Terminal de reconocimiento facial

Manual de usuario

V1.0.0

Prefacio

General

Este manual presenta la instalación y el funcionamiento básico del terminal de reconocimiento facial (en lo sucesivo, "terminal").

Las instrucciones de seguridad

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

Palabras de advertencia	Sentido
NOTA	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento	septiembre 2019

Sobre el Manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por las operaciones que no cumplen con el manual.
- El manual se actualizaría de acuerdo con las últimas leyes y reglamentos 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 reciente y la documentación complementaria.
- Todavía puede haber desviación en los datos técnicos, 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 del lector convencional si no se puede abrir el manual (en formato PDF).

- Todas las marcas comerciales, marcas comerciales registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio al cliente si ocurre algún problema al usar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

Medidas de seguridad y advertencias importantes

Este Capítulo describe el contenido que cubre el manejo adecuado del terminal, la prevención de riesgos y la prevención de daños a la propiedad. Lea este contenido detenidamente antes de utilizar el terminal, respételo cuando lo utilice y guárdelo para futuras consultas.

Requisito de operación

- No coloque ni instale el terminal en un lugar expuesto a la luz solar o cerca de una fuente de calor. Mantenga
- el terminal alejado de la humedad, el polvo o el hollín.
- Mantenga el terminal instalado horizontalmente en un lugar estable para evitar que se caiga. No deje
- caer ni salpique líquido sobre el terminal y asegúrese de que no haya ningún objeto lleno de líquido sobre el terminal para evitar que el líquido fluya hacia el terminal.
- Instale el terminal en un lugar bien ventilado y no bloquee la ventilación del terminal.

- Opere el terminal dentro del rango nominal de entrada y salida de
- energía. No desmonte el terminal.
- Transporte, utilice y almacene el terminal 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. Cuando reemplace la batería, asegúrese de usar 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 proporcionado con el terminal; de lo contrario, podría provocar lesiones personales y daños en el dispositivo.
- La fuente de alimentación debe cumplir con los requisitos del estándar de seguridad de voltaje extra bajo (SELV) y suministrar energía con un voltaje nominal que cumpla con el requisito de fuente de alimentación limitada de acuerdo con IEC60950-1. Tenga en cuenta que el requisito de fuente de alimentación está sujeto a la etiqueta del dispositivo.
- Conecte el dispositivo (estructura tipo I) a la toma de corriente con puesta a tierra de protección. El acoplador
- del aparato es un dispositivo de desconexión. Cuando use el acoplador, mantenga el ángulo para facilitar la operación.

Tabla de contenido

1 Visión de conjunto

1.1 Introducción

El terminal es un panel de control de acceso que admite desbloqueo a través de rostros, contraseñas y admite desbloqueo a través de sus combinaciones.

1.2 Características

- Admite desbloqueo facial y desbloqueo de contraseña; desbloquear por período
- Con caja de detección de rostros; la cara más grande entre las caras que aparecen al mismo tiempo se reconoce primero; el tamaño máximo de cara se puede configurar en la web
- Lente WDR gran angular de 2MP; con luz de relleno automática/manual
- Distancia cara-cámara: 0,3 m–2,0 m; altura humana: 0,9 m–2,4 m
- Con el algoritmo de reconocimiento facial, la terminal puede reconocer más de 360 posiciones en el rostro humano
- Precisión de verificación facial> 99.5%; baja tasa de reconocimiento falso
- Admite reconocimiento de perfil; el ángulo del perfil es de 0° a 90° Admite
- detección de vida
- Admite alarma de coacción y alarma de manipulación
- Admite usuarios generales, usuarios de coacción, usuarios de patrulla, usuarios de listas negras, usuarios VIP, usuarios invitados y usuarios discapacitados
- Con 4 modos de visualización de estado de desbloqueo y varios modos de aviso de voz

1.3 Dimensión y componente

Figura 1-1 Dimensiones y componentes (1) (mm [pulgadas])

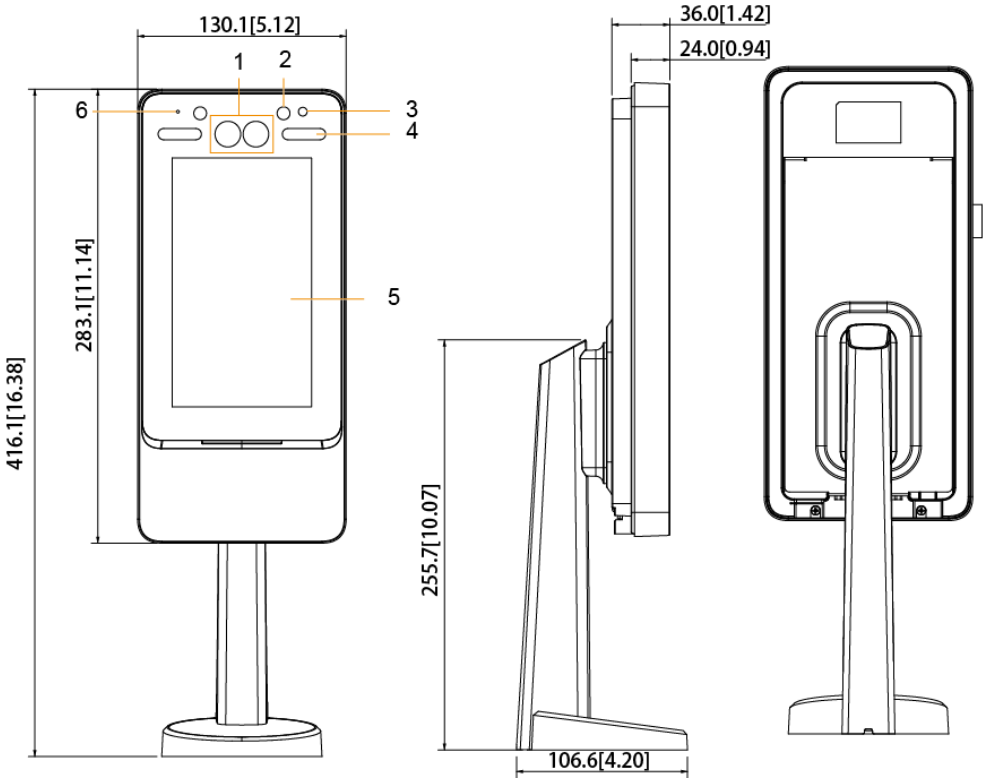


Tabla 1-1 Descripción de los componentes (1)

