Acceso independiente

Manual de usuario

V1.0.1

V1.0.0

Prefacio

General

Este manual presenta la instalación y las operaciones detalladas del Access Standalone (en lo sucesivo, "el autónomo").

Las instrucciones de seguridad

Las siguientes palabras de advertencia categorizadas con significado definido pueden aparecer en el manual.

Palabras de advertencia	Sentido
 **PELIGRO**	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
 **ADVERTENCIA**	Indica un riesgo potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 **PRECAUCIÓN**	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
 **CONSEJOS**	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
 **NOTA**	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de la revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento.	Marzo de 2020
V1.0.1	Agregue la altura de instalación recomendada.	Junio de 2020

Acerca del manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No nos hacemos responsables de ninguna pérdida causada por las operaciones que no cumplan con el manual. El manual se
- actualizará de acuerdo con las últimas leyes y regulaciones de las regiones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.

- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más actualizado y la documentación complementaria. Todavía puede haber desviaciones en los datos técnicos, la
- descripción de funciones y operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final.

- Actualice el software del lector o pruebe con otro software de lectura convencional si no puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y los nombres de empresas que aparecen en el manual son propiedad de sus respectivos propietarios.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si se produce algún problema al utilizar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

Advertencias y medidas de seguridad importantes

Este capítulo describe el contenido que cubre el manejo adecuado de la unidad autónoma, la prevención de peligros y la prevención de daños a la propiedad. Lea atentamente estos contenidos antes de utilizar el dispositivo independiente, cúmplalos al utilizarlos y guárdelos bien para futuras consultas.

Requisito de operación

- No coloque ni instale la unidad independiente en un lugar expuesto a la luz solar o cerca de una fuente de calor.

- Mantenga la unidad independiente alejada de la humedad, el polvo o el hollín.
- Mantenga el autónomo instalado horizontalmente en el lugar estable para evitar que se caiga.
- No deje caer ni salpique líquido sobre el autónomo, y asegúrese de que no haya ningún objeto lleno de líquido sobre el autónomo para evitar que el líquido fluya hacia el autónomo.
- Instale el autónomo en un lugar bien ventilado y no bloquee la ventilación del autónomo.

- Opere el autónomo dentro del rango nominal de entrada y salida de energía. No desarme el
- independiente.
- Transporte, use y almacene el dispositivo independiente en las condiciones de humedad y temperatura permitidas.

Seguridad ELECTRICA

- El uso inadecuado de la batería puede provocar un incendio, una explosión o una inflamación. Al
- reemplazar la batería, asegúrese de utilizar el mismo modelo.
- Utilice los cables de alimentación recomendados en la región y cumpla con la especificación de potencia nominal.

- Utilice el adaptador de corriente que se proporciona con la unidad independiente; de lo contrario, podría provocar lesiones personales y daños al dispositivo.
- La fuente de alimentación debe cumplir con los requisitos del estándar de seguridad de voltaje muy bajo (SELV) y suministrar energía con un voltaje nominal que cumpla con el requisito de fuente de energía limitada de acuerdo con IEC60950-1. Tenga en cuenta que el requisito de suministro de energía está sujeto a la etiqueta del dispositivo.

- Conecte el dispositivo (estructura tipo I) a la toma de corriente con toma de tierra de protección.
- El acoplador del aparato es un dispositivo de desconexión. Cuando utilice el acoplador, mantenga el ángulo para facilitar la operación.

Tabla de contenido

1. Información general

1.1 Introducción

El acceso independiente es un panel de control de acceso que admite el desbloqueo mediante huella digital, contraseñas y tarjeta, y admite sus combinaciones.

1.2 Características

- Admite desbloqueo de tarjetas, desbloqueo de huellas dactilares y desbloqueo de contraseña (botón de desbloqueo y desbloqueo remoto).

- Admite 30.000 usuarios, 30.000 tarjetas y 3000 huellas dactilares. Almacene 150.000
- registros de acceso y 1000 registros de alarmas.
- Admite alarma de coacción, alarma de manipulación e informe de la alarma; admite 1 entrada de alarma y 1 salida de alarma.

- Admite usuarios generales, usuarios restringidos, usuarios invitados, usuarios de patrulla, usuarios VIP y otros usuarios.

- Función de aviso de voz.
- El temporizador puede funcionar normalmente durante un año después de apagarse. Función de
- prueba automática NTP.

1.3 Dimensiones y componentes

Figura 1-1 Vista frontal (mm [pulgadas])

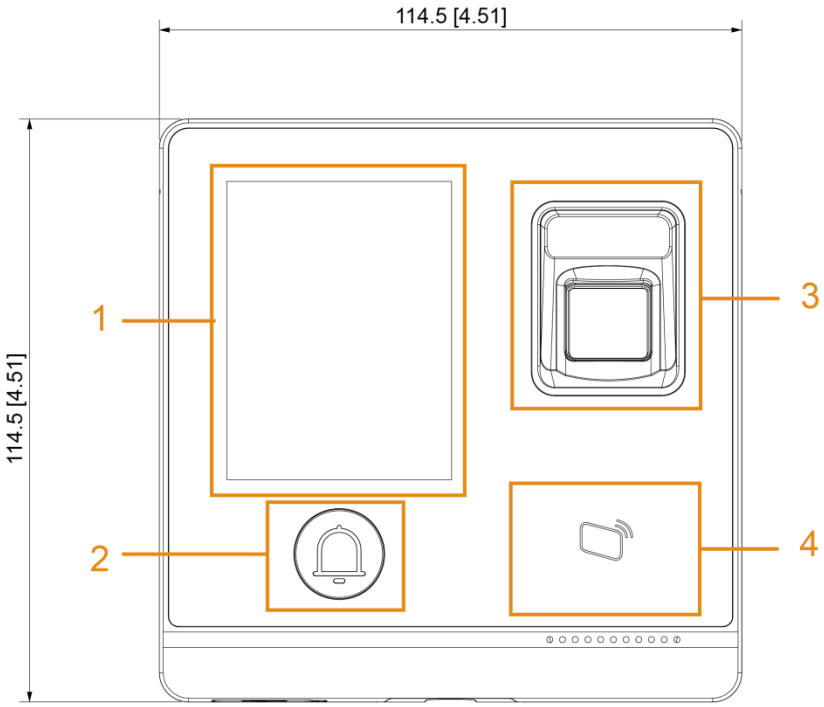


Figura 1-2 Vista posterior (mm [pulgadas])

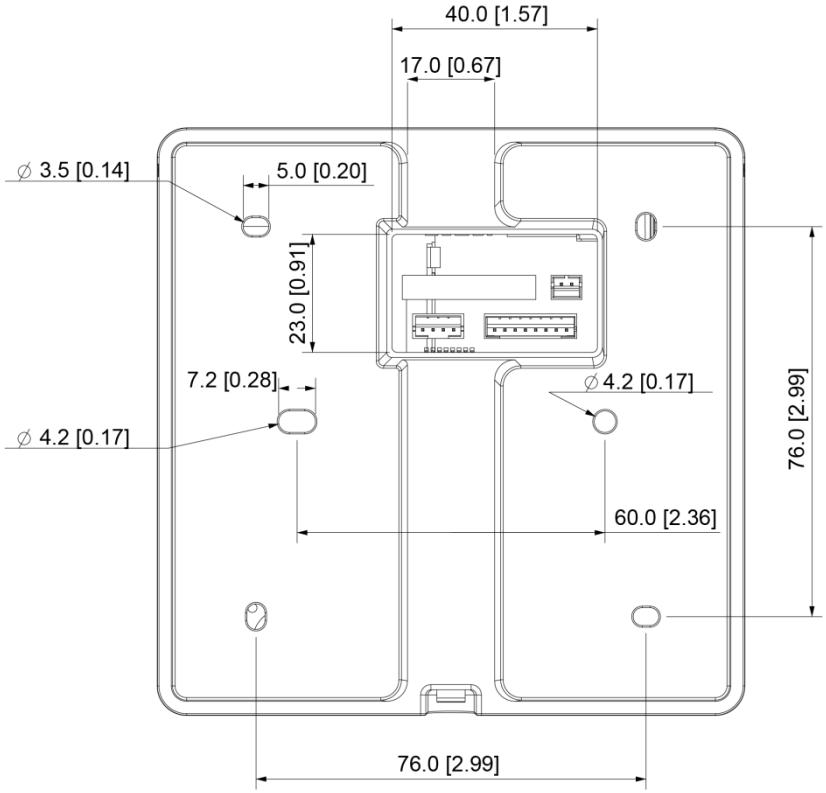


Figura 1-3 Vista lateral e inferior (mm [pulgadas])

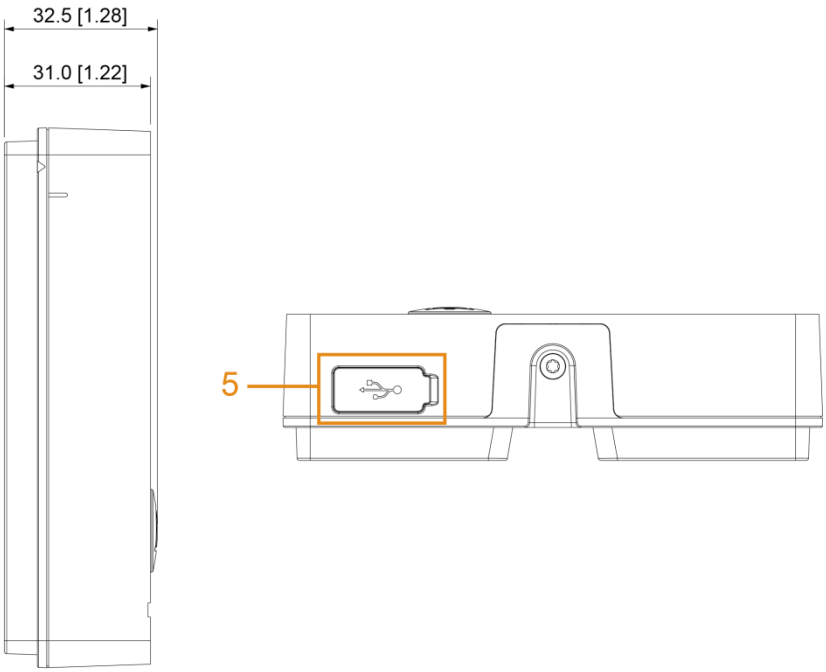


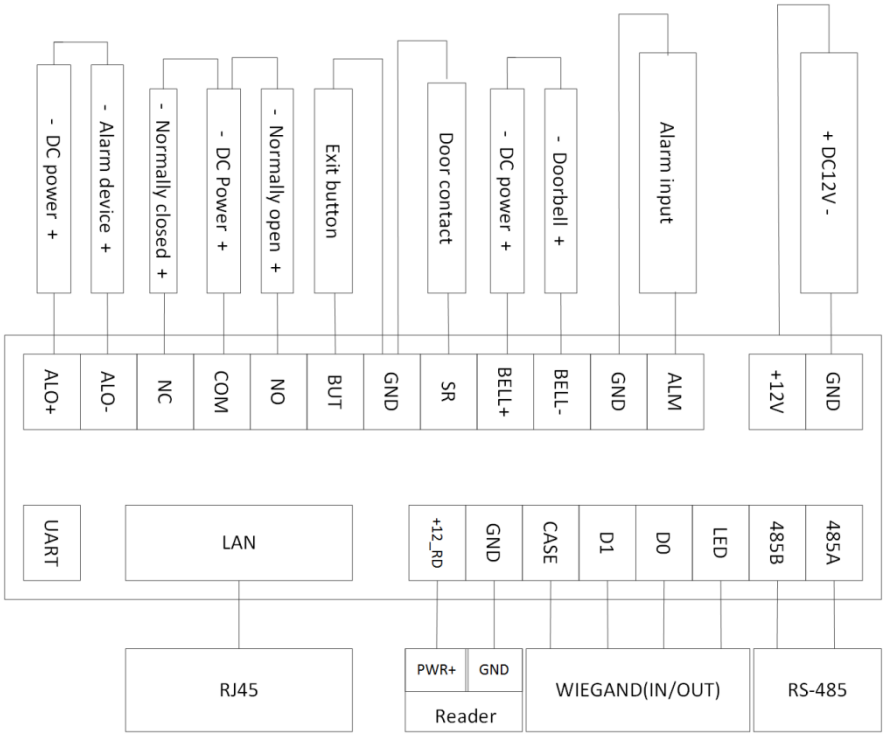
Tabla 1-1 Descripción de los componentes

No.	Nombre
1	Área de VA
2	Botón de timbre
3	Sensor de huellas dactilares
4	Área de deslizamiento de tarjetas
5	Puerto USB

2 Instalación

2.1 Conexiones de cables

Figura 2-1 Conexión de cables



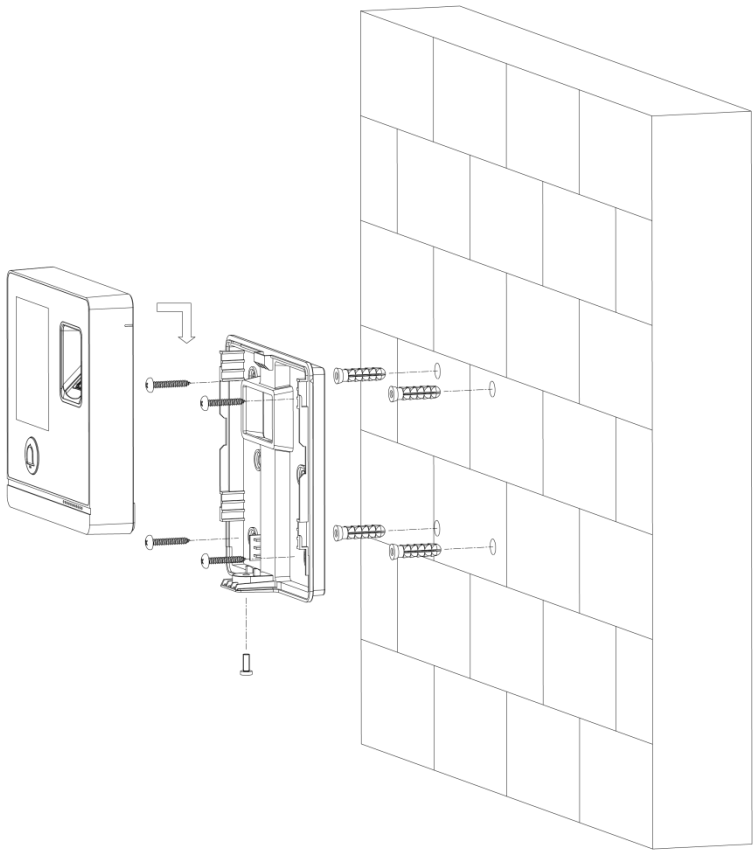
2.2 Instalación del dispositivo

La altura de instalación recomendada es de 1,4 a 1,6 metros.

El independiente admite la instalación en superficie y la instalación oculta.

Instalación en superficie

Figura 2-2 Instalación en superficie



Procedimiento de instalación

Paso 1 Pegue el mapa de instalación en la pared y luego taladre los orificios de acuerdo con las posiciones mapa.

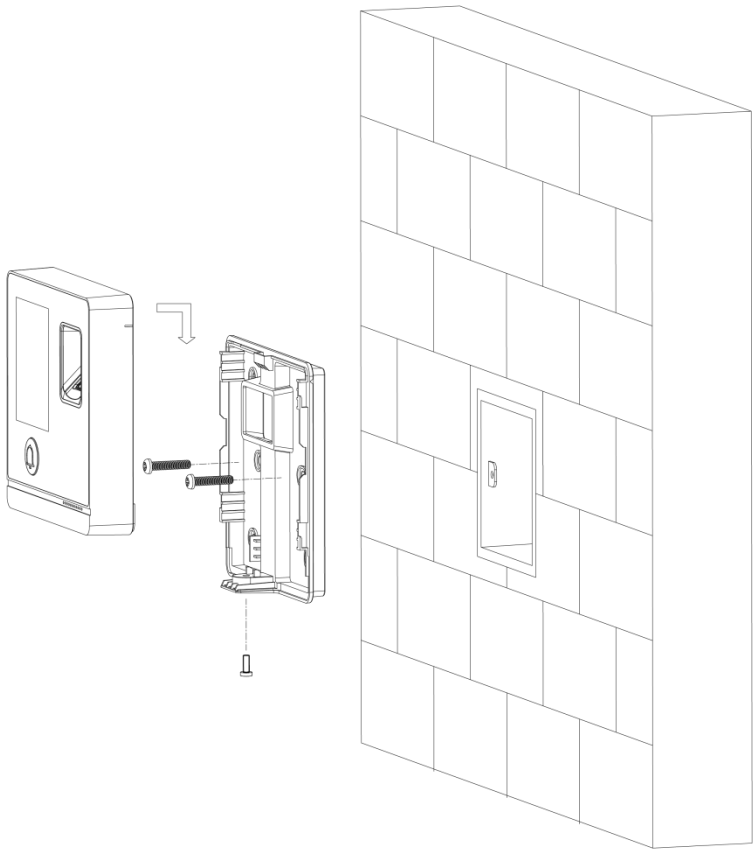
Paso 2 Inserte el perno de expansión en los orificios de instalación.

Paso 3 Fije la cubierta trasera a la pared con tornillos autorroscantes.

Paso 4 Coloque tornillos de máquina a través del orificio inferior; bloquee la cubierta frontal en la cubierta trasera.

Instalación oculta

Figura 2-3 Instalación oculta



Procedimiento de instalación

Paso 1 Pase los cables por la salida.

Paso 2 Fije la cubierta trasera en la caja montada con tornillos.

Paso 3 Fije los cables y abroche la cubierta frontal a la cubierta posterior.

3 Operación del sistema

3.1 Descripción del botón

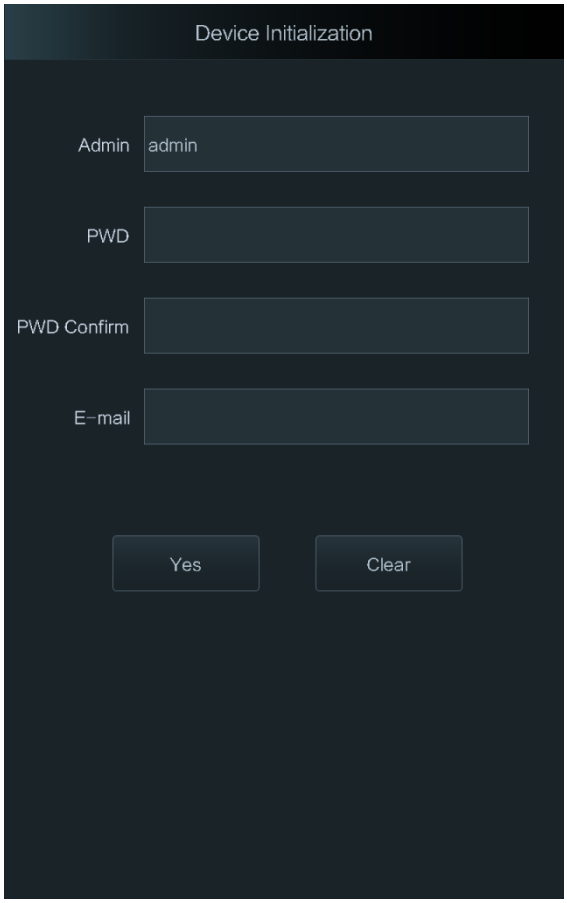
Tabla 3-1 Descripción de los botones

Botón	Descripción
	Vaya a la primera página. Vaya
	a la última página.
	Vaya a la página anterior. Vaya a la
	página siguiente.
	Ir al menú anterior. Vaya al
	siguiente menú.

3.2 Inicialización

La contraseña de administrador y un correo electrónico deben establecerse la primera vez que se enciende el modo autónomo; de lo contrario, no se puede utilizar el independiente.

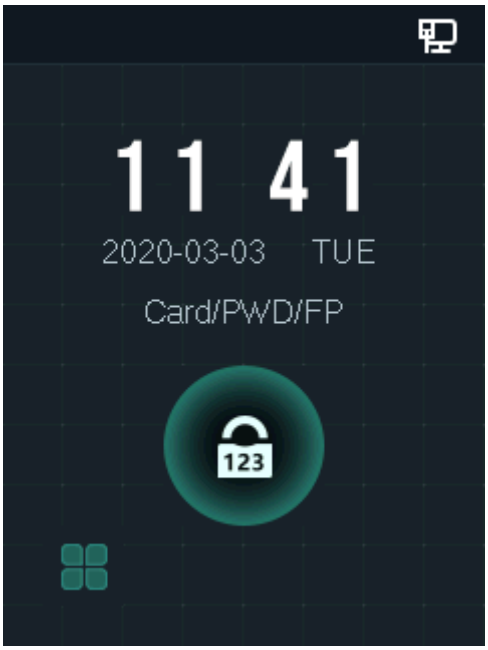
Figura 3-1 Inicialización



- El administrador y la contraseña configurados en esta interfaz se utilizan para iniciar sesión en la plataforma de administración web.
- La contraseña de administrador se puede restablecer a través de la dirección de correo electrónico que ingresó si el administrador olvida la contraseña de administrador.
- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo '";: &).

Una vez completada la inicialización, se muestra la interfaz de espera.

Figura 3-2 Interfaz de espera



3.3 Interfaz de espera

Puede desbloquear la puerta mediante huella digital, contraseñas y tarjeta. Para obtener más detalles, consulte la Tabla 3-2.

- Si no se realizan operaciones en 30 segundos, la unidad independiente pasará al modo de protector de pantalla cuando el protector de pantalla esté habilitado y las imágenes se hayan importado para reproducirlas; Después de 30 segundos de reproducción de protector de pantalla, el autónomo pasa al modo de espera.
- Las siguientes figuras son solo de referencia y prevalecerá la interfaz real.

Figura 3-3 Interfaz en espera

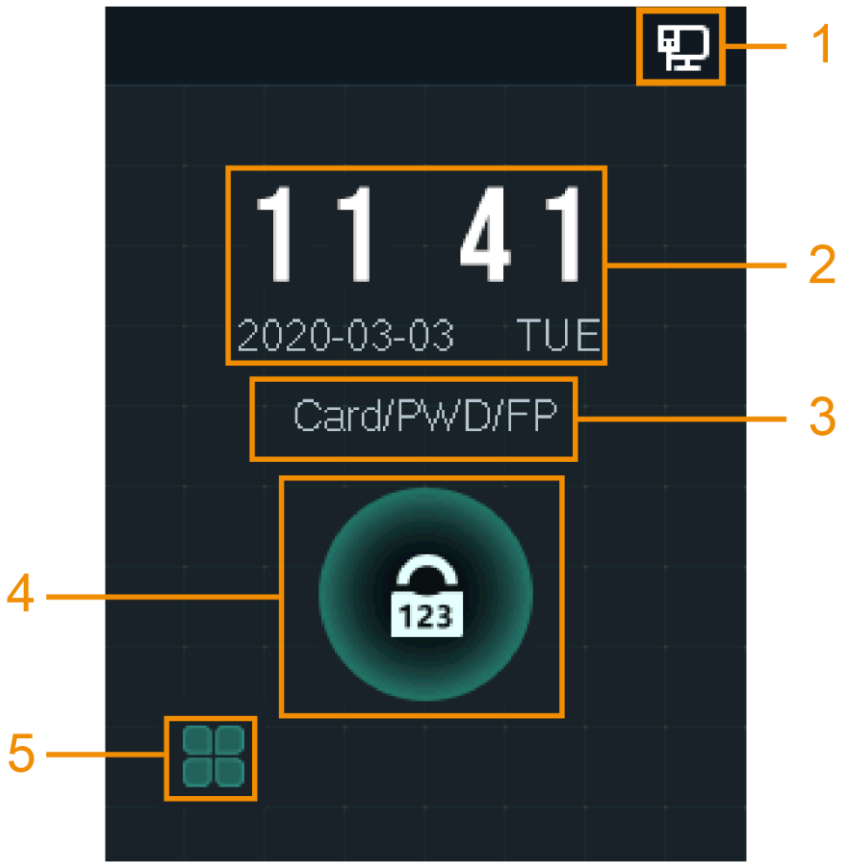


Tabla 3-2 Descripción de la página de inicio

No.	Descripción
1	Estado de la red.
2	Fecha y hora: fecha y hora actuales. Muestra los métodos de
3	desbloqueo configurados. Icono de desbloqueo de contraseña.
4	
5	Icono del menú principal. Solo el administrador puede ingresar al menú principal.

3.4 Métodos de desbloqueo

Puede desbloquear la puerta mediante tarjeta, contraseña, huella digital y el modo de combinación. Para obtener más información, consulte "3.7.1 Modo de desbloqueo".

3.4.1 Contraseñas de usuario

Ingrese las contraseñas de usuario y luego podrá desbloquear la puerta.

Paso 1 toque en la interfaz de espera.

Paso 2 Toque 

e ingrese el ID de usuario y luego toque **OKAY.**

Paso 3 Ingrese la contraseña de usuario y luego toque **OKAY.**

Paso 4 Toque  .

La puerta está desbloqueada.

3.4.2 Contraseña de administrador

Ingrese la contraseña de administrador y luego podrá desbloquear la puerta. La contraseña del administrador puede desbloquear la puerta sin estar sujeta a los niveles de usuario, modos de desbloqueo, períodos, planes de vacaciones y anti-passback.

- Solo puede establecer una contraseña de administrador para una independiente. DSS Pro puede
- emitir 100 contraseñas para una sola como máximo. Administrador no es la contraseña que se
- estableció durante la inicialización.

Paso 1 toque 

en la página de inicio.

Paso 2 Toque 

.

Paso 3 Ingrese la contraseña de administrador y luego toque **OKAY.**

La puerta está desbloqueada.

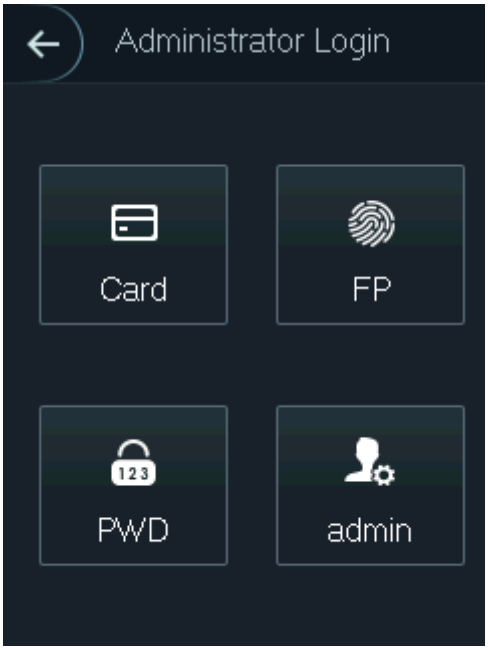
Puede configurar y habilitar Administrator PWD en el **Administrador PWD** interfaz.

3.5 Menú principal

Los administradores pueden agregar usuarios de diferentes niveles, establecer parámetros relacionados con el acceso, realizar la configuración de la red, ver registros de acceso e información del sistema, y más en el menú principal.

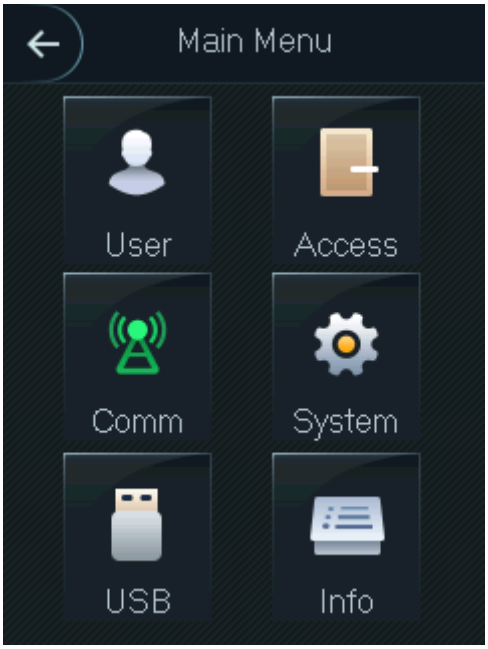
Paso 1 toque  en la interfaz de espera.

Figura 3-4 Inicio de sesión de administrador



Paso 2 Seleccione un método de entrada al menú principal.

Figura 3-5 Menú principal



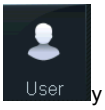
3.6 Gestión de usuarios

Puede agregar nuevos usuarios, ver listas de usuarios, listas de administradores y modificar la contraseña de administrador en el **Usuario** interfaz.

3.6.1 Agregar nuevos usuarios

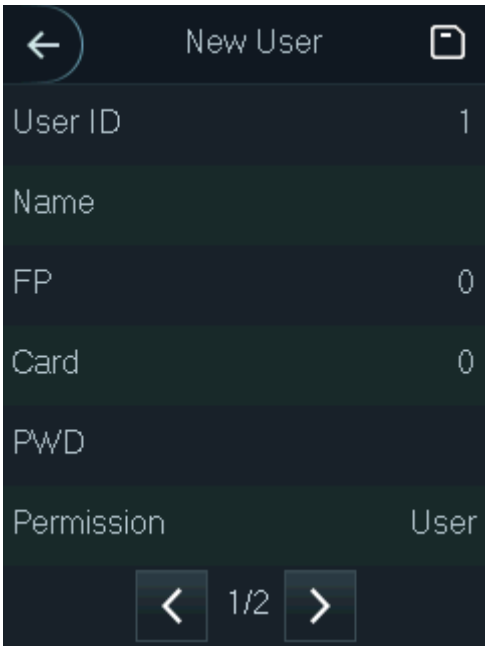
Puede agregar nuevos usuarios ingresando ID de usuario, nombres, importando huellas digitales, tarjetas, contraseñas, seleccionando niveles de usuario y más.

