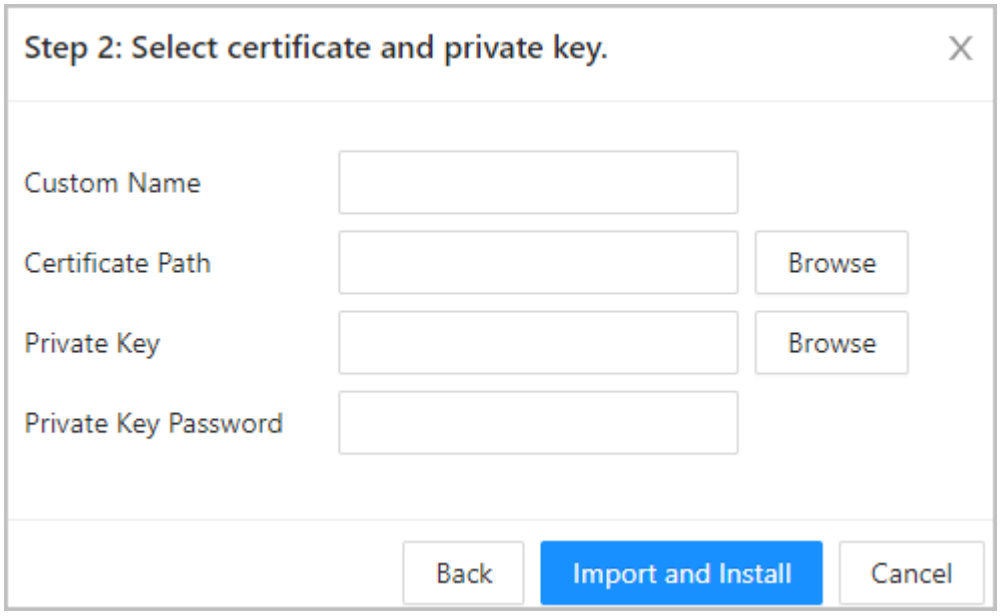
Paso 1 Seleccionar**Seguridad**>**Certificado CA**>**Certificado del dispositivo**.

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

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

Paso 4 Hacer clic**Navegar**para seleccionar el certificado y el archivo de clave privada e ingresar la contraseña de la clave privada.

Figura 3-48 Certificado y clave privada



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

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

Operaciones relacionadas

- Hacer clic**Entrar al modo de edición**en el**Certificado del dispositivo**Página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

3.10.5 Instalación del certificado de CA de confianza

Un certificado de CA de confianza es un certificado digital que se utiliza para validar la identidad 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 fondo

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.

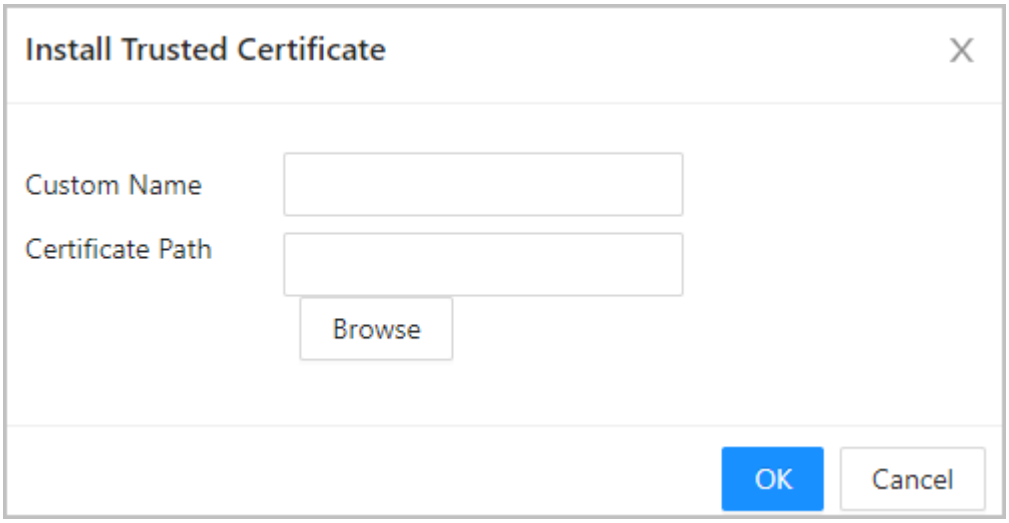
Procedimiento

Paso 1 Seleccionar > **Certificado CA**>**Certificados de CA de confianza**.

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

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

Figura 3-49 Instalar el certificado de confianza



Paso 4 Hacer clic**DE ACUERDO**.

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

Operaciones relacionadas

- Hacer clic**Entrar al modo de edición**en el**Certificado del dispositivo**Página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

3.10.6 Advertencia de seguridad

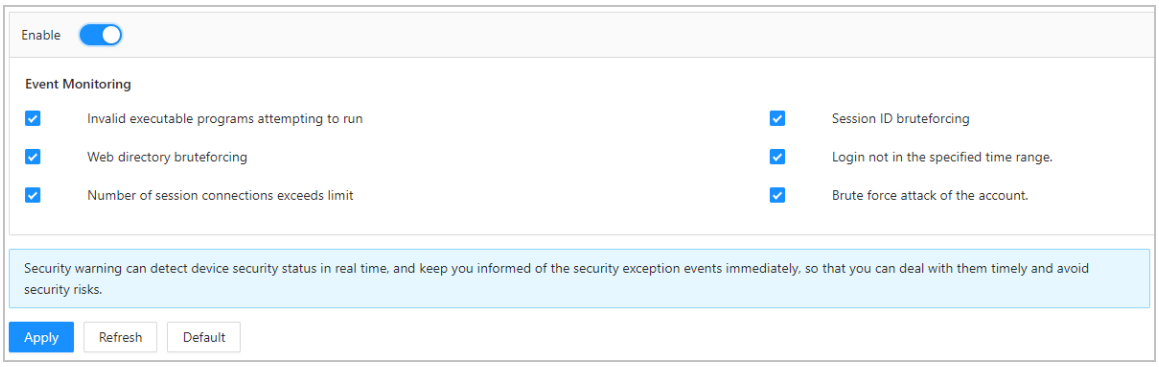
Procedimiento

Paso 1 Seleccionar > **Advertencia de seguridad**.

Paso 2 Habilite la función de advertencia de seguridad.

Paso 3 Seleccione los elementos de monitoreo.

Figura 3-50 Advertencia de seguridad



Paso 4 Hacer clic**Aplicar**.

3.10.7 Autenticación de seguridad

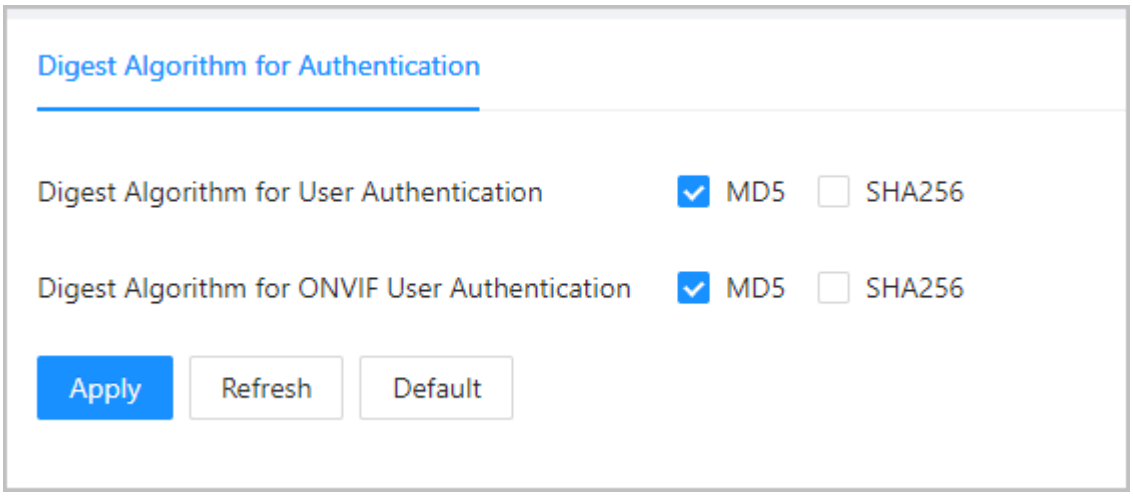
Procedimiento

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

Paso 2 Seleccione un algoritmo de resumen del mensaje.

Paso 3 Hacer clic**Aplicar**.

Figura 3-51 Autenticación de seguridad



4 Operaciones telefónicas

Antes de iniciar sesión en la página web del dispositivo en su teléfono, asegúrese de haber inicializado el dispositivo a través de la página web en la computadora.

Le recomendamos usar su teléfono en modo vertical y modo diurno. Puede acceder a la página web del dispositivo desde su teléfono mediante los siguientes métodos.

- Conecte el dispositivo a la red mediante el cable de red. Asegúrese de que el teléfono y el dispositivo estén en la misma red. Abra el navegador del teléfono e introduzca la dirección IP del dispositivo.
- Conecte el dispositivo y el teléfono a la red mediante la misma red Wi-Fi. Abra el navegador en el teléfono e introduzca la dirección IP correspondiente a la red Wi-Fi conectada.
- Conecte el teléfono a la red a través del Wi-Fi del dispositivo. Abra el navegador del teléfono e introduzca la dirección IP correspondiente al punto de acceso Wi-Fi del dispositivo (por defecto, es 192.168.3.1).

El nombre del dispositivo Wi-Fi se muestra en la**Número de serie del dispositivo + Modelo del dispositivo**modo.

- El Wi-Fi y el AP Wi-Fi están disponibles en modelos seleccionados.
- Al iniciar sesión en la página web desde el teléfono, solo se admite el idioma inglés.

4.1 Inicialización

Cuando el teléfono está en la misma LAN que el controlador de acceso, puede inicializar el controlador de acceso por primera vez o después de que el dispositivo se restaure a los valores predeterminados de fábrica en la página web del teléfono.

Prerrequisitos

Asegúrese de que el controlador de acceso no esté conectado a la red Wi-Fi o 4G.

Existen principalmente tres maneras de conectar el dispositivo y el teléfono a la misma red. Esta sección presenta la inicialización del teléfono mediante un punto de acceso Wi-Fi.

- Conecte el dispositivo a la red mediante el cable de red. Asegúrese de que el teléfono y el dispositivo estén en la misma red. Abra el navegador en el teléfono e introduzca la dirección IP del dispositivo.
- Conecte el dispositivo y el teléfono a la red mediante la misma red Wi-Fi. Abra el navegador en el teléfono e introduzca la dirección IP correspondiente a la red Wi-Fi conectada.
- Conecte el teléfono a la red a través del Wi-Fi del dispositivo. Abra el navegador del teléfono e introduzca la dirección IP correspondiente al punto de acceso Wi-Fi del dispositivo (por defecto, es 192.168.3.1).

El Wi-Fi y el AP Wi-Fi están disponibles en modelos seleccionados.

Procedimiento

Paso 1 Encienda el controlador de acceso.

Paso 2 Conéctate al punto de acceso Wi-Fi de tu teléfono. El nombre del punto de acceso es**número de serie del producto + modelo del dispositivo**.

Si no se ha conectado al punto de acceso Wi-Fi en 30 minutos, el punto de acceso estará desactivado.

Paso 3 Abra un navegador en su teléfono y vaya a la dirección IP (la dirección predeterminada es 192.168.3.1) del punto de acceso.

Paso 4 Grifo**Inicialización inicial**.

Paso 5 Ingrese y confirme la contraseña, ingrese una dirección de correo electrónico.

- La contraseña debe tener entre 8 y 32 caracteres (no espacios en blanco) y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excepto ' " ; : &). Establezca una contraseña de alta seguridad siguiendo las instrucciones de seguridad.
- Mantenga la contraseña segura después de la inicialización y cámbiela periódicamente para mejorar la seguridad.

Paso 6 (Opcional) Habilite la dirección de correo electrónico y luego configure la dirección.

Si desea restablecer la contraseña de administrador escaneando el código QR, debe habilitar la función de correo electrónico y configurar la dirección de correo electrónico para recibir el código de seguridad.

Paso 7 (Opcional) Seleccionar**He leído y acepto el Acuerdo de licencia de software y la Política de privacidad.**. Grifo

Paso 8 **Próximo**.

Paso 9 Permitir**Búsqueda automática de actualizaciones**según sea necesario y luego toque**Terminado**.

Se muestra la página de inicio de sesión.

4.2 Iniciar sesión en la página web

Prerrequisitos

Asegúrese de que el teléfono utilizado para iniciar sesión en la página web esté en la misma LAN que el dispositivo.

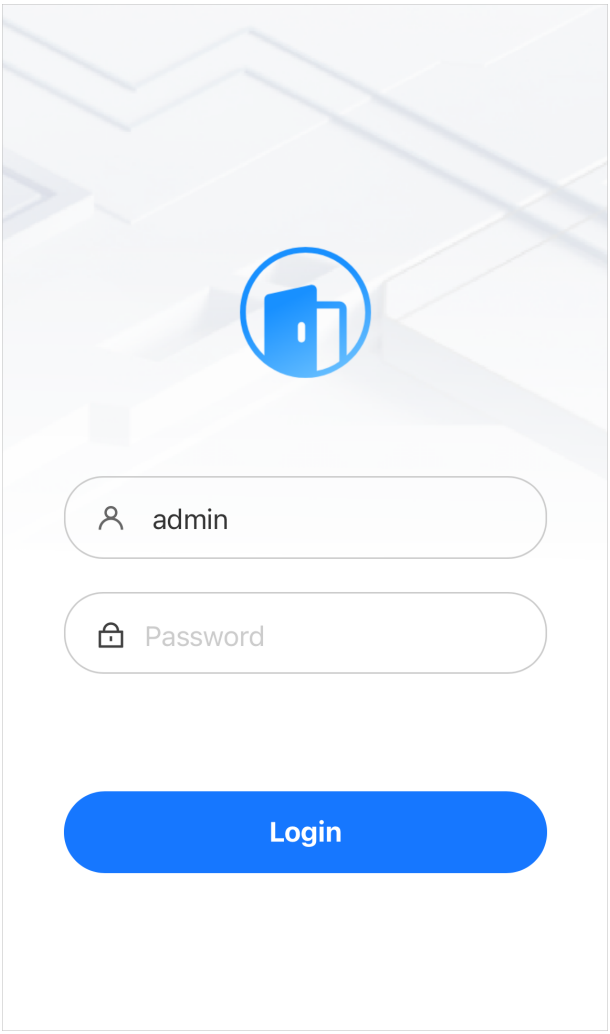
Procedimiento

Paso 1 Abra un navegador e ingrese la dirección IP del dispositivo. Ingrese el

Paso 2 nombre de usuario y la contraseña.

- El nombre de administrador predeterminado es admin y la contraseña es la que se configuró durante la inicialización. Se recomienda cambiar la contraseña de administrador periódicamente para mayor seguridad.
- Si olvida la contraseña de inicio de sesión del administrador, puede restablecerla a través de la página web en la computadora.

Figura 4-1 Página de inicio de sesión



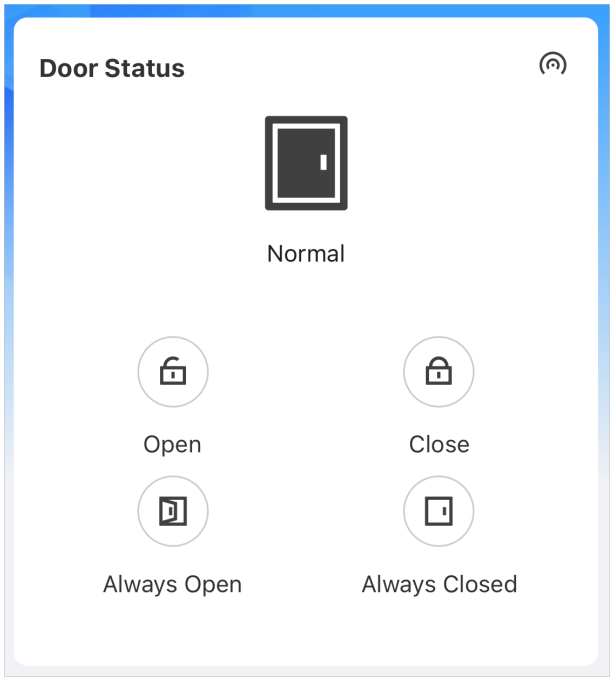
Paso 3 Hacer clic**Acceso**.

4.3 Página de inicio

La página de inicio se muestra después de iniciar sesión correctamente.

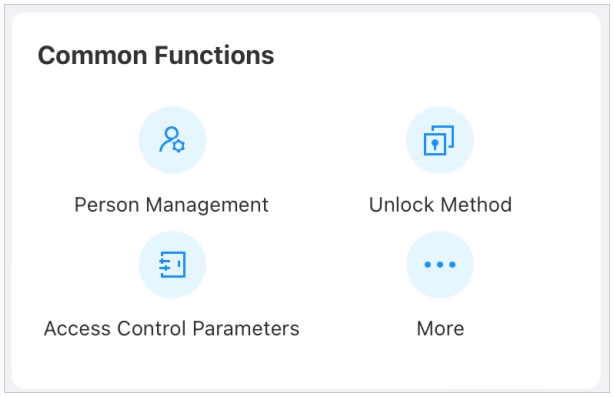
- El**Estado de la puerta**El área muestra el estado de la puerta. Puede abrirla o cerrarla remotamente. También puede configurar el estado de la puerta como**Siempre abierto**o**Siempre cerrado**.