No.	Nombre
1	Cámara doble
2	luz infrarroja
3	fototransistor
4	Luz de relleno blanca
5	Mostrar
6	MICRÓFONO

Figura 1-2 Dimensiones y componentes (2) (mm [pulgadas])

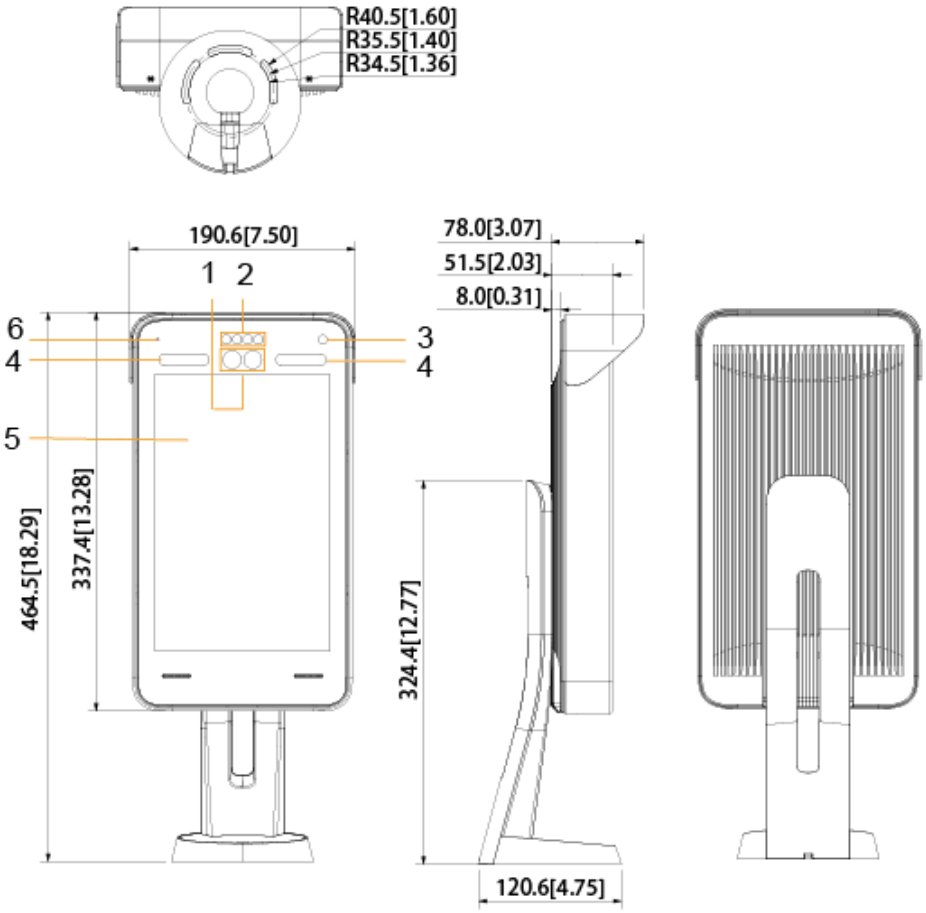


Tabla 1-2 Descripción de los componentes (2)

No.	Nombre
1	Cámara doble
2	luz infrarroja
3	fototransistor
4	Luz de relleno blanca
5	Mostrar
6	MICRÓFONO

2 Instalación

2.1 Conexiones de cables

El terminal debe estar conectado a dispositivos como sirenas, lectores y contactos de puerta. Para la conexión de cables, consulte la Tabla 2-1.

Tabla 2-1 Descripción del puerto

Puerto	Cable color	Nombre del cable	Descripción
CON1	Negro	RD–	Electrodo negativo de alimentación del lector externo.
	rojo	RD+	Electrodo positivo de alimentación del lector externo.
	Azul	CASO	Entrada de alarma de sabotaje del lector externo.
	blanco	D1	Entrada/salida Wiegand D1 (conectada a lector externo) (conectada a controlador).
	Verde	D0	Entrada/salida Wiegand D0 (conectada a lector externo) (conectada a controlador).
	marrón	LED	Entrada/salida de señal de confirmación Wiegand (conectada al lector de tarjetas externo) (conectada al controlador).
	Amarillo	B	Entrada/salida de electrodo negativo RS-485 (conectado a lector externo) (conectado a controlador, o conectado a módulo de seguridad de control de puerta). - Si el módulo de seguridad está habilitado, debe comprar el módulo de seguridad de control de acceso por separado. El módulo de seguridad necesita una fuente de alimentación separada para proporcionar energía. - Una vez que el módulo de seguridad está habilitado, el botón de salida, el control de bloqueo y el enlace de extinción de incendios no serán válidos.
	Púrpura	A	Entrada/salida de electrodo positivo RS-485 (conectado a lector externo) (conectado a controlador, o conectado a módulo de seguridad de control de puerta). - Si el módulo de seguridad está habilitado, debe comprar el módulo de seguridad de control de acceso por separado. El módulo de seguridad necesita una fuente de alimentación separada para proporcionar energía. - Una vez que el módulo de seguridad está habilitado, el botón de salida, el control de bloqueo y el enlace de extinción de incendios no serán válidos.