Las siguientes figuras son solo de referencia y prevalecerá la interfaz real.

Paso 1 toque 

y luego toque  .

Figura 3-6 Información de nuevo usuario



Paso 2 Configure los parámetros en la interfaz.

Tabla 3-3 Descripción del nuevo parámetro de usuario

Parámetro	Descripción
ID de usuario	Puede ingresar ID de usuario. Los ID constan de 18 caracteres (incluidos números y letras, pero no caracteres especiales) y cada ID es único. La identificación se asignará cuando no ingrese una.
Nombre	Puede ingresar nombres con un máximo de 32 caracteres (incluidos números, símbolos y letras).
FP	Registro de huellas dactilares. Registre las huellas digitales del usuario. Registro de
Tarjeta	tarjeta. Registre la información de la tarjeta.
PWD	La contraseña de desbloqueo de la puerta. La longitud máxima de los dígitos de identificación es 8. Establezca el permiso del
Permiso	usuario: **Usuario** o **Administración.** • Usuario: **Usuario** solo tiene permiso para abrir la puerta. Administración: **Administración** tiene permiso para • desbloquear la puerta y configurar los parámetros.
Período	Puede establecer un período en el que el usuario puede desbloquear la puerta.
Fiesta Plan	Puede establecer un plan de vacaciones en el que el usuario puede abrir la puerta.
Fecha válida	Puede establecer un período durante el cual la información de desbloqueo del usuario es válida.

Parámetro	Descripción
Tipo de usuario	• General: los usuarios generales pueden desbloquear la puerta normalmente. • Restringido: cuando los usuarios de la lista negra desbloquean la puerta, el personal de servicio recibirá un aviso. • Invitado: los invitados pueden abrir la puerta en determinados momentos en determinados períodos. Una vez que superan los tiempos y períodos máximos, no pueden volver a desbloquear la puerta. • Patrulla: los usuarios que patrullan pueden hacer un seguimiento de su asistencia, pero no tienen autoridad de desbloqueo. • VIP: cuando VIP abre la puerta, el personal de servicio recibirá un aviso. Otro: cuando usuarios • especiales (como personas discapacitadas y embarazadas) desbloquean la puerta, habrá un retraso de 5 segundos antes de que se cierre la puerta.
Usar tiempo	Cuando el nivel de usuario es **Invitado,** puede establecer el número máximo de veces que el huésped puede abrir la puerta.

Paso 3 Una vez que haya configurado todos los parámetros, toque  para guardar la configuración.

3.6.2 Visualización de la información del usuario

Puede buscar usuarios, ver la lista de usuarios, la lista de administradores, habilitar la contraseña del administrador y editar y eliminar la información del usuario a través del **Usuario** interfaz.

3.7 Gestión de acceso

Puede realizar la gestión de acceso en el modo de desbloqueo, el estado de la puerta, el tiempo de retención de la cerradura, el tipo de sensor de la puerta y la verificación remota.

Grifo 

para ir a la interfaz de gestión de acceso.

3.7.1 Modo de desbloqueo

Cuando el **Modo de desbloqueo** está activado, los usuarios pueden desbloquear la tarjeta, la contraseña, la huella digital y el modo de combinación.

Paso 1 Seleccione **Evaluar> Modo de desbloqueo.**

Figura 3-7 Elemento (opción múltiple)

Paso 2 Seleccione los modos de desbloqueo.

Toque de nuevo un modo de desbloqueo seleccionado, se eliminará el modo de desbloqueo.

Paso 3 Seleccione un modo de combinación.

- **+ Y** significa "y". Por ejemplo, si seleccionó tarjeta + FP, significa que para desbloquear la puerta, primero debe deslizar su tarjeta y luego escanear su huella digital.
- **/ O** significa "o". Por ejemplo, si seleccionó tarjeta / FP, significa que para desbloquear la puerta, puede deslizar su tarjeta o escanear sus huellas digitales.

Paso 4 Toque para guardar la configuración.

Y luego el **Acceso** se muestra la interfaz.

Paso 5 Habilite el **Modo de desbloqueo.**

- significa habilitado.
- significa no habilitado.

3.7.2 Estado de la puerta

Hay tres opciones: **NO C,** y **Normal.**

- NO: Si **NO** está seleccionado, el estado de la puerta es normalmente abierto, lo que significa que la puerta nunca se cerrará.
- NC: Si **CAROLINA DEL NORTE** está seleccionado, el estado de la puerta es normalmente cerrado, lo que significa que la puerta no se desbloqueará.
- Normal: si **Normal** está seleccionado, la puerta se desbloqueará y bloqueará según su configuración.

3.7.3 Bloquear tiempo de espera

Bloquear tiempo de espera es el tiempo en el que se abre la puerta. Si la puerta ha estado desbloqueada por un período que excede la duración, la puerta se bloqueará automáticamente.

3.7.4 Tipo de sensor de puerta

Hay dos tipos de sensores de puerta: **NO** y **CAROLINA DEL NORTE.**

3.7.5 Verificación remota

Grifo **Verificación remota** para establecer la hora efectiva y luego toque  para habilitarlo. Remoto se requiere verificación al desbloquear las puertas. Para desbloquear la puerta, se necesita una instrucción de desbloqueo de puerta enviada por la plataforma de gestión.

-  significa habilitado.
-  significa no habilitado.

3.8 Comunicación de red

Para que el funcionamiento independiente funcione normalmente, debe configurar los parámetros para la red, los puertos serie y los puertos Wiegand.

3.8.1 Dirección IP

3.8.1.1 Configuración de IP

Configure una dirección IP para el autónomo para que se conecte a la red. Para obtener más detalles, consulte la Tabla 3-4.

Figura 3-8 Configuración de la dirección IP

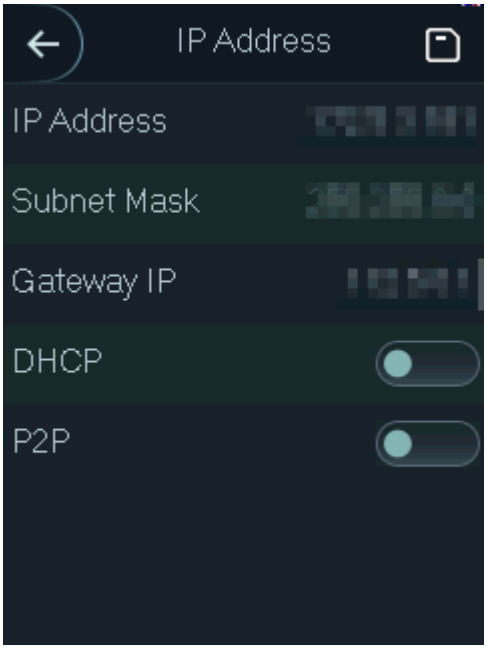


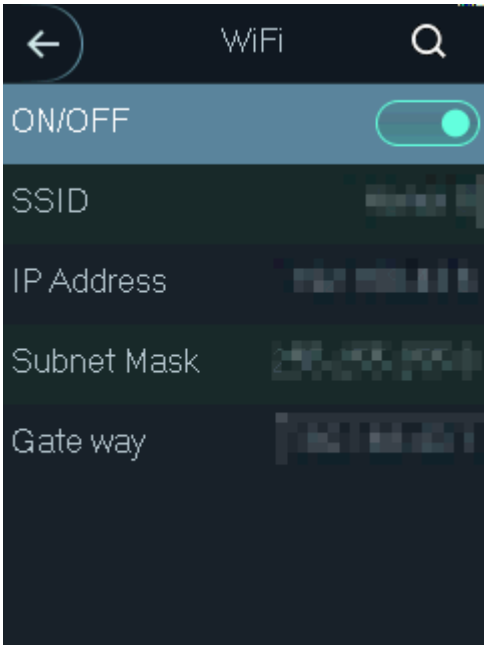
Tabla 3-4 Parámetros de configuración de IP

Parámetro	Descripción
Dirección IP / Subred Máscara / IP de puerta de enlace Habla a	La dirección IP, la máscara de subred y la dirección IP de la puerta de enlace deben estar en el mismo segmento de red. Después de la configuración, toque para salvar el configuraciones.
DHCP	DHCP (Protocolo de configuración dinámica de host). Cuando el DHCP está habilitado, la dirección IP se puede adquirir automáticamente y la dirección IP, la máscara de subred y la dirección IP de la puerta de enlace no se pueden configurar manualmente.
P2P	P2P es una tecnología transversal de red privada que permite al usuario administrar dispositivos sin necesidad de DDNS, mapeo de puertos o servidor de tránsito.

3.8.1.2 Wi-Fi

Puede conectar el dispositivo independiente a la red a través de Wi-Fi cuando la función Wi-Fi está habilitada.

Figura 3-9 Wi-Fi

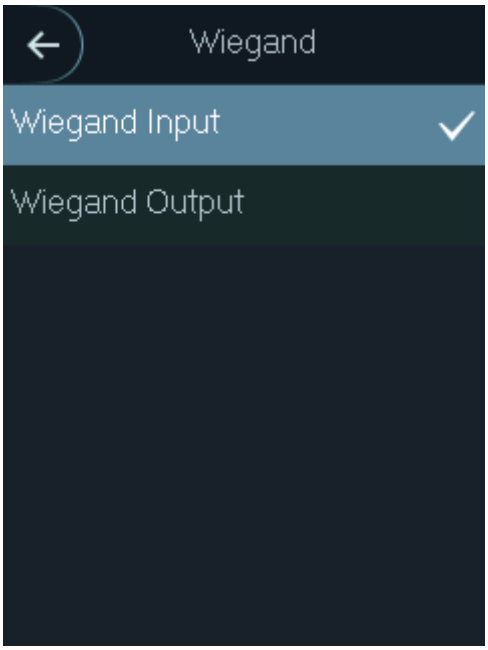


3.8.2 Configuración Wiegand

Seleccione **Entrada Wiegand** o **Salida Wiegand** de acuerdo con la dirección de entrada y salida.

Seleccione **Comunicaciones> Wiegand,** y luego el **Wiegand** se muestra la interfaz.

Figura 3-10 Wiegand



- Seleccione **Entrada Wiegand** cuando un mecanismo de deslizamiento de tarjeta externo está conectado al autónomo.
- Seleccione **Salida Wiegand** cuando el autónomo funciona como un lector que se puede conectar al controlador. Consulte la Tabla 3-5.

Tabla 3-5 Salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	El tipo de salida Wiegand determina el número de tarjeta o el dígito del número que puede ser reconocido por el autónomo. • Wiegand26, tres bytes, seis dígitos. Wiegand34, • cuatro bytes, ocho dígitos. Wiegand66, ocho bytes, • dieciséis dígitos.
Ancho de pulso	Puede configurar el ancho de pulso y el intervalo de pulso.
Intervalo de pulso	
Tipo de datos de salida	Puede seleccionar los tipos de datos de salida. • ID de usuario: si se selecciona ID de usuario, se mostrará la ID de usuario. No de tarjeta: si se • selecciona el número de tarjeta, se emitirá el número de tarjeta.

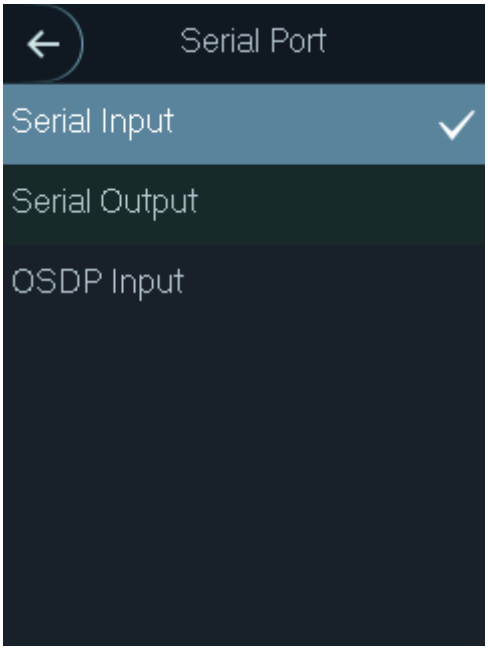
3.8.3 Puerto TCP

El rango es 1025-65535 y 37777 de forma predeterminada. Si modifica el puerto, el sistema se reiniciará automáticamente.

3.8.4 Configuración del puerto serie

Seleccione la entrada en serie o la salida en serie de acuerdo con la dirección de entrada y salida. Seleccione **Comm> Puerto serie.**

Figura 3-11 Puerto serie



- Seleccione **Entrada serial** cuando los dispositivos externos que tienen funciones de lectura y escritura de tarjetas están conectados al autónomo. **Entrada serial** se selecciona para permitir que la información de la tarjeta de acceso se envíe a la plataforma independiente y de gestión.
- Para autónomos con reconocimiento de huellas dactilares, funciones de lectura y escritura de tarjetas, si selecciona **Salida serial,** standalone enviará el número de tarjeta o la identificación de usuario al controlador.

- Seleccione **Entrada OSDP** cuando el lector de tarjetas del protocolo OSDP está conectado al autónomo.

3.9 Sistema

3.9.1 Hora

Puedes habilitar **Sistema de 24 horas,** y realizar la configuración del formato de fecha, la configuración de la fecha, la configuración de la hora y la configuración de la zona horaria.

3.9.2 Ajuste de volumen

Grifo  o  para ajustar el volumen.

3.9.3 Salvapantallas

Habilitar **Salvapantallas,** el protector de pantalla se mostrará si no se realiza ninguna operación en 30 segundos.

- Para mostrar el protector de pantalla, primero debe importar las imágenes. Para obtener más información, consulte "3.10.4 Salvapantallas".
-  significa habilitado.
-  significa no habilitado.

3.9.4 Configuración de privacidad

Figura 3-12 Configuración de privacidad

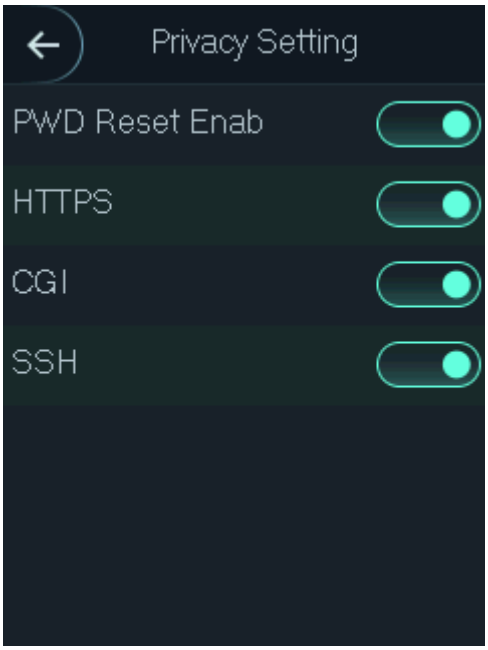


Tabla 3-6 Características

Parámetro	Descripción
Reinicio de PWD Habilitar	Si el **Habilitar restablecimiento de PWD** La función está habilitada, puede restablecer la contraseña. La función de reinicio de PWD está habilitada de forma predeterminada.
HTTPS	El Protocolo de transferencia de hipertexto seguro (HTTPS) es un protocolo para la comunicación segura a través de una red informática. Cuando HTTPS está habilitado, HTTPS se utilizará para acceder a los comandos CGI; de lo contrario, se utilizará HTTP.
CGI	Common Gateway Interface (CGI) ofrece un protocolo estándar para que los servidores web ejecuten programas que se ejecutan como aplicaciones de consola que se ejecutan en un servidor que genera páginas web de forma dinámica. Cuando CGI está habilitado, se pueden usar comandos CGI. El CGI está habilitado de forma predeterminada.
SSH	Secure Shell (SSH) es un protocolo de red criptográfico para operar servicios de red de forma segura a través de una red no segura. Cuando SSH está habilitado, SSH proporciona un servicio criptográfico para la transmisión de datos.

Cuando HTTPS está habilitado, el modo independiente se reiniciará automáticamente.

3.9.5 Número de tarjeta inverso

Si es necesario conectar el lector de tarjetas de terceros al terminal a través del puerto de salida Wiegand, debe habilitar la función de reverso de número de tarjeta; de lo contrario, la comunicación entre el terminal y el lector de tarjetas de terceros podría fallar debido a una discrepancia de protocolo.

3.9.6 Prueba automática

Cuando utilice el autónomo por primera vez o cuando el autónomo no funcione correctamente, puede utilizar la función de prueba automática para comprobar si el autónomo puede funcionar normalmente. Realice acciones de acuerdo con las indicaciones.

Cuando seleccionas **Auto prueba,** el independiente lo guiará para realizar todas las pruebas automáticas.

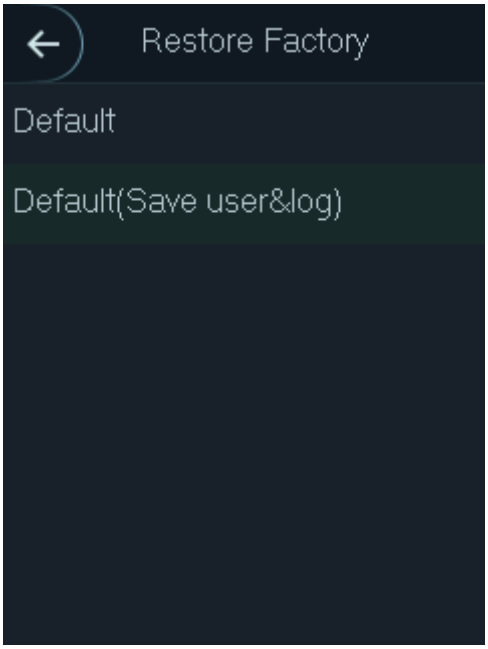
3.9.7 Restaurar la configuración de fábrica

Los datos se perderán si restaura el controlador de acceso a la configuración de fábrica.

Puede seleccionar si desea conservar la información y los registros del usuario.

- Grifo **Defecto** para restaurar el sistema autónomo a la configuración de fábrica con toda la información del usuario y la información del dispositivo eliminada.
- Grifo **Predeterminado (Guardar usuario y registro)** para restaurar el sistema autónomo a la configuración de fábrica conservando la información del usuario y la información del dispositivo.

Figura 3-13 Restaurar fábrica



3.9.8 Reiniciar

Seleccione **Sistema> Reiniciar,** grifo **Si,** y se reiniciará el autónomo.

3.10 USB

- Asegúrese de que el USB esté insertado antes de exportar la información del usuario y actualizar. Durante la exportación o actualización, no extraiga el USB ni realice otras operaciones; de lo contrario, la exportación o la actualización fallarán.
- Debe importar información de un dispositivo independiente al USB antes de usar el USB para importar información a otro dispositivo independiente.
- También se puede utilizar USB para actualizar el programa.

3.10.1 Exportación USB

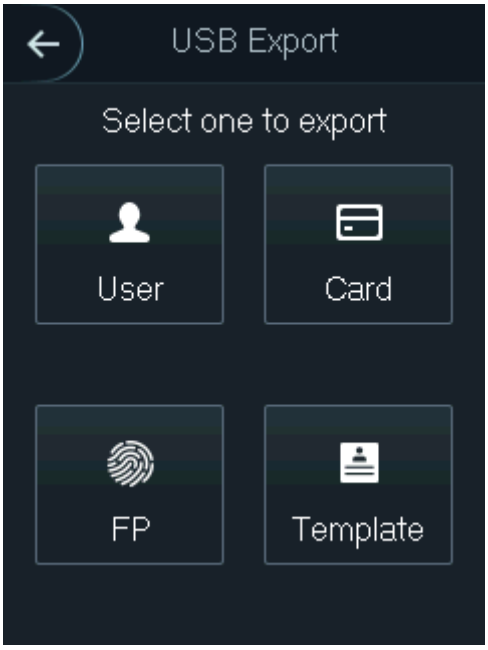
Puede exportar datos desde el dispositivo independiente al USB después de insertar el USB. La plantilla exportada está en formato .xml y puede editar la información del usuario e importarla de forma independiente. Los primeros tres datos están cifrados y no se pueden editar.

Solo se admite el sistema de archivos FAT32.

Paso 1 Seleccione **USB> Exportación USB.**

los **Exportación USB** se muestra la interfaz.

Figura 3-14 Exportación USB



Paso 2 Seleccione el tipo de datos que desea exportar.

El aviso **Confirmar para exportar** se visualiza.

Paso 3 Toque **OKAY.**

Los datos exportados se guardarán en el USB.

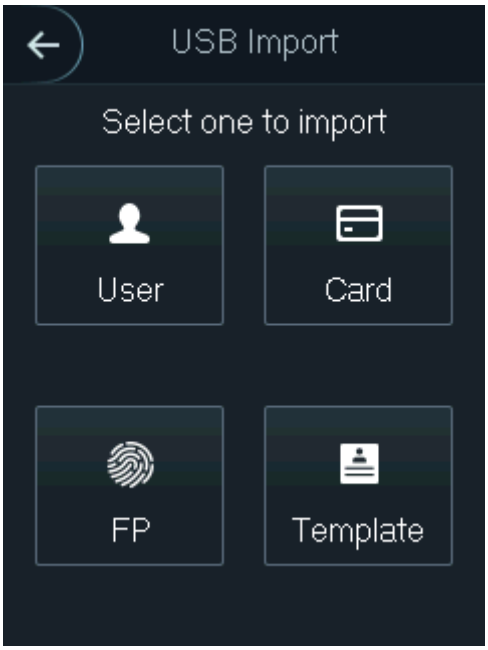
3.10.2 Importación USB

Edite la información del usuario en la plantilla exportada y luego impórtela a la versión independiente.

Paso 1 Seleccione **USB> Importación USB.**

los **Importación USB** se muestra la interfaz.

Figura 3-15 Importación USB



Paso 2 Seleccione el tipo de datos que desea importar.

El aviso **Confirmar para importar** se visualiza.

Paso 3 Toque **OKAY.**

Los datos en el USB se importarán al modo autónomo.

3.10.3 Actualización USB

Se puede utilizar USB para actualizar el sistema.

Paso 1 Cambie el nombre del archivo de actualización a "update.bin" y guarde el archivo "update.bin" en el directorio raíz del USB.

Paso 2 Seleccione **USB> Actualización USB.**

El aviso **Confirmar para actualizar** se visualiza.

Paso 3 Toque **OKAY.**

La actualización comienza y el sistema autónomo se reinicia una vez finalizada la actualización.

3.10.4 Salvapantallas

Inserte un USB con imágenes y toque **Salvapantallas** para importar imágenes desde el USB como protector de pantalla.

- El formato de la imagen debe ser .png y no se admite .jpg. Las imágenes deben
- estar en la misma escala con 240 × 320. El nombre de la imagen debe ser
- Screensaver1-5.

3.10.5 Exportación de registros

Puede buscar y exportar todos los registros de desbloqueo.

3.11 Información del sistema

Puede buscar todos los registros de desbloqueo y ver la capacidad de datos y la versión del dispositivo independiente en el **Información del sistema** interfaz.

4 Operación web

El autónomo se puede configurar y operar en la web. A través de la web, puede establecer parámetros de red, parámetros de video y parámetros independientes; y también puede mantener y actualizar el sistema.

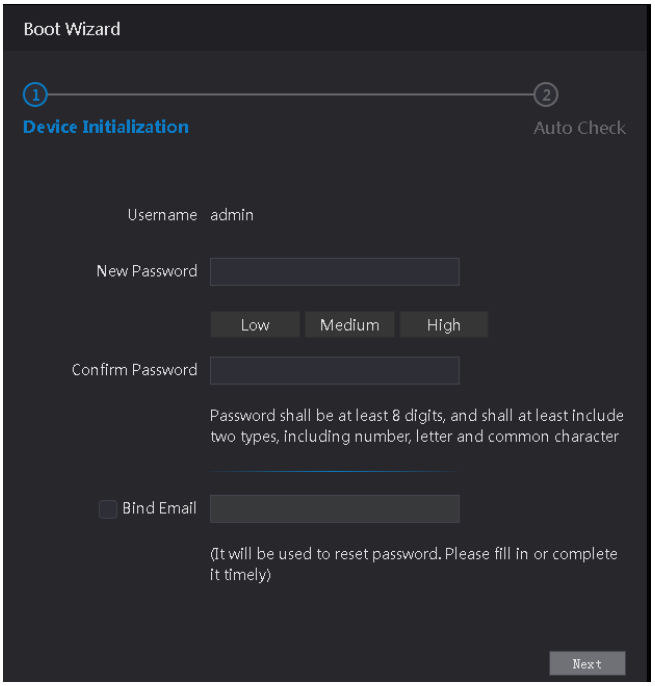
4.1 Inicialización

Debe establecer una contraseña y una dirección de correo electrónico antes de iniciar sesión en la web por primera vez.

Paso 1 Abra el navegador web IE, ingrese la dirección IP (la dirección predeterminada es 192.168.1.108) independiente en la barra de direcciones y luego presione la tecla Intro. los **Inicialización** se muestra la interfaz.

Utilice un navegador más reciente que IE 8; de lo contrario, es posible que no inicie sesión en la web.

Figura 4-1 Inicialización



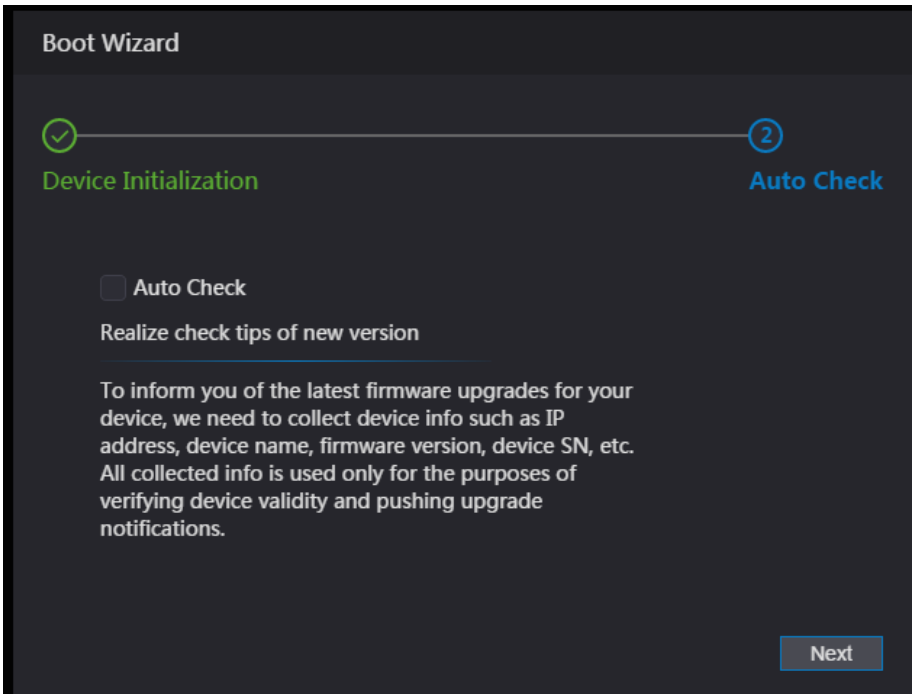
Paso 2 Ingrese la nueva contraseña, confirme la contraseña, ingrese una dirección de correo electrónico y luego toque **Próximo.**

- Por seguridad, mantenga la contraseña correctamente después de la inicialización y cámbiela con regularidad.
- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo '";: &). Establezca una contraseña de alto nivel de seguridad según la solicitud de seguridad de la contraseña.
- Cuando necesite restablecer la contraseña de administrador escaneando el código QR, necesita una dirección de correo electrónico para recibir el código de seguridad.

Paso 3 Haga clic en **Próximo.**

Se muestra la interfaz de verificación automática.

Figura 4-2 Prueba automática



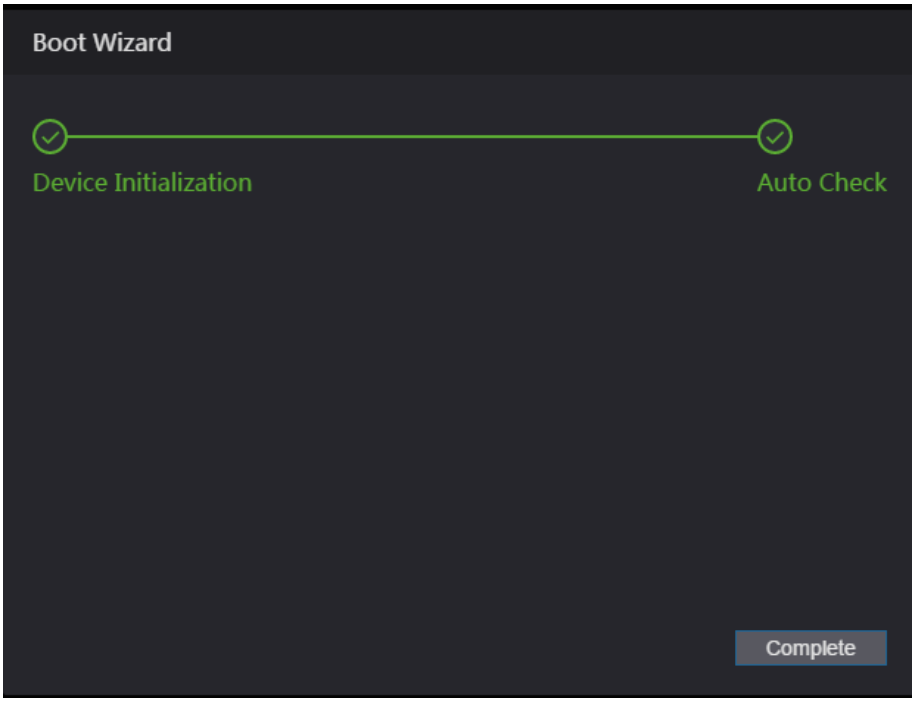
Paso 4 Puede decidir si desea seleccionar **Verificación automática.**

Se recomienda que **Verificación automática** ser seleccionado para obtener el último programa a tiempo.