Figura 4-2 Estado de la puerta



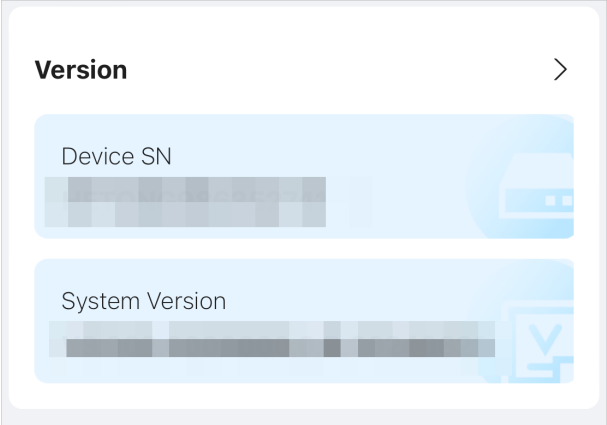
- El**Función común**El área muestra el menú de configuración del dispositivo. Haga clic en**Más**para ver todos los menús de configuración.

Figura 4-3 Funciones comunes



- Ver el número de serie y la información de la versión en el**Versión**área. Haga clic**>**para ver los detalles de la versión.

Figura 4-4 Versión



4.4 Gestión de personas

Añade la persona y configura los permisos.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Hacer clic**Gestión de personas**,y luego haga clic**+**.

Paso 3 Configurar la información del usuario.

Figura 4-5 Agregar la persona (1)

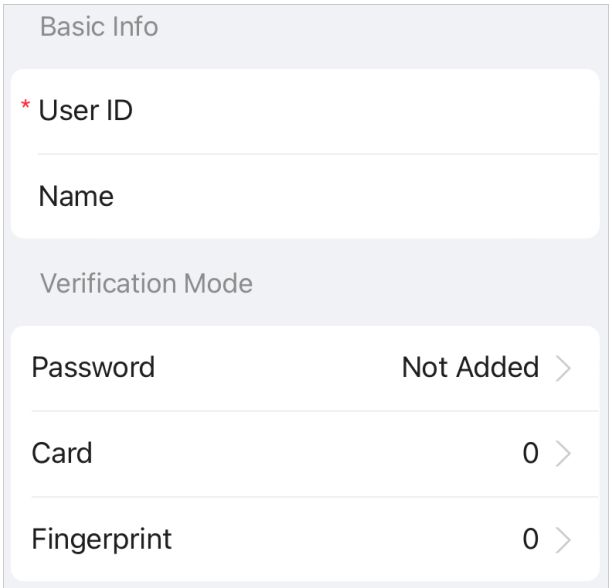


Figura 4-6 Agregar la persona (2)

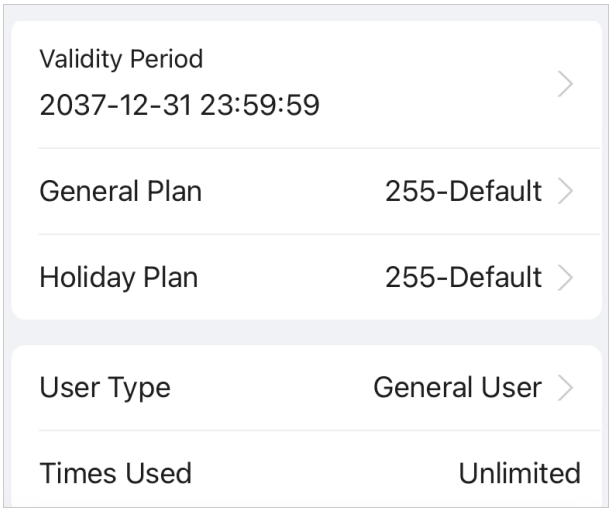


Tabla 4-1 Descripción de parámetros

Parámetro	Descripción
ID de usuario	El ID de usuario es como el ID de empleado, que puede ser números, letras y sus combinaciones, y la longitud máxima del número es de 30 caracteres.
Nombre	El nombre puede tener hasta 32 caracteres (incluidos números, símbolos y letras).
Contraseña	Configure la contraseña de usuario. La contraseña tiene una longitud máxima de 8 dígitos. La contraseña de coacción es la contraseña de desbloqueo + 1. Por ejemplo, si la contraseña de usuario es 12345, la contraseña de coacción será 12346. Se activará una alarma de coacción cuando se use una contraseña de coacción para desbloquear la puerta.

Parámetro	Descripción
Tarjeta	• Introduzca el número de tarjeta manualmente. 1. Haga clic**Agregar**. 2. Ingrese el número de tarjeta y luego haga clic en**Agregar**. • Lea el número automáticamente a través del dispositivo. 1. Haga clic**Agregar**. 2. Pase la tarjeta por el lector. Se muestra una cuenta regresiva 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**de nuevo para iniciar una nueva cuenta regresiva. 3. Haga clic**DE ACUERDO**. Un usuario puede registrar hasta 5 tarjetas. Ingrese su número de tarjeta o deslícela, y el dispositivo leerá la información. Puedes habilitar el**Tarjeta de coacción**Función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta. • **Tarjeta de coacción**:Haga clic para configurar la tarjeta de coacción. • **Cambiar número de tarjeta**:Haga clic para cambiar el número de tarjeta. Un usuario sólo puede configurar una tarjeta de coacción.
Huella dactilar	Registrar huellas dactilares. Un usuario puede registrar hasta tres huellas dactilares, y se puede configurar una como huella de coacción. Se activará una alarma cuando se use la huella de coacción para abrir la puerta. Inscriba huellas dactilares a través de un lector de inscripción o del Dispositivo. 1. Haga clic**Agregar**. 2. Presione el dedo sobre el escáner de acuerdo con las instrucciones en pantalla. 3. Haga clic**DE ACUERDO**. • La función de huella dactilar solo está disponible en modelos seleccionados. • No recomendamos que establezca la primera huella dactilar como huella dactilar de coacción. • Un usuario solo puede configurar una huella digital de coacción.
Permiso	• **Usuario**:Los usuarios sólo tienen permisos de acceso a puertas o de control de asistencia. • **Administración**:Los administradores pueden configurar el dispositivo además del acceso a la puerta y los permisos de asistencia.
Periodo de validez	Establecer una fecha en la que expirarán los permisos de acceso a la puerta y asistencia de la persona.

Parámetro	Descripción
Plan General	Las personas pueden desbloquear la puerta o tomar asistencia durante el período definido. Puede seleccionar más de un plan.
Plan de vacaciones	Las personas pueden desbloquear la puerta o tomar asistencia durante el día festivo definido. Puede seleccionar más de un día festivo.
Tipo de usuario	• **Usuario general**:Los usuarios generales pueden desbloquear la puerta. • **Usuario de la lista negra**:Cuando los usuarios de la lista de bloqueo desbloquean la puerta, el personal de servicio recibirá una notificación. • **Usuario invitado**:Los huéspedes pueden desbloquear la puerta dentro de un periodo definido o por un número determinado de veces. Una vez transcurrido el periodo definido o el tiempo de desbloqueo, no podrán desbloquear la puerta. • **Usuario de patrulla**:Los usuarios de patrulla pueden tomar asistencia en el dispositivo, pero no tienen permisos de puerta. • **Usuario VIP**:Cuando el VIP desbloquee la puerta, el personal de servicio recibirá un aviso. • **Otro usuario**:Cuando desbloqueen la puerta, ésta permanecerá desbloqueada durante 5 segundos más. • Usuario personalizado 1/Usuario personalizado 2: Lo mismo que los usuarios generales.
Tiempo utilizado	Establezca un límite de desbloqueo para los usuarios invitados. Una vez transcurrido el tiempo de desbloqueo, no podrán abrir la puerta.

Paso 4 Hacer clic**Agregar**.

4.5 Configuración del sistema

4.5.1 Visualización de la información de la versión

En la página web, seleccione**Más**>**Sistema**>**Versión**, y puede ver la información de la versión en el dispositivo.

4.5.2 Mantenimiento

Reinicie periódicamente el dispositivo durante su tiempo de inactividad para mejorar su rendimiento.

Procedimiento

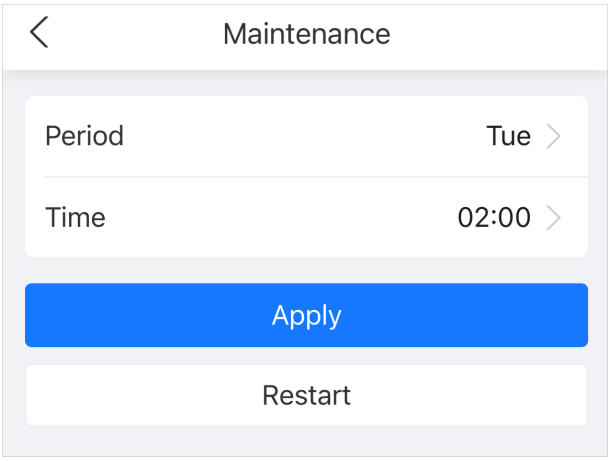
Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Más**>**Sistema**>**Mantenimiento**.

Paso 3 Establezca la hora y luego haga clic en**Aplicar**.

El dispositivo se reiniciará a la hora programada, o puede hacer clic**Reanudar**para reiniciarlo inmediatamente.

Figura 4-7 Mantenimiento



4.5.3 Configuración de la hora

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccione**Más**>**Sistema**>**Tiempo**.

Paso 3 Configurar la hora.

Figura 4-8 Configurar los parámetros de tiempo

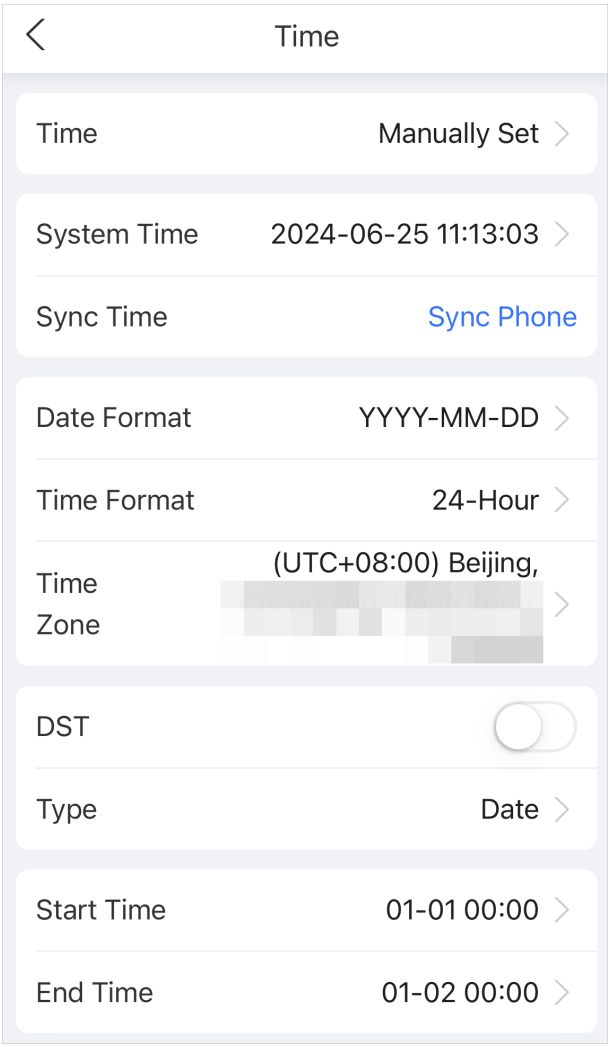


Tabla 4-2 Descripción de la configuración de tiempo

Parámetro	Descripción
Tiempo	● Configuración manual: ingrese la hora manualmente o puede hacer clic**Sincronizar teléfono** para sincronizar la hora con el teléfono. ● NTP: El dispositivo sincronizará automáticamente la hora con el servidor NTP. ◇ **Servidor**:Introduzca el dominio del servidor NTP. ◇ **Puerto**:Introduzca el puerto del servidor NTP. ◇ **Intervalo**:Introduzca su hora con el intervalo de sincronización.
Formato de fecha	Seleccione el formato de fecha y el formato de hora.
Formato de hora	
Huso horario	Seleccione la zona horaria.
Horario de verano	1. (Opcional) Habilitar el horario de verano. 2. Seleccionar**Fecha**o**Semana**como el**Tipo**. 3. Configure la hora de inicio y la hora de finalización del horario de verano.

Paso 4 Hacer clic**Aplicar**.

4.5.4 Capacidad de datos

Puede ver cuántos usuarios, tarjetas, huellas dactilares, registros, registros de desbloqueo y otra información que el dispositivo puede almacenar.

Inicie sesión en la página web y seleccione**Más**>**Sistema**>**Capacidad de datos**.

4.6 Configuración del control de acceso

4.6.1 Configuración de métodos de desbloqueo

Puedes usar varios métodos de desbloqueo, como huella dactilar, tarjeta y contraseña. También puedes combinarlos para crear tu propio método de desbloqueo.

Procedimiento

Paso 1 Inicie sesión en la página web.

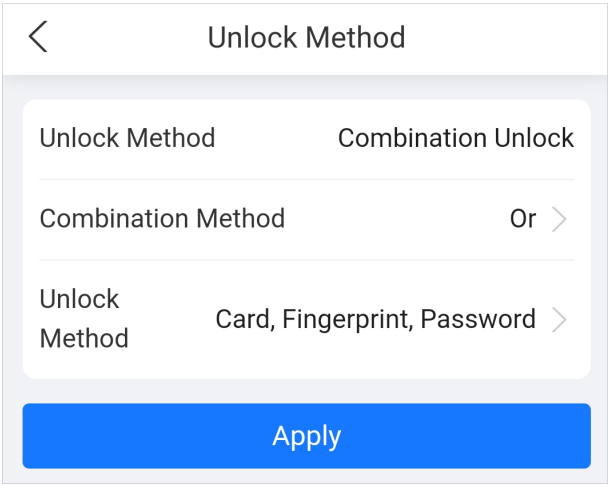
Paso 2 Hacer clic**Método de desbloqueo**en el menú principal, o seleccione**Más**>**Control de acceso**>**Método de desbloqueo**.

Paso 3 (Opcional) Configure el método de combinación y el método de desbloqueo y luego haga clic en **Aplicar**.

- Método de combinación
  - ◇ O bien: Utilice uno de los métodos de desbloqueo seleccionados para abrir la puerta. Y
  - ◇ bien: Utilice todos los métodos de desbloqueo seleccionados para abrir la puerta.
- Método de desbloqueo

  Seleccione el método de desbloqueo según las capacidades admitidas por el dispositivo.

Figura 4-9 Método de desbloqueo



4.6.2 Configuración de parámetros de control de acceso

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Hacer clic**Parámetros de control de acceso**en el menú principal, o seleccione**Más**>**Control de acceso**> **Parámetros de control de acceso**.

Paso 3 Configure los parámetros básicos para el control de acceso y luego haga clic en**Aplicar**.

Figura 4-10 Parámetros de control de acceso (1)

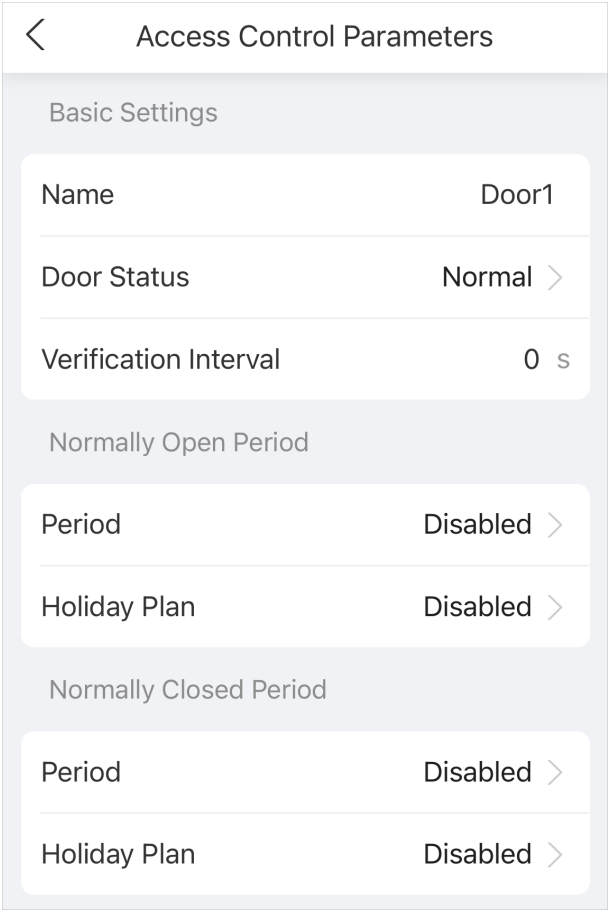


Figura 4-11 Parámetros de control de acceso (2)

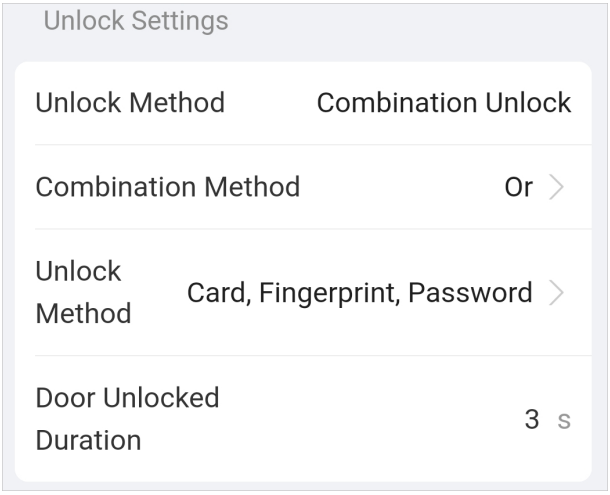


Tabla 4-3 Descripción de los parámetros de control de acceso

Parámetro		**Descripción**
Configuración básica	Nombre	El nombre de la puerta.