Puerto	Cable color	Nombre del cable	Descripción
CON2	blanco y rojo	ALARMA1_NO	La alarma 1 normalmente abre el puerto de salida.
	blanco y naranja	ALARMA1_COM	Puerto de salida común de alarma 1.
	blanco y azul	PUERTA2_NO	El control de la máquina de puerta normalmente abre el puerto.
	blanco y gris	PUERTA2_COM	Puerto común de control de la máquina de puerta.
	blanco y verde	TIERRA	Puerto común GND.
	blanco marrón	ALARMA1	Puerto de entrada de alarma 1.
	blanco y amarillo	TIERRA	Puerto común GND.
	blanco y púrpura	PUSH2	Botón de salida de la puerta No.2.
CON3	Negro y rojo	RX	Puerto de recepción RS-232.
	Negro y naranja	Texas	Puerto de envío RS-232.
	Negro y azul	TIERRA	Puerto común GND.
	Negro y gris	SR1	N / A.
	Negro y verde	EMPUJAR1	Botón de salida de la puerta No.1
	Negro y marrón	PUERTA1_COM	Puerto normalmente cerrado del control de la máquina de puerta.
	Negro y amarillo	PUERTA1_NO	Puerto común de control de la máquina de puerta.
	Negro y púrpura	PUERTA1_NC	El control de la máquina de puerta normalmente abre el puerto.

2.2 Instalación

Figura 2-1 Instalación del terminal de 7 pulgadas

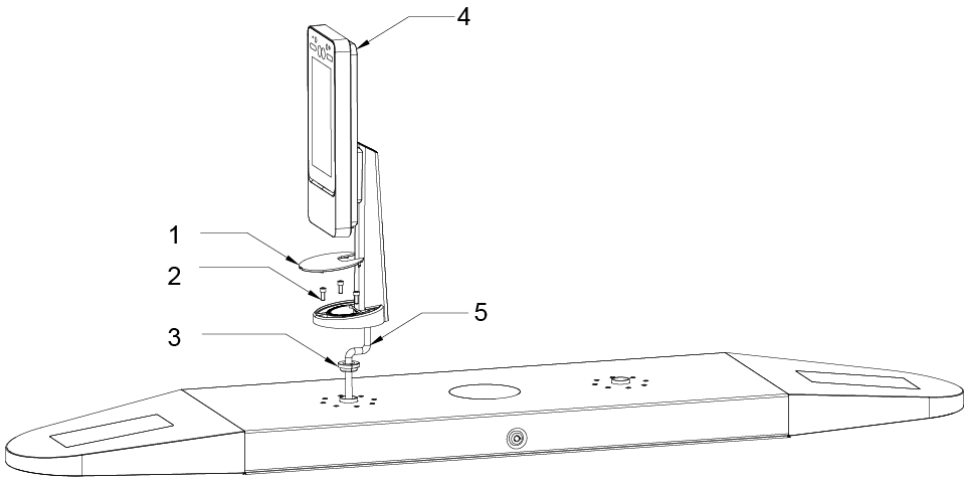


Tabla 2-2 Descripción de los componentes (2)

No.	Nombre
1	cubierta ornamental
2	tornillo M5
3	Tapón de gel de sílice resistente al agua
4	Terminal
5	Cable

Figura 2-2 Instalación del terminal de 10 pulgadas

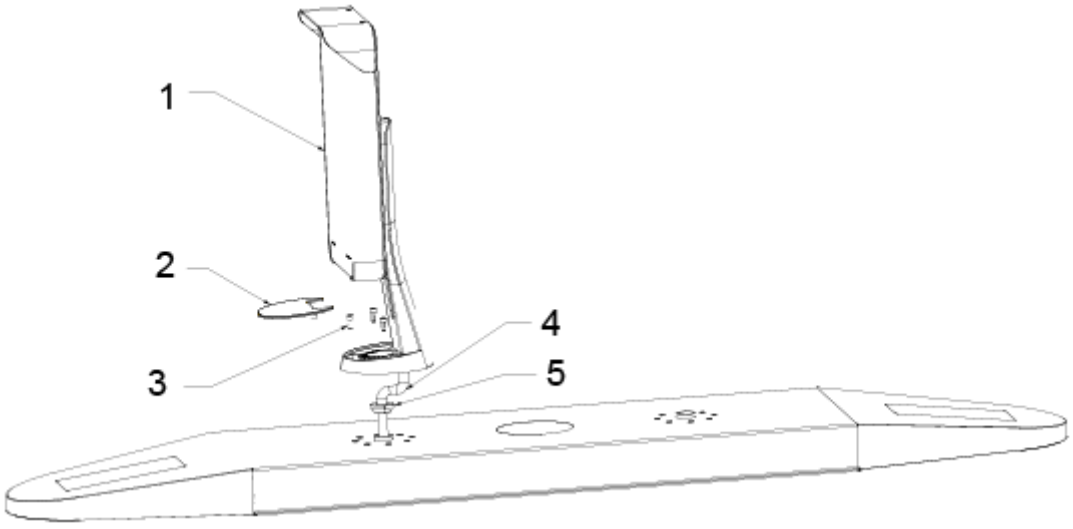


Tabla 2-3 Descripción de los componentes (3)

No.	Nombre
1	Terminal
2	cubierta ornamental
3	tornillo M5
4	Cable
5	Tapón de gel de sílice resistente al agua

Procedimiento de instalación

Paso 1 Pase el cable a través del torniquete.

Paso 2 Coloque el enchufe de gel de sílice a prueba de agua en el cable. Fije el

Paso 3 terminal en el torniquete con tornillo M5. Conecte los cables para el terminal.

Consulte "2.1 Conexiones de cables".

Etapa 4 Aplique sellador a los espacios entre el tapón impermeable de gel de sílice y el

Paso 5 torniquete. Instale la cubierta ornamental en la base del terminal.

La instalación está terminada.