Paso 5 Haga clic en **Próximo.**

La configuración está terminada.

Figura 4-3 Configuración finalizada



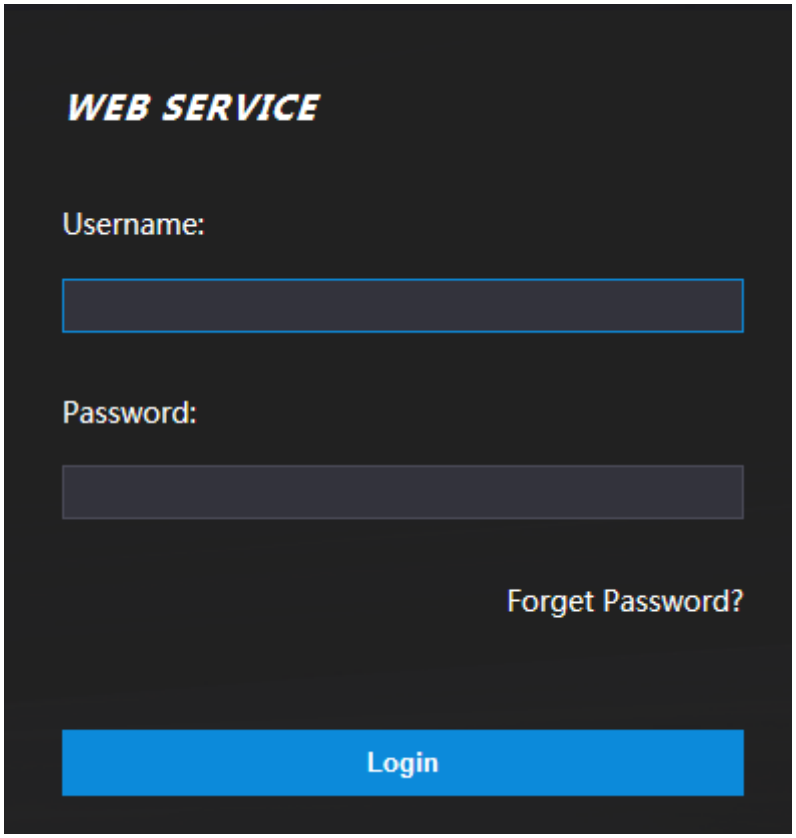
Paso 6 Haga clic en **Completar,** y se completa la inicialización.

Se muestra la interfaz de inicio de sesión web.

4.2 Iniciar sesión

Paso 1 Abra el navegador web IE, ingrese la dirección IP del autónomo en la barra de direcciones y luego presione Enter. Se muestra la interfaz de inicio de sesión.

Figura 4-4 Inicio de sesión



Paso 2 Ingrese el nombre de usuario y la contraseña.

- El nombre de administrador predeterminado es admin y la contraseña es la contraseña de inicio de sesión después de inicializar el sistema autónomo. Modifique la contraseña con regularidad y consérvela correctamente por motivos de seguridad.
- Si olvida la contraseña de inicio de sesión de administrador, puede hacer clic en **¿Contraseña olvidada?** para restablecerlo. Consulte "4.3 Restablecimiento de la contraseña".

Paso 3 Haga clic en **Iniciar sesión.**

La interfaz web está registrada.

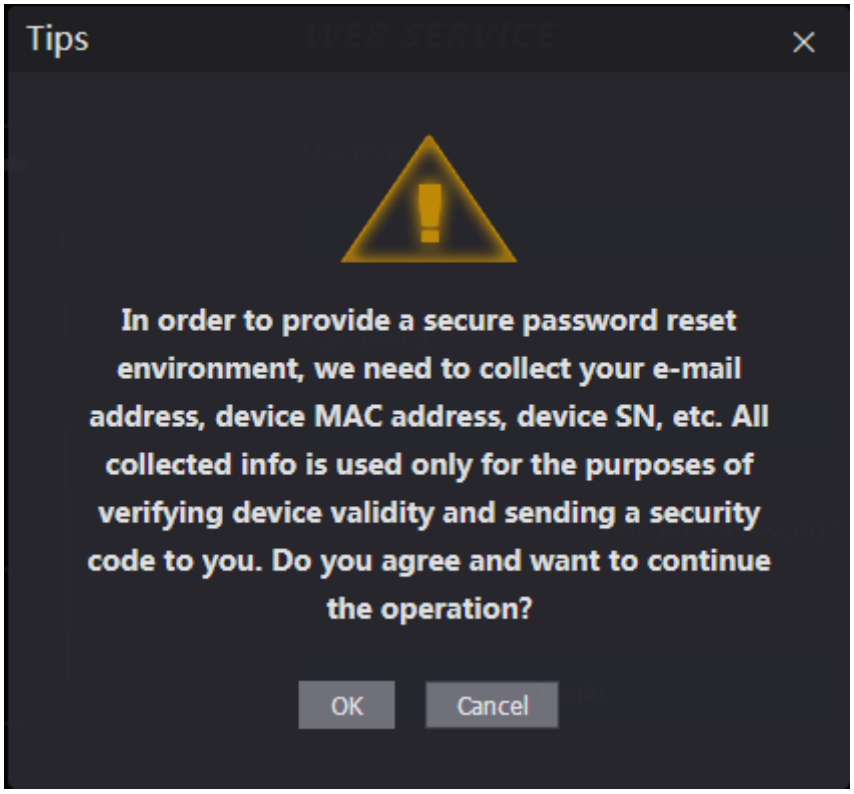
4.3 Restablecimiento de la contraseña

Al restablecer la contraseña de la cuenta de administrador, se necesitará su dirección de correo electrónico.

Paso 1 clic **¿Contraseña olvidada?** en la interfaz de inicio de sesión.

los **Consejos** se muestra la interfaz.

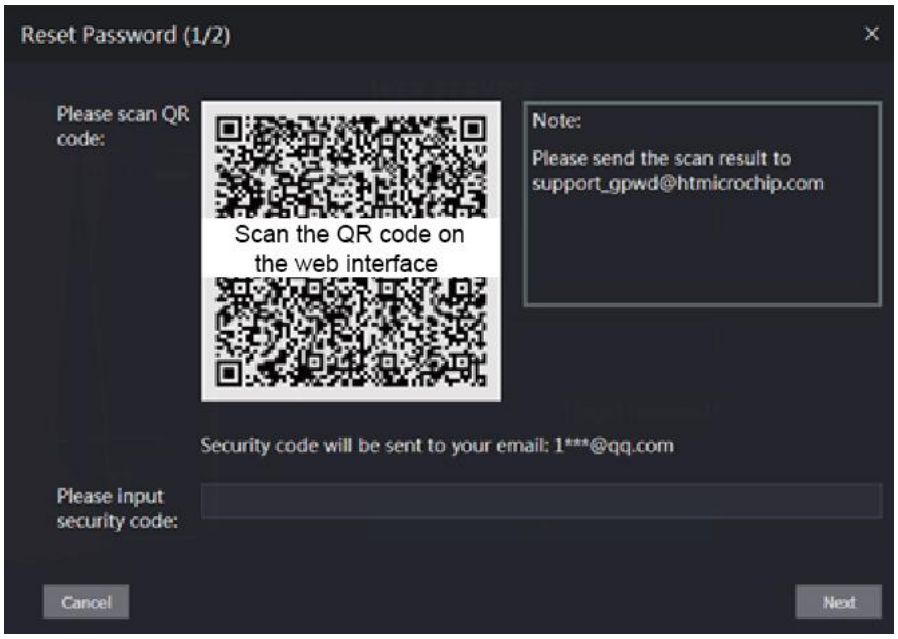
Figura 4-5 Consejos



Paso 2 Lea los consejos y haga clic en **OKAY.**

los **Restablecer la contraseña** se muestra la interfaz.

Figura 4-6 Restablecer contraseña



Paso 3 Escanee el código QR en la interfaz y obtendrá el código de seguridad.

- Se generarán como máximo dos códigos de seguridad escaneando el mismo código QR. Para obtener más código de seguridad, actualice el código QR.
- Debe enviar el contenido que obtiene después de escanear el código QR a la dirección de correo electrónico designada, y luego obtendrá el código de seguridad.

- Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, dejará de ser válido.
- Si se ingresan códigos de seguridad incorrectos cinco veces consecutivas, el administrador quedará congelado durante cinco minutos.

Paso 4 Ingrese el código de seguridad que recibió.

Paso 5 Haga clic en **Próximo.**

los **Restablecer la contraseña** se muestra la interfaz.

Paso 6 Restablezca y confirme la nueva contraseña.

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

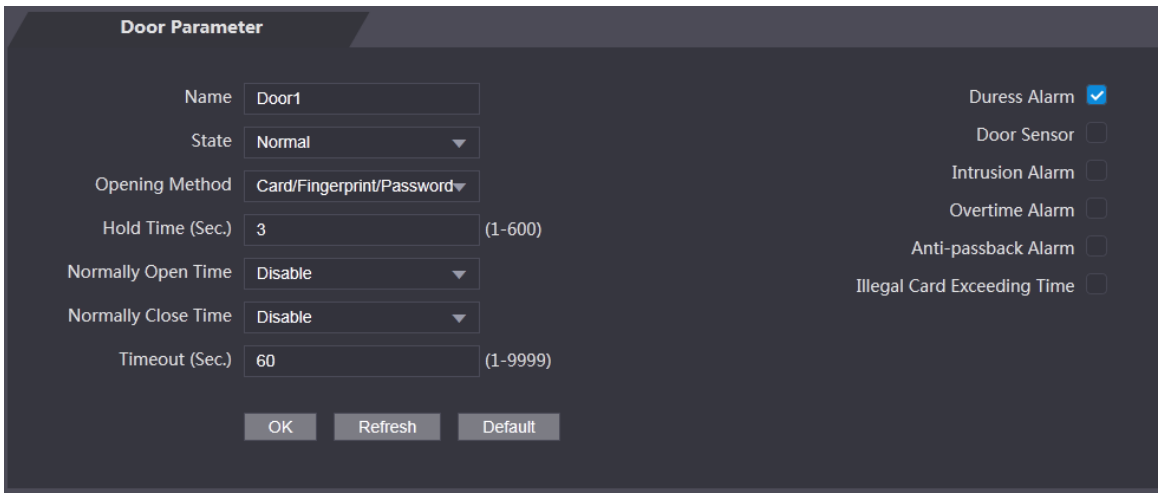
Paso 7 Haga clic en **OKAY,** y se completa el reinicio.

4.4 Parámetro de puerta

Configure los parámetros de la puerta, incluidos el nombre, el estado, el método de apertura, el tiempo del agujero, el tiempo normalmente abierto, el tiempo normalmente cerrado, el tiempo de espera y habilite las alarmas que podrían activarse durante el desbloqueo de la puerta.

Paso 1 clic **Parámetro de puerta.**

Figura 4-7 Parámetro de puerta



Paso 2 Configure los parámetros de la puerta

Tabla 4-1 Descripción de los parámetros de la puerta

Parámetro	Descripción
Nombre	Ingrese un nombre de puerta. Hay tres opciones: **Normal, NC,**
Estado	y **NO.** • Normal: si **Normal** está seleccionado, la puerta se desbloqueará y bloqueará según su configuración. • NC: Si **CAROLINA DEL NORTE** está seleccionado, el estado de la puerta es normalmente cerrado, lo que significa que la puerta no se desbloqueará. • NO: Si **NO** está seleccionado, el estado de la puerta es normalmente abierto, lo que significa que la puerta nunca se cerrará.

Parámetro	Descripción
Método de apertura	Seleccione un método de desbloqueo.
Tiempo de espera (seg.)	La duración en la que se desbloquea la puerta. Si la puerta ha estado desbloqueada por un período que excede la duración, la puerta se bloqueará automáticamente, y el rango es de 1 a 600 segundos.
Normalmente abierto Hora	Seleccione el período que estableció **Sección de tiempo.** Durante el período seleccionado, la puerta normalmente está abierta. Y está deshabilitado por defecto. Seleccione el período que estableció **Sección**
Normalmente cerca Hora	**de tiempo.** Durante el período seleccionado, la puerta normalmente está cerrada. Y está deshabilitado por defecto.
Tiempo de espera (seg.)	Cuando la puerta se abre más tiempo del configurado, se disparará la alarma de horas extras.

Paso 3 Active las alarmas según sea necesario.

Sólo cuando **Sensor de puerta** está habilitado, puedo **alarma de intrusión** y **Alarma de horas extras** ser activado.

4.5 Enlace de alarma

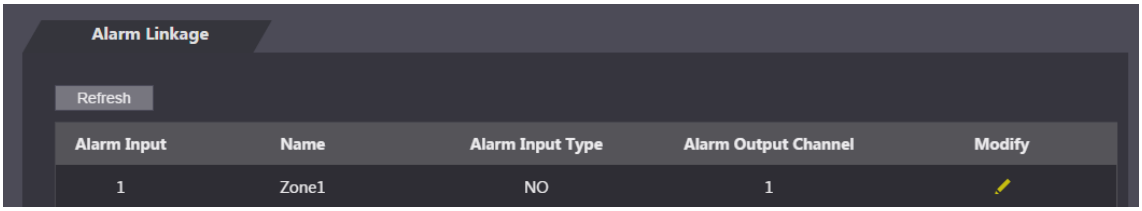
4.5.1 Configuración del enlace de alarma

Los dispositivos de entrada de alarma se pueden conectar al independiente y puede modificar el parámetro de enlace de alarma según sea necesario.

Paso 1 Seleccione **Enlace de alarma> Enlace de alarma** en la barra de navegación.

los **Enlace de alarma** se muestra la interfaz.

Figura 4-8 Enlace de alarma



Paso 2 Haga clic en y luego puede modificar los parámetros de vinculación de alarmas.

Figura 4-9 Modificación del parámetro de vinculación de alarmas

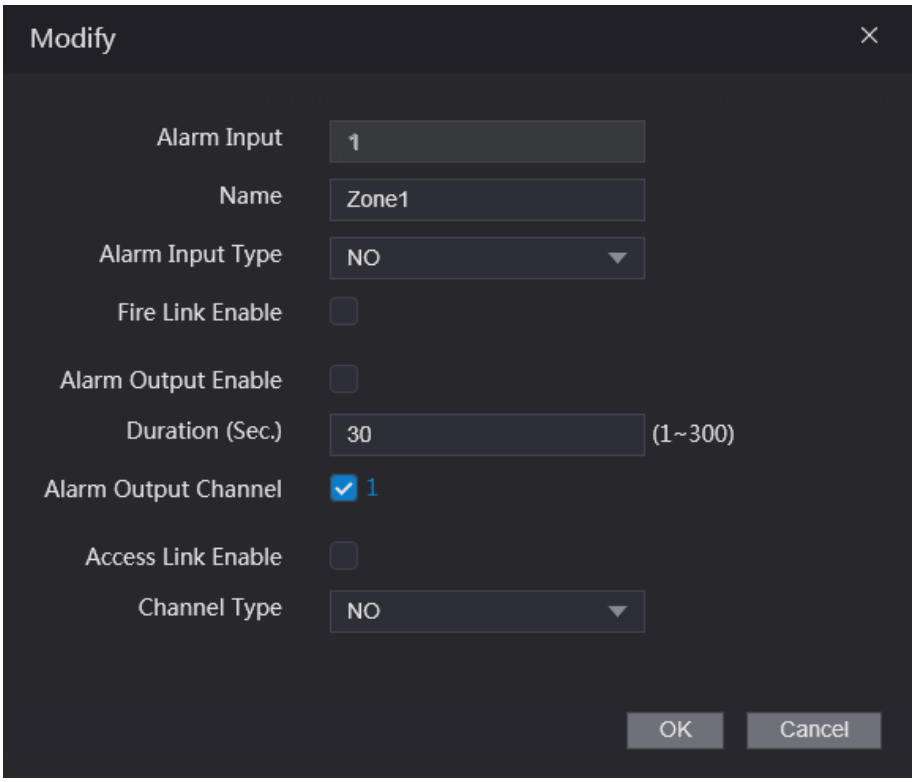


Tabla 4-2 Descripción del parámetro de vinculación de alarmas

Parámetro	Descripción
Entrada de alarma	No puede modificar el valor. Manténgalo predeterminado. Ingrese un
Nombre	nombre de zona.
Tipo de entrada de alarma	Hay dos opciones: **NO** y **CAROLINA DEL NORTE.** Si el tipo de entrada de alarma del dispositivo de alarma que compró es **NO,** entonces deberías seleccionar **NO;** de lo contrario deberías seleccionar **CAROLINA DEL NORTE.**
Activar enlace de fuego	Si el enlace de incendio está habilitado, el autónomo emitirá alarmas cuando se activen las alarmas de incendio. Los detalles de la alarma se mostrarán en el registro de alarmas. La salida de alarma y el enlace de acceso son NO de forma predeterminada si el enlace de incendio está
Salida de alarma Habilitar	habilitado. El relé puede emitir información de alarma (se enviará a la plataforma de gestión) si el **Salida de alarma** está habilitado. La duración de la alarma y el rango es de 1 a 300 segundos.
Duración (seg.)	
Salida de alarma Canal	Puede seleccionar un canal de salida de alarma según el dispositivo de alarma que haya instalado. Cada dispositivo de alarma puede considerarse un canal.
Enlace de acceso Habilitar	Una vez habilitado el enlace de acceso, el autónomo estará normalmente abierto o normalmente cerrado cuando haya señales de alarma de entrada.
Tipo de canal	Hay dos opciones: **NO** y **CAROLINA DEL NORTE.**

Paso 3 Haga clic en **OKAY,** y luego se completa la configuración.

La configuración en la web se sincronizará con la configuración en el cliente si se agrega el independiente a un cliente.

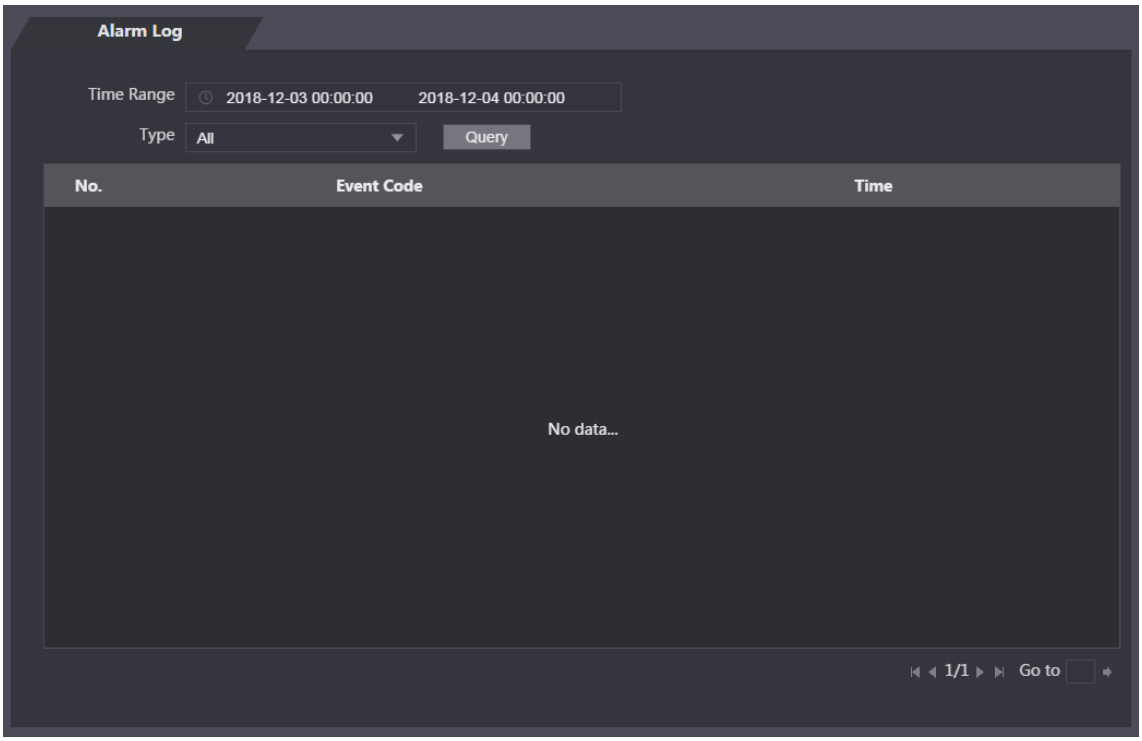
4.5.2 Registro de alarmas

Puede ver el tipo de alarma y el rango de tiempo en la **Registro de alarmas** interfaz.

Paso 1 Seleccione **Enlace de alarmas> Registro de alarmas.**

los **Registro de alarmas** se muestra la interfaz.

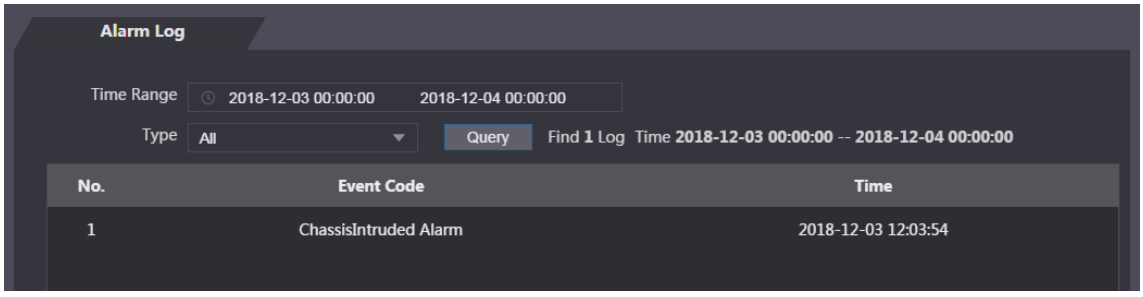
Figura 4-10 Registro de alarmas



Paso 2 Seleccione un rango de tiempo y un tipo de alarma y luego haga clic en **Consulta.**

Se muestran los resultados de la consulta.

Figura 4-11 Resultados de la consulta



4.6 Configuración de la sección de tiempo

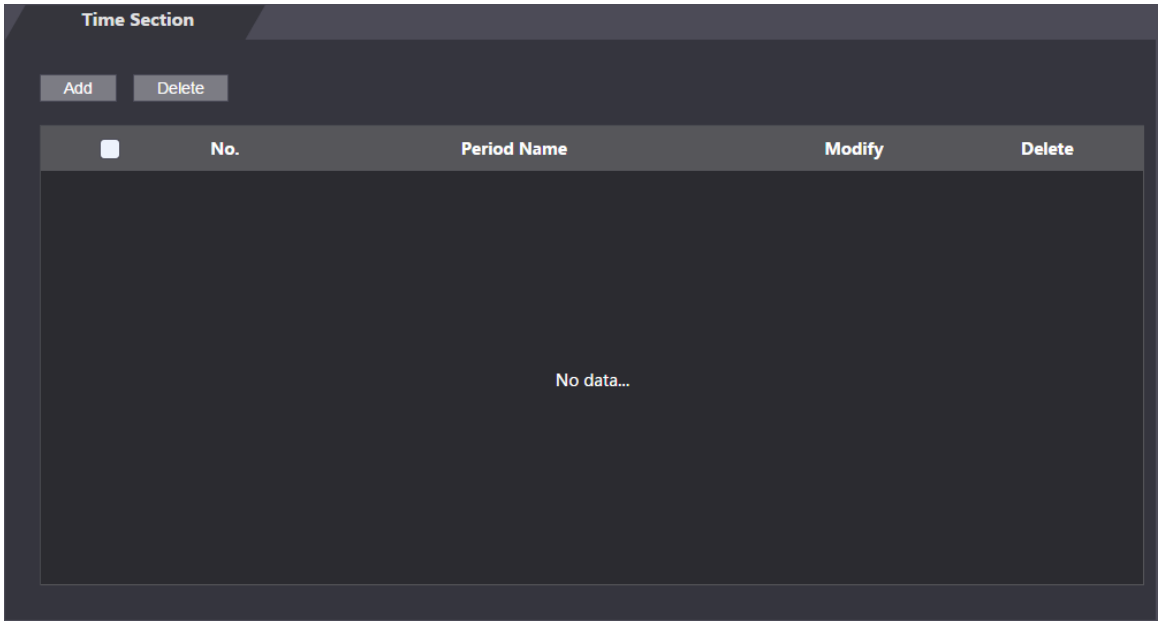
Puede establecer períodos, períodos de vacaciones y períodos de planes de vacaciones.

4.6.1 Sección de tiempo

Después de establecer el período, los usuarios solo pueden desbloquear la puerta en los períodos que haya establecido.

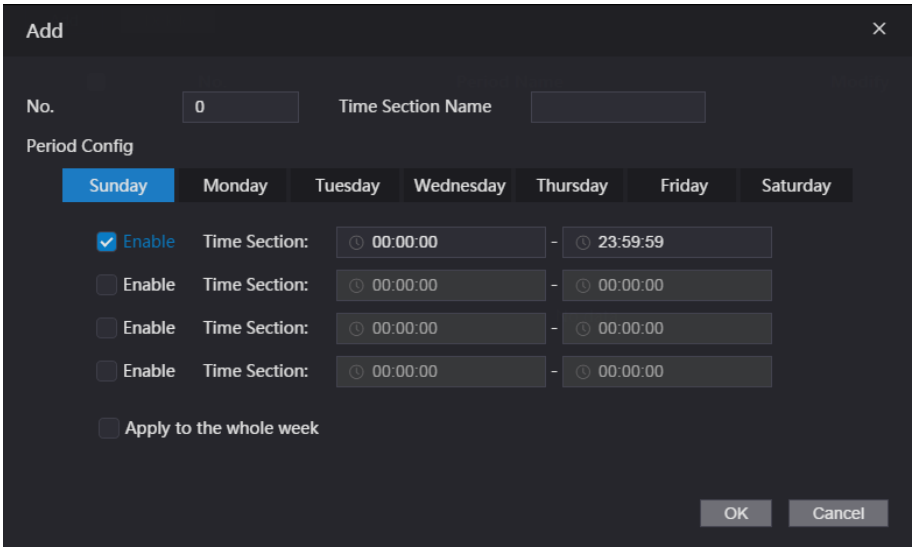
Paso 1 Seleccione **Sección de tiempo> Sección de tiempo.**

Figura 4-12 Sección de tiempo



Paso 2 Haga clic en **Añadir.**

Figura 4-13 Agregar período



Paso 3 Configure el número de período y el nombre de la sección de tiempo. Selecciona el **Habilitar** casilla de verificación y la sección de tiempo según sea necesario.

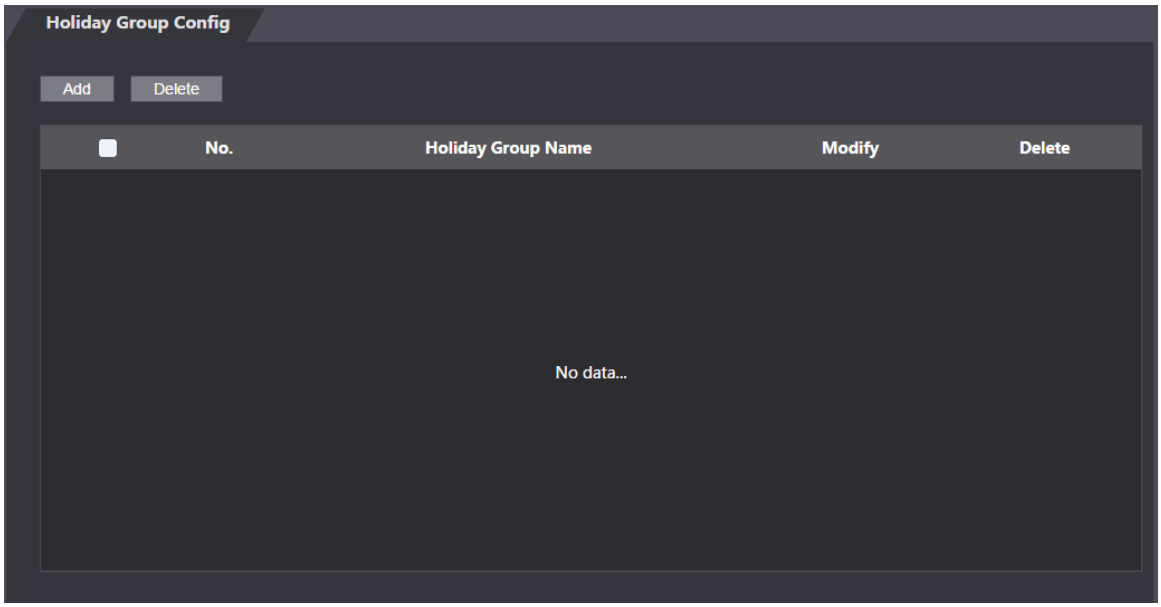
Puede configurar 128 períodos (semanas) cuyo rango de números es 0-127, y establecer cuatro períodos en cada día de un período (semana). El valor predeterminado es 255, lo que indica que el período no está configurado; 0-127 es el período configurado manualmente. Puede editar el período configurado en el **Lista de usuarios** en el independiente.

4.6.2 Configuración del grupo de vacaciones

Configure la hora de inicio y la hora de finalización de un grupo de vacaciones, y los usuarios no podrán desbloquear la puerta en los períodos que haya establecido.