Parámetro		Descripción
	Estado de la puerta	Establecer el estado de la puerta. ● Normal: La puerta se desbloqueará y bloqueará según su configuración. ● Siempre abierto: la puerta permanece desbloqueada todo el tiempo. ● Siempre cerrado: la puerta permanece bloqueada todo el tiempo.
	Intervalo de verificación	Si verifica su identidad varias veces dentro de un período establecido, solo se considerará válida la verificación más antigua y la puerta no se abrirá después de la segunda o posteriores. Si la puerta no se abre, deberá esperar el tiempo de verificación configurado antes de volver a intentar verificar su identidad.
Normalmente abierto Período	Plan de Periodo/Vacaciones	Cuando seleccionas**Normal**Puede seleccionar una plantilla de tiempo en la lista desplegable. La puerta permanece abierta o cerrada durante el tiempo definido. ● Cuando el período normalmente abierto entra en conflicto con período normalmente cerrado, período normalmente abierto tiene prioridad sobre el período normalmente cerrado. ● Cuando el período entra en conflicto con el plan de vacaciones, los planes de vacaciones tienen prioridad sobre los períodos.
Normalmente cerrado Período	Plan de Periodo/Vacaciones	
Desbloquear configuraciones	Método de desbloqueo	**Desbloqueo de combinación**por defecto.
	Combinación Método	● O bien: utilice uno de los métodos de desbloqueo seleccionados para abrir la puerta. ● Y: Utilice todos los métodos de desbloqueo seleccionados para abrir la puerta.
	Método de desbloqueo	Seleccione el método de desbloqueo según las capacidades admitidas por el dispositivo.
	Puerta desbloqueada Duración	Configure el tiempo que la puerta permanece abierta. El tiempo predeterminado es de 3 segundos. Si la puerta se abre más tiempo del configurado, se cierra.

Paso 4 Hacer clic**Aplicar**.

4.6.3 Configuración de alarmas

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

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Más**>**Control de acceso**>**Alarma**. Configure los

Paso 3 parámetros de alarma y luego haga clic en**Aplicar**.

Figura 4-12 Configuración de alarma

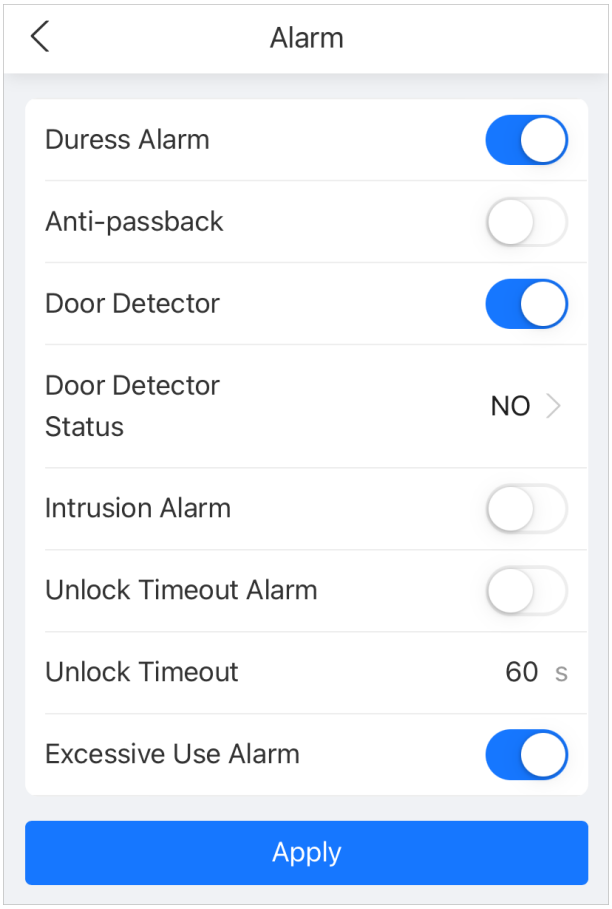


Tabla 4-4 Descripción de los parámetros de alarma

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.

Parámetro	Descripción
Anti-passback	Los usuarios deben verificar su identidad tanto al entrar como al salir; de lo contrario, se activará una alarma. Esto ayuda a evitar que el titular de la tarjeta la entregue a otra persona para acceder. Cuando la función antirretorno está activada, el titular de la tarjeta debe salir del área protegida a través de un lector de salida antes de que el sistema le permita entrar de nuevo. ● Si una persona ingresa después de una autorización y sale sin autorización, se activará una alarma cuando la persona intente ingresar nuevamente y se le negará el acceso al mismo tiempo. ● Si una persona ingresa sin autorización y sale después de la autorización, se activará una alarma cuando la persona intente ingresar nuevamente y se le negará el acceso al mismo tiempo.  Si el dispositivo solo puede conectar una cerradura, la verificación en el dispositivo indica la dirección de entrada y la verificación en el lector de tarjetas externo indica la dirección de salida por defecto. Puede modificar la configuración en la plataforma de administración.
Detector de puerta	Con el detector de puerta conectado a su dispositivo, se puede activar una alarma si las puertas se abren o cierran de forma anormal. El detector de puerta incluye dos tipos: detector NC y detector NO. ● NC: El sensor está en una posición de cortocircuito cuando la puerta o ventana está cerrada. ● NO: Se crea un circuito abierto cuando la ventana o puerta está realmente cerrada.
Alarma de intrusión	Si la puerta se abre de forma anormal, se activará una alarma de intrusión que durará un tiempo definido.  El detector de puerta y la intrusión deben habilitarse al mismo tiempo.
Alarma de tiempo de espera de desbloqueo Desbloquear tiempo de espera	Cuando la puerta permanece desbloqueada durante más tiempo que el tiempo de espera definido, se activará la alarma de tiempo de espera de la puerta y durará el tiempo definido.  El detector de puerta y la función de tiempo de espera de la puerta deben habilitarse al mismo tiempo.
Alarma de uso excesivo	Si se utiliza una contraseña o tarjeta incorrecta 5 veces seguidas en 60 segundos, se activará la alarma por uso excesivo de tarjeta ilegal y durará un tiempo definido.

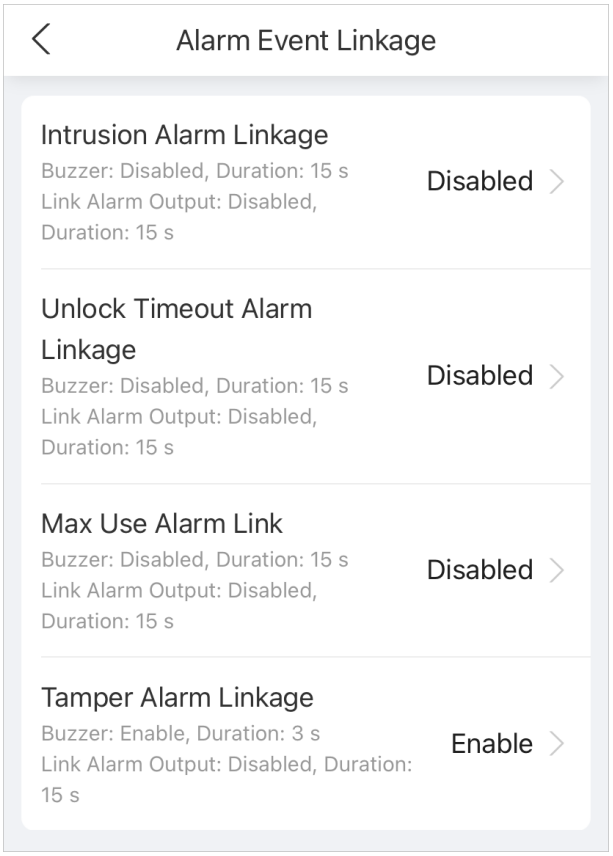
4.6.4 Configuración de la vinculación de eventos de alarma

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Más**>**Control de acceso**>**Vinculación de eventos de alarma**.

Figura 4-13 Vinculación de eventos de alarma



Paso 3 Haga clic en el enlace para configurar el enlace de alarma y luego haga clic en**DE ACUERDO**.

Tabla 4-5 Vinculación de eventos de alarma

Parámetro	Descripción
Vinculación de alarma de intrusión	Si la puerta se abre de forma anormal, se activará una alarma de intrusión. Zumbador: El zumbador suena cuando se activa una alarma de intrusión. Puede configurar la duración de la alarma.
Alarma de tiempo de espera de desbloqueo Enlace	Cuando la puerta permanece desbloqueada durante más tiempo que el tiempo de espera definido, se activará la alarma de tiempo de espera de la puerta y durará el tiempo definido. Zumbador: El zumbador suena cuando se activa la alarma de tiempo de desbloqueo. Puede configurar la duración de la alarma.

Parámetro	Descripción
Enlace de alarma de uso máximo	Si se utiliza una contraseña o tarjeta incorrecta 5 veces seguidas en 60 segundos, se activará la alarma por uso excesivo de tarjeta ilegal y durará un tiempo definido. Timbre: El timbre suena cuando se activa la alarma de uso excesivo. Puede configurar su duración.
Conexión de alarma antimanipulación	La alarma de manipulación se activa cuando alguien intenta dañar físicamente el dispositivo. ● Zumbador: El zumbador suena cuando se activa la alarma antimanipulación. Puede configurar su duración. ● Salida de alarma local: El dispositivo de alarma externo genera alarmas cuando se activa la alarma antimanipulación. Puede configurar la duración de la alarma.

4.6.5 Configuración de los ajustes de la tarjeta

Información de fondo

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Más**>**Control de acceso**>**Configuración de la tarjeta**.

Paso 3 Configure los parámetros de la tarjeta y luego haga clic en**Aplicar**.

Figura 4-14 Configuración de la tarjeta

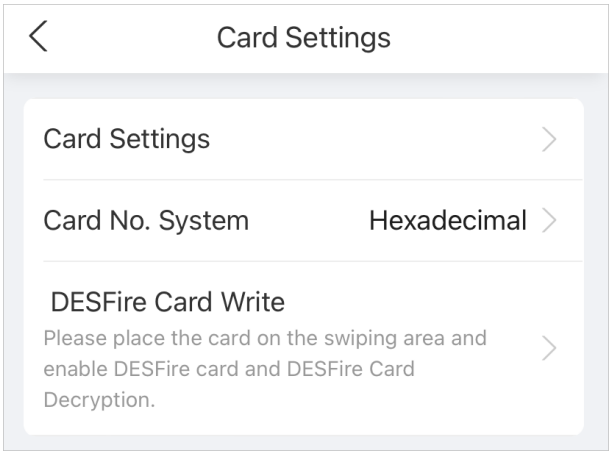


Tabla 4-6 Descripción de los parámetros de la tarjeta

Artículo	Parámetro	Descripción
Configuración de la tarjeta	Tarjeta IC	La tarjeta IC se puede leer cuando esta función está habilitada. Esta función sólo está disponible en modelos seleccionados.

Artículo	Parámetro	Descripción
	Cifrado y verificación de tarjetas IC	La tarjeta cifrada se puede leer cuando esta función está habilitada. Cerciorarse**Tarjeta IC**está habilitado.
	Bloquear tarjetas NFC	Evitar el desbloqueo mediante tarjeta NFC duplicada después de habilitar esta función. • Esta función sólo está disponible en modelos que admiten tarjetas IC. • Cerciorarse**Tarjeta IC**está habilitado. • La función NFC solo está disponible en algunos modelos de teléfonos.
	Habilitar tarjeta Desfire	El dispositivo puede leer el número de tarjeta de la tarjeta Desfire cuando esta función y**Tarjeta IC** se habilitan al mismo tiempo. • Esta función sólo está disponible en modelos que admiten tarjetas IC. • Sólo admite formato hexadecimal.
	Descifrado de la tarjeta Desfire	La información de la tarjeta Desfire se puede leer cuando**Tarjeta IC**,**Habilitar tarjeta Desfire**y **Descifrado de la tarjeta Desfire**se habilitan al mismo tiempo. • Esta función sólo está disponible en modelos que admiten tarjetas IC. • Asegúrese de que la tarjeta Desfire esté habilitada.
Sistema de N.º de Tarjeta	Sistema de N.º de Tarjeta	Seleccione el formato decimal o hexadecimal para el número de tarjeta al conectar un lector de tarjetas Wiegand. El sistema de numeración de tarjeta es el mismo para la entrada y la salida de números de tarjeta.
Escritura de tarjeta DESFire	Número de tarjeta	Coloque la tarjeta en el lector, ingrese el número de tarjeta y luego haga clic**Escribir**para escribir el número de tarjeta en la tarjeta. • La función de tarjeta Desfire debe estar habilitada. • Sólo admite formato hexadecimal. • Admite hasta 8 caracteres.

Paso 4 Hacer clic**Aplicar**.

4.7 Configuración de comunicación

4.7.1 Configuración de TCP/IP

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

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Más**>**Configuración de comunicación**>**TCP/IP**.

Paso 3 Configure los parámetros y luego haga clic en**Aplicar**.

Figura 4-15 TCP/IP

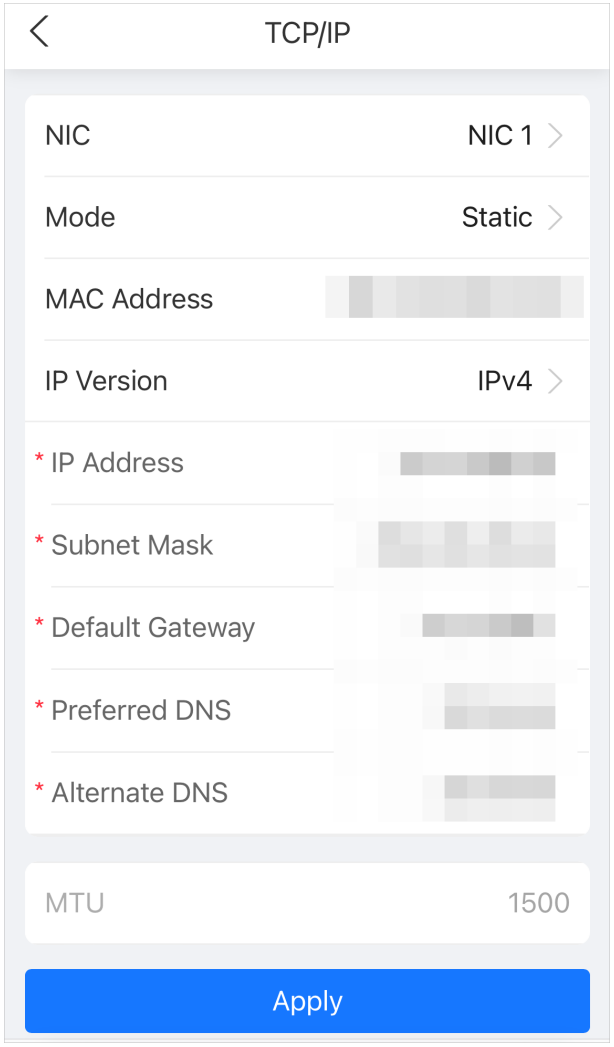


Tabla 4-7 Descripción de TCP/IP

Parámetro	Descripción
Modo	• Estático: ingrese manualmente la dirección IP, la máscara de subred y la puerta de enlace. • DHCP: Protocolo de Configuración Dinámica de Host. Al activar DHCP, se le asignará automáticamente al dispositivo una dirección IP, una máscara de subred y una puerta de enlace.
Dirección MAC	Dirección MAC del dispositivo.
Versión IP	IPv4 o IPv6.
Dirección IP	Si configura el modo en**Estático**, configure la dirección IP, la máscara de subred y la puerta de enlace. • La dirección IPv6 se representa en hexadecimal. • La versión IPv6 no requiere configurar máscaras de subred. • La dirección IP y la puerta de enlace predeterminada deben estar en el mismo segmento de red.
Máscara de subred	
Puerta de enlace predeterminada	
DNS preferido	Establecer la dirección IP del servidor DNS preferido.
DNS alternativo	Establecer la dirección IP del servidor DNS alternativo.
Unidad de tratamiento de datos móviles (MTU)	La MTU (Unidad Máxima de Transmisión) se refiere al tamaño máximo de datos que se puede transmitir en un solo paquete de red en redes informáticas. Un valor de MTU mayor puede mejorar la eficiencia de la transmisión de la red al reducir la cantidad de paquetes y la sobrecarga asociada. Si un dispositivo en la ruta de red no puede procesar paquetes de un tamaño específico, puede producirse fragmentación de paquetes o errores de transmisión. En redes Ethernet, el valor de MTU habitual es de 1500 bytes. Sin embargo, en ciertos casos, como al usar PPPoE o VPN, pueden requerirse valores de MTU menores para cumplir con los requisitos de protocolos o servicios de red específicos. A continuación, se recomiendan los valores de MTU: • 1500: Valor máximo para paquetes Ethernet, también el valor predeterminado. Esta configuración es típica para conexiones de red sin PPPoE ni VPN, así como para algunos routers, adaptadores de red y switches. • 1492: Valor óptimo para PPPoE • 1468: Valor óptimo para DHCP. • 1450: Valor óptimo para VPN.