3 Operación del sistema

3.1 Descripción del botón

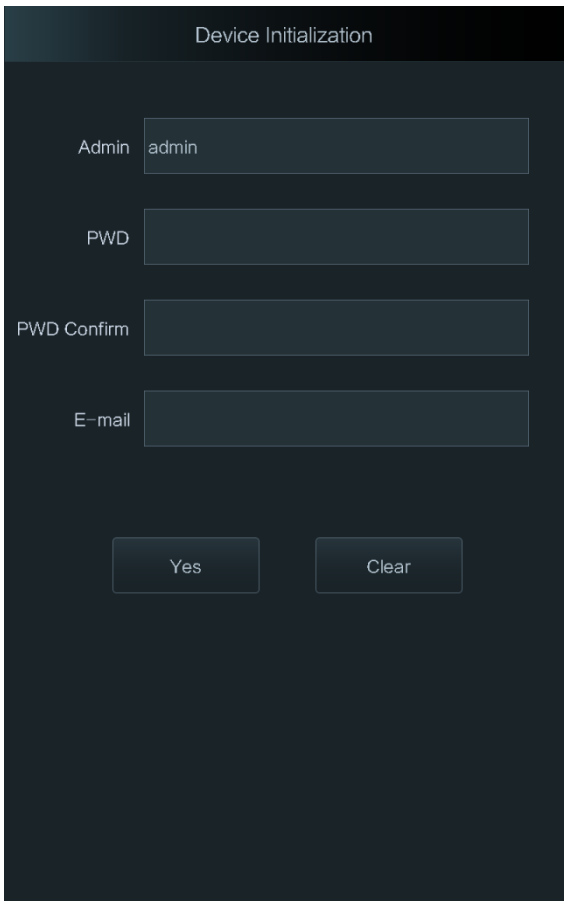
Tabla 3-1 Descripción del botón

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

3.2 Inicialización

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

Figura 3-1 Inicialización



- El administrador y la contraseña establecidos en esta interfaz se utilizan para iniciar sesión en la administración web plataforma.

- La contraseña de administrador se puede restablecer a través de la dirección de correo electrónico que ingresó si el 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 ' " ; : &).

3.3 Interfaz de espera

Puede desbloquear la puerta a través de rostros, contraseñas y código QR. Consulte la Tabla 3-2.

- Si no hay operaciones en 30 segundos, el terminal pasará al modo de espera.
- Las siguientes figuras son solo de referencia y prevalecerá la interfaz real.

Figura 3-2 Página de inicio

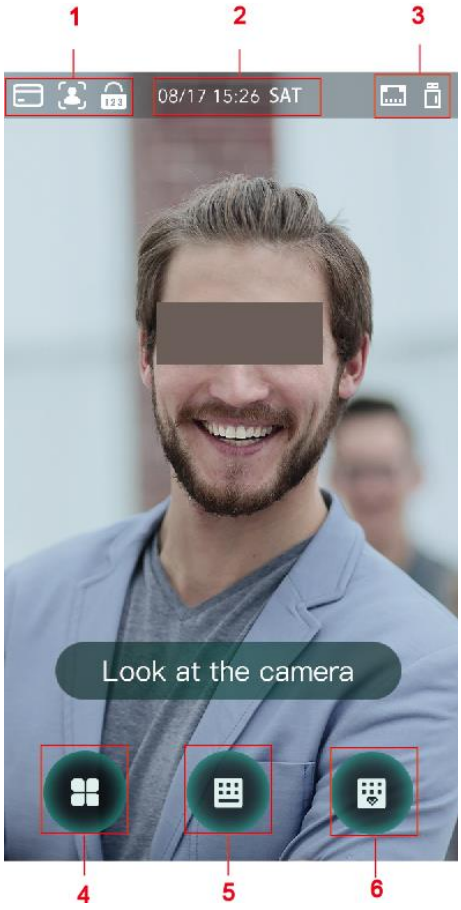


Tabla 3-2 Descripción de la página de inicio

No.	Descripción
1	Métodos de desbloqueo: tarjeta, rostro y contraseña.
2	Fecha y hora: aquí se muestra la fecha y la hora actuales.
3	El estado de la red y el estado de la batería se muestran aquí.
4	Icono del menú principal. Solo el administrador puede ingresar al menú principal.
5	Icono de desbloqueo de contraseña.
6	Icono de desbloqueo de contraseña de administrador.

3.4 Métodos de desbloqueo

Puede desbloquear la puerta a través de la cara, las contraseñas y la tarjeta.

3.4.1 Cara

Asegúrese de que su rostro esté centrado en el marco de reconocimiento facial y luego podrá desbloquear la puerta.

3.4.2 Contraseñas de usuario

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

Paso 1 Grifo  en la página de inicio.

Paso 2 Ingrese la ID de usuario y luego toque  .

Paso 3 Ingrese la contraseña de usuario y luego toque  .

La puerta está desbloqueada.

3.4.3 Contraseña de administrador

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

La contraseña de administrador no se puede utilizar cuando se selecciona NC en "Período NC".

Paso 1 Grifo  en la página de inicio.

Paso 2 Grifo**Ingrese el PWD del administrador**.

Paso 3 Ingrese la contraseña del administrador y luego toque  .

La puerta está desbloqueada.

3.5 Menú principal

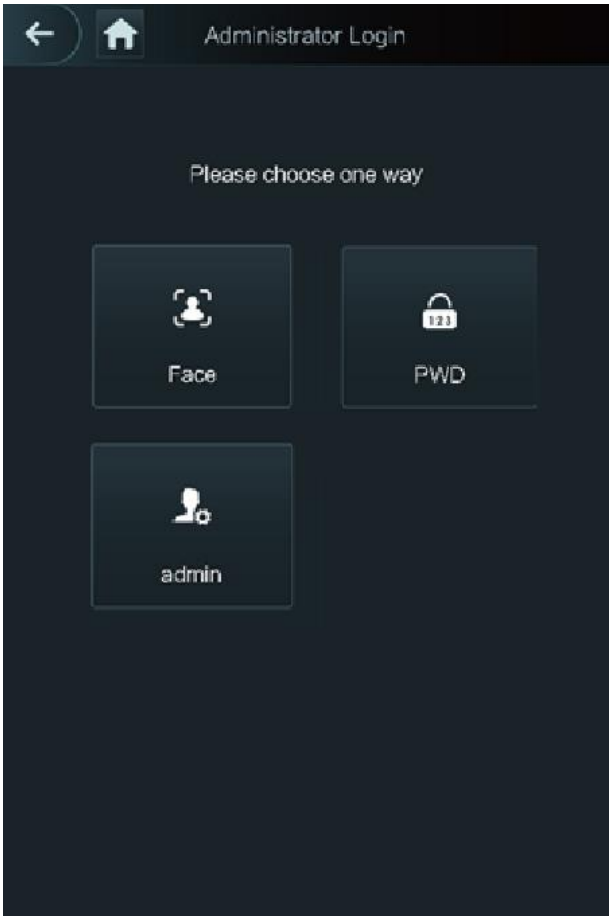
Los administradores pueden agregar usuarios de diferentes niveles, establecer parámetros relacionados con el acceso, configurar la red, ver registros de acceso e información del sistema, y más en el menú principal.