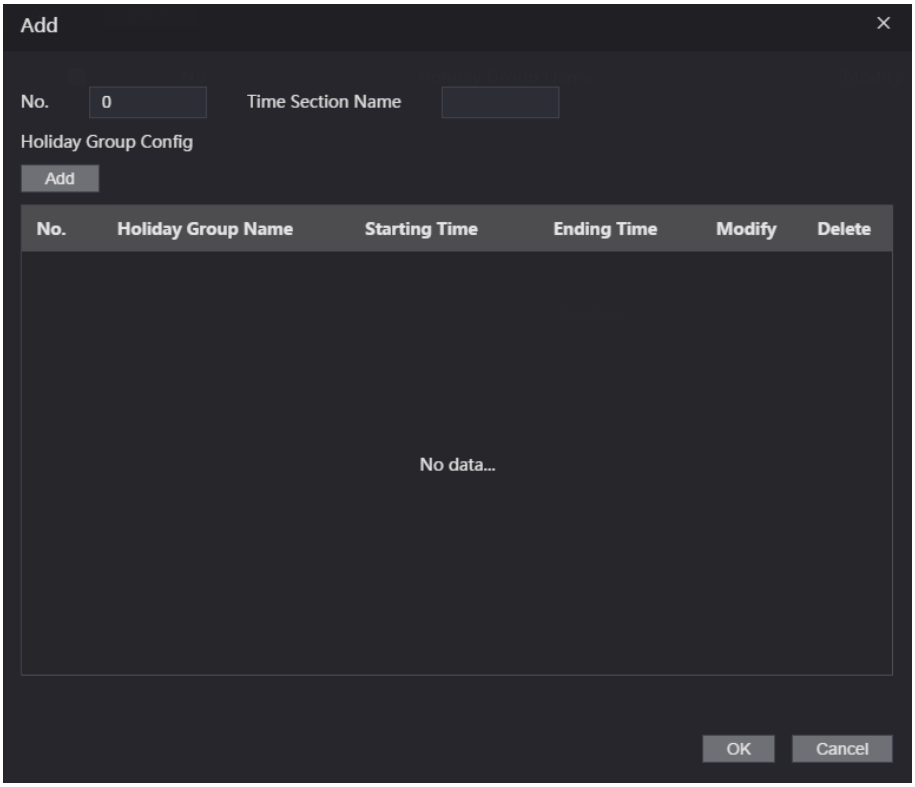
Paso 1 Seleccione **Sección de tiempo> Configuración de grupo de vacaciones.**

Figura 4-14 Configuración del grupo de vacaciones



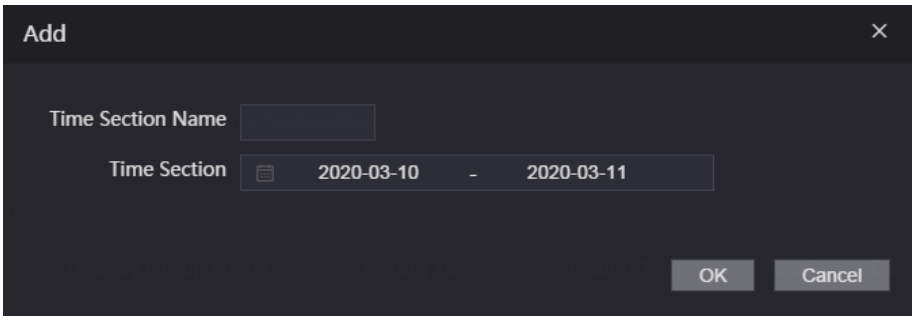
Paso 2 Haga clic en **Añadir.**

Figura 4-15 Agregar grupo de vacaciones



Paso 3 Configure el número de período y el nombre de la sección de tiempo y luego haga clic en **Añadir.**

Figura 4-16 Agregar configuración de grupo de vacaciones



Paso 4 Configure el nombre de la sección de tiempo y la sección de tiempo según sea necesario.

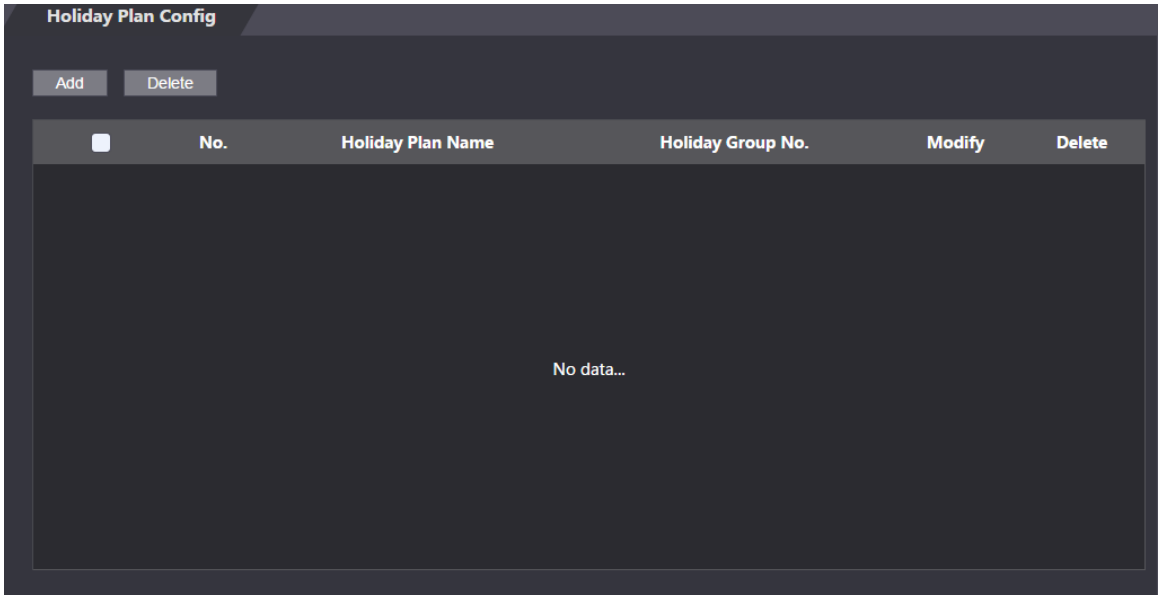
Puede establecer vacaciones en grupo y, a continuación, puede establecer planes para grupos de vacaciones. Puede configurar 128 grupos cuyo rango de números es 0-127. Puede agregar 16 días festivos a un grupo.

4.6.3 Configuración del plan de vacaciones

Puede agregar grupos de vacaciones a los planes de vacaciones y los usuarios solo pueden desbloquear la puerta en el período que establezca.

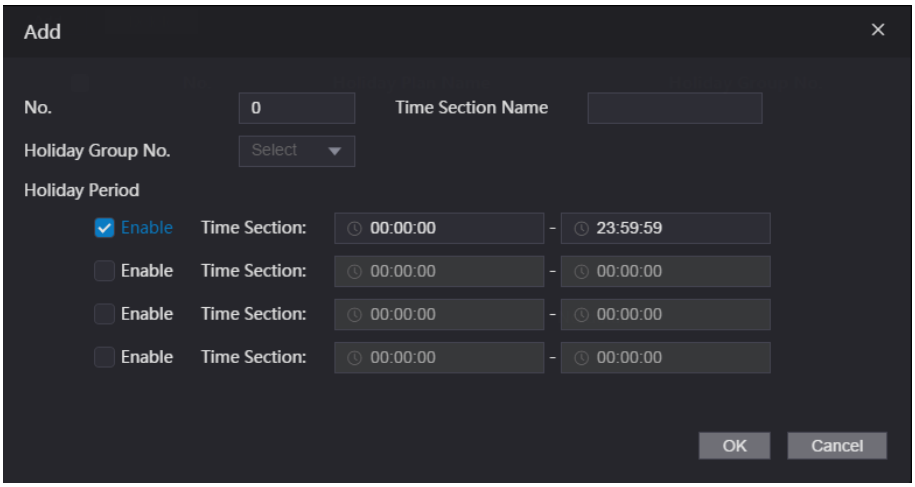
Paso 1 Seleccione **Sección de tiempo> Configuración del plan de vacaciones.**

Figura 4-17 Configuración del plan de vacaciones



Paso 2 Haga clic en **Añadir.**

Figura 4-18 Agregar plan de vacaciones



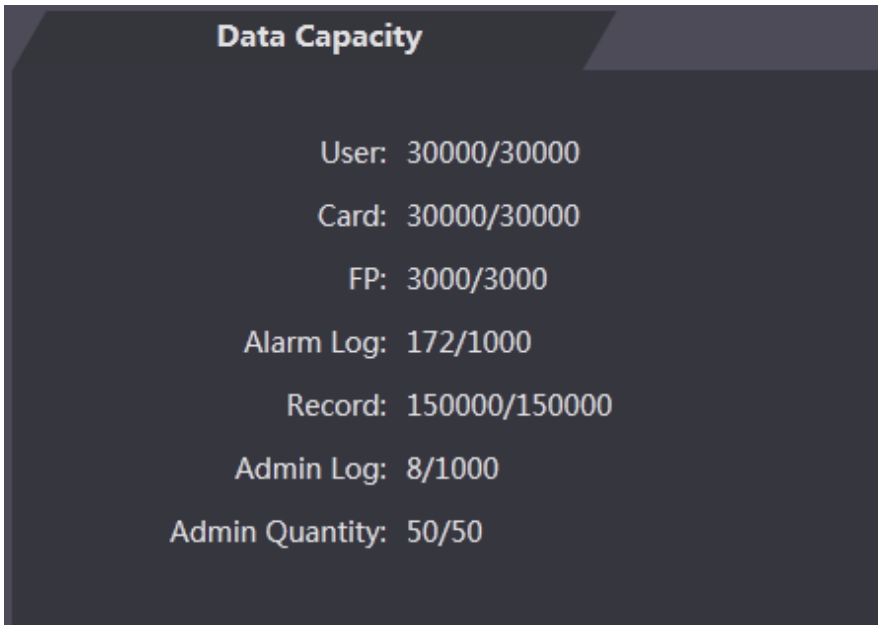
Paso 3 Configure el número de período y el nombre de la sección de tiempo, seleccione el número de grupo de vacaciones, seleccione la **Habilitar** casilla de verificación y luego establezca la sección de tiempo.

Paso 4 Haga clic en **OKAY.**

4.7 Capacidad de datos

Puede ver cuántos usuarios, tarjetas, huellas dactilares, registros de alarmas, registros, registros de administración y cantidad de administración puede retener la unidad independiente en el **Capacidad de datos** interfaz.

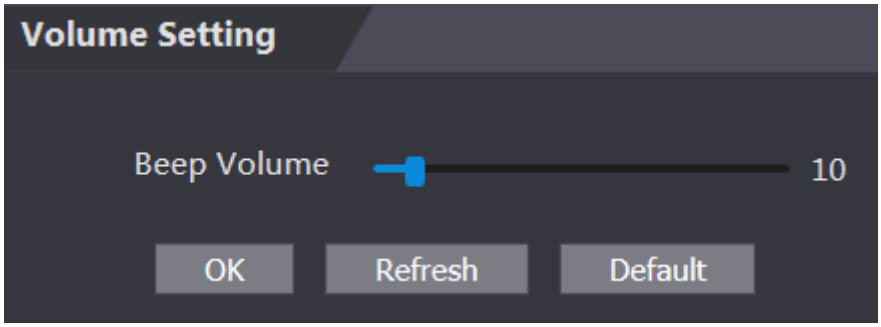
Figura 4-19 Capacidad de datos



4.8 Ajuste de volumen

Puede configurar el volumen del pitido en el **Ajuste de volumen** interfaz.

Figura 4-20 Configuración de volumen



4.9 Configuración de red

4.9.1 TCP / IP

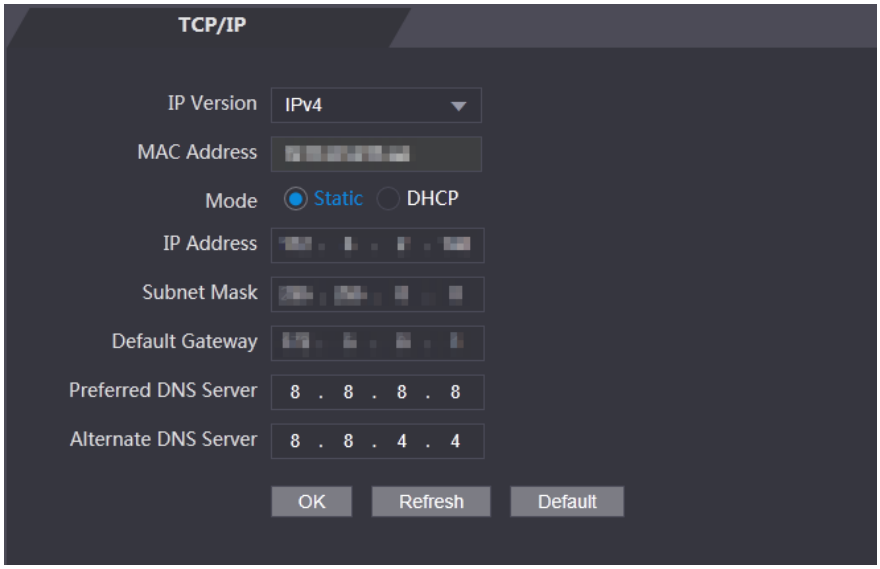
Debe configurar la dirección IP y el servidor DNS para asegurarse de que el autónomo pueda comunicarse con otros dispositivos.

Condición previa

Asegúrese de que el autónomo esté conectado a la red correctamente.

Paso 1 Seleccione **Configuración de red> TCP / IP.**

Figura 4-21 TCP / IP



Paso 2 Configure los parámetros.

Tabla 4-3 TCP / IP

Parámetro	Descripción
Versión IP	Hay una opción: IPv4.
MAC	Se muestra la dirección MAC del autónomo.
Modo	• Estático Configure la dirección IP, la máscara de subred y la dirección de la puerta de enlace manualmente. • DHCP • Una vez que se habilita DHCP, la dirección IP, la máscara de subred y la dirección de la puerta de enlace no se pueden configurar. • Si DHCP es efectivo, la dirección IP, la máscara de subred y la dirección de la puerta de enlace se mostrarán automáticamente; si DHCP no es efectivo, la dirección IP, la máscara de subred y la dirección de la puerta de enlace serán todas cero.
Dirección IP Máscara de subred Puerta	Ingrese la dirección IP y luego configure la máscara de subred y la dirección de la puerta de enlace. La dirección IP y la dirección de la puerta de enlace deben estar en el mismo segmento de red.
Privilegiado DNS Servidor	Configure la dirección IP del servidor DNS preferido.
Alterno DNS Servidor	Configure la dirección IP del servidor DNS alternativo.

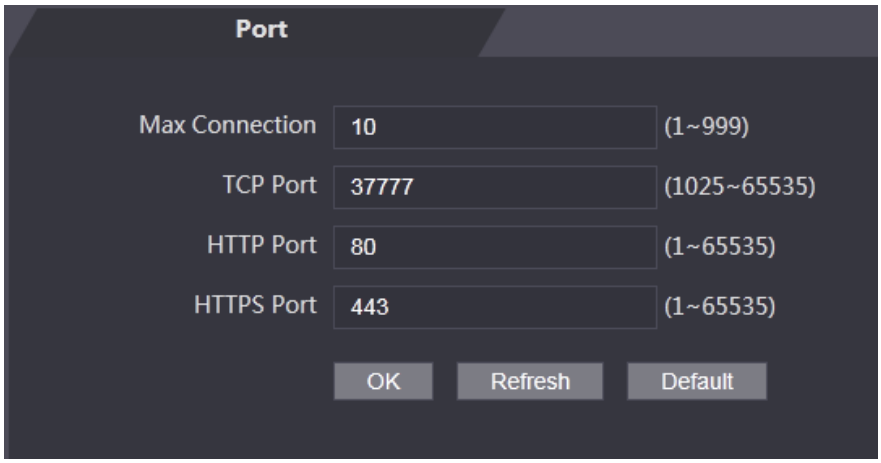
Paso 3 Haga clic en **Okay** para completar el ajuste.

4.9.2 Puerto

Establezca el número máximo de clientes a los que se puede conectar el autónomo y los números de puerto.

Paso 1 Seleccione **Configuración de red> Puerto.**

Figura 4-22 Puerto



Paso 2 Configure los números de puerto. Consulte la siguiente tabla.

Excepto la conexión máxima, debe reiniciar el sistema autónomo para que la configuración sea efectiva después de modificar los valores.

Tabla 4-4 Descripción del puerto

Parámetro	Descripción
Max Conexión	Puede establecer el número máximo de clientes a los que se puede conectar el autónomo. Los clientes de plataforma como SmartPSS no se cuentan. El valor
Puerto TCP	predeterminado es 37777.
Puerto HTTP	El valor predeterminado es 80. Si se usa otro valor como número de puerto, debe agregar este valor detrás de la dirección al iniciar sesión a través de los navegadores. El valor predeterminado es 443.
Puerto HTTPS	

Paso 3 Haga clic en **Okay** para completar el ajuste.

4.9.3 P2P

La informática o las redes de igual a igual es una arquitectura de aplicación distribuida que divide tareas o cargas de trabajo entre pares. Los usuarios pueden descargar la aplicación móvil escaneando el código QR y luego registrar una cuenta para poder administrar más de una independiente en la aplicación móvil. No necesita aplicar un nombre de dominio dinámico, hacer un mapeo de puertos o no necesita un servidor de tránsito.

Si va a utilizar P2P, debe conectar el autónomo a una red externa; de lo contrario, no se puede utilizar el independiente.

Paso 1 Seleccione **Configuración de red> P2P.**

Figura 4-23 P2P

Paso 2 Seleccione **Habilitar** para habilitar la función P2P.

Paso 3 Haga clic en **Okay** para completar el ajuste.

Escanee el código QR en su interfaz web para obtener el número de serie del autónomo.

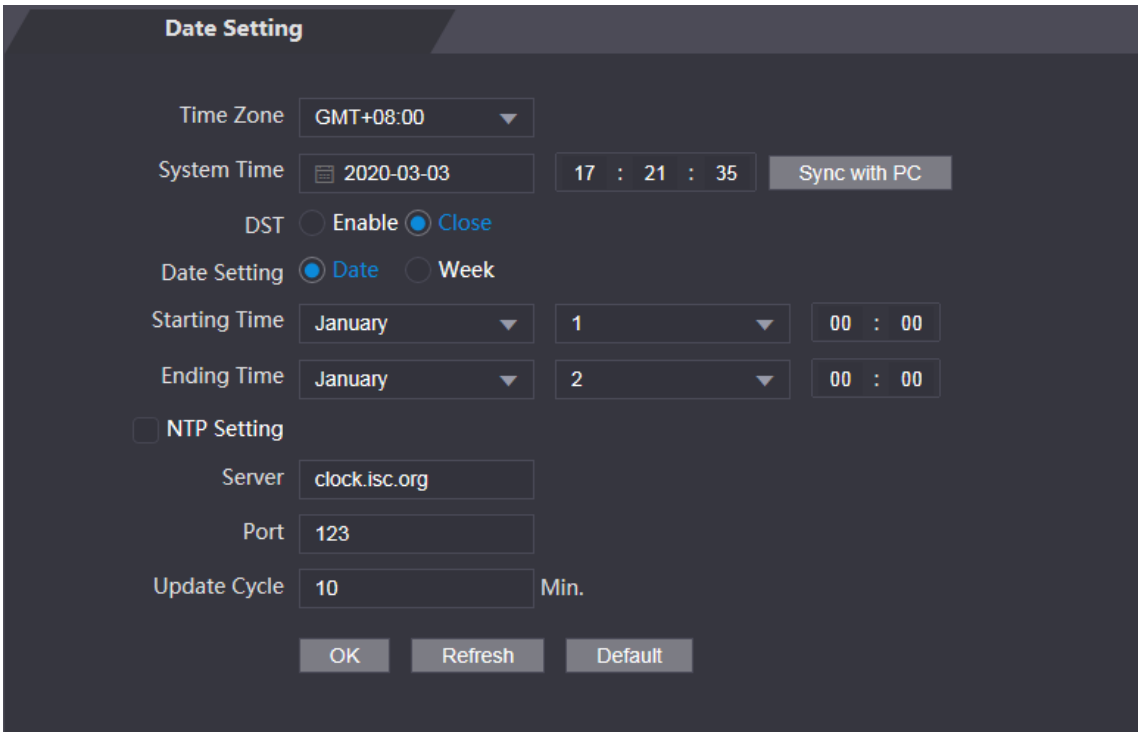
4.10 Configuración de datos

Puede configurar la zona horaria, la hora del sistema, la fecha, DST y NTP.

Cuando selecciona Network Time Protocol (NTP), debe configurar los siguientes parámetros. Primero debe habilitar la función NTP Check.

- Servidor: ingrese la dirección IP del servidor de hora, y la hora del servidor autónomo se sincronizará con el servidor de hora.
- Puerto: introduzca el número de puerto del servidor horario.
- Ciclo de actualización (min): intervalo de verificación NPT. Toque el icono de guardar para guardar.

Figura 4-24 Configuración de fecha

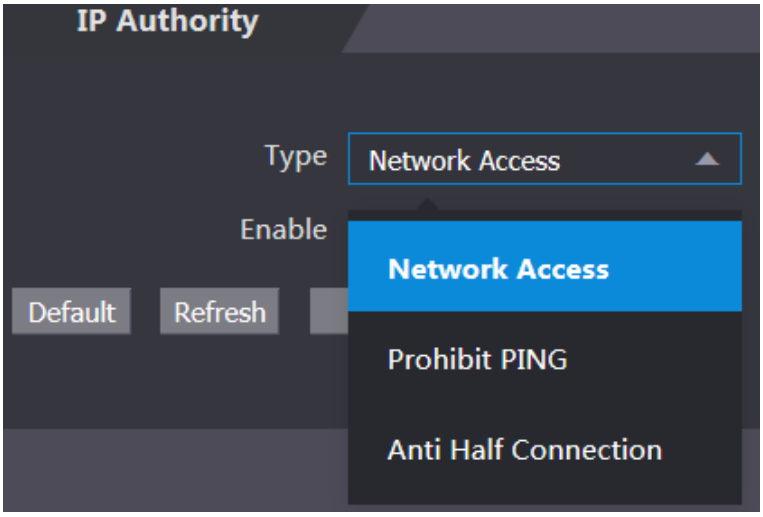


4.11 Gestión de la seguridad

4.11.1 Autoridad de propiedad intelectual

Seleccione un modo de seguridad cibernética según sea necesario.

Figura 4-25 Autoridad de IP



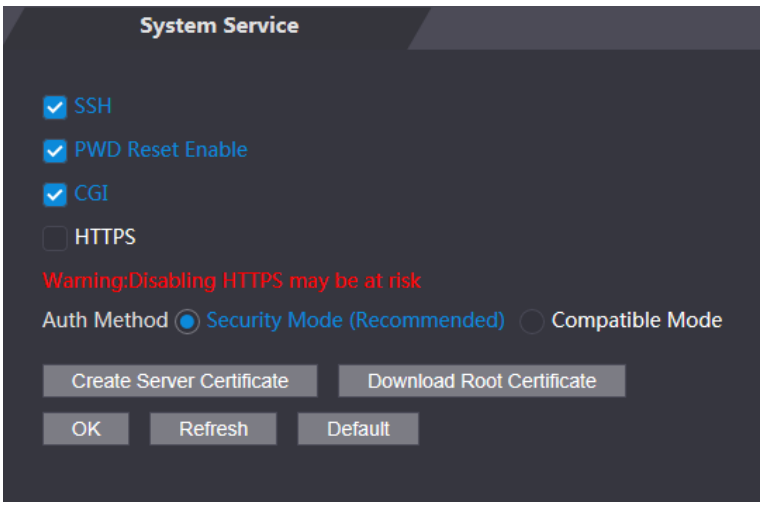
4.11.2 Sistema

4.11.2.1 Servicio del sistema

Hay cuatro opciones: SSH, PWD Reset Enable, CGI y HTTPS. Para obtener más información, consulte "3.9.4 Configuración de privacidad".

La configuración del servicio del sistema realizada en la página web y la configuración en el **Configuración de privacidad** Se sincronizará la interfaz del autónomo.

Figura 4-26 Servicio del sistema



4.11.3 Gestión de usuarios

Puede agregar y eliminar usuarios, modificar las contraseñas de los usuarios e ingresar una dirección de correo electrónico para restablecer la contraseña cuando la olvide.

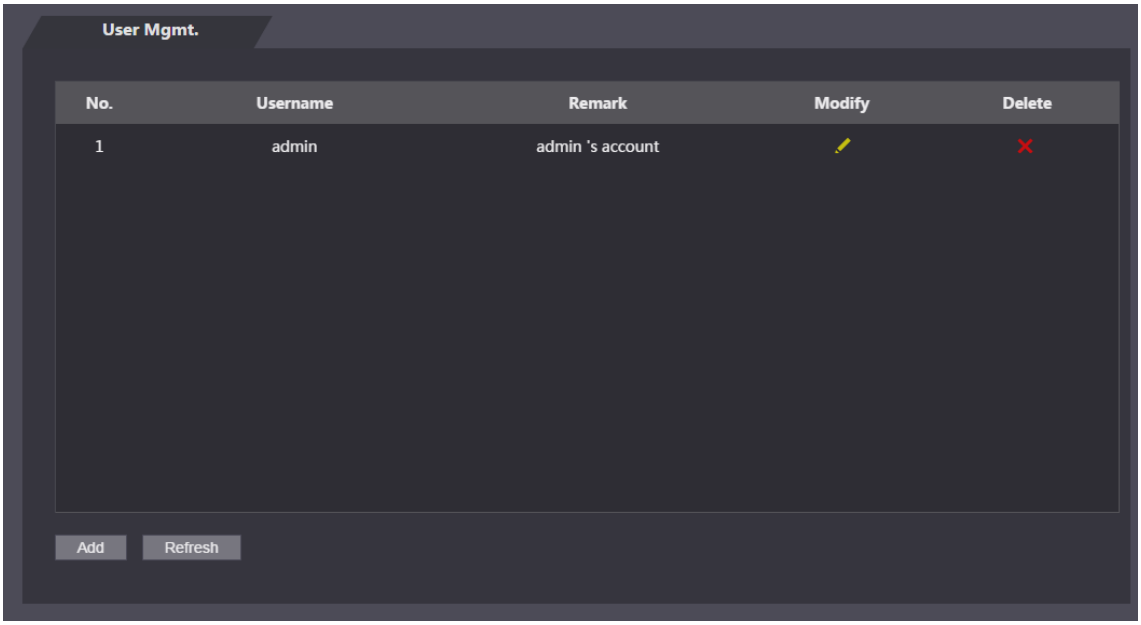
4.11.3.1 Agregar usuarios

Hacer clic **Añadir** sobre el **Gestión de usuarios** interfaz para agregar usuarios y luego ingrese el nombre de usuario, la contraseña, la contraseña confirmada y el comentario. Hacer clic **Okay** para completar la adición del usuario.

4.11.3.2 Modificar la información del usuario

Puede modificar la información del usuario haciendo clic en  sobre el **Gestión de usuarios** interfaz.

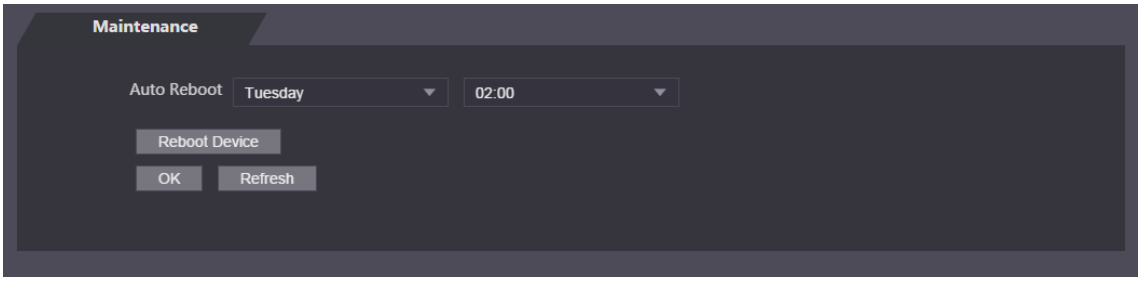
Figura 4-27 Gestión de usuarios



4.11.4 Mantenimiento

Puede hacer que el autónomo se reinicie automáticamente en tiempo de inactividad para mejorar la velocidad de funcionamiento del autónomo.

Figura 4-28 Mantenimiento

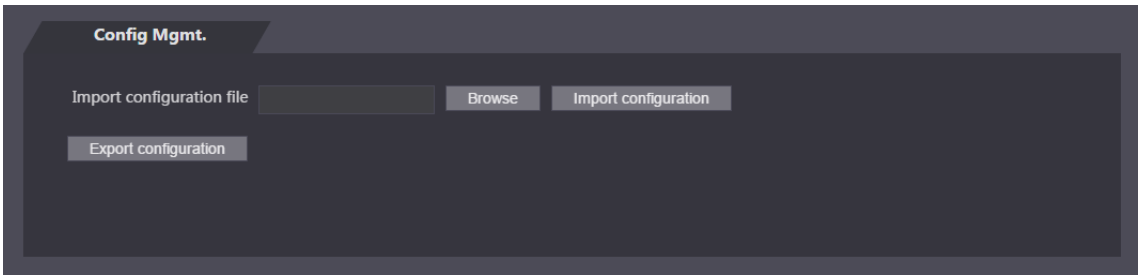


Seleccione la fecha y la hora de reinicio automático. La hora de reinicio predeterminada es a las 2 de la mañana del martes. Hacer clic **Reiniciar dispositivo,** el independiente se reiniciará inmediatamente. Hacer clic **OKAY,** el independiente se reiniciará a las 2 de la mañana todos los martes.

4.11.5 Gestión de la configuración

Cuando más de uno independiente necesita la misma configuración, puede configurar parámetros para ellos importando o exportando archivos de configuración.