4.7.2 Configuración de Wi-Fi

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Más**>**Configuración de comunicación**>**Wi-Fi**

Paso 3 Encienda el Wi-Fi.

Se muestran todas las conexiones WiFi disponibles.

- La función Wi-Fi está disponible en modelos seleccionados.
- No se pueden habilitar Wi-Fi y Wi-Fi AP al mismo tiempo.

Paso 4 Haga clic en Wi-Fi y luego ingrese la contraseña.

El wifi está conectado

Operaciones relacionadas

- DHCP: Seleccione el**DHCP**modo y haga clic**Aplicar**, al dispositivo se le asignará automáticamente una dirección Wi-Fi.
- Estático: Seleccione el**Estático**modo, ingrese manualmente una dirección Wi-Fi y luego haga clic en**Aplicar**, el dispositivo se conectará al Wi-Fi.

4.7.3 Configuración del punto de acceso Wi-Fi

- La función Wi-Fi está disponible en modelos seleccionados.
- No se pueden habilitar Wi-Fi y Wi-Fi AP al mismo tiempo.

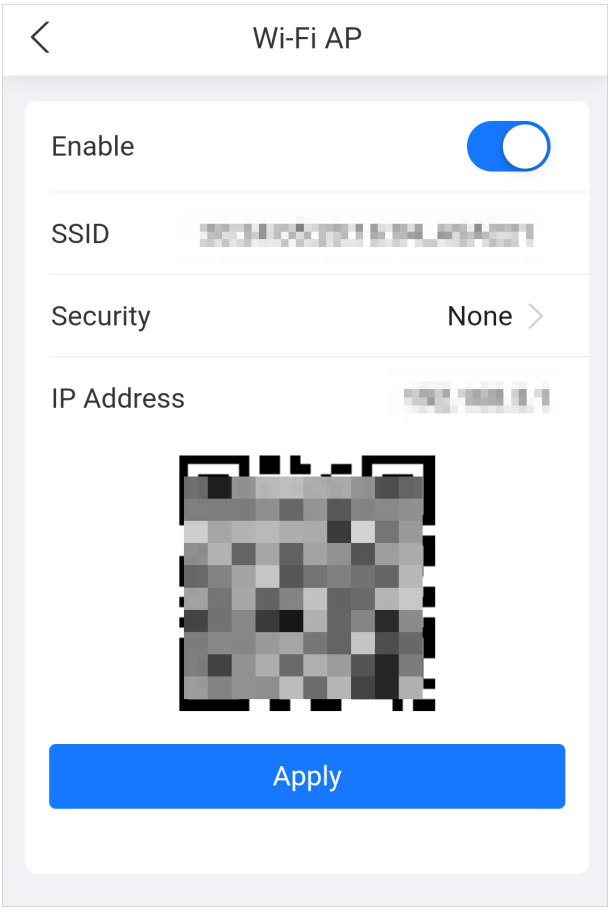
Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Más**>**Configuración de comunicación**>**Punto de acceso**

Paso 3 **Wi-Fi**Habilite la función y luego haga clic en**Aplicar**.

Figura 4-16 Punto de acceso Wi-Fi



4.7.4 Configuración del servicio en la nube

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Más**>**Configuración de comunicación**>**Servicio en la nube**.

Paso 3 Activa la función de servicio en la nube.

El servicio en la nube se conecta si el P2P y el PaaS están conectados. Haga clic

Paso 4 en**Aplicar**.

4.7.5 Configuración del registro automático

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Más**>**Configuración de red**>**Registro automático**.

Paso 3 Habilite la función de registro automático, configure los parámetros y luego haga clic en**Aplicar**.

Figura 4-17 Registro automático

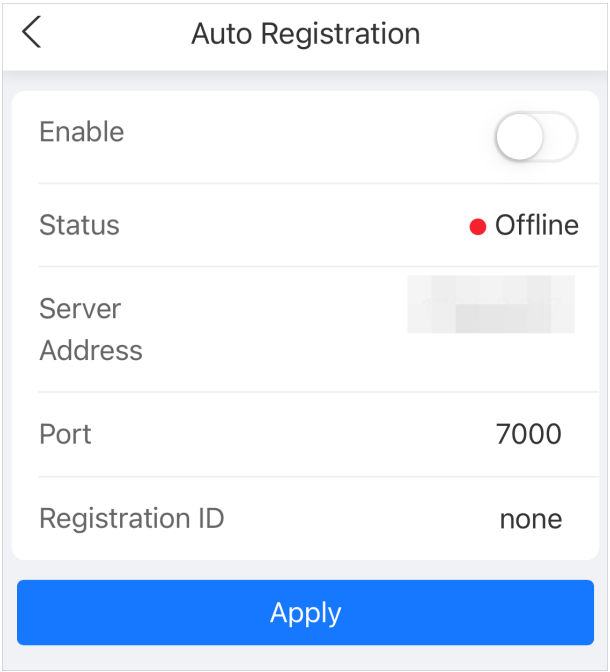


Tabla 4-8 Descripción del registro automático

Parámetro	Descripción
Estado	Muestra el estado de la conexión del registro automático.
Dirección del servidor	La dirección IP o el nombre de dominio del servidor.
Puerto	El puerto del servidor que se utiliza para el registro automático.
ID de registro	El ID de registro del dispositivo (definido por el usuario). Para añadir el dispositivo a la administración, introduzca el ID de registro en la plataforma.

4.7.6 Configuración de Wiegand

Procedimiento

Paso 1 Inicie sesión en la página web.

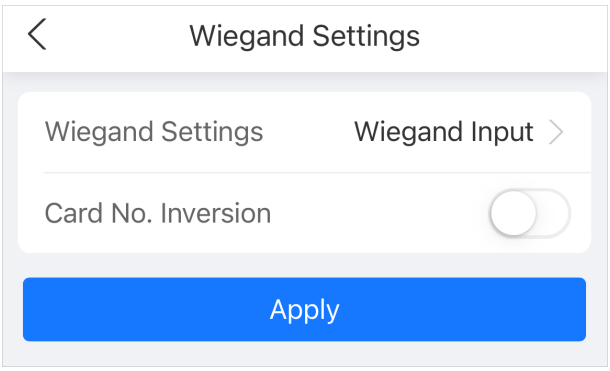
Paso 2 Seleccionar**Más**>**Configuración de comunicación**>**Wiegand**.

Paso 3 Seleccione un tipo de Wiegand, configure los parámetros y luego haga clic en**Aplicar**.

- Seleccionar**Entrada Wiegand**cuando conecta un lector de tarjetas externo al dispositivo.

  Cuando el dispositivo se conecta a un dispositivo de terceros a través del puerto de entrada Wiegand, y el número de tarjeta que lee el dispositivo está en orden inverso al número real de la tarjeta. En este caso, puede activar**Tarjeta n.° Inversión**función.

  Figura 4-18 Entrada Wiegand



- Seleccionar**Salida Wiegand**cuando el dispositivo funciona como lector de tarjetas y necesita conectarlo a otro controlador de acceso.

Figura 4-19 Salida Wiegand

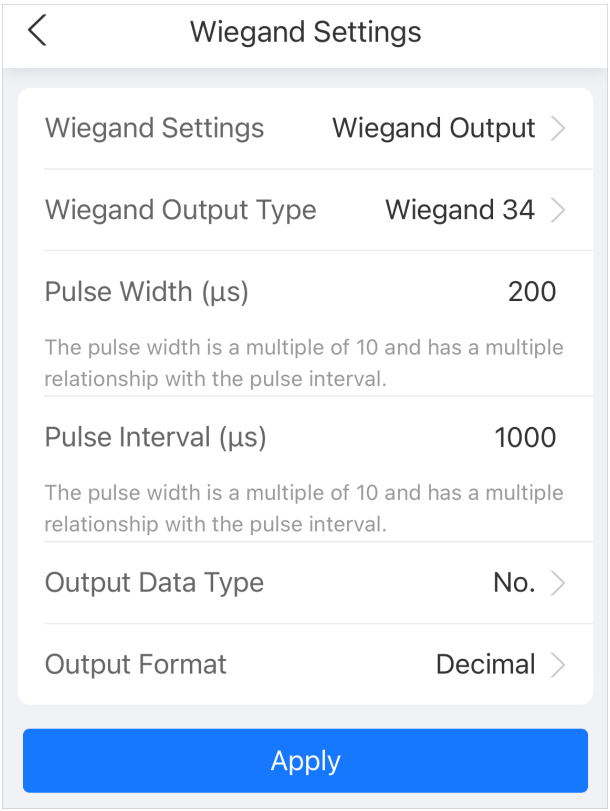


Tabla 4-9 Descripción de la salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	Seleccione un formato Wiegand para leer números de tarjeta o números de identificación. ◇ **Wiegand26**:Lee 3 bytes o 6 dígitos. ◇ **Wiegand34**:Lee 4 bytes u 8 dígitos. ◇ **Wiegand66**:Lee 8 bytes o 16 dígitos.
Ancho de pulso	Introduzca el ancho de pulso y el intervalo de pulso de la salida Wiegand.
Intervalo de pulso	
Tipo de datos de salida	Seleccione el tipo de datos de salida. ◇ **No.**:Genera datos según el ID del usuario. El formato de los datos es hexadecimal o decimal. ◇ **Número de tarjeta**:Genera datos basados en el primer número de tarjeta del usuario.

4.7.7 Configuración de RS-485

Configure los parámetros RS-485 si conecta un dispositivo externo al puerto RS-485.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Más**>**Configuración de comunicación**>**Configuración RS-485**.

Paso 3 Configure los parámetros y luego haga clic en**Aplicar**.

Figura 4-20 Configuración RS-485

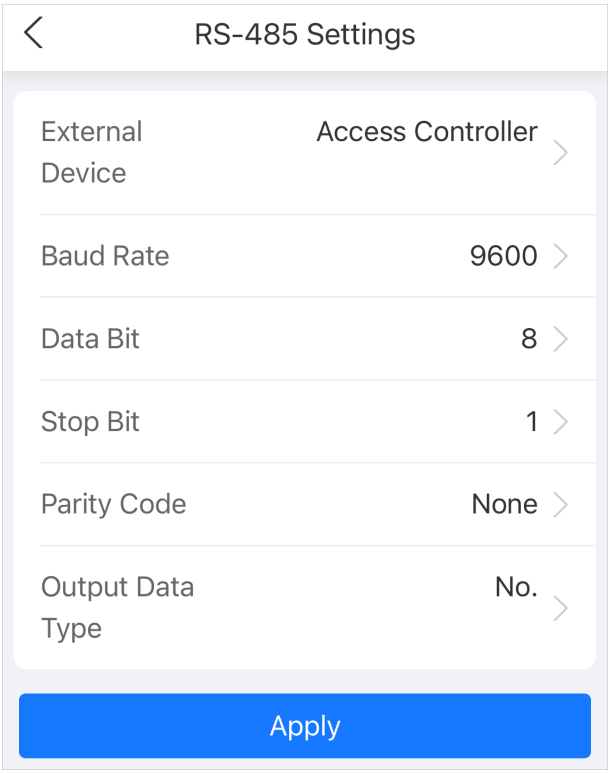


Tabla 4-10 Descripción de los parámetros RS-485

Parámetro	Descripción
Dispositivo externo	● Controlador de acceso Seleccionar**Controlador de acceso**cuando el dispositivo funciona como un lector de tarjetas y envía datos a otros controladores de acceso externos para controlar el acceso. ◇ **Autenticación por dispositivo local**:La identidad se verifica tanto en el dispositivo como en el controlador. ◇ **Autenticación por parte del controlador**:La identidad se verifica únicamente en el controlador. ● Lector de tarjetas: el dispositivo funciona como un controlador de acceso y se conecta a un lector de tarjetas externo. ● Lector (OSDP): El dispositivo está conectado a un lector de tarjetas basado en el protocolo OSDP. ● Seguridad de control de puerta: El botón de salida de la puerta, la cerradura y el enlace de incendio no son efectivos después de que se habilita el módulo de seguridad.
Tasa de Baud	Seleccione la velocidad en baudios. La velocidad predeterminada es 9600.
Bit de datos	El número de bits utilizado para transmitir los datos en una comunicación serial. Representa los dígitos binarios que contienen la información transmitida.

Parámetro	Descripción
Bit de parada	Un bit enviado después de los datos y los bits de paridad opcionales para indicar el final de una transmisión de datos. Permite al receptor prepararse para el siguiente byte de datos y proporciona sincronización en el protocolo de comunicación.
Código de paridad	Un bit adicional que se envía después de los bits de datos para detectar errores de transmisión. Ayuda a verificar la integridad de los datos transmitidos al garantizar un número específico de bits lógicos altos o bajos.
Tipo de datos de salida	Cuando configure el dispositivo externo como**Controlador de acceso**. ● Número de tarjeta: emite datos basados en el número de tarjeta cuando los usuarios pasan la tarjeta para desbloquear la puerta; emite datos basados en el primer número de tarjeta del usuario cuando utilizan otros métodos de desbloqueo. ● No.: Genera datos basados en el ID del usuario.

4.8 Visualización de registros

Ver registros como registros del sistema, registros de desbloqueo y registros de alarmas.

4.8.1 Registros del sistema

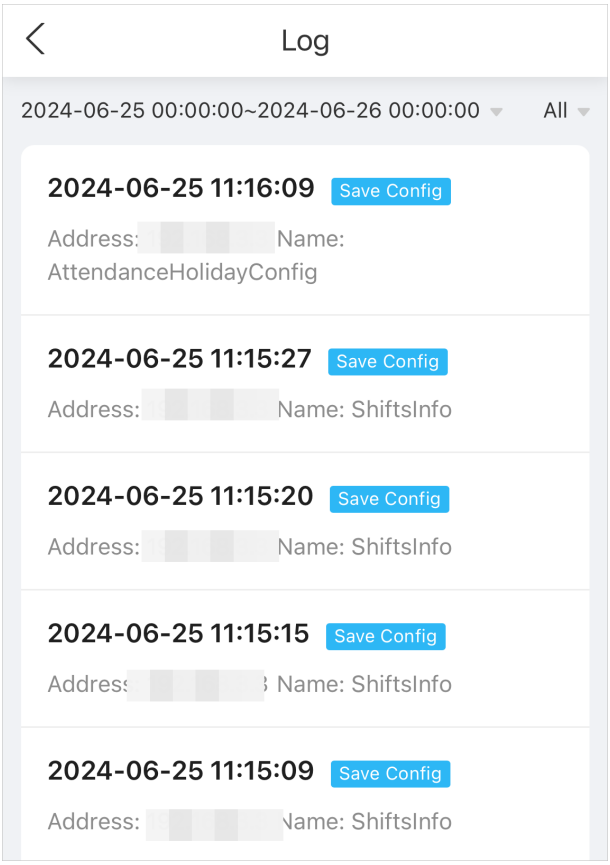
Ver y buscar registros del sistema.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccione**Más**>**Registro**>**Registro**.

Figura 4-21 Registros



4.8.2 Desbloquear registros

Buscar registros de desbloqueo.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Más**>**Registro**>**Desbloquear registros**.

Paso 3 Haga clic en el registro para ver los detalles.

4.8.3 Registros de alarmas

Ver registros de alarmas.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccione**Más**>

Paso 2 **Registro**>**Registro de alarmas**.

5 Configuración inteligente de PSS Lite

Esta sección explica cómo administrar y configurar el dispositivo mediante Smart PSS Lite. Para más información, consulte el manual del usuario de Smart PSS Lite.

5.1 Instalación

Contacte con el soporte técnico o visite el sitio web oficial para obtener el SmartPSS Lite. Si obtiene el paquete de software del SmartPSS Lite, instálelo y ejecútelo según las instrucciones de la página.

5.2 Inicialización

Inicialice SmartPSS Lite cuando inicie sesión por primera vez, incluida la configuración de una contraseña para iniciar sesión y preguntas de seguridad para restablecer la contraseña.