Paso 1 Grifo  en la interfaz de espera.

los**Inicio de sesión del administrador**se muestra la interfaz.

Los diferentes modos admiten diferentes métodos de desbloqueo y prevalecerá la interfaz real.

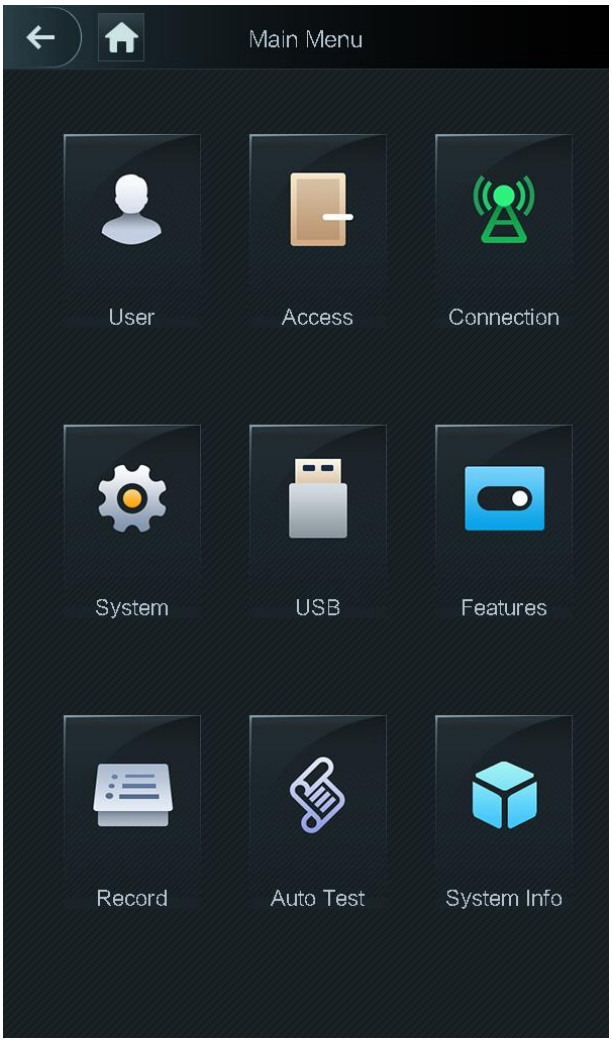
Figura 3-3 Inicio de sesión del administrador



Paso 2 Seleccione un método de entrada del menú principal.

Se muestra la interfaz del menú principal.

Figura 3-4 Menú principal



3.6 Gestión de usuarios de terminales

Puede agregar nuevos usuarios, ver listas de usuarios, listas de administradores y modificar la contraseña del administrador en la interfaz de usuario.

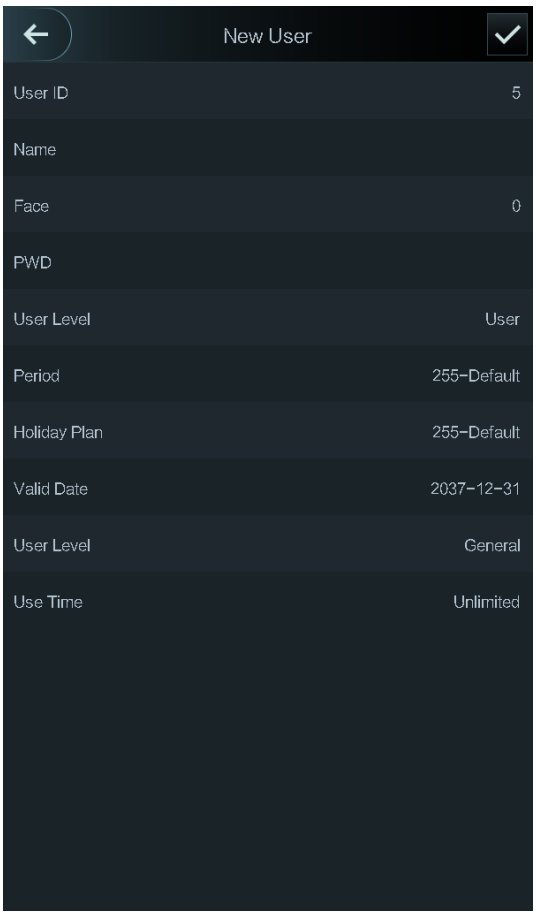
3.6.1 Adición de nuevos usuarios

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

Las siguientes figuras son solo de referencia y prevalecerá la interfaz real. Paso 1 Seleccione**Usuario > Nuevo usuario**.

los**Información de nuevo usuario**se muestra la interfaz. Consulte la Figura 3-5.

Figura 3-5 Información de nuevo usuario



Paso 2 Configure los parámetros en la interfaz. Consulte la Tabla 3-3.