Figura 4-29 Gestión de la configuración



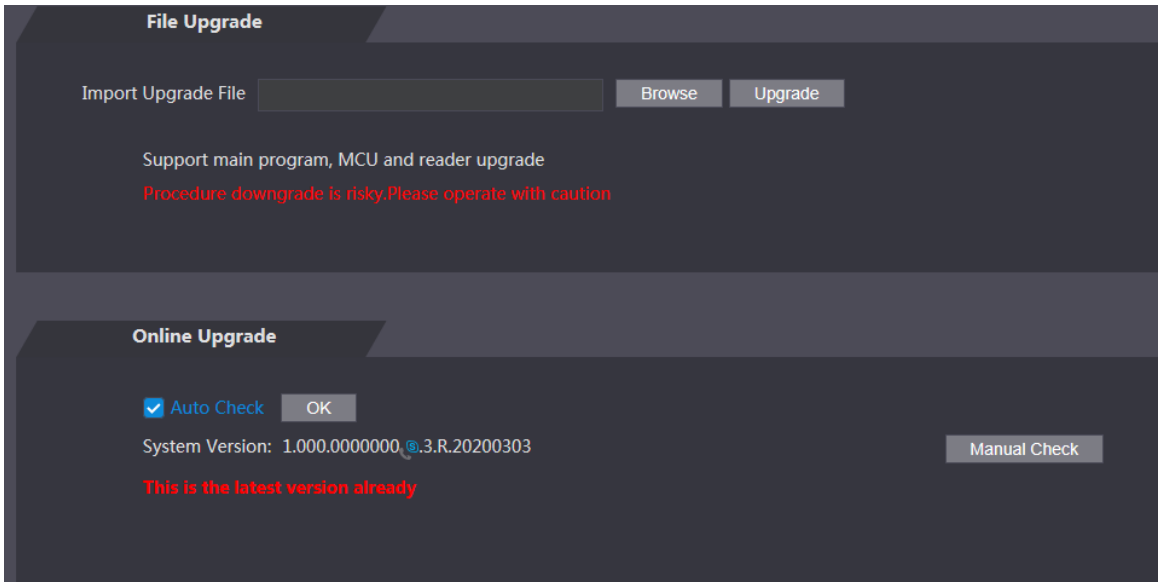
4.11.6 Actualización

La actualización al último sistema puede perfeccionar las funciones independientes y mejorar la estabilidad.

Si se ha utilizado un archivo de actualización incorrecto, el sistema le indicará que la actualización falla y reiniciará el dispositivo automáticamente.

Paso 1 clic **Potenciar** en la barra de navegación.

Figura 4-30 Actualización



Paso 2 Seleccione el método de actualización de acuerdo con las necesidades reales.

- Actualización de archivo

1) Hacer clic **Vistazo,** y luego cargue el archivo de actualización. El archivo de actualización debe ser un archivo .bin. Hacer clic **Potenciar.**

2) Comienza la actualización.

- Actualización en línea

1) Selecciona el **Verificación automática** casilla de verificación y haga clic en **OKAY.**

El sistema verifica la actualización una vez al día automáticamente y habrá un aviso del sistema si hay alguna actualización disponible.

Necesitamos recopilar datos como el nombre del dispositivo, la versión de firmware y el número de serie del dispositivo para preceder a la verificación automática. La información recopilada solo se utiliza para verificar la legalidad de las cámaras y el aviso de actualización.

2) Si hay alguna actualización disponible, haga clic en **Potenciar,** y luego el sistema se inicia actualización.

Hacer clic **Verificación manual** para comprobar la actualización manualmente.

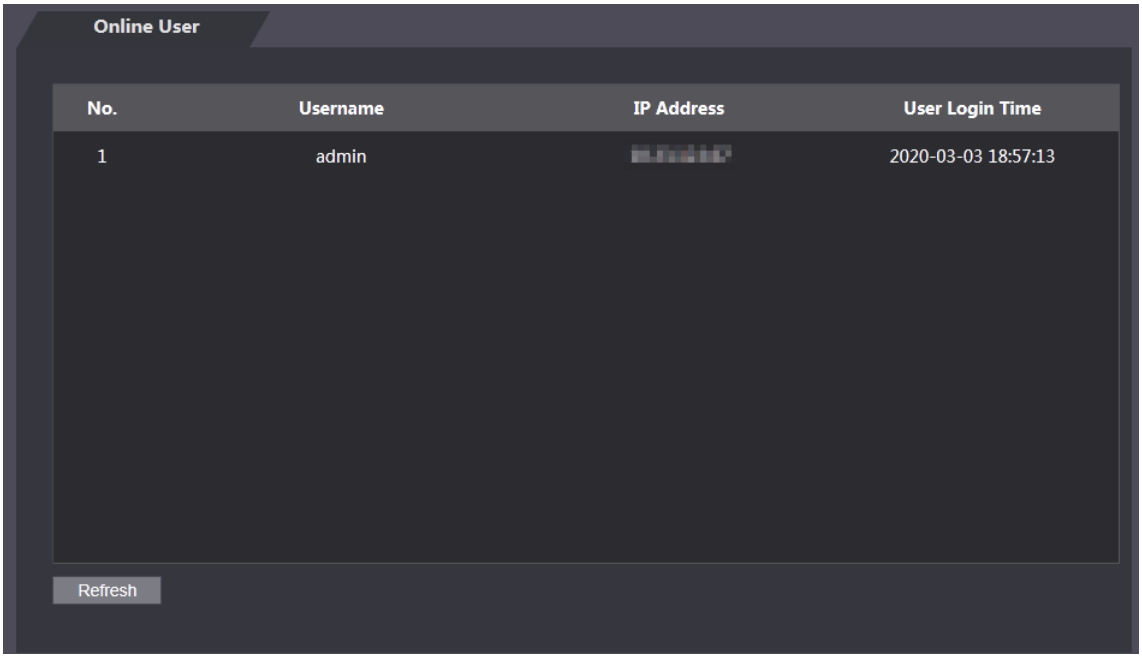
4.11.7 Información de la versión

Puede ver información, incluida la dirección MAC, el número de serie, la versión de MCU, la versión web, la versión de referencia de seguridad, la versión del sistema y la versión de firmware.

4.11.8 Usuario en línea

Puede ver el nombre de usuario, la dirección IP y la hora de inicio de sesión del usuario en el **Usuario en línea** interfaz.

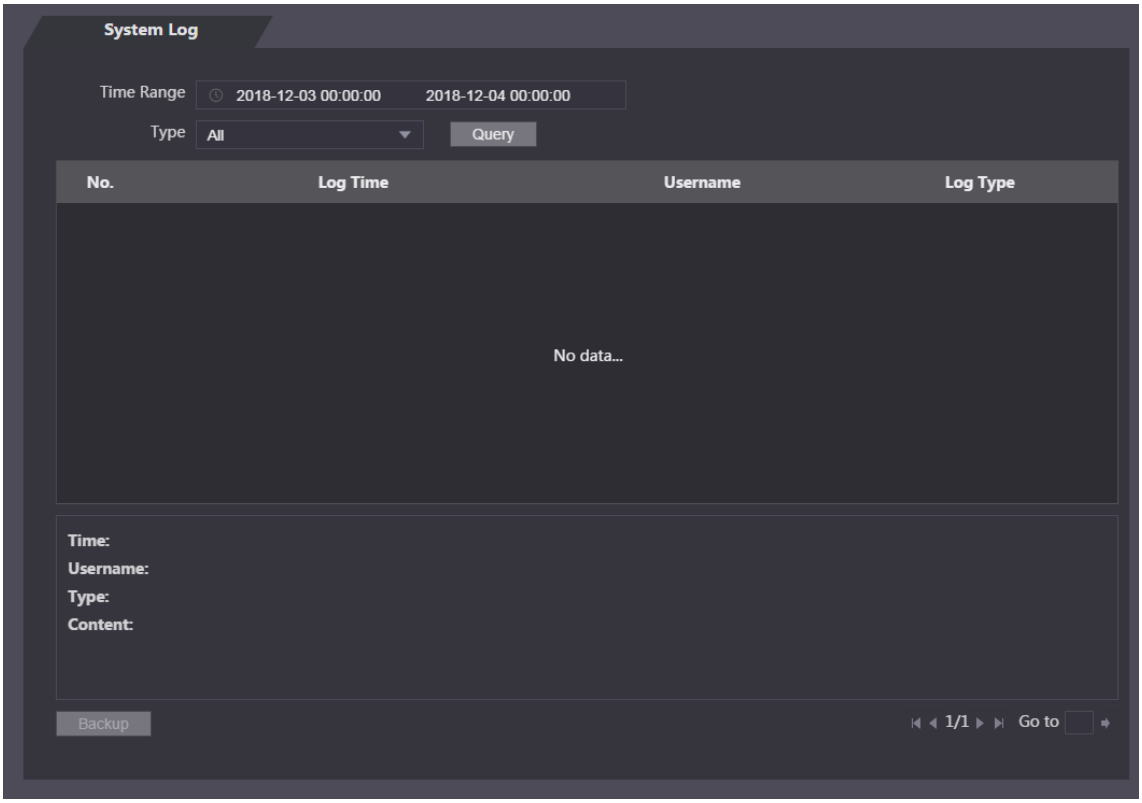
Figura 4-31 Usuario en línea



4.12 Registro del sistema

Puede ver y hacer una copia de seguridad del registro del sistema en el **Registro del sistema** interfaz.

Figura 4-32 Registro del sistema



4.12.1 Registros de consultas

Seleccione un rango de tiempo, escriba, haga clic **Consulta,** y se mostrarán los registros que cumplan las condiciones.

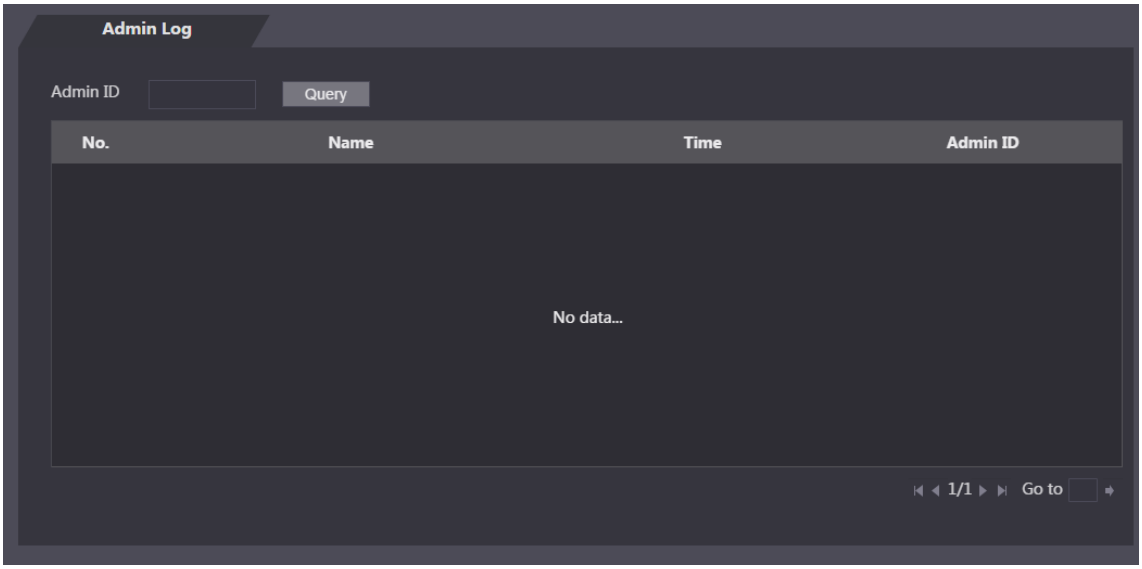
4.12.2 Registros de respaldo

Hacer clic **Apoyo** para hacer una copia de seguridad de los registros mostrados.

4.13 Registro de administración

Ingrese el ID de administrador en el **Registro de administración** interfaz, haga clic en **Consulta,** y luego verá los registros de operaciones del administrador.

Figura 4-33 Registro de administración



4.14 Salir

Hacer clic , haga clic en **OKAY,** y luego cerrará la sesión de la interfaz web.

Coloca el cursor sobre y, a continuación, podrá ver información detallada del usuario actual.

5 Funcionamiento del teléfono móvil

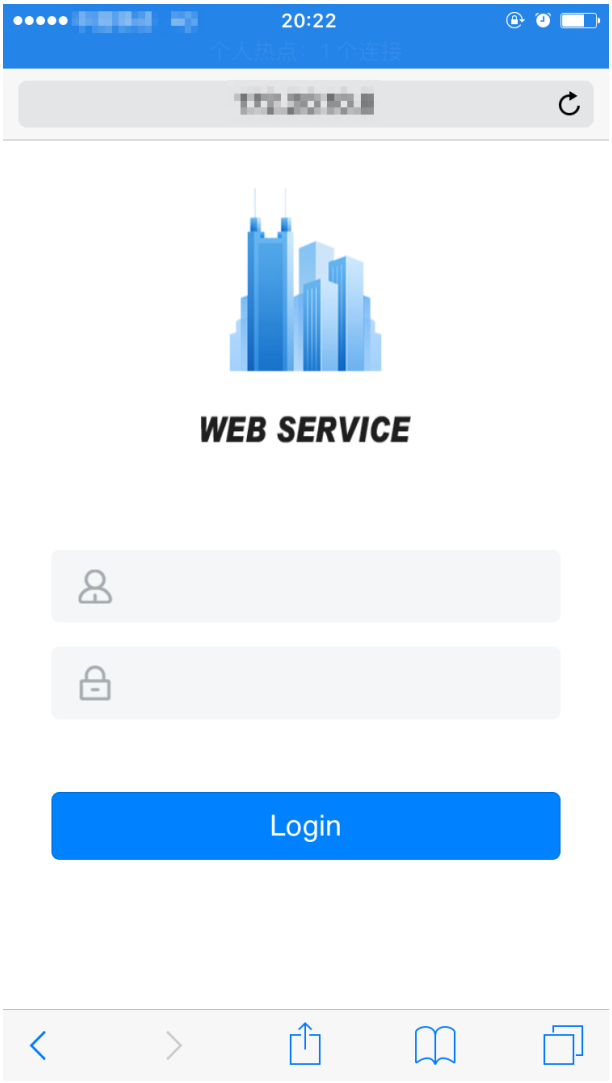
El autónomo se puede configurar y operar en el teléfono móvil. A través del teléfono móvil, puede configurar parámetros, incluidos parámetros de red, parámetros de video y parámetros independientes; y también puede mantener y actualizar el sistema.

Iniciar sesión

Paso 1 Conecte el dispositivo y el teléfono móvil a la misma red.

Paso 2 Abra el navegador en el teléfono móvil, ingrese la dirección IP del dispositivo (se muestra en la interfaz Wi-Fi y 192.168.1.108 de forma predeterminada) del independiente en la barra de direcciones y luego presione Entrar.

Figura 5-1 Inicio de sesión



Paso 3 Introduzca el nombre de usuario y la contraseña.

El nombre de usuario predeterminado del administrador es admin, y la contraseña es la contraseña de inicio de sesión después de inicializar el sistema independiente. Modifique la contraseña de administrador con regularidad y consérvela correctamente por motivos de seguridad.

Paso 4 Haga clic en **Iniciar sesión.**

Se muestra la página de inicio de la web.

6 Configuración en DSS Pro

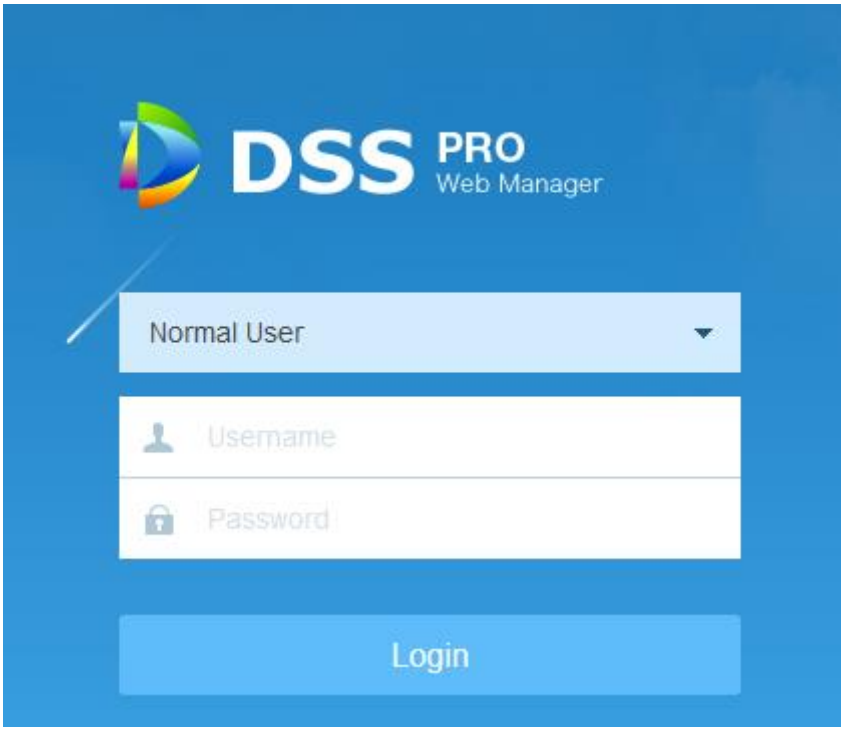
Antes de realizar configuraciones de control de acceso, debe agregar roles, usuarios y dispositivos de control de acceso a DSS Pro; y puede configurar el período y el modo de bloqueo / desbloqueo para ciertos usuarios, dispositivos y grupos de puertas; y luego puede otorgar permiso de acceso a ciertos usuarios o usuarios en diferentes grupos de puertas en DSS Pro Client. Para un funcionamiento detallado, consulte *Manual del usuario de DSS Pro.*

6.1 Agregar dispositivos

Primero debe agregar un dispositivo al DSS Pro para poder realizar la administración de desbloqueo, administración de períodos, configuración de permisos de acceso y más en DSS Pro.

Paso 1 Ingrese DSS Pro IP en la barra de direcciones del navegador y presione Enter.

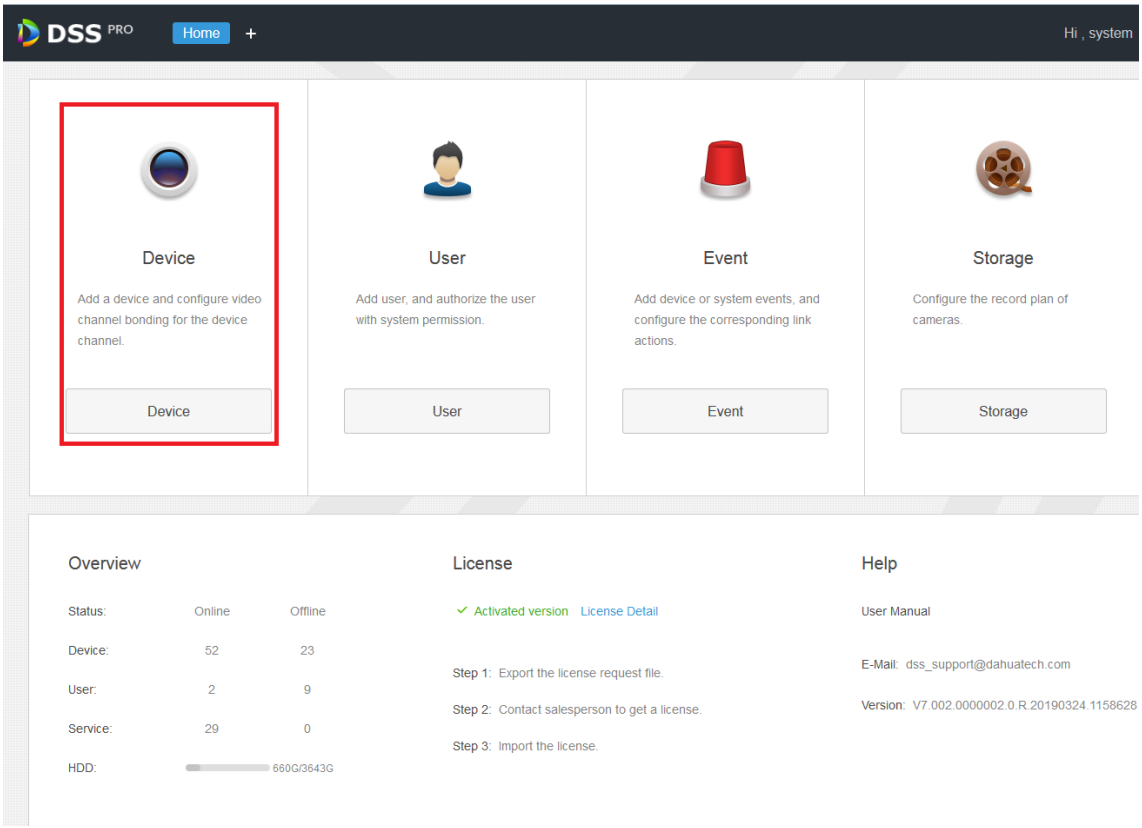
Figura 6-1 Inicio de sesión



Paso 2 Ingrese el nombre de usuario y la contraseña

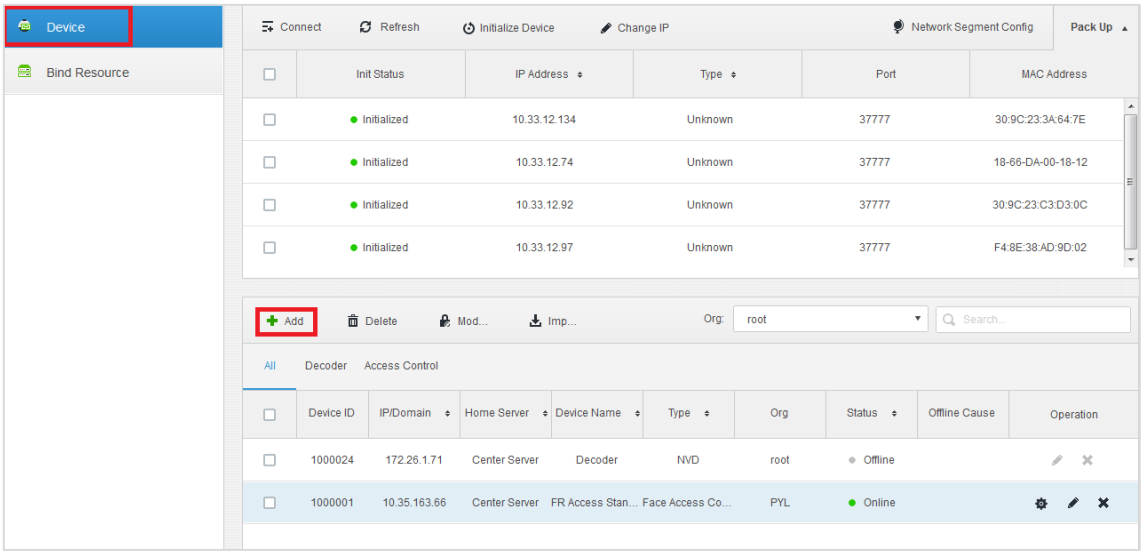
Paso 3 Haga clic en **Iniciar sesión.**

Figura 6-2 Página de inicio



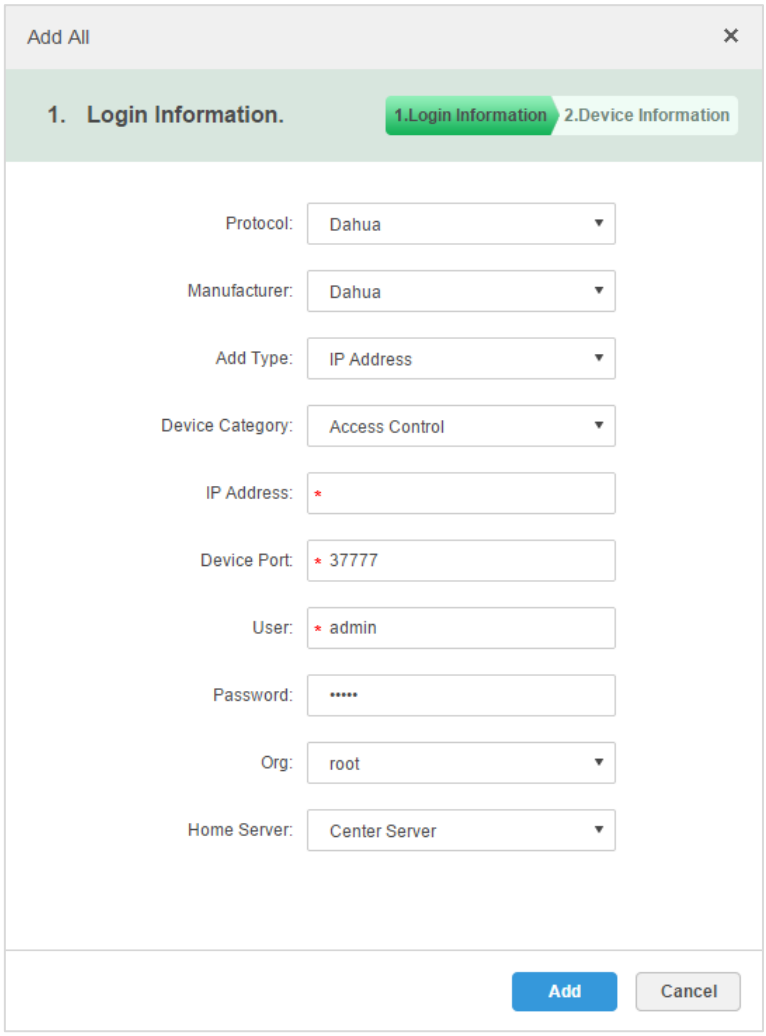
Paso 4 En la página de inicio, haga clic en **Dispositivo.**

Figura 6-3 Dispositivo



Paso 5 Haga clic en **Añadir.**

Figura 6-4 Agregar todo

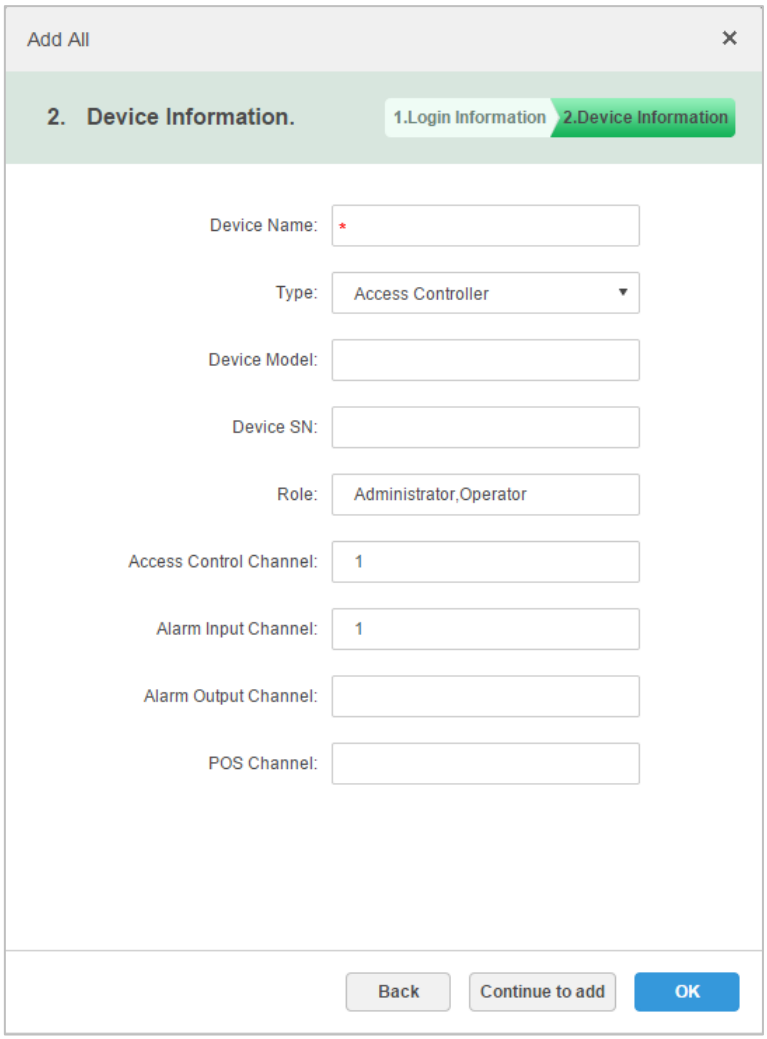


Paso 6 Seleccione Protocolo, Fabricante, Agregar tipo y Categoría de dispositivo; e ingrese la dirección IP, Puerto de dispositivo, usuario, contraseña y más.

- Seleccione **Control de acceso** como **Categoría de dispositivo.**
- Diferentes protocolos significan que establecerá diferentes parámetros; prevalecerá la interfaz real.
- Cuando **Dirección IP** está seleccionado, debe ingresar la dirección IP del dispositivo que desea agregar.
- Cuando se selecciona Registro automático, debe ingresar el ID de registro del dispositivo que desea agregar. El registro automático es solo para agregar codificador, y el ID de registro debe ser el mismo que el ID de registro configurado en el codificador.
- Cuando se selecciona el nombre de dominio. Debe ingresar el nombre de dominio del dispositivo que va a agregar.

Paso 7 Haga clic en **Añadir.**

Figura 6-5 Información del dispositivo



Paso 8 Introduzca el nombre del dispositivo, el tipo, el número de serie del dispositivo, el rol, el canal de control de acceso, la entrada de alarma Canal, canal de salida de alarma y canal POS.

El tipo se obtiene automáticamente después del Paso 7. Puede ver el dispositivo que agregó en el **Dispositivo** interfaz.