Procedimiento

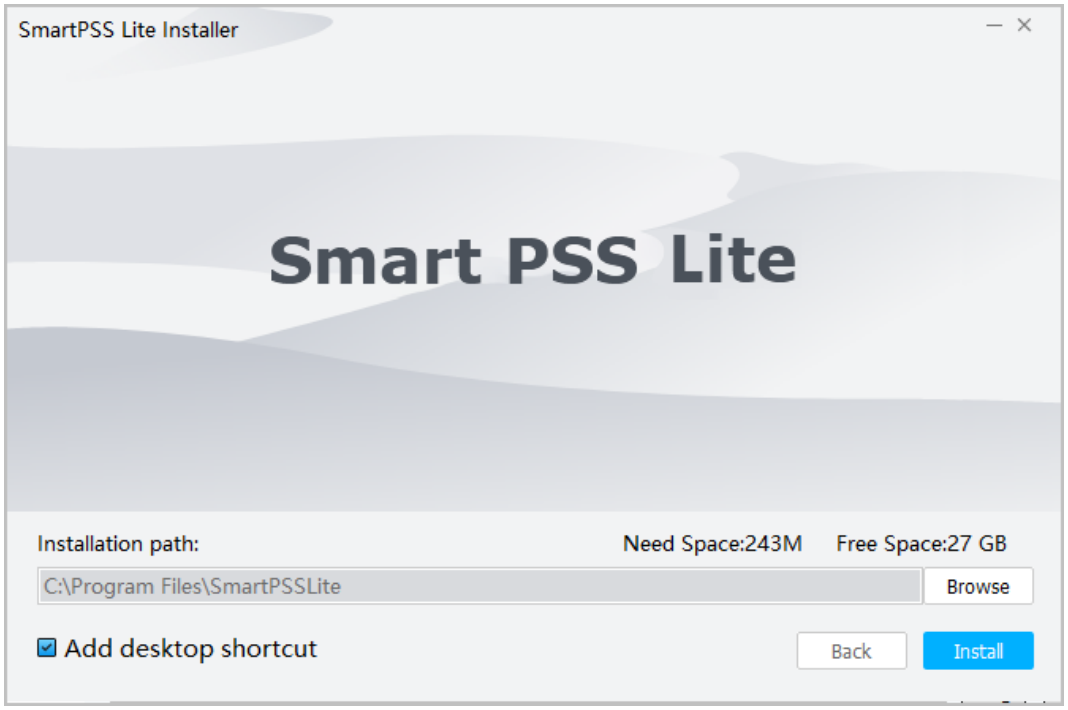
Paso 1 Haga doble clic en SmartPSSLite.exe.

Paso 2 Seleccione el idioma de la lista desplegable, seleccione**He leído y acepto el acuerdo de software.**,y luego haga clic**Próximo**.

Figura 5-1 Seleccionar idioma

Paso 3 Hacer clic**Navegar**para seleccionar la ruta de instalación y luego haga clic en**Instalar**.

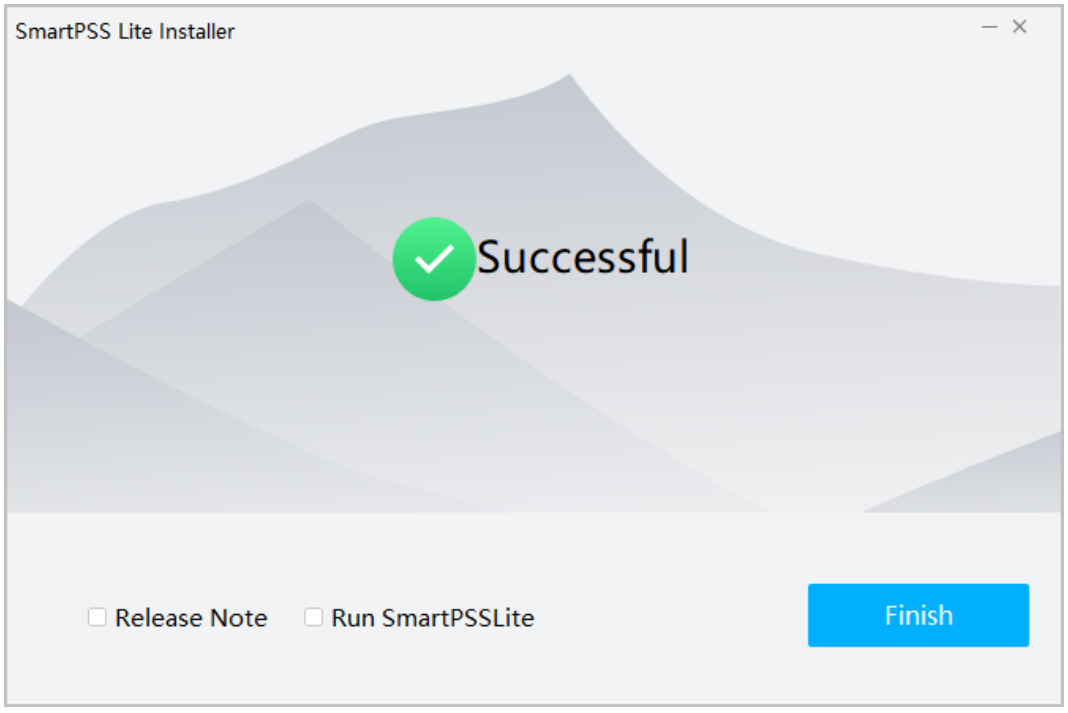
Figura 5-2 Seleccionar ruta de instalación



Paso 4 Hacer clic**Finalizar**para completar la instalación.

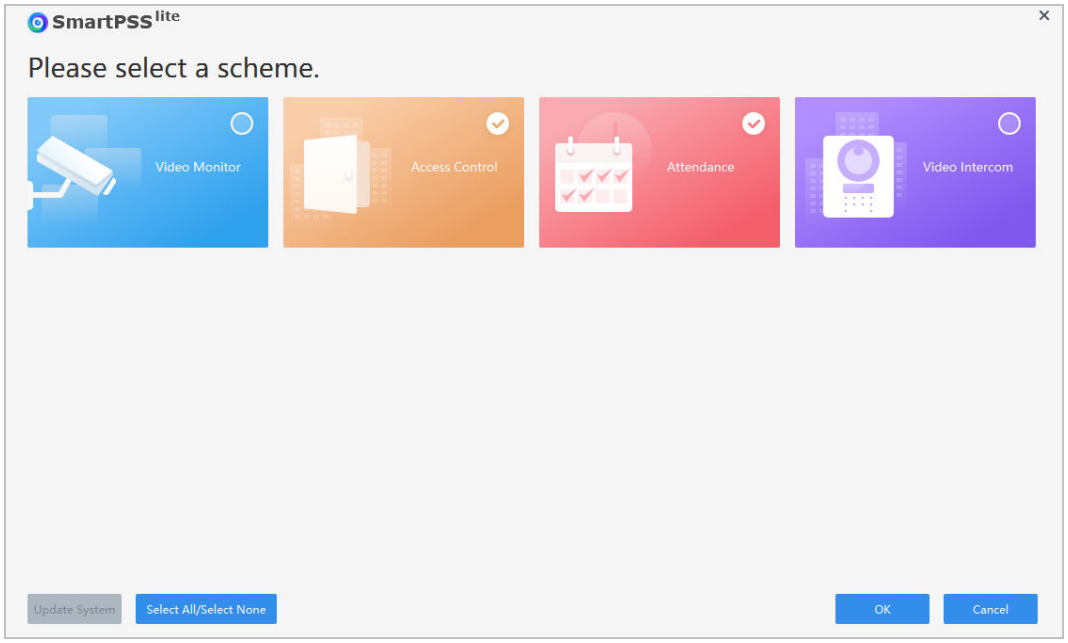
Seleccionar**Ejecutar SmartPSSLite**para iniciar SmartPSS Lite.

Figura 5-3 Instalación completada



Paso 5 Seleccione las escenas de aplicación que desea agregar y luego haga clic en**DE ACUERDO**.

Figura 5-4 Seleccionar escenas de aplicación



Paso 6 Hacer clic**Aceptar y continuar**estar de acuerdo**Acuerdo de licencia de software**y**Política de privacidad del producto**.

Paso 7 Establecer contraseña en el**Inicialización**página y luego haga clic en**Próximo**.

Figura 5-5 Establecer contraseña

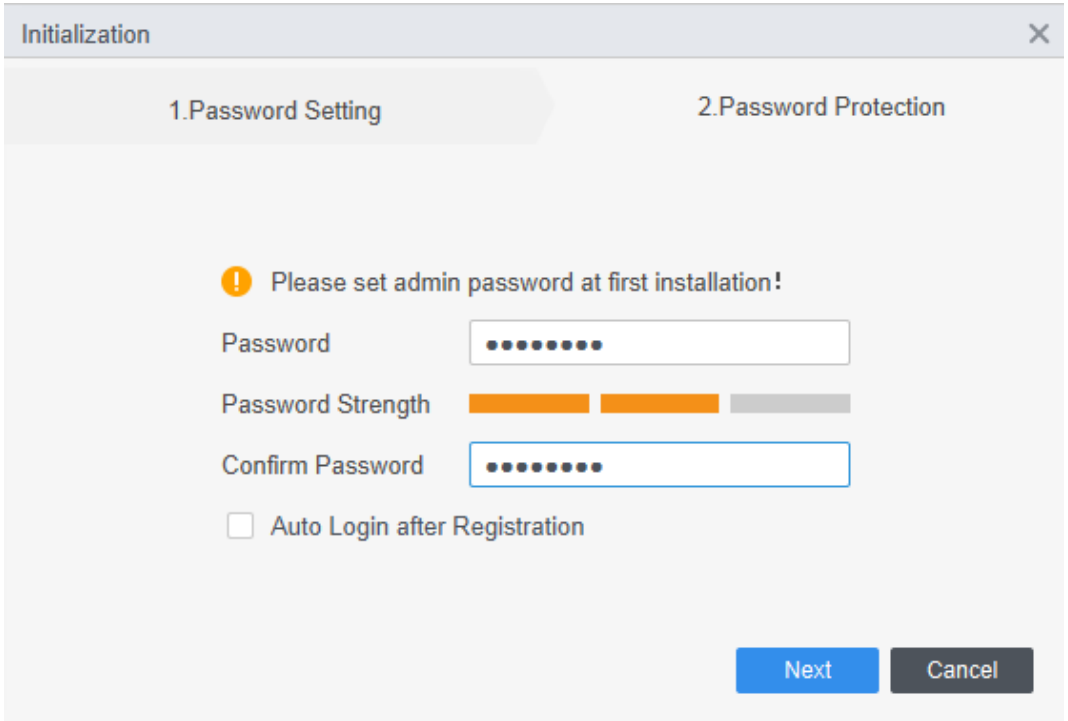
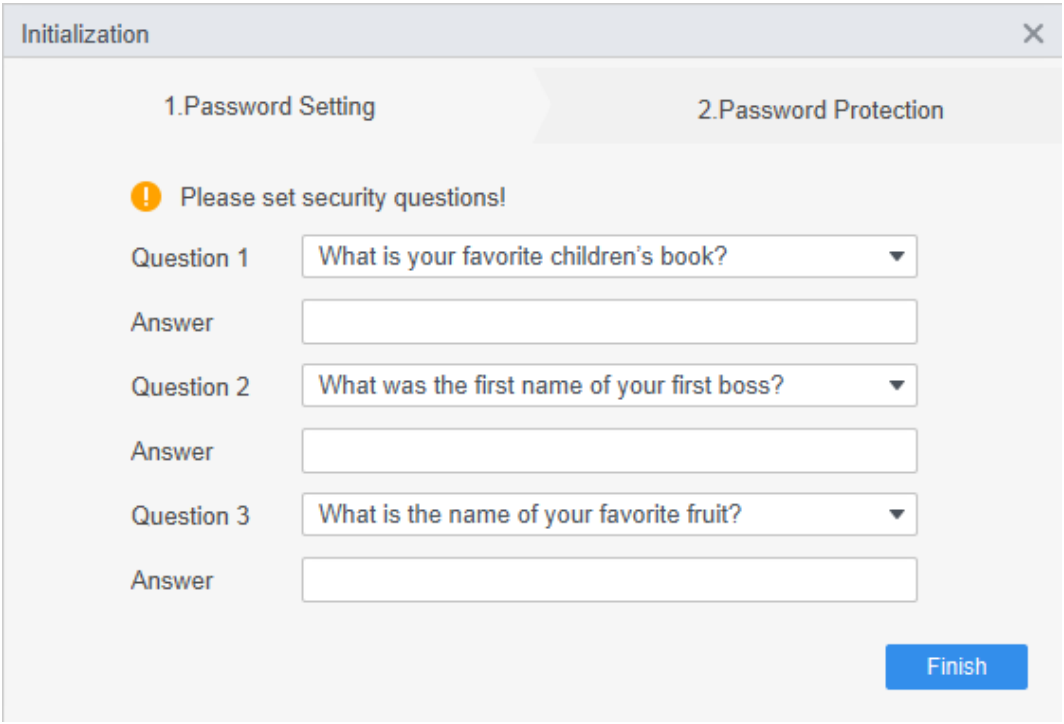


Tabla 5-1 Parámetros de inicialización

Parámetro	Descripción
Contraseña	La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos dos tipos de caracteres: mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &).
Fuerza de la contraseña	Muestra la eficacia de una contraseña contra intentos de adivinación o ataques de fuerza bruta. El verde indica que la contraseña es suficientemente segura y el rojo, que es menos segura. Establezca una contraseña de alto nivel de seguridad según la solicitud de seguridad.
confirmar Contraseña	Ingrese la contraseña nuevamente para confirmarla.
Inicio de sesión automático después del registro	Permitir**Inicio de sesión automático después del registro**para que SmartPSS Lite inicie sesión automáticamente después de la inicialización; de lo contrario, se muestra la página de inicio de sesión.

Paso 8 Establezca preguntas de seguridad y luego haga clic en**Finalizar**.

Figura 5-6 Establecer preguntas de seguridad



5.3 Agregar dispositivos

Hay varios métodos disponibles para agregar dispositivos.

- Buscar automáticamente
- Añadiendo manualmente
- Importar en lotes

5.3.1 Agregar dispositivo mediante búsqueda

Puede agregar varios dispositivos buscándolos en el segmento de red actual o en otros segmentos de red.

Información de fondo

Le recomendamos que agregue dispositivos mediante la búsqueda cuando desee agregar varios dispositivos que estén en el mismo segmento de red, o cuando desee agregar dispositivos con un segmento de red conocido pero no conozca la dirección IP exacta de los dispositivos.

Procedimiento

Paso 1 En la página de inicio, haga clic en**Dispositivos**.

Paso 2 Seleccione un método de búsqueda.

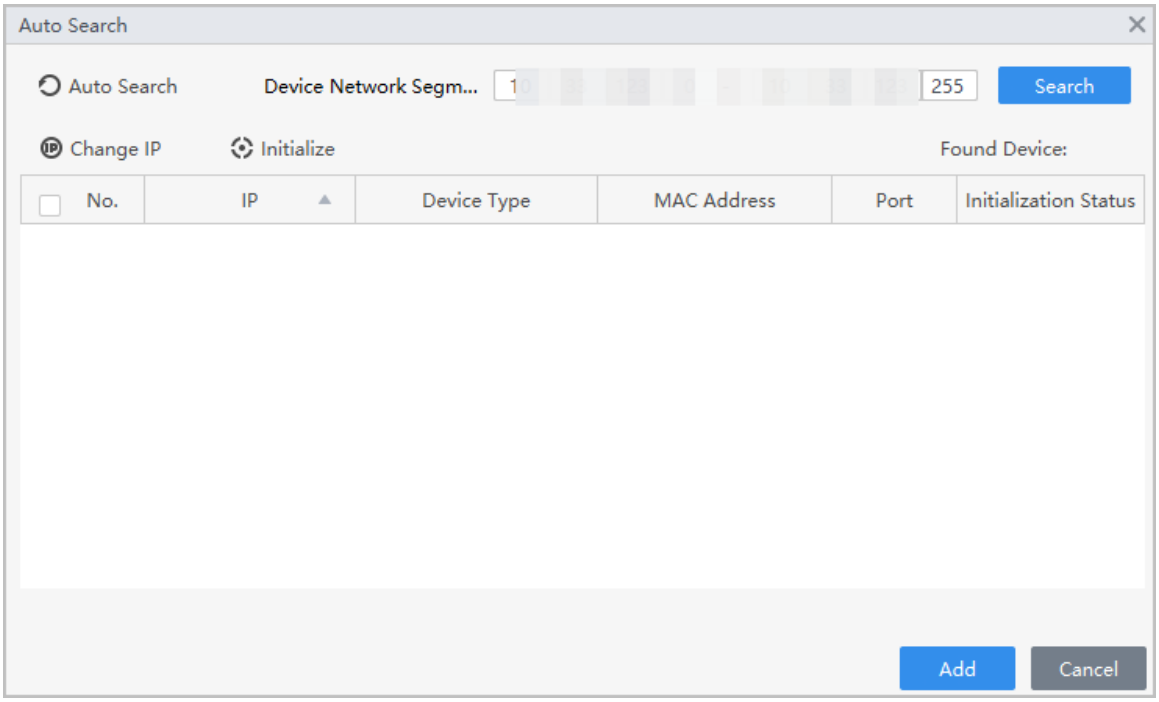
- Búsqueda automática: Ingrese el nombre de usuario y la contraseña del dispositivo. El sistema buscará automáticamente dispositivos que estén en la misma red que su computadora.
- Segmento de red del dispositivo: Introduzca el nombre de usuario y la contraseña del dispositivo, y luego defina la IP inicial y la IP final. El sistema buscará automáticamente dispositivos en este rango de IP.

Paso 3 Hacer clic**Búsqueda automática**.

Paso 4 Ingrese un rango de IP y luego haga clic**Buscar**.

El sistema busca automáticamente dispositivos en este rango de IP. También puede hacer clic en **Búsqueda automática**para buscar automáticamente dispositivos en la misma red a la que está conectada su computadora.

Figura 5-7 Búsqueda de dispositivos



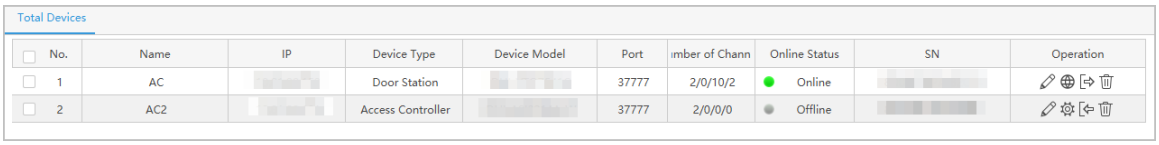
Paso 5 Seleccione los dispositivos y luego haga clic en**Agregar**.