Tabla 3-3 Descripción del nuevo parámetro de usuario

Parámetro	Descripción
ID de usuario	Puede introducir ID de usuario. Los ID pueden ser números, letras y sus combinaciones, y la longitud máxima del ID es de 32 caracteres.
Nombre	Puede ingresar nombres con un máximo de 32 caracteres (incluidos números, símbolos y letras).
Rostro	Asegúrese de que su rostro esté centrado en el marco de captura de imágenes y luego se capturará automáticamente una imagen de su rostro. Para obtener más información sobre la grabación de imágenes de rostros, consulte la *Guía de inicio rápido.*
Clave	La contraseña de desbloqueo de la puerta. La longitud máxima de los dígitos de identificación es 8. Si el terminal no tiene pantalla táctil, debe conectar el terminal a un lector de tarjetas periférico. Hay botones en el lector de tarjetas.
Nivel	Puede seleccionar un nivel de usuario para los nuevos usuarios. Hay dos opciones. - Usuario: los usuarios solo tienen autoridad para desbloquear puertas. - Admin: los administradores no solo pueden desbloquear la puerta, sino que también tienen autoridad para configurar parámetros. No importa si hay un administrador en el controlador de acceso, se necesita la autenticación de identidad del administrador.
Período	Puede establecer un período en el que el usuario puede desbloquear la puerta. Para obtener información detallada sobre la configuración del período, consulte el manual de configuración.

Parámetro	Descripción
Fiesta Plan	Puede establecer un plan de vacaciones en el que el usuario puede desbloquear la puerta. Para obtener información detallada sobre los ajustes del plan de vacaciones, consulte el manual de configuración.
Fecha válida	Puede establecer un período durante el cual la información de desbloqueo del usuario es válida.
Nivel de usuario	Hay seis niveles: - General: los usuarios generales pueden desbloquear la puerta normalmente. - Lista negra: cuando los usuarios en la lista negra abren la puerta, el personal de servicio recibirá un aviso. - Invitado: los invitados pueden desbloquear la puerta en ciertos momentos en ciertos períodos. Una vez superados los tiempos y plazos máximos, no podrán volver a desbloquear la puerta. - Patrulla: los usuarios de Patrulla 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. Deshabilitar: - cuando las personas discapacitadas abren la puerta, habrá un retraso de 5 segundos antes de que se cierre la puerta.
tiempo de uso	Cuando el nivel de usuario es Invitado, puede establecer el número máximo de veces que el invitado puede desbloquear la puerta.

Paso 3 Después de haber configurado todos los parámetros, toque  para guardar la configuración.

3.6.2 Visualización de la información del usuario

Puede ver la lista de usuarios, la lista de administradores y habilitar la contraseña de administrador a través de la interfaz de usuario.

3.7 Gestión de acceso

Puede administrar el acceso según el período, el modo de desbloqueo, la alarma, el estado de la puerta y el tiempo de retención de la cerradura.

Grifo**Acceso**para ir a la interfaz de gestión de acceso.

3.7.1 Gestión de períodos

Puede establecer periodos, periodos de vacaciones, periodos de plan de vacaciones, periodos de puerta normalmente abierta, periodos de puerta normalmente cerrada y periodos de verificación remota.

3.7.1.1 Configuración del período

Puede configurar 128 períodos (semanas) cuyo rango de números es 0–127. Puede establecer cuatro períodos en cada día de un período (semana). Los usuarios solo pueden desbloquear la puerta en los períodos que establezca.

3.7.1.2 Grupo de vacaciones

Puede establecer vacaciones grupales y luego 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. Configurar el

hora de inicio y hora de finalización de un grupo de vacaciones, y luego los usuarios solo pueden desbloquear la puerta en los períodos que establezca.

Puede ingresar nombres con 32 caracteres (incluidos números, símbolos y letras). Grifo para guardar el nombre del grupo de vacaciones.

3.7.1.3 Plan de vacaciones

Puede agregar grupos de vacaciones a los planes de vacaciones. Puede utilizar los planes de vacaciones para administrar la autoridad de acceso de los usuarios en diferentes grupos de vacaciones. Los usuarios solo pueden desbloquear la puerta en el período que establezca.

3.7.1.4 SIN Período

Si se añade un punto a la**NO**período, entonces la puerta está normalmente abierta en ese período.

los**NO C**los permisos del período son más altos que los permisos en otros períodos.

3.7.1.5 Período NC

Si se agrega un período al período NC, la puerta normalmente se cierra en ese período. Los usuarios no pueden desbloquear la puerta en este período.

3.7.1.6 Período de verificación remota

Si configuró el período de verificación remota, cuando desbloquee las puertas durante el período que configuró, se requiere la verificación remota. Para desbloquear la puerta en este período, se necesita una instrucción de desbloqueo de puerta enviada por la plataforma de gestión.

Debe habilitar el Período de verificación remota.

- 

significa habilitado.
- 

significa no habilitado.

3.7.2 Desbloquear

Hay tres modos de desbloqueo: modo de desbloqueo, desbloqueo por período y combinación de grupo. Los modos de desbloqueo varían según los modelos de acceso al controlador y prevalecerá el acceso real al controlador.