Si desea agregar más dispositivos, haga clic en **Continuar agregando.**

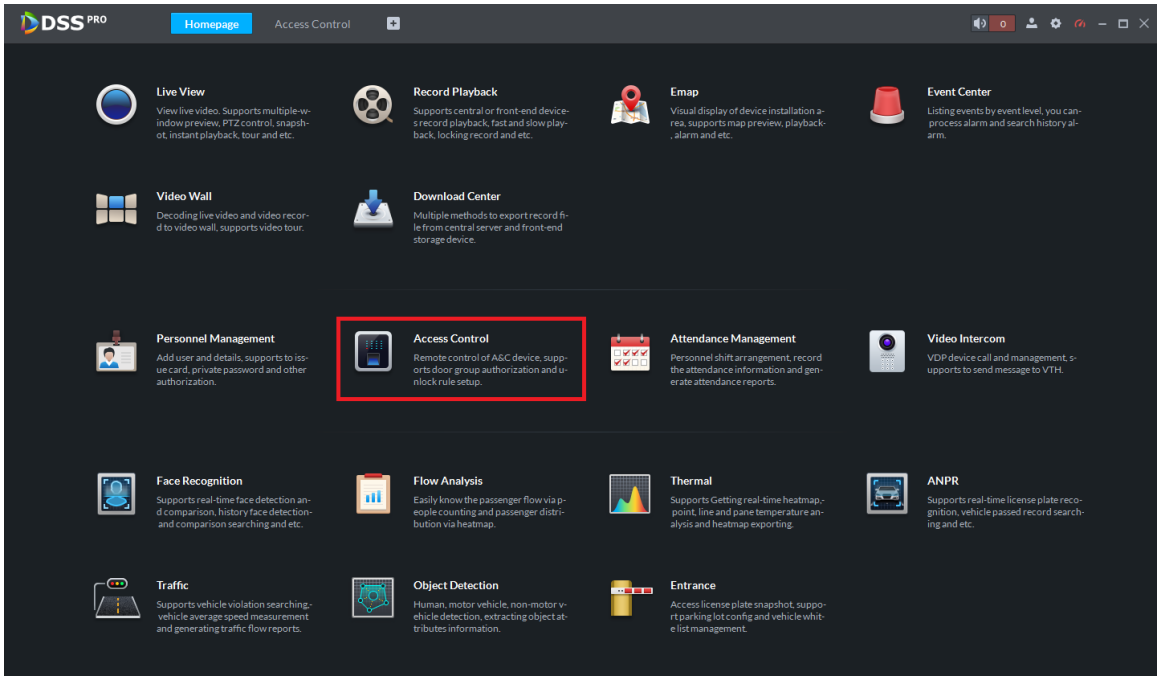
6.2 Gestión del control de acceso

Puede realizar la configuración de la puerta (estado de la puerta, período NO, período NC, activación de alarma, longitud de desbloqueo, método de desbloqueo) en DSS Pro Client según sus necesidades.

6.2.1 Configuración de la puerta

Paso 1 Inicie sesión en DSS Pro Client.

Figura 6-6 Página de inicio



Paso 2 Haga clic en **Control de acceso.**

Paso 3 En el lado izquierdo de la interfaz, haga clic con el botón derecho en un canal de control de acceso en el árbol de dispositivos,

y seleccione **Configuración de puerta.**

Figura 6-7 Control de acceso

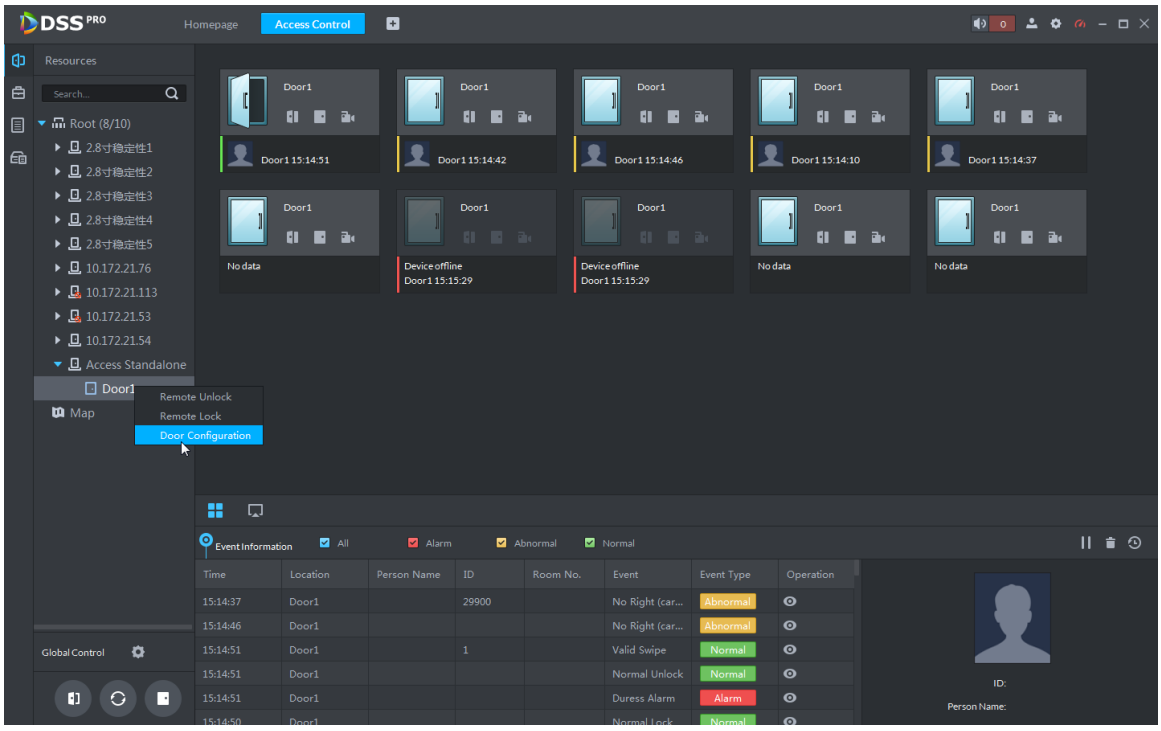


Figura 6-8 Configuración de la puerta

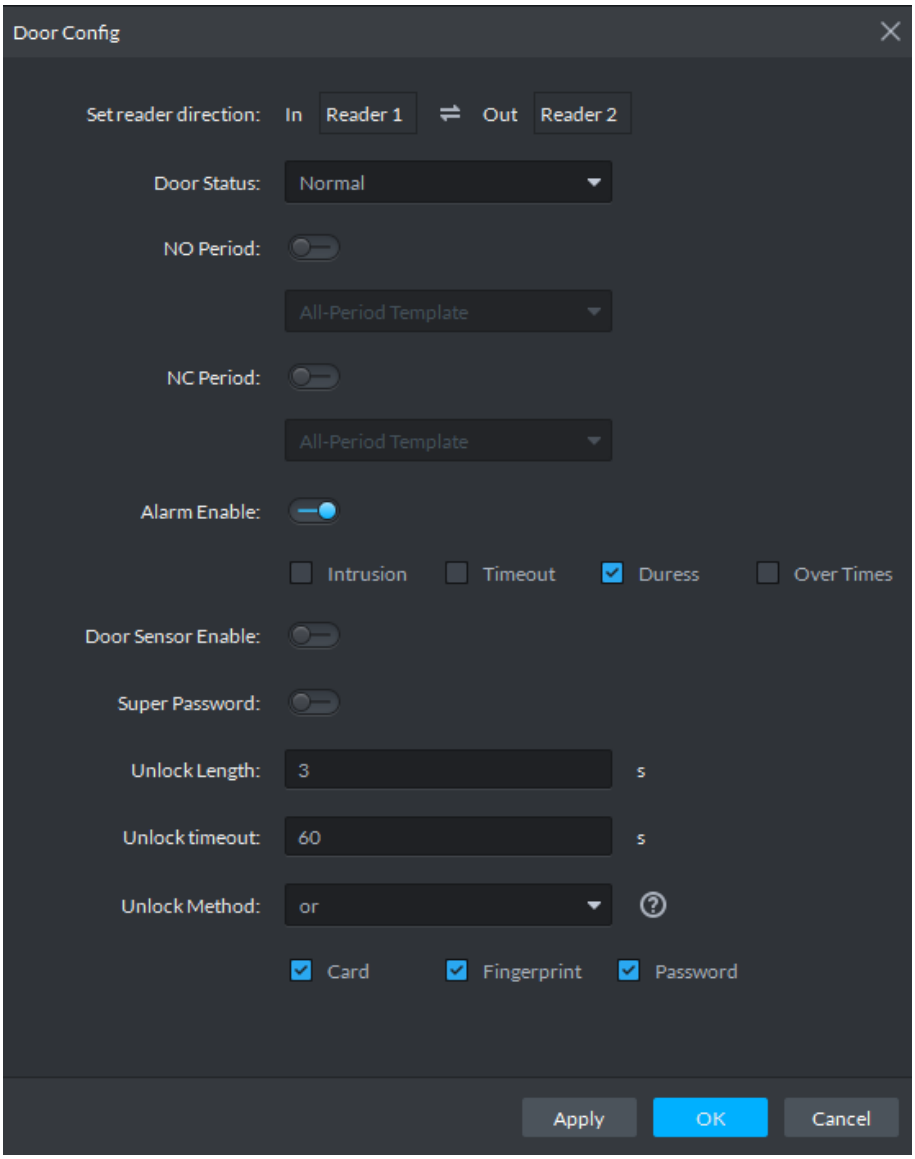


Tabla 6-1 Descripción de la configuración de la puerta

Parámetro	Descripción
Establecer la dirección del lector	Indica el lector de entrada / salida según el cableado del ACS. Establece el estado del control de
Estado de la puerta	acceso en **Normal, siempre abierto,** o **Siempre cerca.**
NO período	Si está habilitado, puede establecer un período durante el cual la puerta siempre estará abierta. Si está habilitado,
Período NC	puede establecer un período durante el cual la puerta siempre estará cerrada.
Activar alarma	• Si la puerta no se abre según lo previsto, el sensor de puerta se activa y activa una alarma de intrusión. • La entrada con la tarjeta de coacción, la contraseña de coacción o la huella dactilar de coacción activa una alarma de coacción. • La duración del desbloqueo que excede el tiempo de espera de desbloqueo activa una alarma de tiempo de espera. • Deslizar una tarjeta ilegal más de cinco veces activa una alarma maliciosa.

Parámetro	Descripción
Sensor de puerta Habilitar	Habilita el sensor de puerta. La alarma de intrusión y la alarma de tiempo de espera surten efecto solo cuando el sensor de puerta está habilitado.
Super contraseña	Ingrese la contraseña de administrador.
Longitud de desbloqueo	Establece la duración del desbloqueo de la puerta. La puerta se bloquea automáticamente cuando termina la duración.
Desbloquear tiempo de espera	La duración del desbloqueo que excede el tiempo de espera de desbloqueo activa una alarma de tiempo de espera.
Método de desbloqueo	Puede usar cualquiera de los métodos, tarjeta, huella digital y contraseña, o cualquiera de sus combinaciones para desbloquear la puerta.

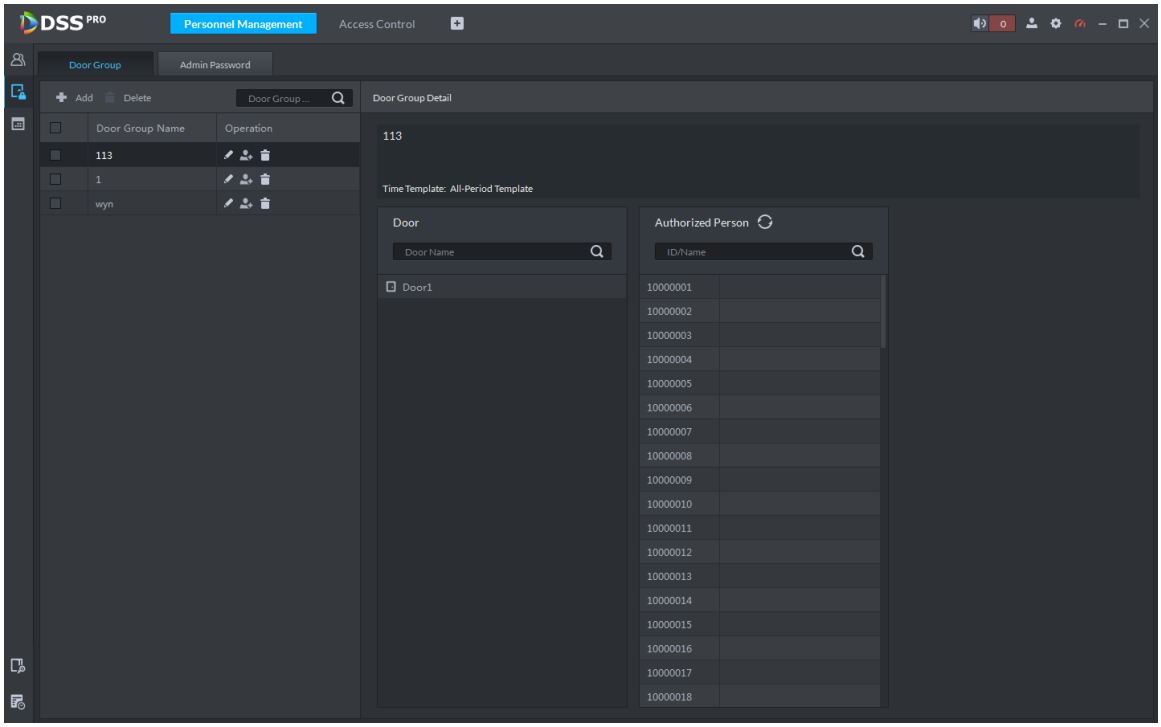
Paso 4 Haga clic en **OKAY.**

6.2.2 Creación de grupos de puertas

Puede agrupar puertas, y luego no tiene que otorgar permisos de acceso de ciertas puertas a ciertos usuarios uno por uno (al crear reglas de puertas a continuación, debe seleccionar qué personas tienen permiso de acceso de qué grupos de puertas).

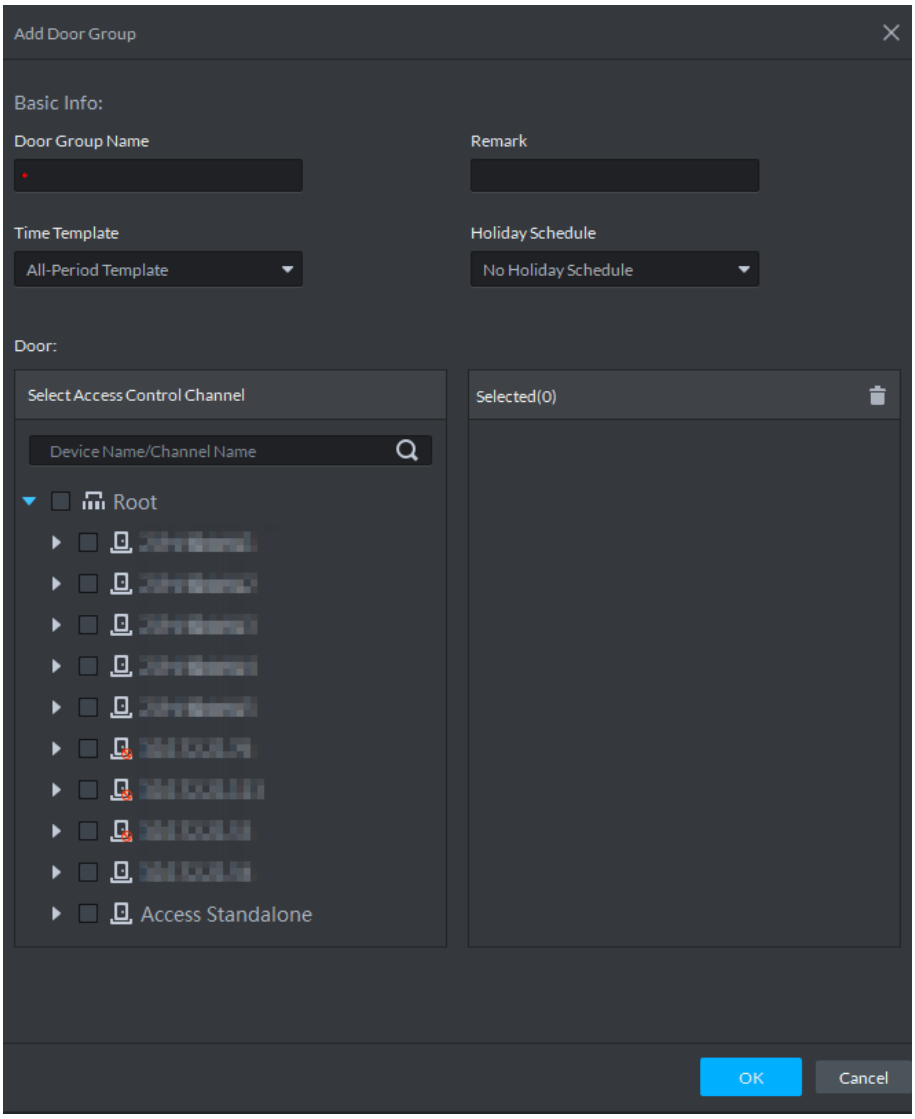
Paso 1 clic  sobre el **Gestión de personal** interfaz.

Figura 6-9 Grupo de puertas



Paso 2 Haga clic en **Añadir** sobre el **Grupo de puertas** interfaz.

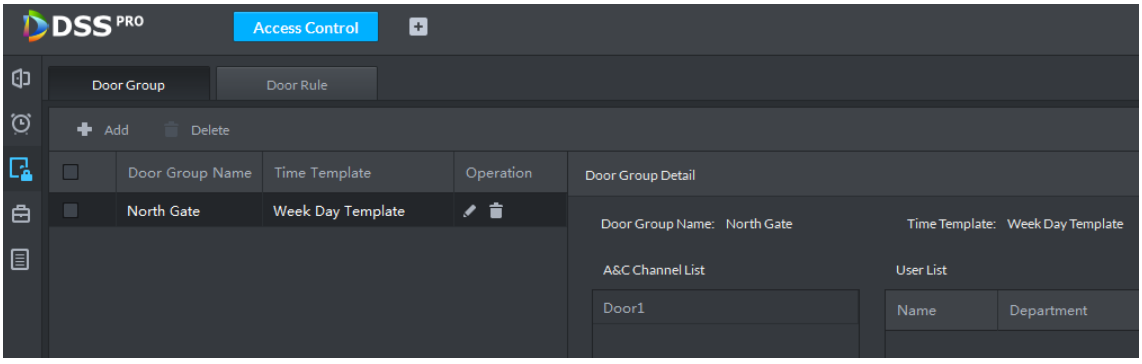
Figura 6-10 Agregar grupo de puertas



Paso 3 Ingrese el nombre del grupo de puertas, seleccione una plantilla de tiempo y configure el horario de vacaciones.

Paso 4 Seleccione un canal y haga clic en **OKAY.**

Figura 6-11 Grupo de puertas



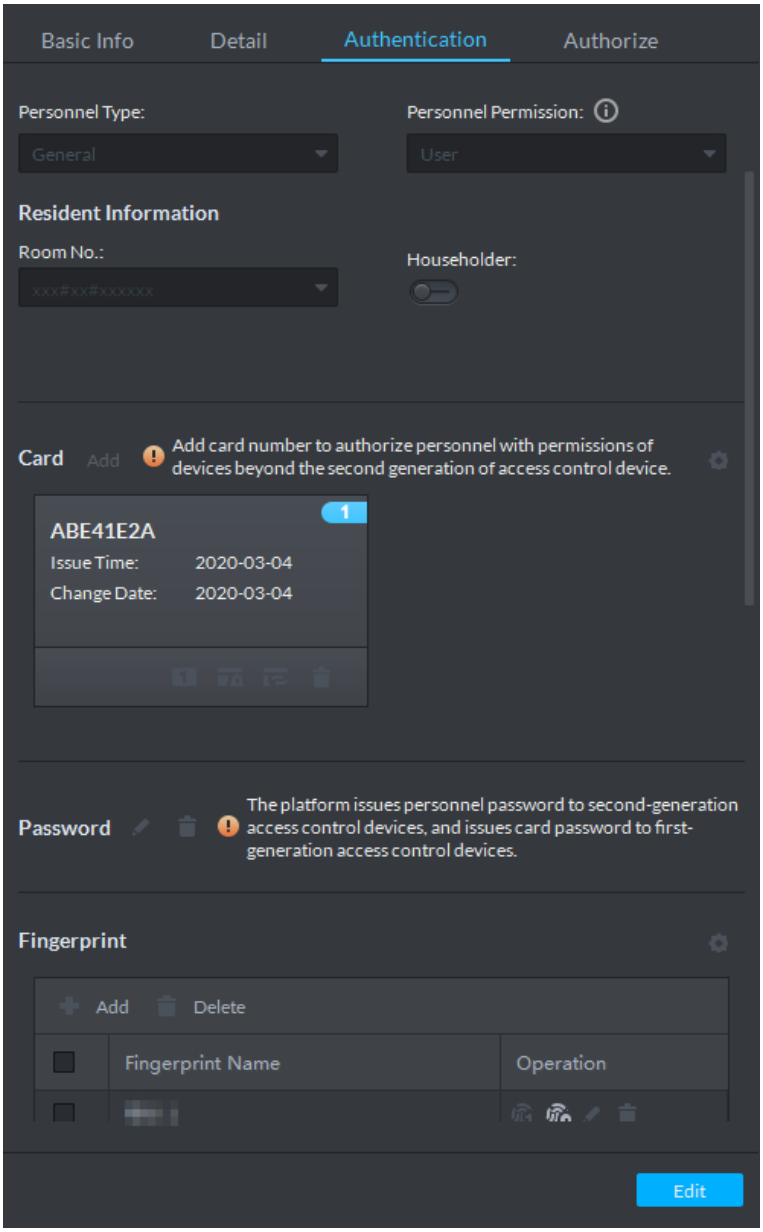
6.2.3 Emisión de tarjetas de acceso

Puede emitir tarjetas de acceso a las personas una a una o en lotes.

Paso 1 En el **Gestión de personal** interfaz, haga doble clic en las personas que necesite emitir

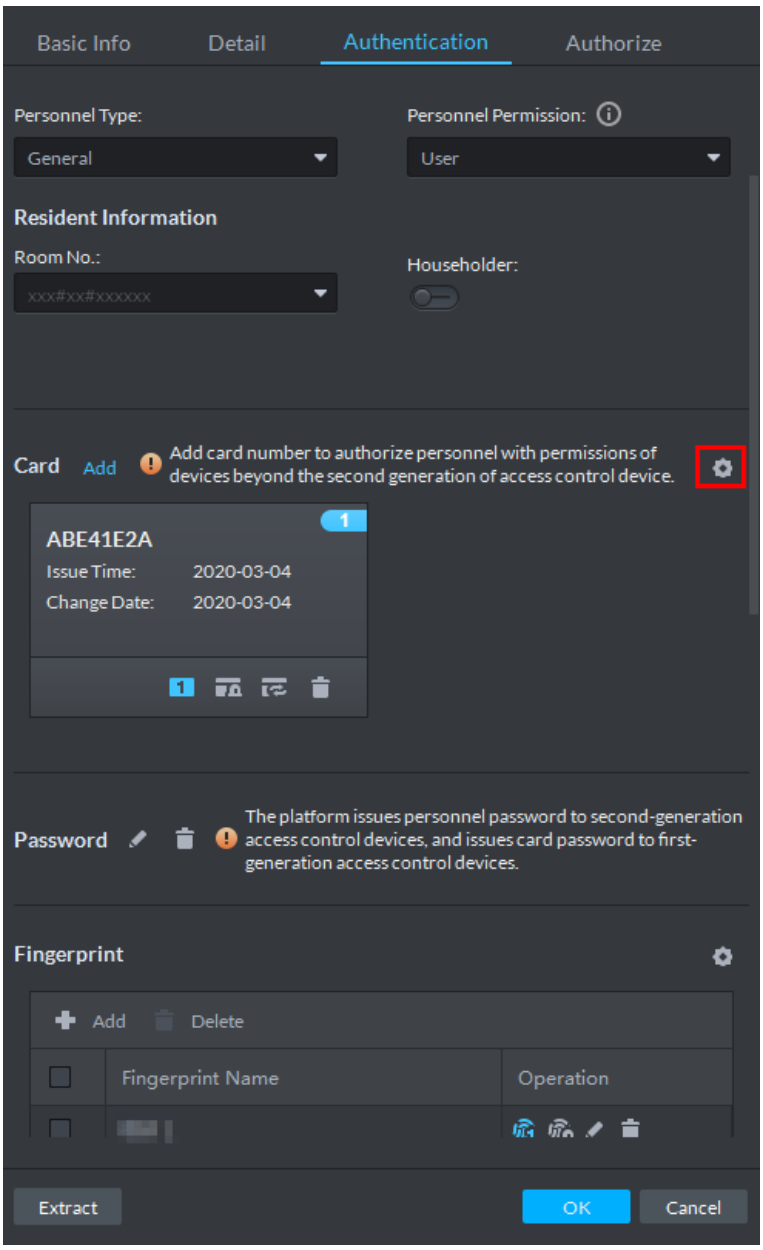
acceder a la tarjeta y luego haga clic en **Autenticación** lengüeta.

Figura 6-12 Autenticación



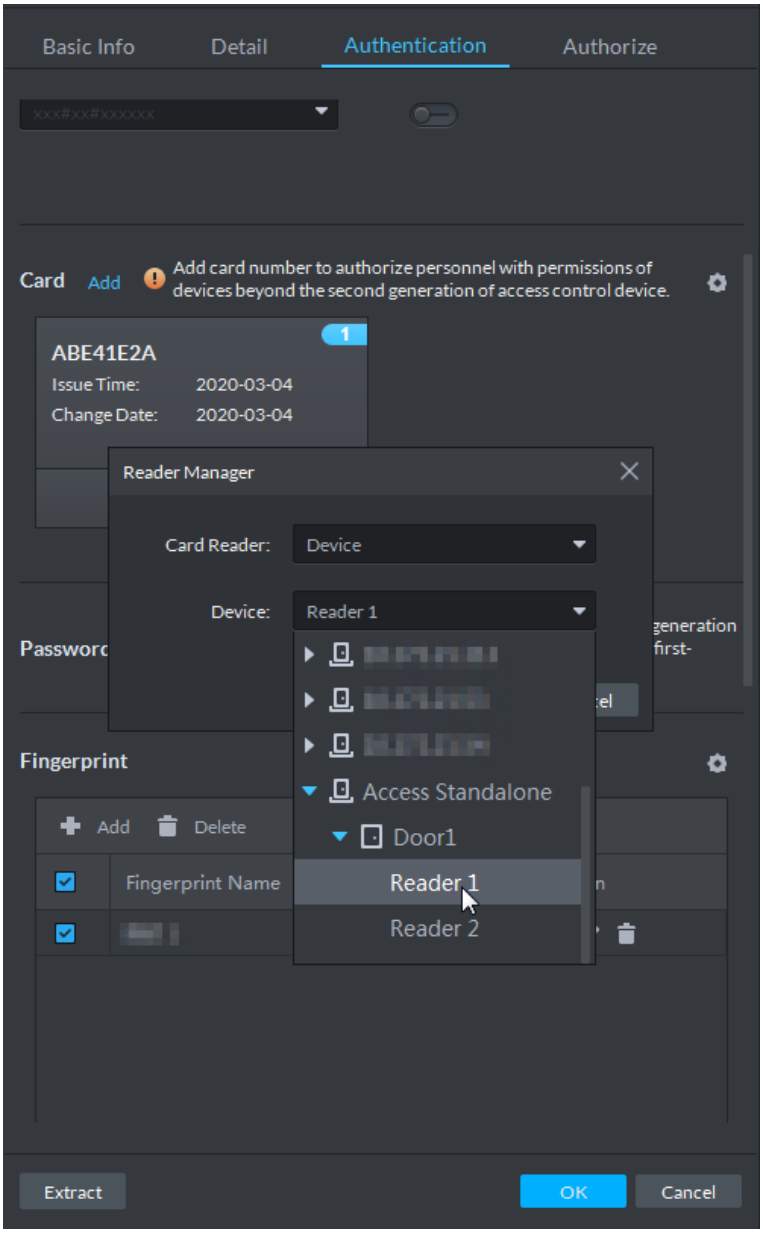
Paso 2 Haga clic en **Editar,** y luego haga clic en  en **Tarjeta** sección.

Figura 6-13 Edición



Paso 3 Seleccione el lector de tarjetas del acceso independiente según sea necesario.