Paso 6 Ingrese el nombre de usuario y la contraseña de inicio de sesión de los dispositivos seleccionados y luego haga clic en**DE ACUERDO**Ingrese

Paso 7 el nombre de usuario y la contraseña de inicio de sesión y luego haga clic en**DE ACUERDO**.

Los dispositivos se agregarán a la plataforma.

Figura 5-8 Dispositivos agregados



- :Cambiar la información del dispositivo.
- :va a la**Configuración del dispositivo**Módulo en la plataforma.
- :Va a la página web del dispositivo.
- : Cierre la sesión del dispositivo y el estado del dispositivo pasará a ser**Desconectado**.
- : Inicie sesión en el dispositivo y el estado del mismo se mostrará**En línea**.
- :Eliminar el dispositivo.

Operaciones relacionadas

- Cambiar IP uno por uno: Seleccione un dispositivo y luego haga clic en**Cambiar IP**para cambiar la IP del dispositivo.
- Cambiar IP en lotes: seleccione varios dispositivos y luego haga clic en**Cambiar**para cambiar su IP.

  Ingrese la IP inicial y el sistema asignará automáticamente una IP a los dispositivos incrementando la IP en una unidad según la IP inicial. Por ejemplo, si la IP inicial es 10.XX.XXX.52, las siguientes IP de los dispositivos serán 10.XX.XXX.53, 10.XX.XXX.54 y superiores.
- Inicializar dispositivos: Haga clic en**Inicializar**para inicializar dispositivos.

  Solo se admite la activación de dispositivos que estén en el mismo segmento de red que su computadora.

5.3.2 Agregar dispositivos uno por uno

Si ya conoce la dirección IP de un dispositivo, puede agregarlo manualmente a la plataforma.

Procedimiento

Paso 1 En la página de inicio, haga clic en**Dispositivos**.

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

Figura 5-9 Agregar dispositivos

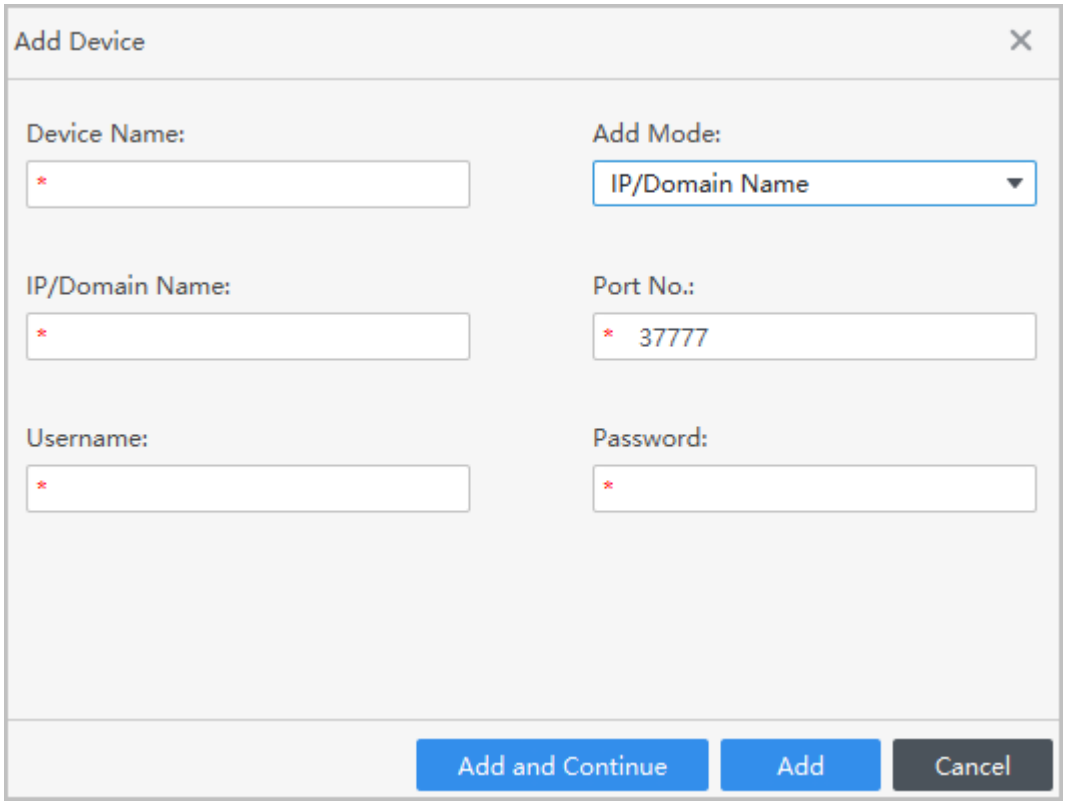


Tabla 5-2 Parámetros de adición de IP

Parámetro	Descripción
Nombre del dispositivo	El nombre del dispositivo.
Modo Agregar	• Nombre de dominio/IP: agregue dispositivos a través de la dirección IP. • SN (Disponible en dispositivos que admiten P2P): agrega dispositivos a través de su número de serie.
Nombre de dominio/IP	Introduzca la dirección IP o el nombre de dominio del dispositivo.
Puerto No.	Introduzca el número de puerto (80 por defecto).
Nombre de usuario	Introduzca el nombre de usuario y la contraseña del dispositivo.
Contraseña	

Paso 3 Hacer clic**Agregar**.

También puedes hacer clic**Agregar y continuar**para agregar más dispositivos.

5.3.3 Importación de dispositivos en lotes

Puede exportar la información del dispositivo y luego importarla a otra plataforma para agregarlos por lotes. Le recomendamos agregar dispositivos importándolos cuando no estén en el mismo segmento de red.

Prerrequisitos

Se exportó un archivo .xml con la información del dispositivo. Para más detalles, consulte el manual del usuario correspondiente.

Procedimiento

Paso 1 En la página de inicio, haga clic en**Dispositivos**.

Paso 2 Hacer clic**Importar**para importar el archivo a la plataforma.

Los dispositivos se iniciarán sesión automáticamente después de agregarlos.

5.4 Gestión de usuarios

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

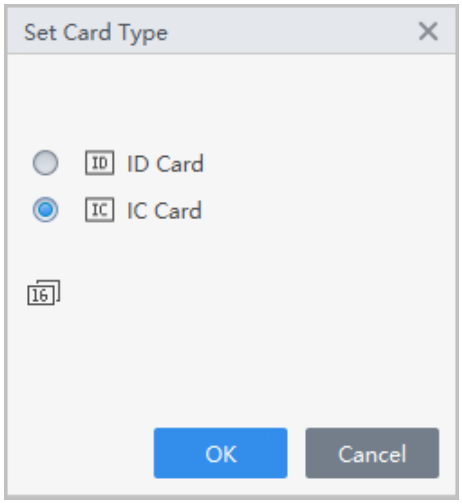
5.4.1 Configuración del tipo de tarjeta

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

Antes de emitir la tarjeta, configure el tipo de tarjeta. Por ejemplo, si se trata de un documento de identidad, seleccione el tipo.

El sistema usa el número de tarjeta hexadecimal por defecto. Haga clic en el para cambiarlo a tarjeta decimal número.

Figura 5-10 Establecer tipo de tarjeta



5.4.2 Configuración del tipo de tarjeta

Configure el tipo de tarjeta antes de asignarlas a los usuarios. Por ejemplo, si la tarjeta asignada es una tarjeta de identificación, configure el tipo como tarjeta de identificación.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

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

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

Paso 4 Hacer clic**DE ACUERDO**.

5.4.3 Agregar usuarios

5.4.3.1 Agregar personal uno por uno

Procedimiento

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

Paso 2 Ingrese información básica de la persona.

1. Seleccionar**Información básica**.
2. Agregar información básica del personal.
3. Tome una instantánea o cargue una imagen y luego haga clic en**Finalizar**.
4. Configure los métodos de verificación de identidad.

- Establecer contraseña

  Hacer clic**Agregar**Para agregar la contraseña. Para controladores de acceso de segunda generación, configure contraseñas personales; para otros dispositivos, configure contraseñas de tarjeta. Las nuevas contraseñas deben tener entre 6 y 8 dígitos.

- Configurar tarjeta

  a. Haga clic para seleccionar**Dispositivo**o**emisor de la tarjeta**como lector de tarjetas.

  b. Agregar tarjeta.

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

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

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

- Configurar huella digital

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

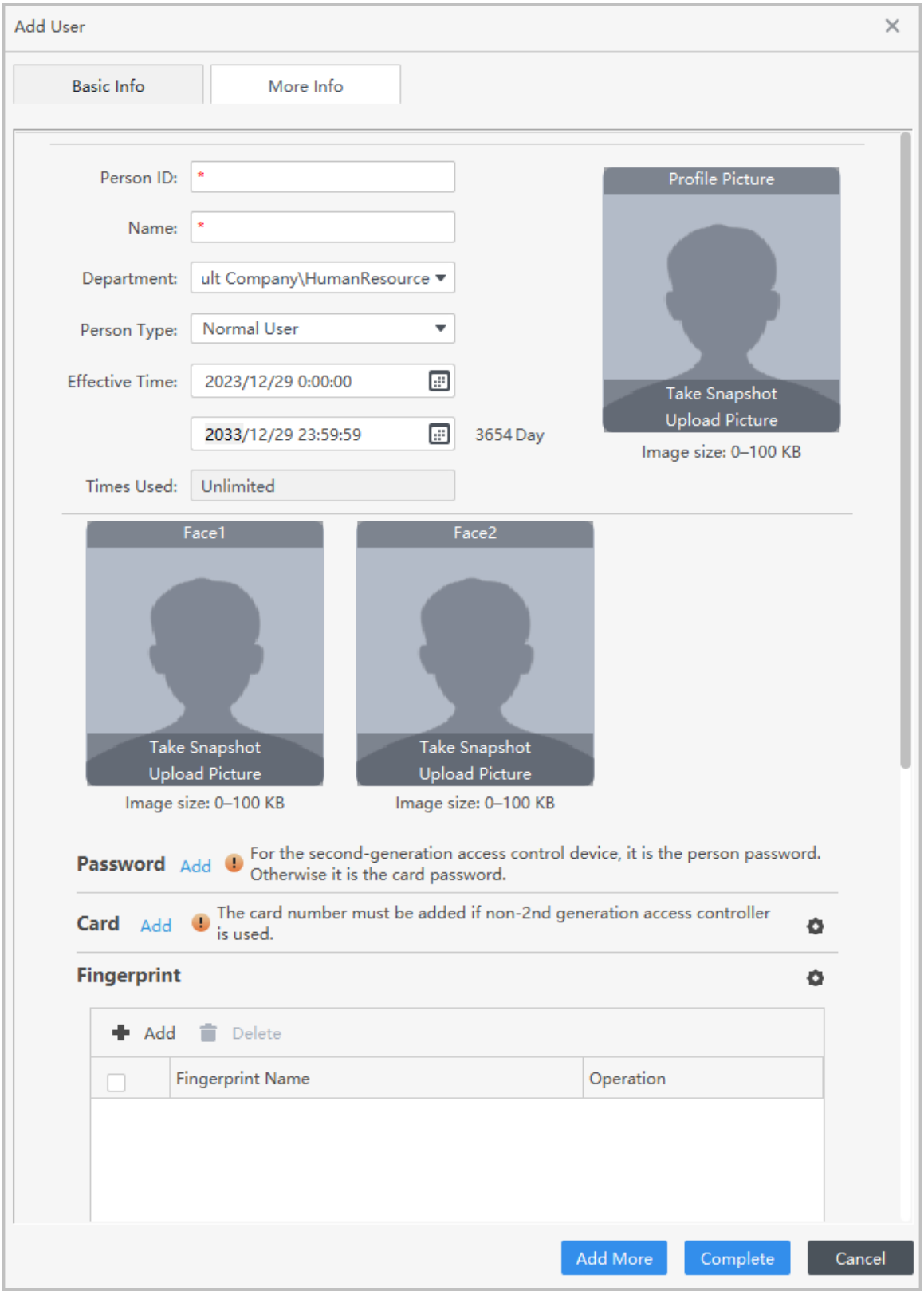
  b. Agregar huella dactilar. Seleccionar**Agregar**>**Agregar huella digital**y luego presione el dedo sobre el escáner tres veces seguidas.

- Configurar códigos de características

  a. Haga clic en y luego seleccione un dispositivo.

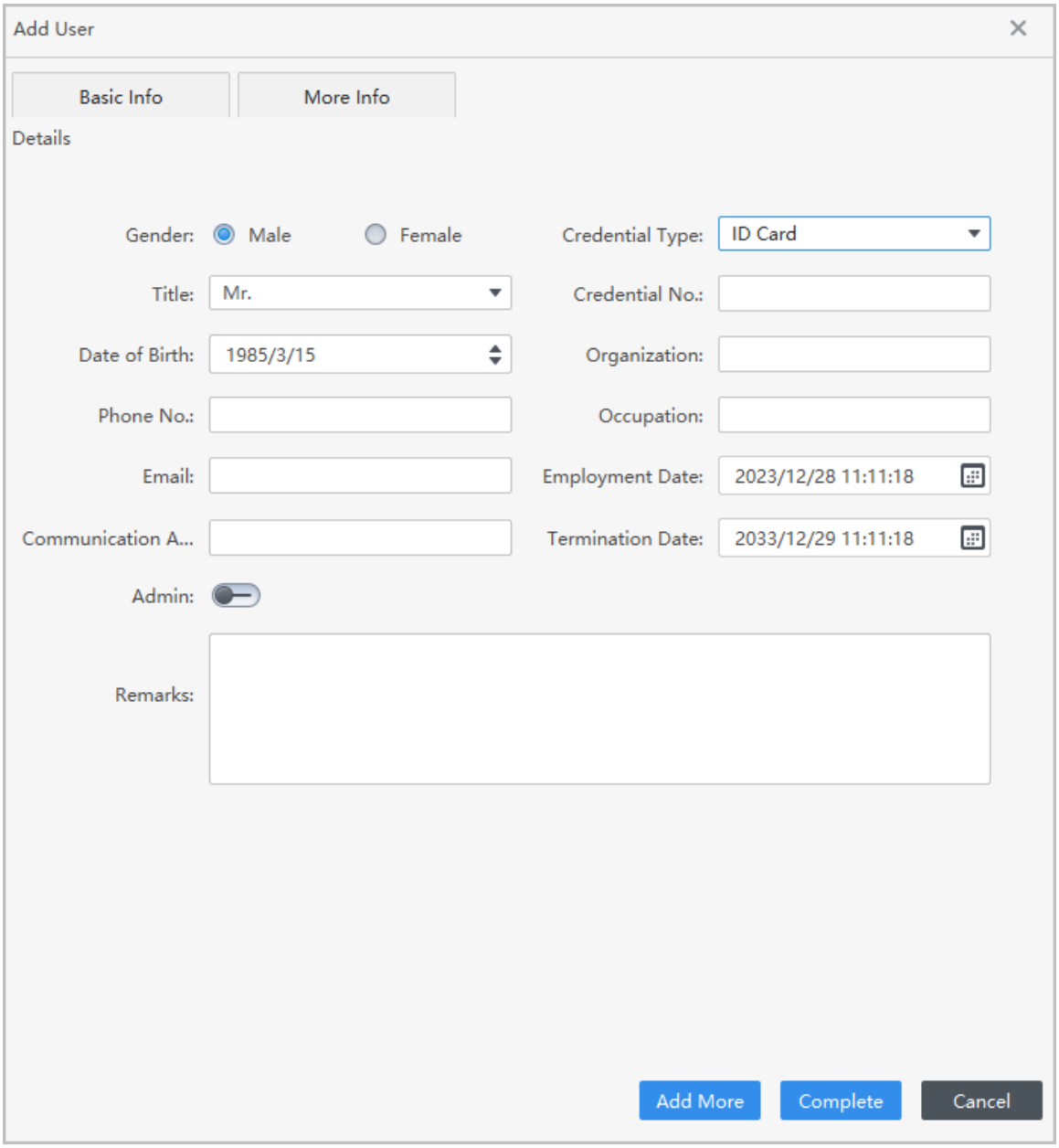
  b. Haga clic**Extracto**y luego el dispositivo extraerá las características de la cara.

Figura 5-11 Agregar información básica



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

Figura 5-12 Agregar más información



Paso 4 Hacer clic**Completo**.

Después de terminar de agregar, puedes hacer clic en Para modificar información o agregar detalles en la lista la persona.