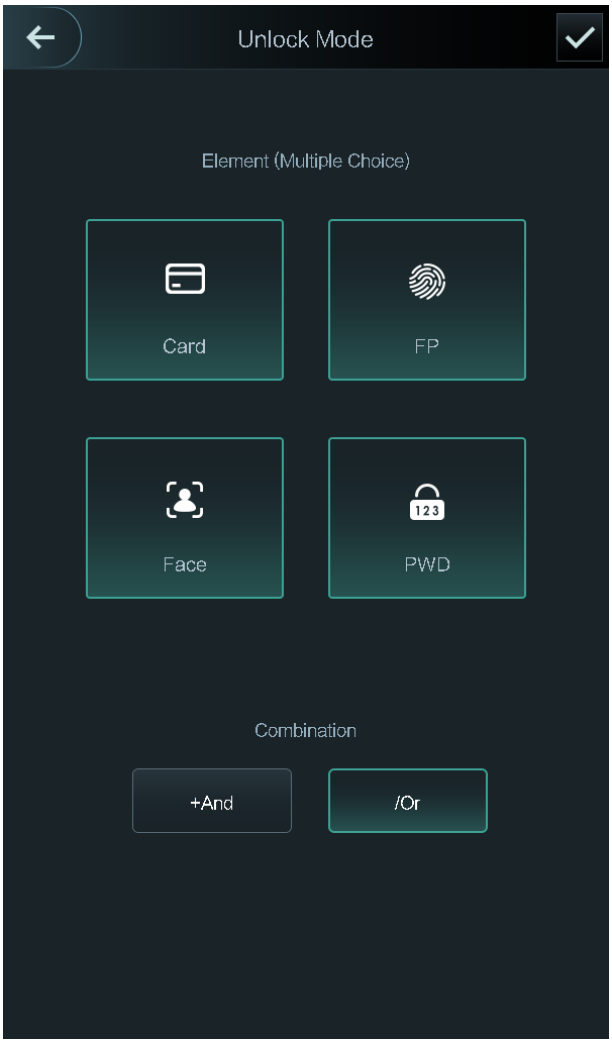
3.7.2.1 Modo de desbloqueo

Cuando el**Modo de desbloqueo**está activado, los usuarios pueden desbloquear a través de tarjetas, huellas dactilares, caras, contraseñas o cualquiera de todos los métodos de desbloqueo.

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

los**Elemento (opción múltiple)**se muestra la interfaz. Consulte la Figura 3-6.

Figura 3-6 Elemento (opción múltiple)



Paso 2 Seleccione el(los) modo(s) de desbloqueo.

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

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 dactilares.

Etapa 4 Grifo para guardar la configuración.

y luego el**Modo de desbloqueo**se muestra la interfaz.

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

- ON significa habilitado.
- OFF significa no habilitado.

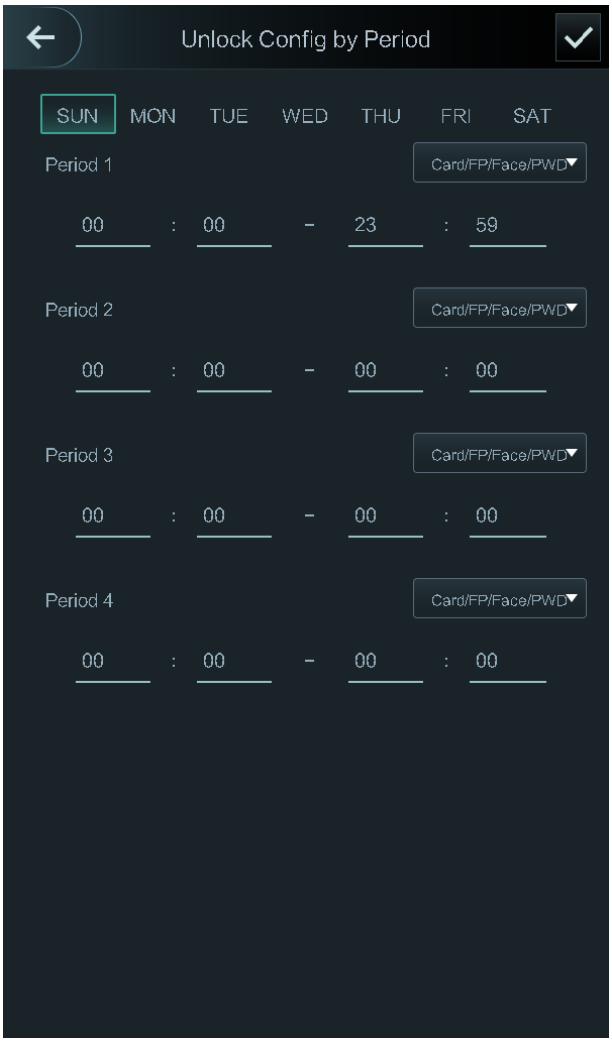
3.7.2.2 Desbloqueo por período

Las puertas se pueden desbloquear a través de diferentes modos de desbloqueo en diferentes períodos. Por ejemplo, en el período 1, la puerta solo se puede desbloquear con tarjeta; y en el período 2, las puertas solo se pueden desbloquear mediante huellas dactilares.

Paso 1 Seleccione**Evaluar > Modo de desbloqueo > Desbloqueo por período**.

los**Desbloquear configuración por período**se muestra la interfaz. Consulte la Figura 3-7.

Figura 3-7 Desbloqueo por período



Paso 2 Establezca la hora de inicio y la hora de finalización para un período y luego seleccione un modo de desbloqueo.

Paso 3 Grifo  para guardar la configuración.

los**Modo de desbloqueo**se muestra la interfaz.

Etapa 4 Habilitar el**Desbloqueo por período**función.

-  significa habilitado.
-  significa no habilitado.

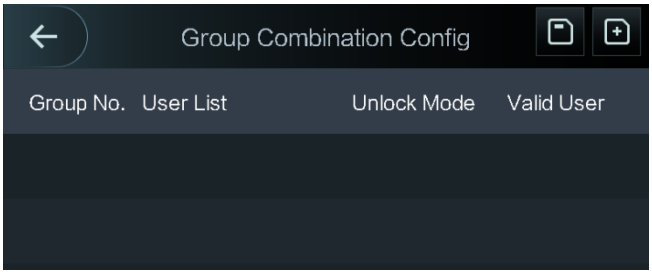
3.7.2.3 Combinación de grupos

Las puertas solo pueden ser desbloqueadas por un grupo o grupos que constan de más de dos usuarios si la combinación de grupos está habilitada.

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

los**Configuración de combinación de grupo**se muestra la interfaz. Consulte la Figura 3-8.

Figura 3-8 Combinación de grupos



Paso 2 Grifo  para crear un grupo.

los**Añadir grupo**se muestra la interfaz. Consulte la Figura 3-9.