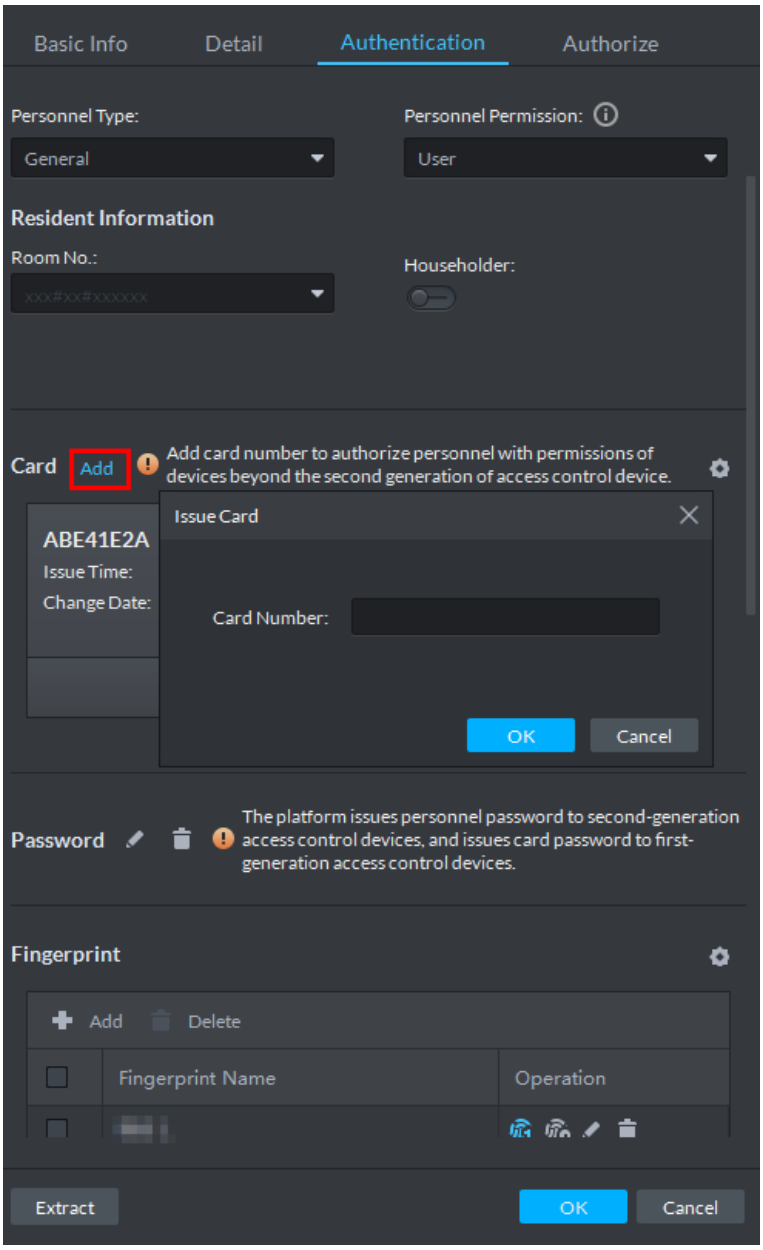
Figura 6-14 Administrador de lectores



Paso 4 Haga clic en **Añadir** cerca de **Tarjeta,** y luego coloque la tarjeta en el lector de tarjetas para emitir la tarjeta.

Se muestra el número de tarjeta.

Figura 6-15 Número de tarjeta



Paso 5 Haga clic en **OKAY.**

La tarjeta se emite a las personas que seleccionó.

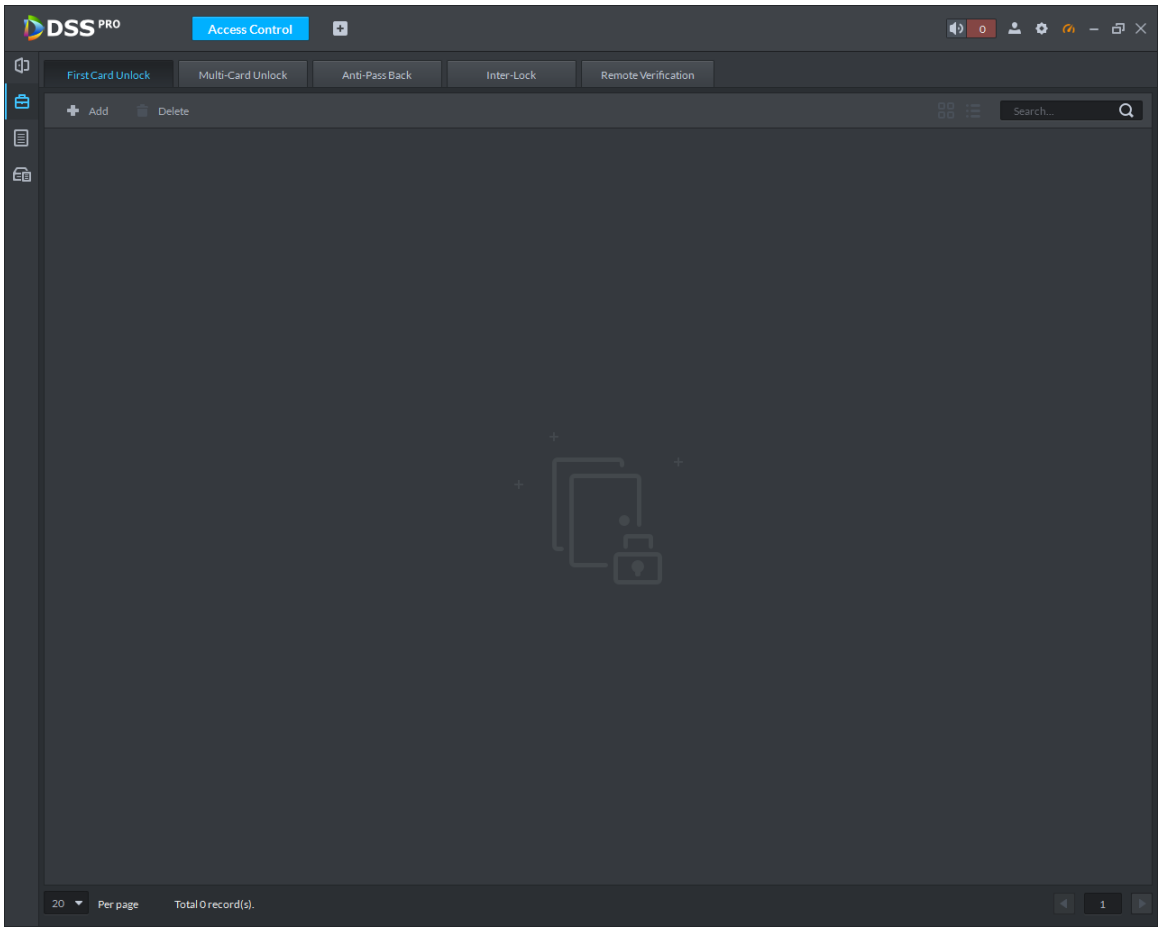
- También puede emitir tarjetas en lotes haciendo clic en **Tarjeta de emisión por lotes.**
- Puede consultar los pasos para emitir tarjetas para registrar huellas digitales.

6.2.4 Desbloqueo de la primera tarjeta

Solo después de que el usuario de la primera tarjeta especificado pase la tarjeta todos los días, otros usuarios pueden abrir la puerta con sus tarjetas. Puede configurar varias primeras cartas. Solo después de que cualquiera de los usuarios pase la primera tarjeta, otros usuarios sin las primeras tarjetas pueden abrir la puerta con sus tarjetas.

Paso 1 En el **Control de acceso** interfaz, haga clic en .

Figura 6-16 Función avanzada

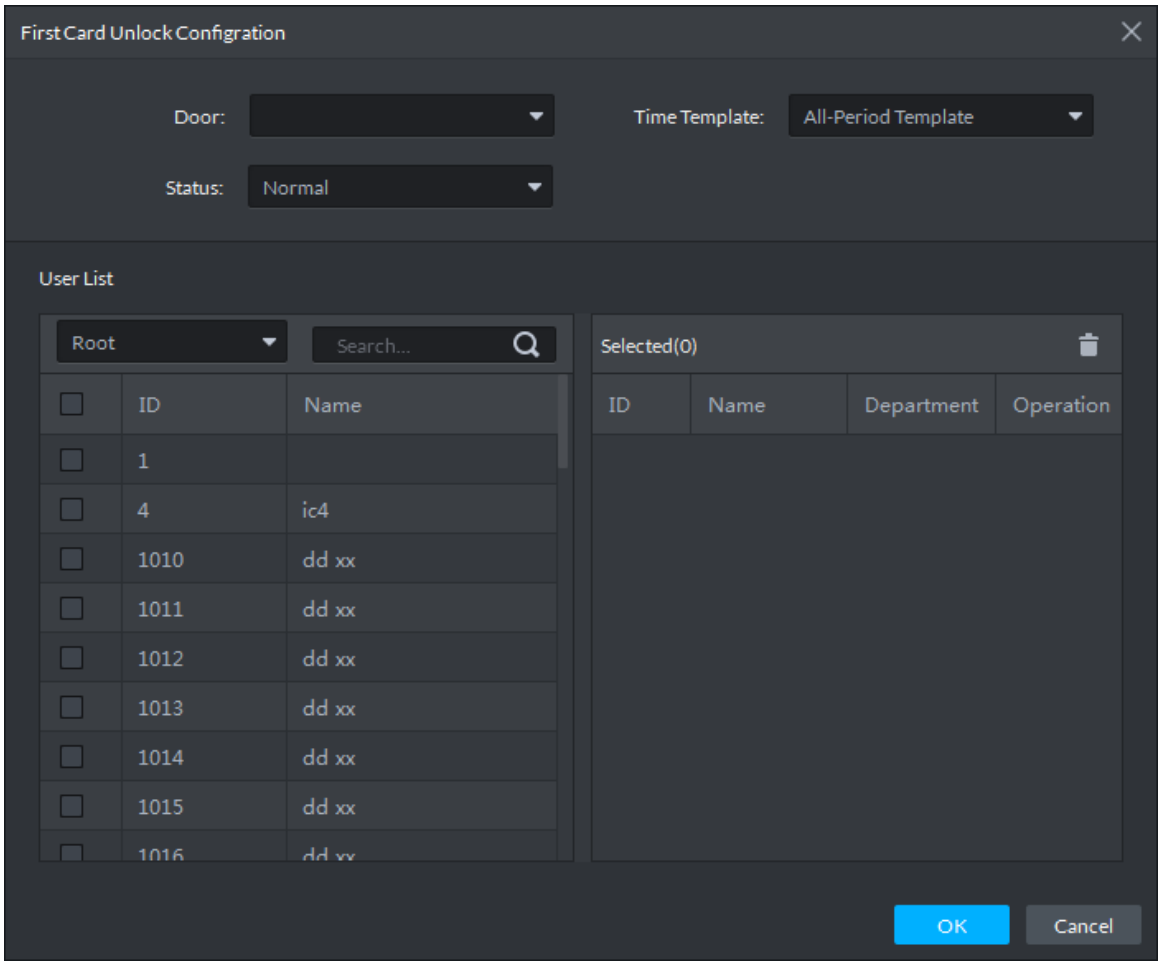


Paso 2 Haga clic en el **Desbloqueo de la primera tarjeta** lengüeta.

los **Desbloqueo de la primera tarjeta** se muestra la interfaz.

Paso 3 Haga clic en **Añadir.**

Figura 6-17 Configuración de desbloqueo de la primera tarjeta



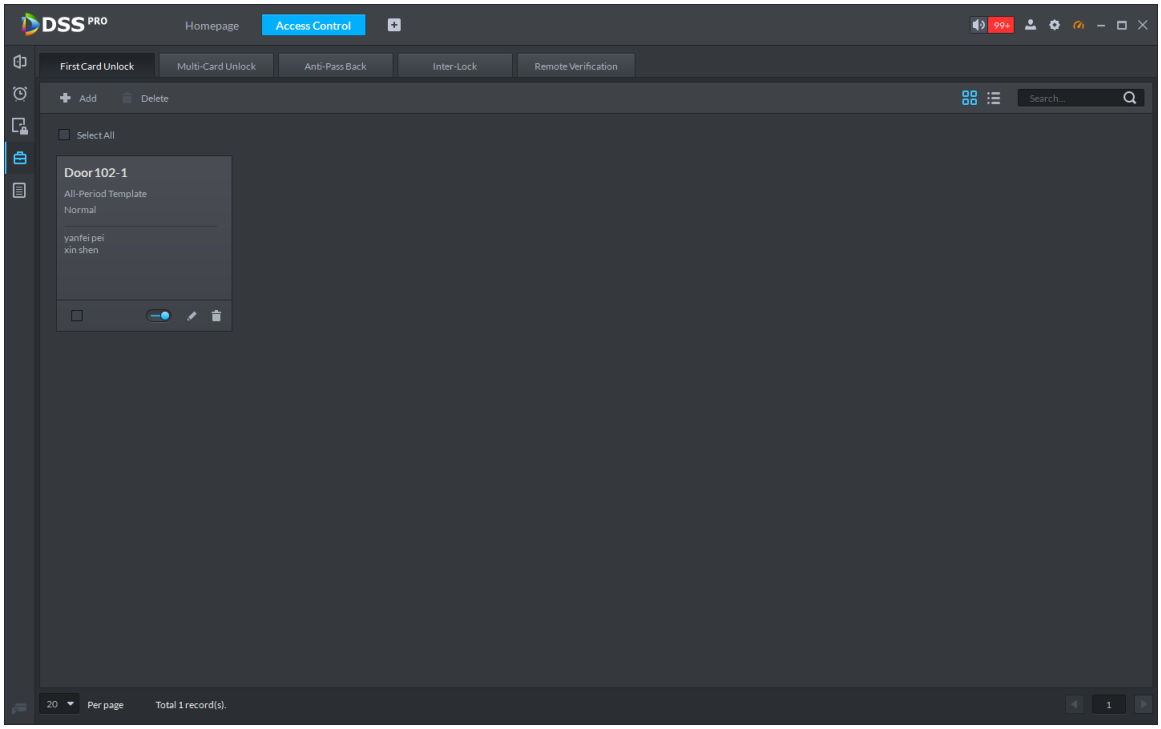
Paso 4 Configure el **Desbloqueo de la primera tarjeta** parámetros y haga clic en **OKAY.** Para obtener más detalles, consulte la Tabla 6-2.

El sistema muestra el **Desbloqueo de la primera tarjeta** información. Vea la Figura 6-18. **Desbloqueo de la primera tarjeta** está habilitado de forma predeterminada.

Tabla 6-2 Parámetros de desbloqueo de la primera tarjeta

Parámetro	Descripción
Puerta	Puede seleccionar el canal de control de acceso de destino para configurar el primer desbloqueo de la tarjeta.
Plantilla de tiempo	El desbloqueo de la primera tarjeta es válido en el período de tiempo de la plantilla de tiempo seleccionada.
Estado	Una vez que se habilita el desbloqueo de la primera tarjeta, la puerta está en el modo Normal o en el modo Siempre abierta.
Usuario	Puede seleccionar el usuario para que tenga la primera tarjeta. Admite la selección de varios usuarios para que tengan las primeras tarjetas. Cualquiera de ellos deslizando la primera tarjeta significa que la primera tarjeta se desbloquea.

Figura 6-18 Información de desbloqueo de la primera tarjeta



Paso 5 Haga clic en  .

El icono cambiando a  indica que el desbloqueo de la primera tarjeta está habilitado.

6.2.5 Desbloqueo de múltiples tarjetas

En este modo, varios grupos de usuarios tienen que pasar tarjetas por un canal de control de acceso en una secuencia establecida para desbloquear la puerta.

- Un grupo puede tener hasta 50 usuarios.
- Con el desbloqueo de múltiples tarjetas habilitado para un canal de control de acceso, admite hasta cuatro grupos de usuarios en el sitio al mismo tiempo para la verificación. El número total de usuarios puede ser 64 como máximo, con hasta cinco usuarios válidos.

Paso 1 En el **Control de acceso** interfaz, haga clic en  .

los **Función avanzada** se muestra la interfaz.

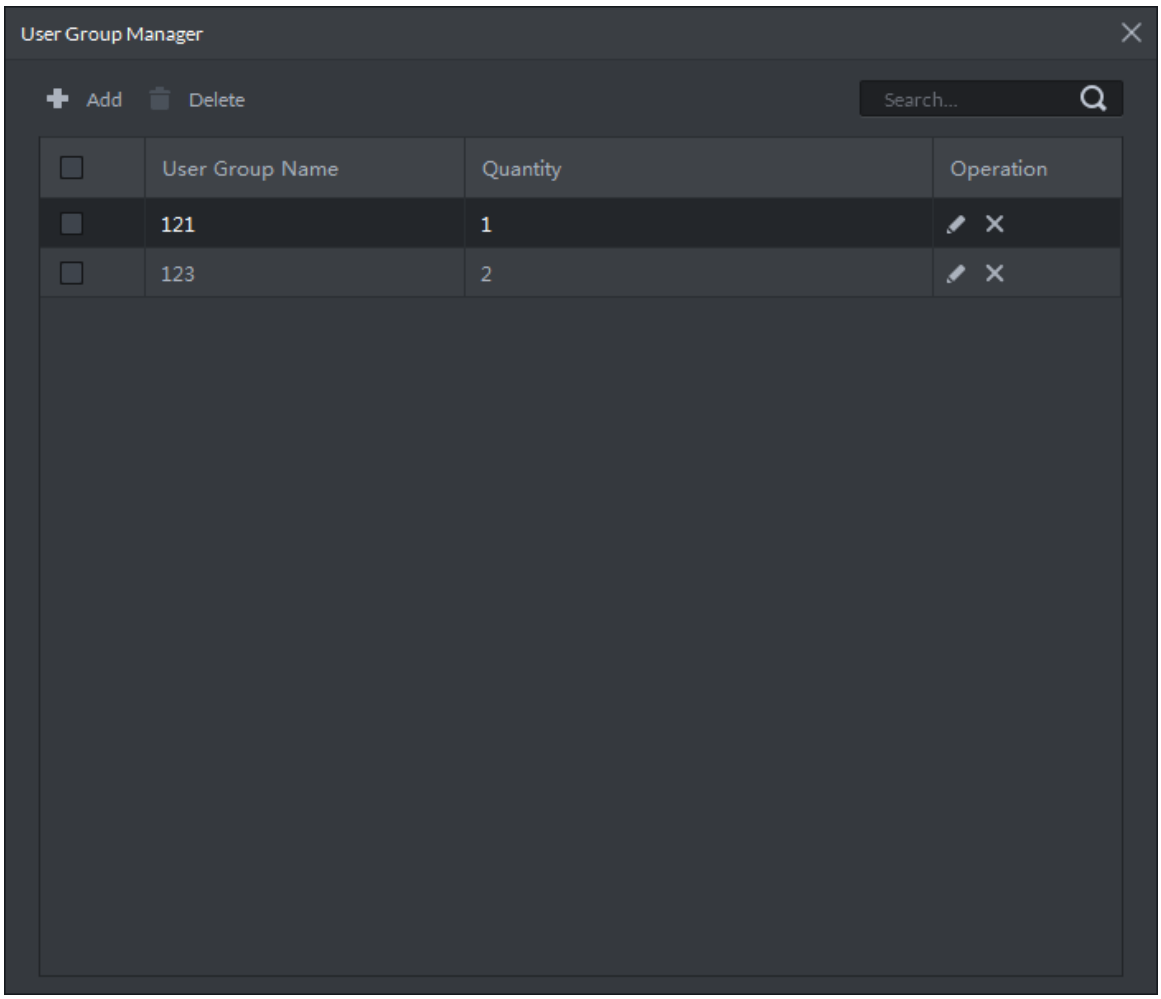
Paso 2 Haga clic en el **Desbloqueo de múltiples tarjetas** lengüeta.

los **Desbloqueo de múltiples tarjetas** se muestra la interfaz.

Paso 3 Agregue un grupo de usuarios.

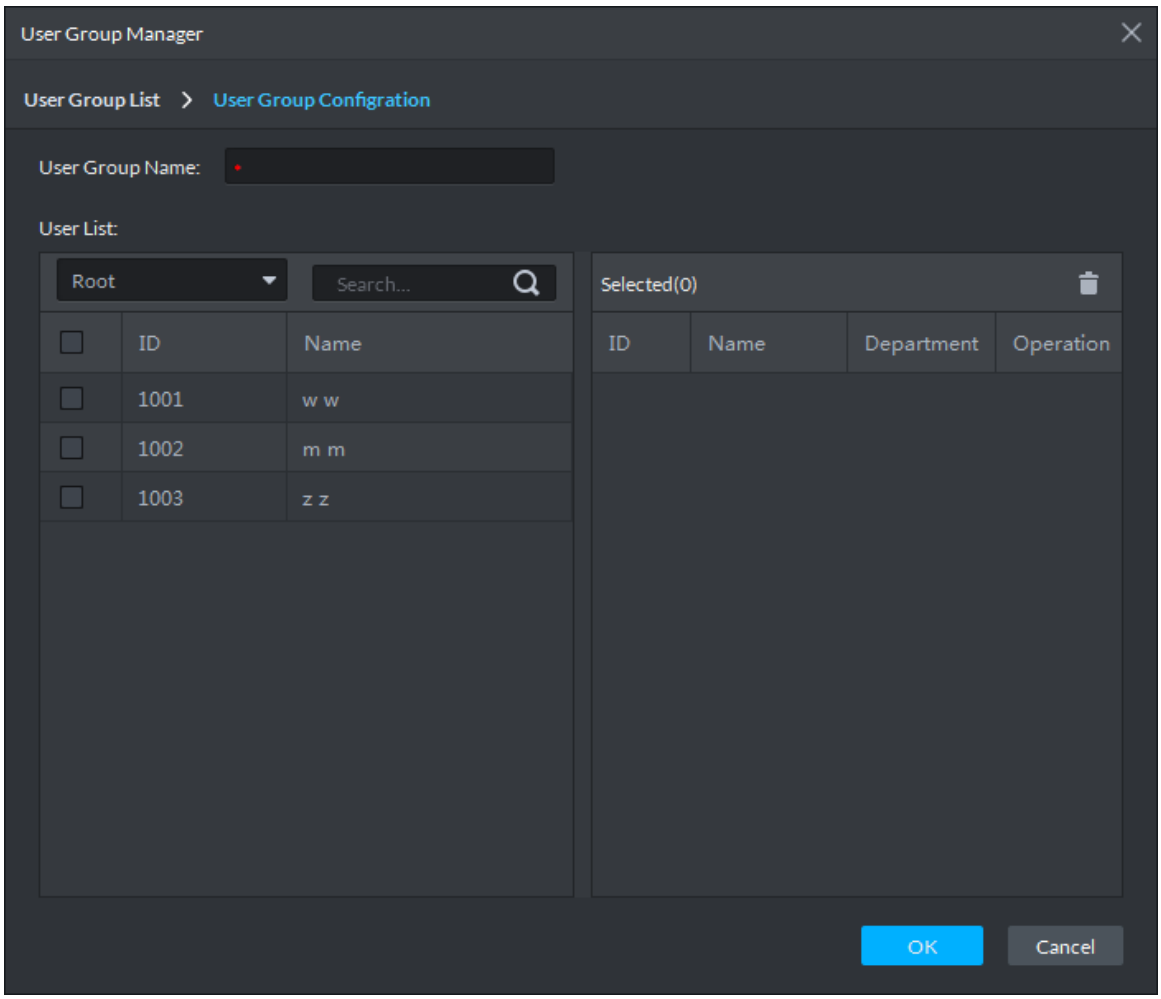
1) Haga clic en **Grupo de personas.**

Figura 6-19 Administrador de grupos de usuarios



2) Haga clic en **Añadir.**

Figura 6-20 Configuración del grupo de usuarios



3) Preparar **Nombre del grupo de usuarios.** Seleccionar usuarios de **Lista de usuarios** y haga clic en **OKAY.** Puede seleccionar hasta 64 usuarios.

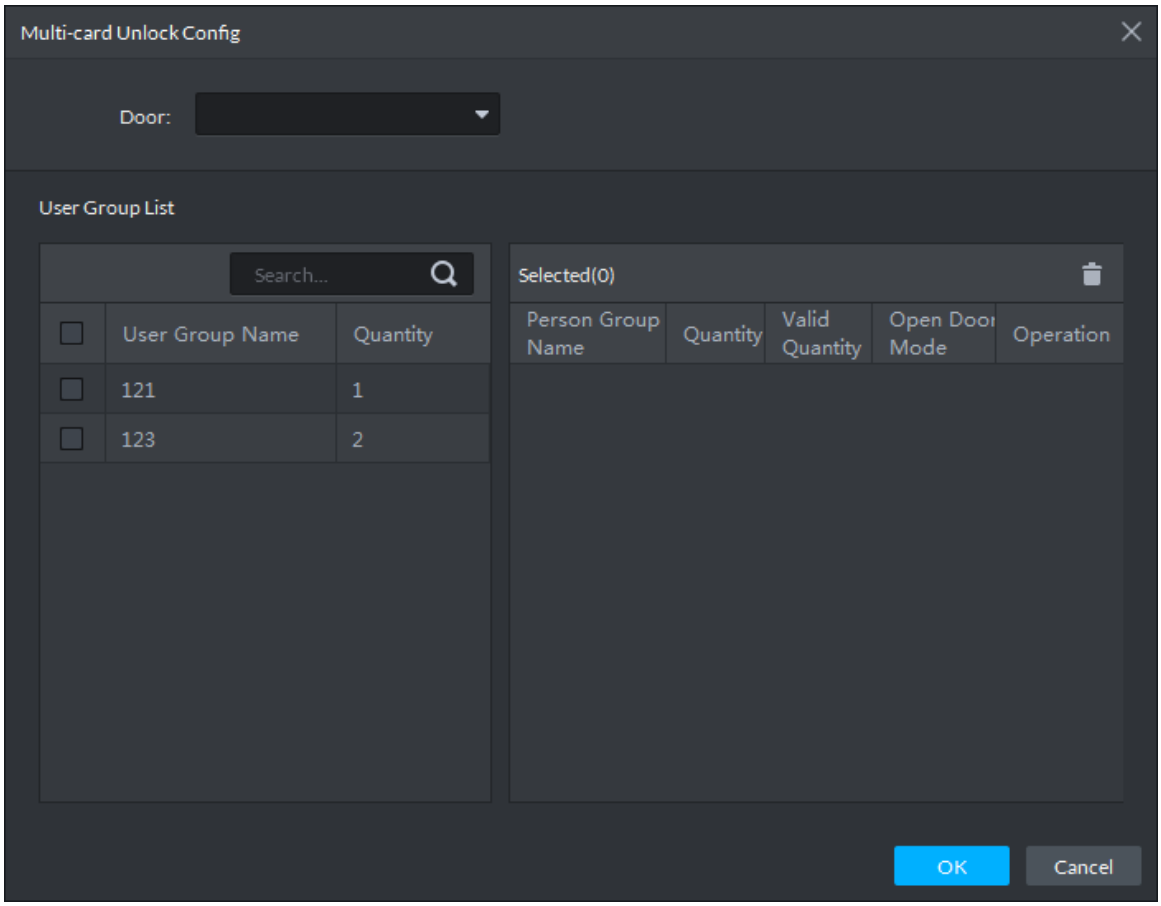
El sistema muestra la información del grupo de usuarios. Hacer clic

4) en la esquina superior derecha de la **Administrador de grupos de usuarios** interfaz.

Paso 4 Configure el desbloqueo de múltiples tarjetas.

1) Haga clic en **Añadir.**

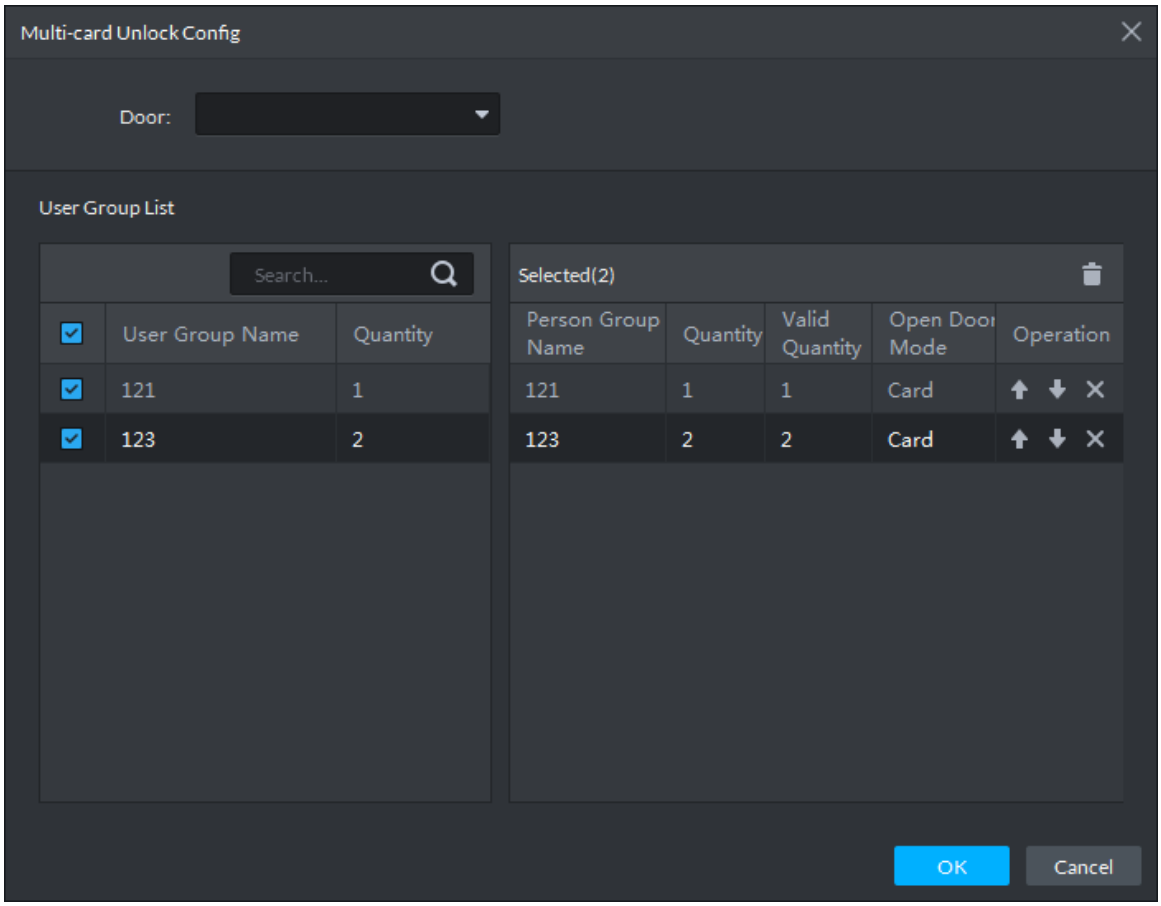
Figura 6-21 Configuración de desbloqueo de múltiples tarjetas



2) Seleccione la puerta para configurar el desbloqueo de múltiples tarjetas.

3) Seleccione el grupo de usuarios. Puede seleccionar hasta cuatro grupos. El sistema muestra la información del grupo de usuarios.