Operaciones relacionadas

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

5.4.3.2 Adición de personal en lotes

Procedimiento

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

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

Paso 3 Configure el departamento, la fecha de vigencia y la fecha de vencimiento de la tarjeta. Haga

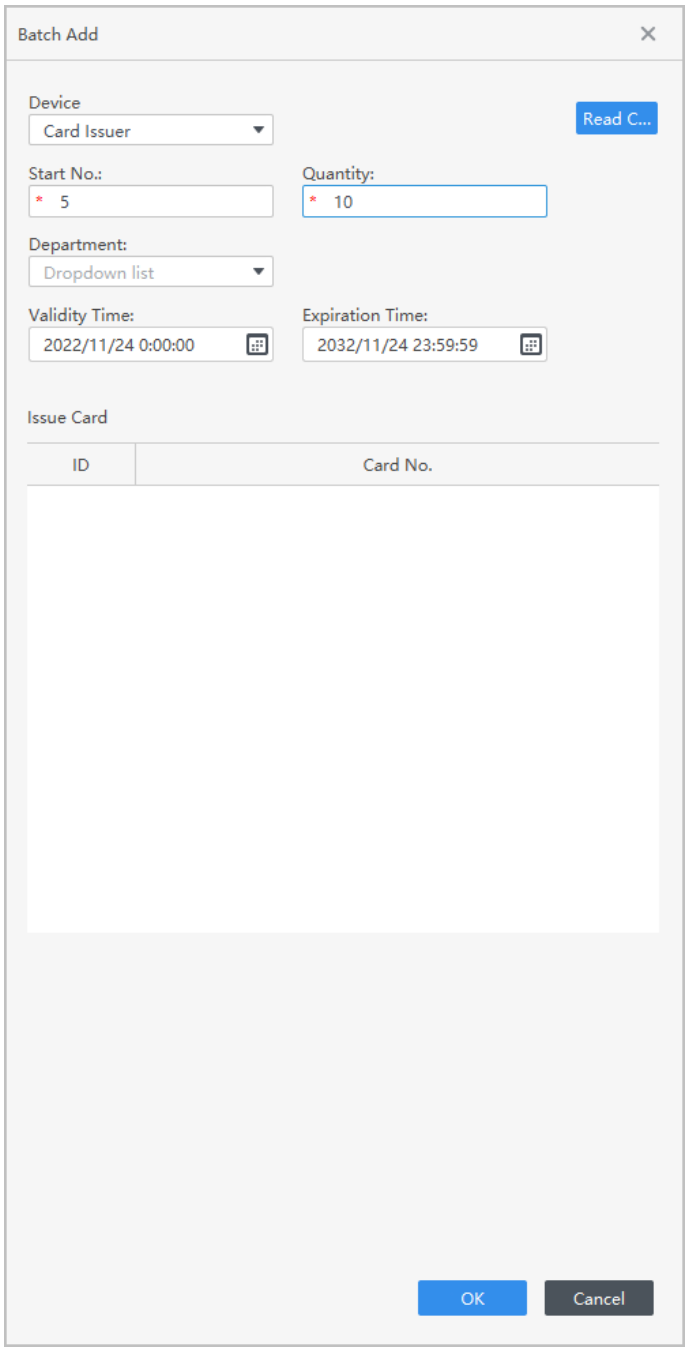
Paso 4 clic.**Leer la tarjeta n.º**.

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

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

Paso 6 **ACUERDO**.

Figura 5-13 Agregar personal en lotes



5.4.4 Asignación de permisos de acceso

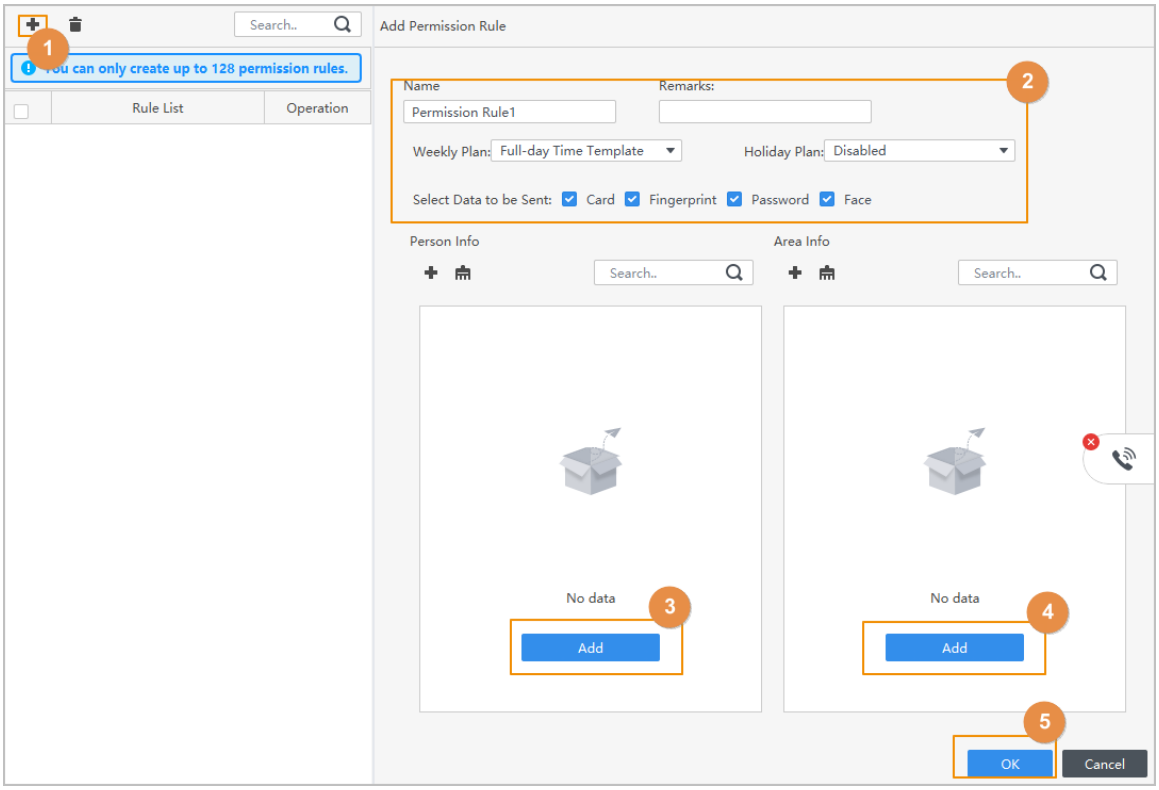
El método para configurar el permiso para el departamento y para el personal es similar, y aquí se utiliza el departamento como ejemplo.

Procedimiento

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

Paso 2 Haga clic para agregar una regla de permiso.

Figura 5-14 Asignar reglas de permisos



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

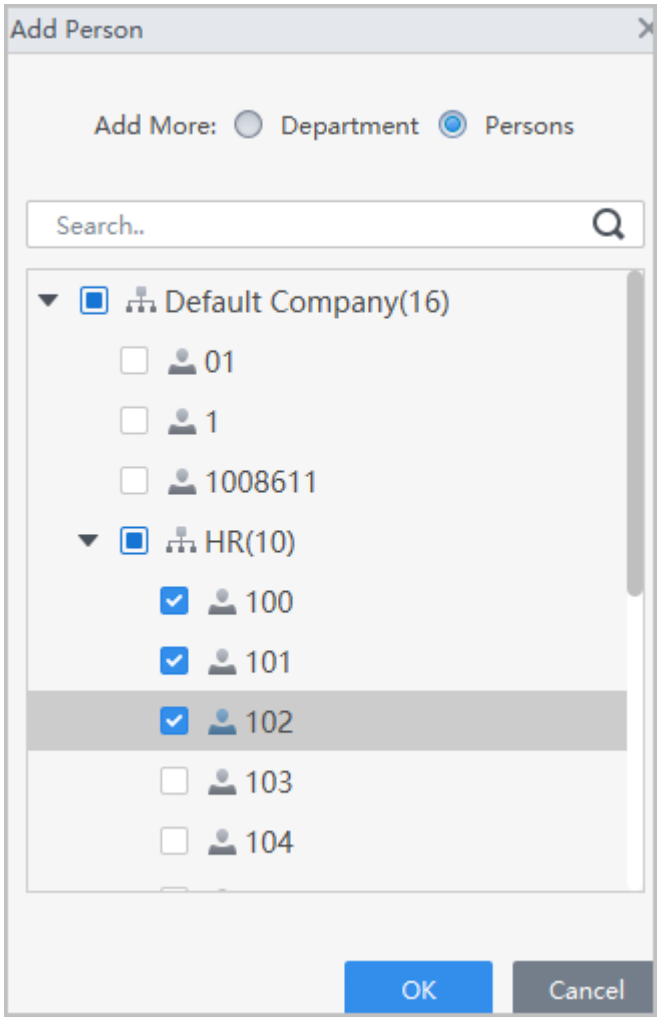
Paso 4 **la persona**área, haga clic**Agregar**para seleccionar personal y luego haga clic en**DE ACUERDO**.

Puede seleccionar personal del departamento o usuarios individuales.

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

Cuando desee asignar permiso a una nueva persona o cambiar los permisos de acceso de una persona existente, puede simplemente 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.

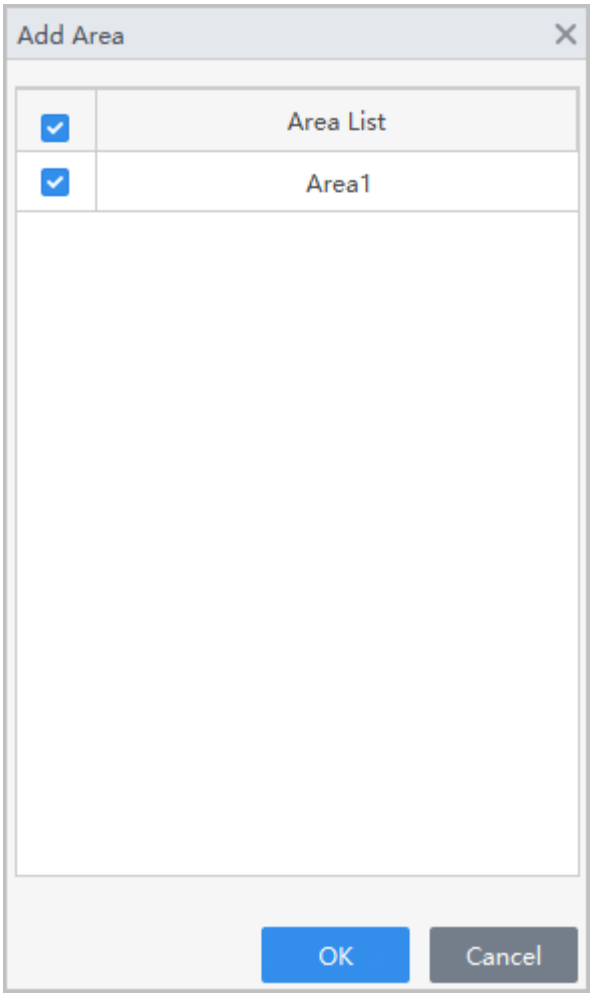
Figura 5-15 Agregar usuarios



Puedes hacer clic + Para crear nuevas áreas de permisos. Para más detalles sobre la creación de áreas de permisos, Consulte el manual de usuario correspondiente.

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

Figura 5-16 Agregar área



Paso 6 Hacer clicDE ACUERDO.

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

Figura 5-17 Progreso de la autorización

Permission Group	Device Name	Progress	Status	Result of Issuing	Operation
Permission Group3	[redacted]	1/1	Finished issuing	Successful: 1, Failed: 0	

5.4.5 Asignación de permisos de asistencia

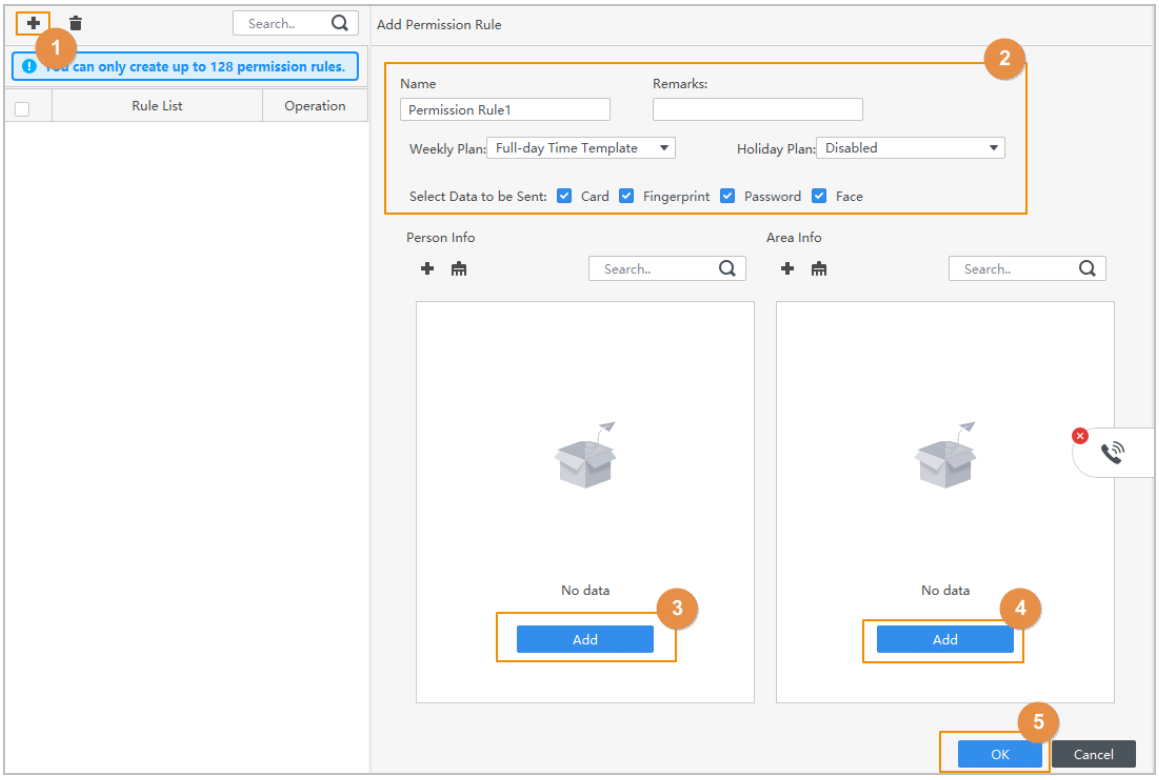
El método para configurar el permiso para el departamento y para el personal es similar, y aquí se utiliza el departamento como ejemplo.

Procedimiento

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

Paso 2 Haga clic para agregar una regla de permiso.

Figura 5-18 Asignar reglas de permisos



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

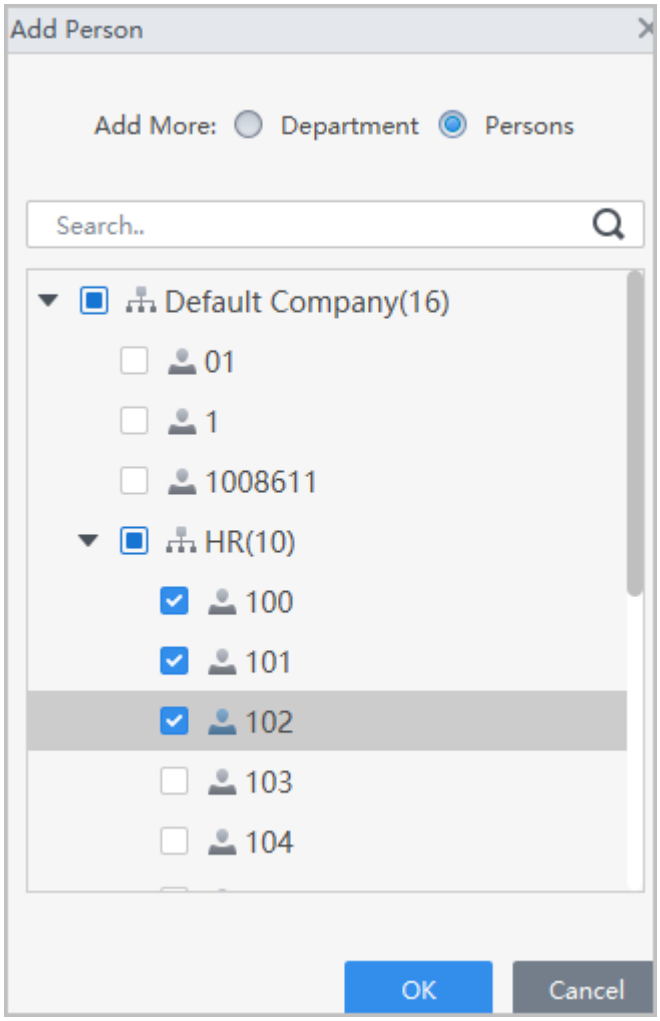
Paso 4 **la persona**área, haga clic**Agregar**para seleccionar personal y luego haga clic en**DE ACUERDO**.

Puede seleccionar personal del departamento o usuarios individuales.

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

Cuando desee asignar permiso a una nueva persona o cambiar los permisos de acceso de una persona existente, puede simplemente 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.

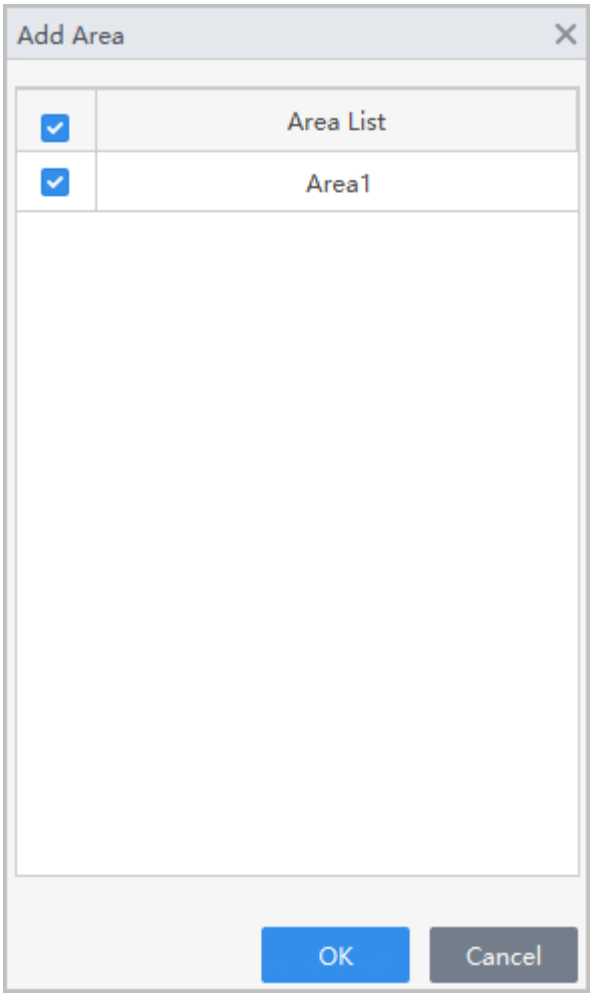
Figura 5-19 Agregar usuarios



Puedes hacer clic + Para crear nuevas áreas de permisos. Para más detalles sobre la creación de áreas de permisos, Consulte el manual de usuario correspondiente.

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

Figura 5-20 Agregar área



Paso 6 Hacer clicDE ACUERDO.

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

Figura 5-21 Progreso de la autorización

Permission Group	Device Name	Progress	Status	Result of Issuing	Operation
Permission Group3	[redacted]	1/1	Finished issuing	Successful: 1, Failed: 0	

5.5 Monitoreo del control de acceso

Procedimiento

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

Paso 2 Gestionar la puerta.

Figura 5-22 Monitorear la puerta

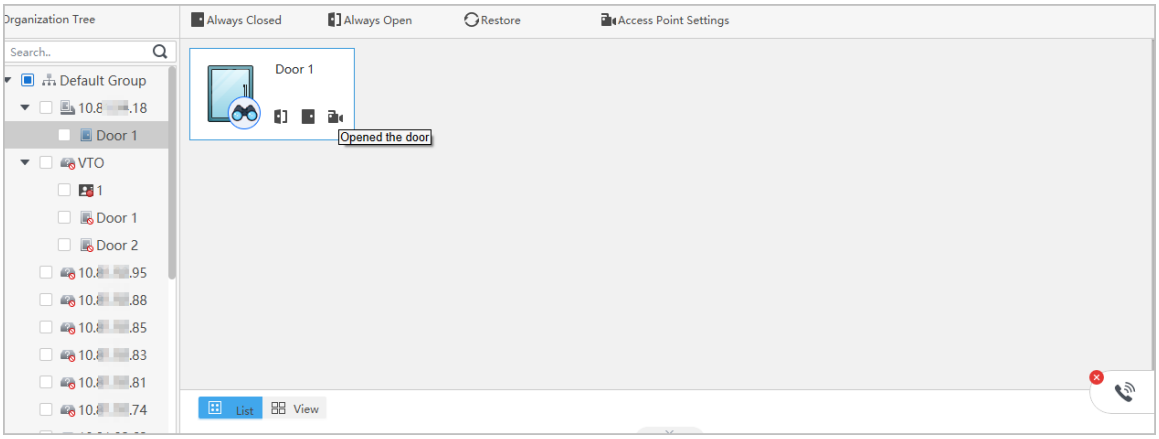


Tabla 5-3 Descripción de parámetros

Función	Descripción
Controlar la puerta de forma remota	Controlar la puerta de forma remota. ● Método 1: Haga clic derecho en una puerta y luego seleccione**Abierto**o**Cerca**. ● Método 2: Haga clic en o para abrir o cerrar la puerta.
	Vea el video capturado por la cámara del controlador de acceso o la cámara externa vinculada. Si no puede ver el video en tiempo real, significa que el dispositivo de control de acceso no tiene cámara ni está conectado a una cámara externa. Configure una cámara externa para el controlador de acceso. Para más detalles, consulte el manual del usuario correspondiente. Si desea ver varios videos en vivo al mismo tiempo, haga clic en View y luego arrastre el dispositivo de control de acceso en la organización árbol a ventanas, o haga doble clic en el dispositivo de control de acceso en el árbol de la organización.
Siempre abierto	Después de configurar la opción "Siempre abierta" o "Siempre cerrada", la puerta permanece abierta o cerrada constantemente y no se puede controlar manualmente. Si desea volver a controlar la puerta manualmente, haga clic en**Normal**para restablecer el estado de la puerta.
Siempre cerrado	
Restaurar	
Configuración del punto de acceso	Configure dispositivos (NVR, IPC, IVSS, etc.) compatibles con el reconocimiento de objetivos como punto de control de acceso. Tras la configuración, los registros de desbloqueo de puertas se subirán a la plataforma.

Paso 3 Haga clic con el botón derecho en un dispositivo de control de acceso para administrarlo.

Figura 5-23 Administrar el dispositivo

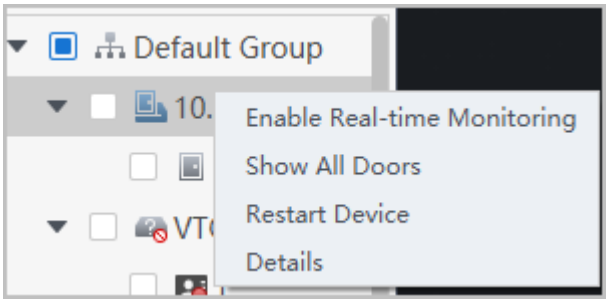


Tabla 5-4 Descripción de parámetros

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

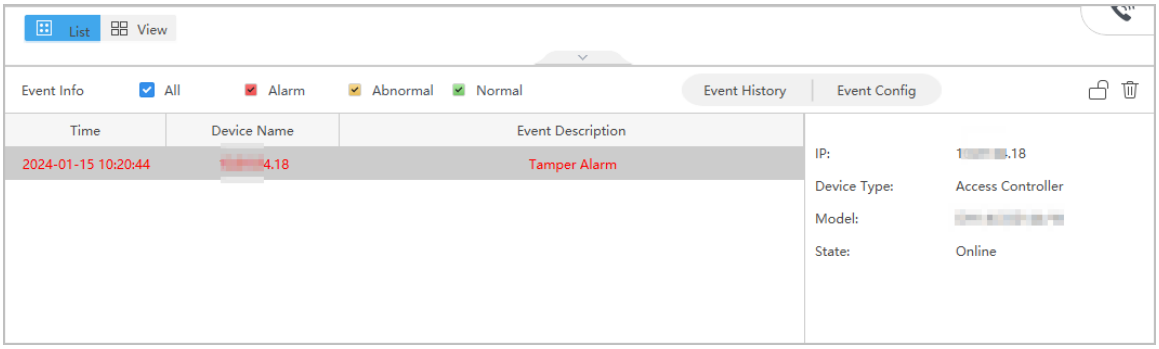
Paso 4 Ver el estado de la puerta en**Información del evento**lista. Para más detalles, consulte el manual del usuario correspondiente.

Operaciones relacionadas

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

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

Figura 5-24 Información del evento



Apéndice 1 Puntos importantes de la toma de huellas dactilares

Instrucciones de registro

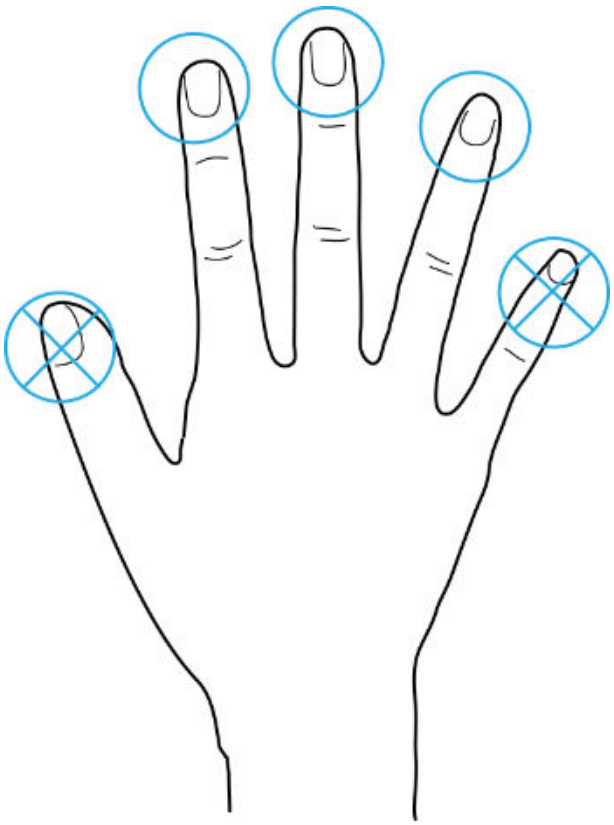
Al registrar la huella dactilar, preste atención a los siguientes puntos:

- Asegúrese de que sus dedos y la superficie del escáner estén limpios y secos.
- Presione su dedo en el centro del escáner de huellas dactilares.
- No coloque el sensor de huellas dactilares en un lugar con luz intensa, alta temperatura y alta humedad.
- Si sus huellas dactilares no están claras, utilice otros métodos de desbloqueo.

Se recomiendan los dedos

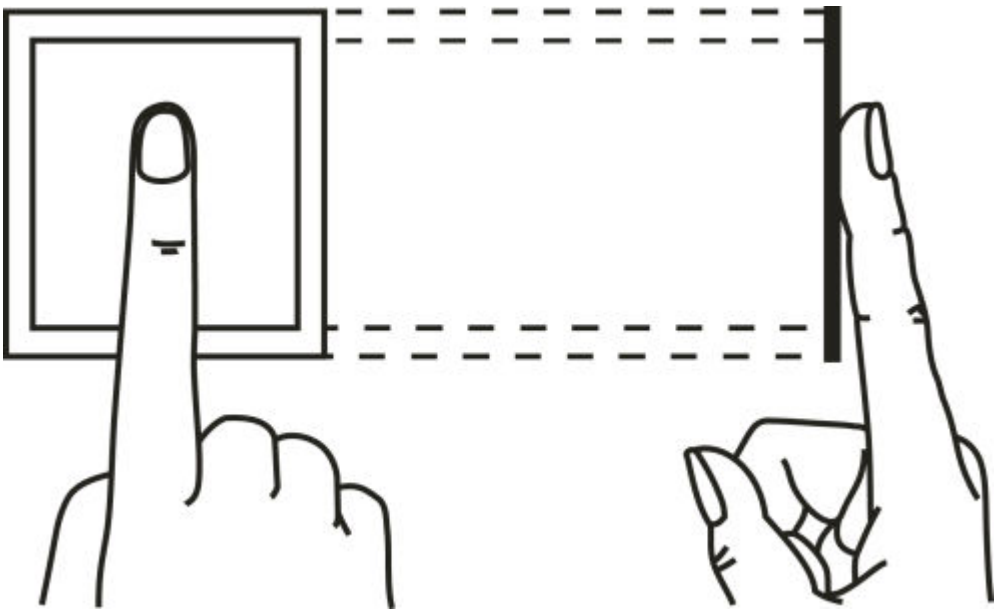
Se recomiendan los dedos índice, medio y anular. Los pulgares y meñiques no se colocan fácilmente en el centro de la grabación.

Apéndice Figura 1-1 Dedos recomendados

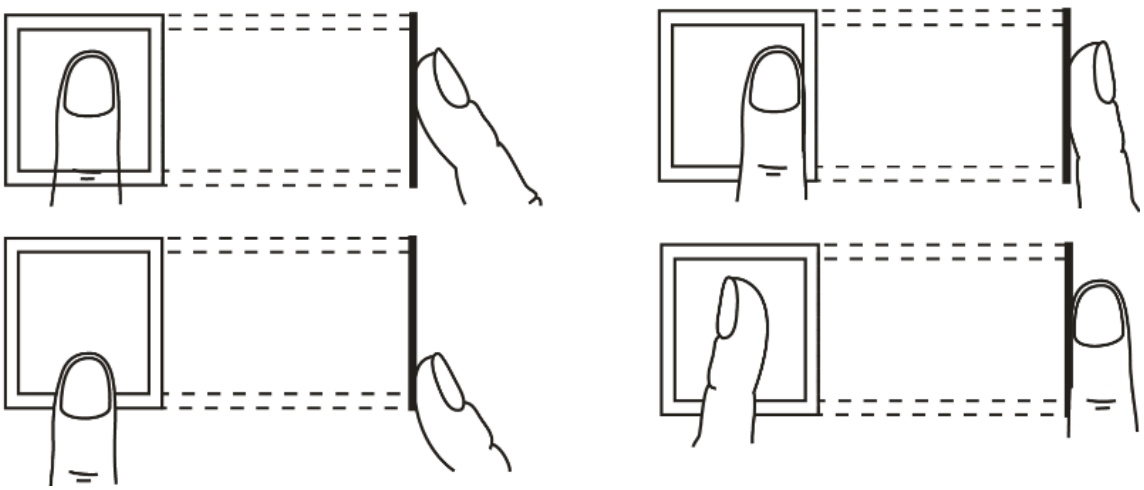


Cómo presionar su huella dactilar en el escáner

Apéndice Figura 1-2 Colocación correcta



Apéndice Figura 1-3 Colocación incorrecta



Apéndice 2 Recomendación de seguridad

Gestión de cuentas

1.**Utilice contraseñas complejas**

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de caracteres: letras mayúsculas y minúsculas, números y símbolos;
- No contenga 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 repetidos, como 111, aaa, etc.

2.**Cambie las contraseñas periódicamente**

Se recomienda cambiar periódicamente la contraseña del dispositivo para reducir el riesgo de que sea adivinada o descifrada.

3.**Asignar cuentas y permisos de forma adecuada**

Agregue usuarios de forma adecuada según los requisitos de servicio y administración y asigne conjuntos de permisos mínimos a los usuarios.

4.**Habilitar la función de bloqueo de cuenta**

La función de bloqueo de cuenta está habilitada por defecto. Se recomienda mantenerla habilitada para proteger la seguridad de la cuenta. Tras varios intentos fallidos de contraseña, la cuenta y la dirección IP de origen correspondientes se bloquearán.

5.**Establecer y actualizar la información de restablecimiento de contraseña de manera oportuna**

El dispositivo admite la función de restablecimiento de contraseña. Para reducir el riesgo de que esta función sea utilizada por cibercriminales, si se produce algún cambio en la información, modifíquela a tiempo. Al configurar las preguntas de seguridad, se recomienda no usar respuestas fáciles de adivinar.

Configuración del servicio

1.**Habilitar HTTPS**

Se recomienda habilitar HTTPS para acceder a servicios web a través de canales seguros.

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

Si el contenido de sus datos de audio y video es muy importante o confidencial, se recomienda utilizar la función de transmisión encriptada para reducir el riesgo de que sus datos de audio y video sean interceptados durante la transmisión.

3.**Desactiva los servicios no esenciales y utiliza el modo seguro**

Si no es necesario, se recomienda desactivar algunos servicios como SSH, SNMP, SMTP, UPnP, AP hotspot, etc., para reducir las superficies de ataque.

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

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

4.**Cambiar HTTP y otros puertos de servicio predeterminados**

Se recomienda cambiar el puerto predeterminado de HTTP y otros servicios a cualquier puerto entre 1024 y 65535 para reducir el riesgo de ser adivinado por actores de amenazas.

Configuración de red

1.**Habilitar lista de permitidos**

Se recomienda activar la lista de permitidos y permitir que solo las IP de dicha lista accedan al dispositivo. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la del dispositivo compatible a la lista de permitidos.

2.**Vinculación de direcciones MAC**

Se recomienda vincular la dirección IP de la puerta de enlace a la dirección MAC del dispositivo para reducir el riesgo de suplantación de ARP.

3.**Construir un entorno de red seguro**

Para garantizar mejor la seguridad de los dispositivos y reducir los posibles riesgos cibernéticos, se recomienda lo siguiente:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde la red externa;
- De acuerdo con las necesidades reales de la red, divida la red: si no hay demanda de comunicación entre las dos subredes, se recomienda utilizar VLAN, puerta de enlace y otros métodos para particionar la red para lograr el aislamiento de la red;
- Establecer un sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso ilegal a terminales de la red privada.

Auditoría de seguridad

1.**Comprobar usuarios en línea**

Se recomienda revisar periódicamente a los usuarios en línea para identificar usuarios ilegales.

2.**Comprobar el registro del dispositivo**

Al ver los registros, puede obtener información sobre las direcciones IP que intentan iniciar sesión en el dispositivo y las operaciones clave de los usuarios registrados.

3.**Configurar el registro de red**

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

Seguridad del software

1.**Actualizar el firmware a tiempo**

Según las especificaciones operativas estándar de la industria, el firmware de los dispositivos debe actualizarse a la última versión oportunamente para garantizar que cuenten con las funciones y la seguridad más recientes. Si el dispositivo está conectado a la red pública, se recomienda activar la función de detección automática de actualizaciones en línea para obtener la información de actualización de firmware publicada por el fabricante de manera oportuna.

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

Se recomienda descargar y utilizar el software de cliente más reciente.

Protección física

Se recomienda que realice una protección física para los dispositivos (especialmente los dispositivos de almacenamiento), como colocar el dispositivo en una sala de máquinas y un gabinete dedicados, y tener control de acceso.

y gestión de claves para evitar que personal no autorizado dañe el hardware y otros equipos periféricos (por ejemplo, disco flash USB, puerto serie).