Figura 6-22 Información del grupo de usuarios



4) Ingrese el **Cantidad válida** para que cada grupo esté en el sitio y el **Modo de puerta abierta.**

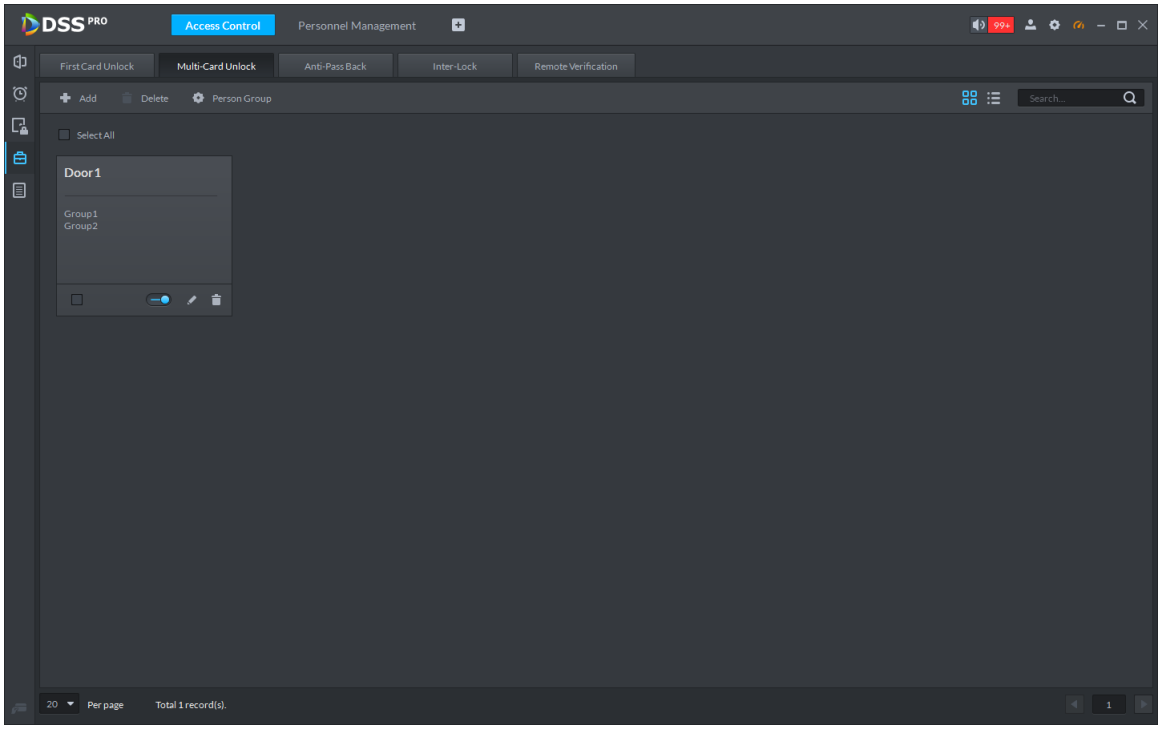
Hacer clic  o  para ajustar la secuencia de usuario para que cada grupo desbloquee la puerta.

La cantidad válida se refiere al número de usuarios en cada grupo que deben estar en el sitio para pasar sus tarjetas.

5) Haga clic en **OKAY.**

El sistema muestra el **Desbloqueo de múltiples tarjetas** información.

Figura 6-23 Detalles de desbloqueo de tarjetas múltiples



Paso 5 Haga clic en  .

El icono cambiando a  indica que el desbloqueo de múltiples tarjetas está habilitado.

6.2.6 Anti-passback

La función Anti-passback requiere que una persona salga por la puerta por la que entró. Para la misma persona, un registro de entrada debe emparejarse con un registro de salida. Si alguien ha entrado siguiendo a otra persona, lo que significa que no hay registro de entrada, esta persona no puede abrir la puerta para salir.

Paso 1 En el **Control de acceso** interfaz, haga clic en  .

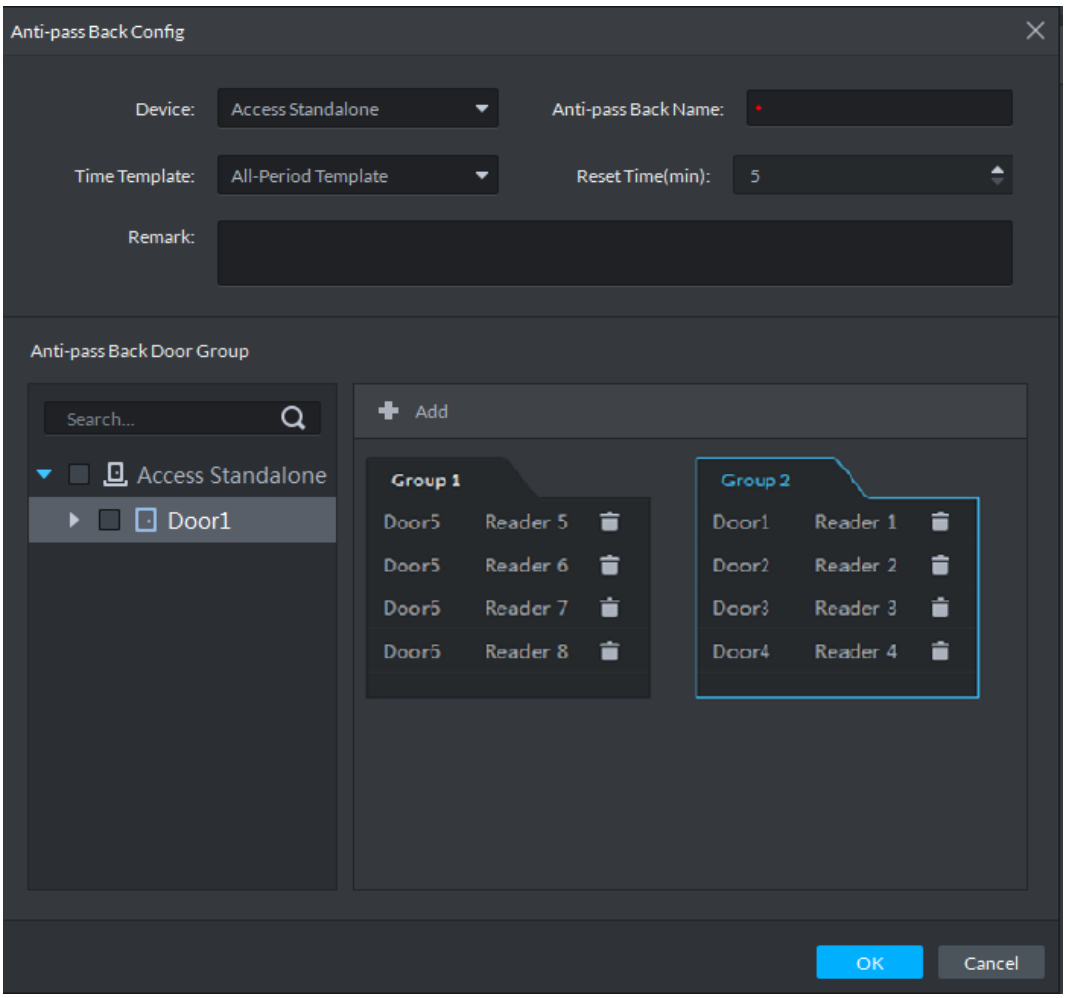
los **Función avanzada** se muestra la interfaz.

Paso 2 Haga clic en el **Anti-passback** lengüeta.

los **Anti-passback** se muestra la interfaz.

Paso 3 Haga clic en **Añadir.**

Figura 6-24 Configuración de anti-passback



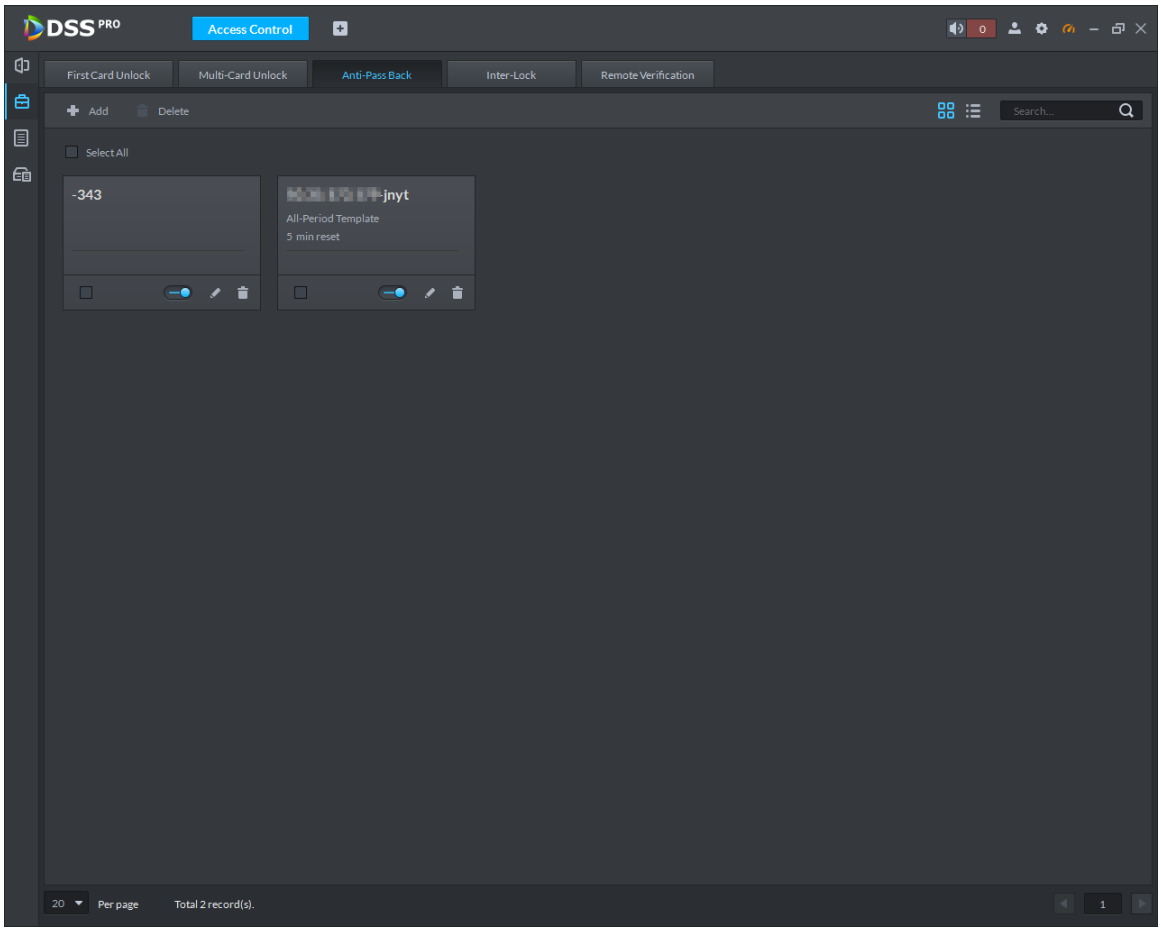
Paso 4 Configure los parámetros de anti-passback y haga clic **OKAY.** Para obtener más información, consulte la Tabla 6-3.

El sistema muestra la información de selección de usuario. Vea la Figura 6-25.

Tabla 6-3 Descripción de la información de selección de usuario

Parámetro	Descripción	
Dispositivo	Puede seleccionar el dispositivo para configurar las reglas de anti-passback.	
Anti-passback nombre	Puede personalizar el nombre de una regla anti-passback.	
Reiniciar Tiempo (min)	La tarjeta de acceso deja de ser válida si se infringe una regla anti-passback. El tiempo de reinicio es la duración de la invalidez.	Cuando el seleccionado dispositivo es un multi-puerta controlador, tú puede configurar los parámetros.
Hora Modelo	Puede seleccionar los períodos de tiempo para implementar las reglas anti-passback.	
Observación	Información de descripción.	
Grupo X	La secuencia de grupo aquí es la secuencia para deslizar y configurar estas tarjetas. Puede agregar hasta 16 lectores para cada grupo. Cada grupo puede pasar tarjetas en cualquiera de los lectores. X es un número.	

Figura 6-25 Información de anti-passback



Paso 5 Haga clic en  .

El icono cambiando a  indica que Anti-passback está habilitado.

6.2.7 Verificación remota

Para dispositivos con verificación remota, cuando los usuarios desbloquean las puertas con tarjeta, huella digital o contraseña en el período de tiempo especificado, se debe confirmar en el cliente de la plataforma antes de que se pueda abrir el controlador de acceso.

Paso 1 En el **Control de acceso** interfaz, haga clic en  .

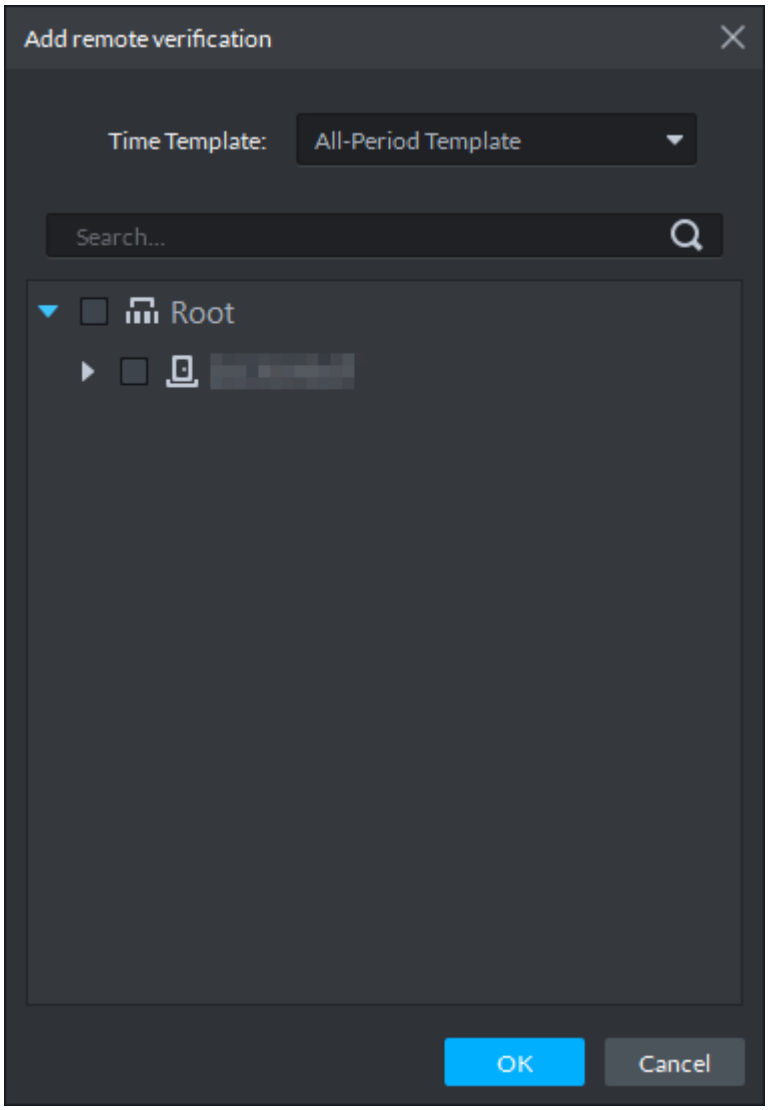
los **Función avanzada** se muestra la interfaz.

Paso 2 Haga clic en el **Verificación remota** lengüeta.

los **Verificación remota** se muestra la interfaz.

Paso 3 Haga clic en **Añadir.**

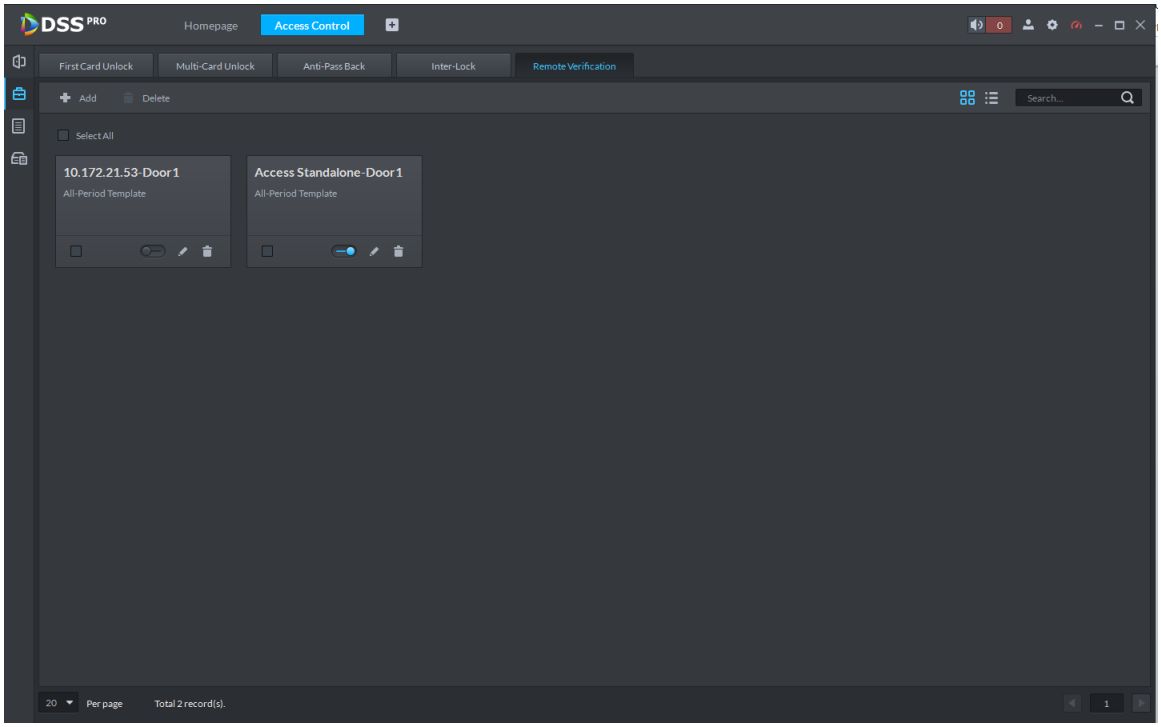
Figura 6-26 Agregar verificación remota



Paso 4 Seleccione **Plantilla de tiempo** y canal de control de acceso, y haga clic en **OKAY.**

El sistema muestra la información de verificación remota.

Figura 6-27 Información de verificación remota



Paso 5 Haga clic en  .

El icono cambiando a  indica **Verificación remota** está habilitado.

6.2.8 Visualización de registros de control de acceso

Puede ver los registros de control de acceso. Hay dos tipos de registros:

- Registros en línea

  Los registros de control de acceso almacenados en la plataforma. Registros sin

- conexión

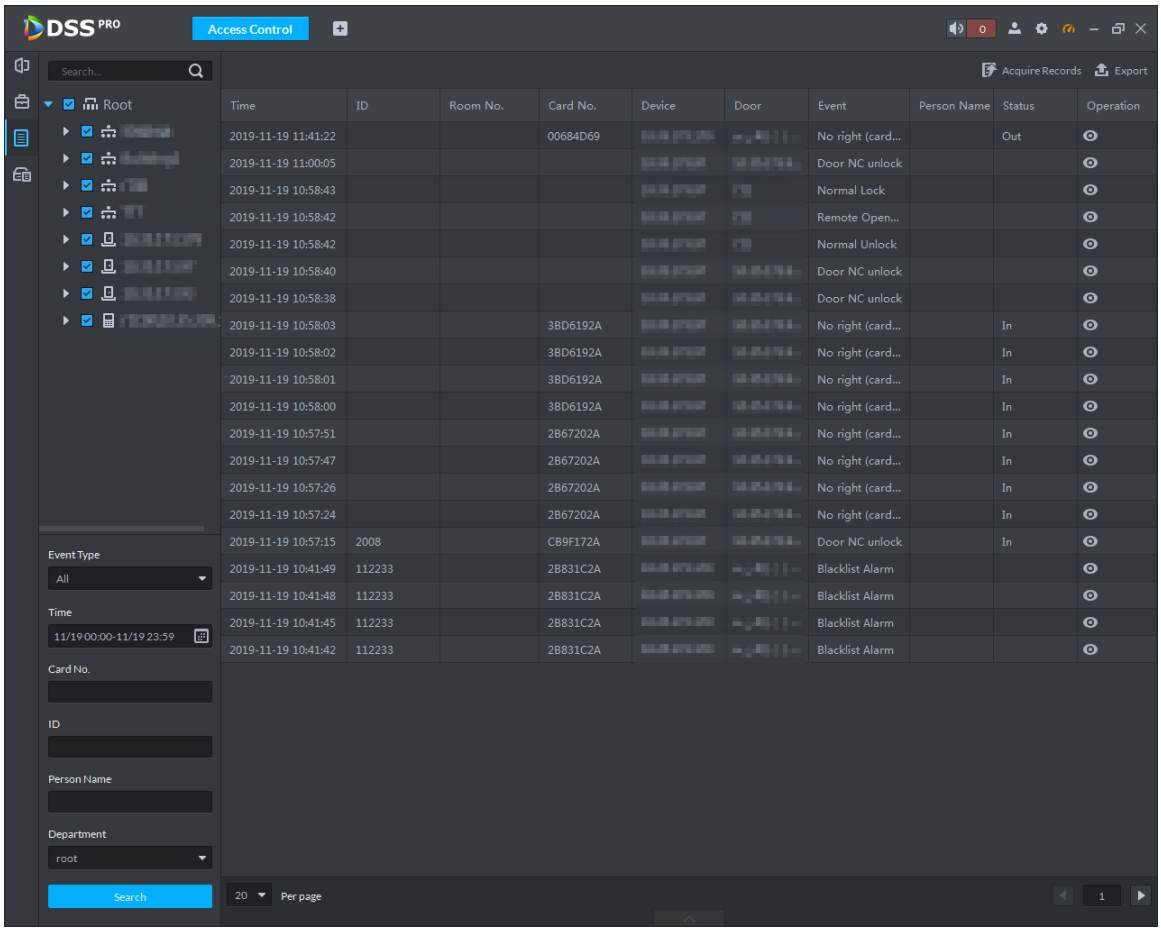
  Los registros de control de acceso almacenados en el dispositivo cuando no se había agregado a la plataforma o estaban desconectados de la plataforma. Una vez que el dispositivo se agrega a la plataforma o se vuelve a conectar a la plataforma, la plataforma leerá los registros generados cuando el dispositivo estaba fuera de línea.

Configure la alarma en Evento manualmente para que la alarma externa se pueda cargar a la plataforma.

6.2.8.1 Registros en línea

Ve a la **Control de acceso** módulo del **Página principal** en el cliente de la plataforma y haga clic en  a vaya a la interfaz de búsqueda de registros de control de acceso. Vea la Figura 6-28. Hacer clic **Exportar** en la esquina superior derecha de la interfaz y guarde el registro exportado en un disco local.

Figura 6-28 Búsqueda de registros

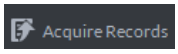


6.2.8.2 Registros sin conexión

Puede extraer registros de desbloqueo y registros de alarma por separado.

Paso 1 encendido **Control de acceso** interfaz, haga clic en  .

los **Registros de control de acceso** se muestra la interfaz.

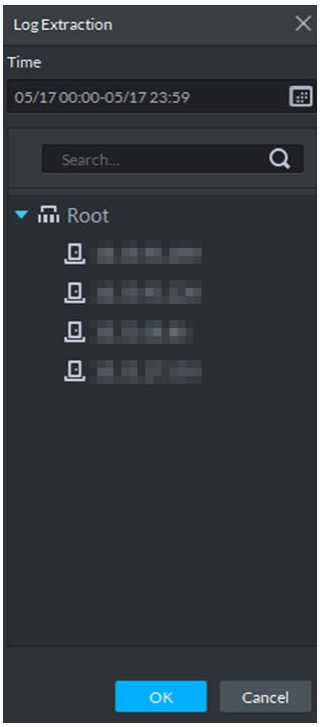
Paso 2 Haga clic en 

en la esquina superior derecha.

los **Verificación de contraseña** se muestra la interfaz.

Paso 3 Introduzca la contraseña de inicio de sesión en el **Verificación de contraseña** interfaz. los **Extracto de registro interfaz** se visualiza.

Figura 6-29 Extraer registros cuando el dispositivo está fuera de línea



Paso 4 Haga clic en y establecer el período.

Paso 5 Haga clic en para mostrar dispositivos y luego seleccione un canal.

Paso 6 Haga clic en **OKAY.**

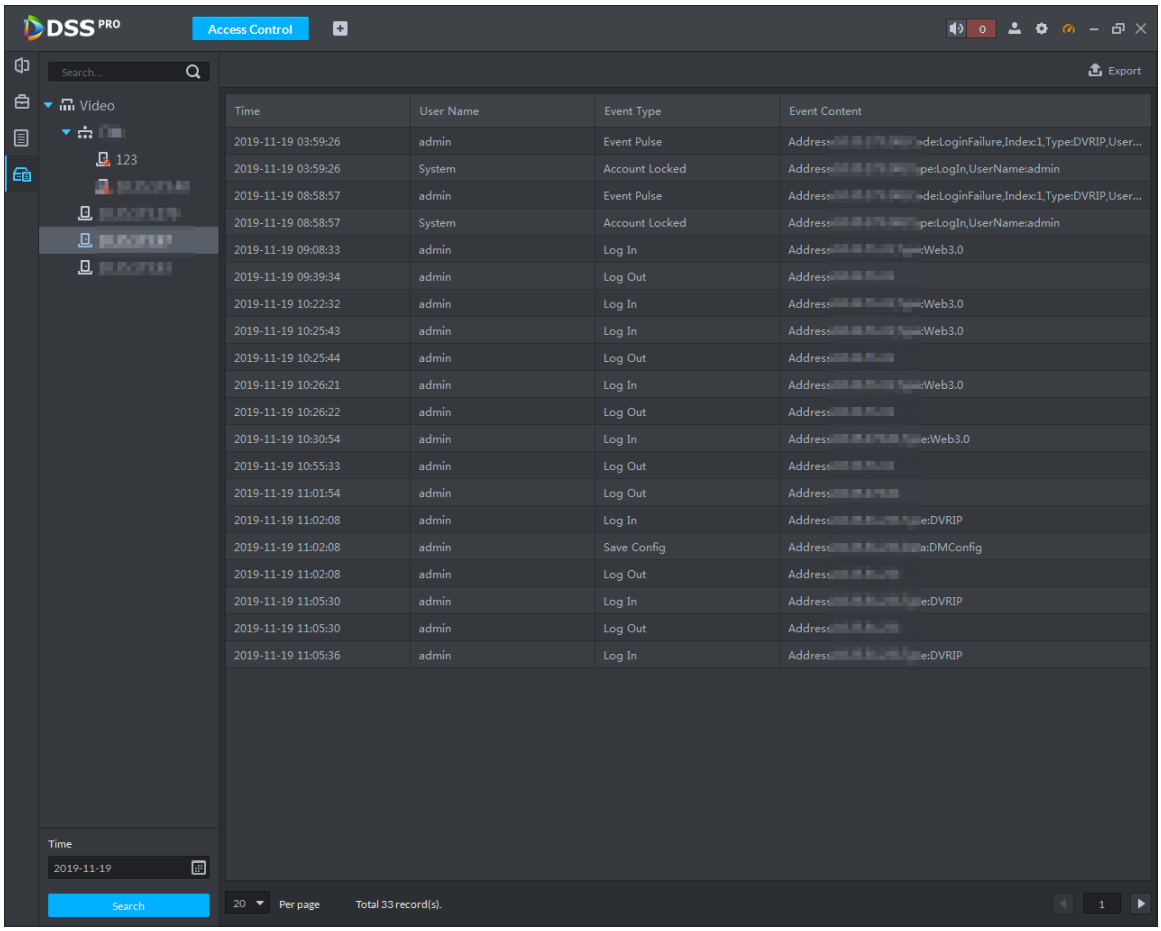
Se muestran los registros.

6.2.9 Visualización de registros de dispositivos

Ver registros de dispositivos de control de acceso, como registros de inicio y cierre de sesión.

Paso 1 En el **Control de acceso** interfaz, haga clic en .

Figura 6-30 Registro del dispositivo



Paso 2 Seleccione un dispositivo y una hora, y luego haga clic **Buscar.**

Se muestran los resultados de la búsqueda.

Apéndice 1 Recomendaciones de ciberseguridad

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

Acciones obligatorias que deben tomarse para la seguridad de la red de equipos básicos:

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Actualice el firmware y el software cliente a tiempo

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

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

Recomendaciones "Es bueno tener" para mejorar la seguridad de la red de su equipo:

1. Protección física

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

2. Cambie las contraseñas con regularidad

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de ser adivinado o descifrado.

3. Establecer y actualizar contraseñas Restablecer información a tiempo

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

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

Le sugerimos que cambie el HTTP predeterminado y otros puertos de servicio en cualquier conjunto de números entre 1024 ~ 65535, reduciendo el riesgo de que personas externas puedan adivinar qué puertos está utilizando.

6. **Habilitar HTTPS**

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

7. **Habilitar lista blanca**

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

8. **Enlace de dirección MAC**

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

9. **Asignar cuentas y privilegios de forma razonable**

   De acuerdo con los requisitos comerciales y de administración, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

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

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

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

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

11. **Transmisión encriptada de audio y video**

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

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

12. **Auditoría segura**

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

13. **Registro de red**

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

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

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

    - Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde una red externa.
    - La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, es

sugirió utilizar VLAN, red GAP y otras tecnologías para particionar la red, a fin de lograr el efecto de aislamiento de la red.

- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Se recomienda que habilite el firewall de su dispositivo o la función de lista negra y lista blanca para reducir el riesgo de que su dispositivo sea atacado.