Figura 3-9 Agregar un grupo

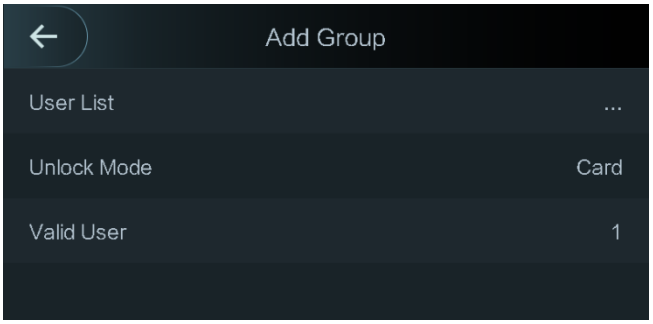


Tabla 3-4 Parámetro de grupo

Parámetro	Descripción
Lista de usuarios	Agregue usuarios al grupo recién creado. 1. Toque**Lista de usuarios**. los**Lista de usuarios**se muestra la interfaz. 2. Toca y, a continuación, introduzca un ID de usuario. 3. Toque para guardar la configuración.
Modo de desbloqueo	Hay dos opciones:**PCD**y**Rostro**.
Usuario válido	Los usuarios válidos son los que tienen autorización de desbloqueo. Las puertas se pueden desbloquear solo cuando el número de usuarios para desbloquear las puertas es igual al número de usuario válido. - Los usuarios válidos no pueden exceder el número total de usuarios en un grupo. Si los usuarios - válidos son iguales al número total de usuarios en un grupo, solo todos los usuarios del grupo pueden desbloquear las puertas. - Si los usuarios válidos son menos que el número total de usuarios en un grupo, cualquier usuario cuyo número sea igual al número de usuario válido puede desbloquear las puertas.

Paso 3 Grifo para volver a la interfaz anterior.

Etapa 4 Grifo para guardar la configuración.

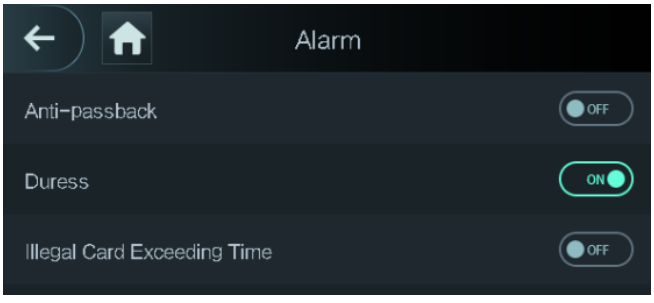
Paso 5 Habilite la combinación de grupos.

- significa habilitado.
- significa no habilitado.

3.7.3 Configuración de alarmas

Los administradores pueden administrar la autoridad de desbloqueo de los visitantes a través de la configuración de alarmas. Seleccione**Acceso > Alarma**. los**Alarma**se muestra la interfaz. Consulte la Figura 3-10.

Figura 3-10 Alarma



- significa habilitado.
- significa no habilitado.

Tabla 3-5 Parámetros en la interfaz de alarma

Parámetro	Descripción
Anti-passback	- Si una persona abre la puerta con la identidad verificada por el controlador de acceso, pero cuando la persona sale sin que el controlador de acceso verifique la identidad, se activará una alarma y la persona ya no tendrá autoridad para desbloquear la puerta. - Si una persona ingresa a un edificio o una habitación sin pasar la tarjeta, y la persona pasó la tarjeta para salir, entonces la persona ya no tendrá autoridad para abrir la puerta.
Coacción	Se activará una alarma cuando se utilice una tarjeta de coacción, una contraseña de coacción o una huella dactilar de coacción para desbloquear la puerta.
Tarjeta ilegal Excesivo Hora	Después de usar una tarjeta no autorizada para desbloquear la puerta más de 5 veces en 50 segundos, se activará una alarma.

3.7.4 Estado de la puerta

Hay tres opciones:**NO**,**CAROLINA DEL NORTE**, 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 se selecciona Normal, la puerta se desbloqueará y bloqueará según su configuración.

3.7.5 Tiempo de retención de bloqueo

Tiempo de retención de bloqueoes la duración en la que la cerradura está desbloqueada. Si la cerradura ha estado desbloqueada por un período que excede la duración, la cerradura se bloqueará automáticamente.

3.8 Red de comunicación

Para que el terminal funcione normalmente, debe configurar los parámetros de red, puertos serie y puertos wiegand.

3.8.1 Dirección IP

3.8.1.1 Configuración IP

Configure una dirección IP para que el terminal se conecte a la red. Consulte la Figura 3-11 y la Tabla 3-6.

Figura 3-11 Configuración de la dirección IP

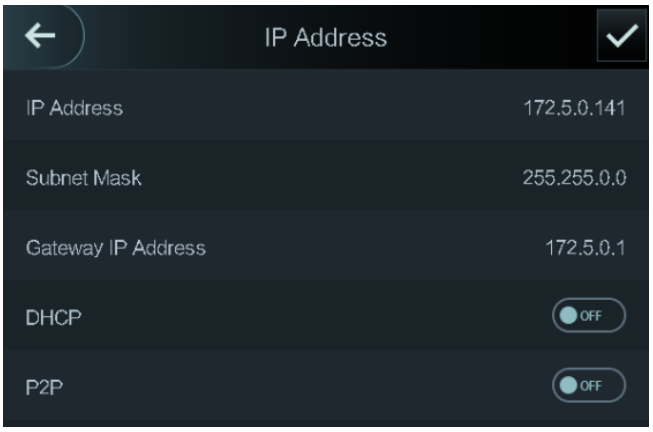


Tabla 3-6 Parámetros de configuración de IP

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 activadas. 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 Registro activo

Mediante el registro activo, puede conectar el terminal a la plataforma de administración y luego puede administrar el terminal a través de la plataforma de administración.

Las configuraciones que ha realizado se pueden borrar en la plataforma de gestión y el terminal puede ser inicializado, debe proteger la autoridad de gestión de la plataforma en caso de pérdida de datos causada por mal funcionamiento.

Para el parámetro de registro activo, consulte la Tabla 3-7.

Tabla 3-7 Registro activo

Nombre	Parámetro
Dirección IP del servidor	Dirección IP de la plataforma de gestión.
Puerto	Número de puerto de la plataforma de gestión.
Identificación del dispositivo	Número de dispositivo subordinado en la plataforma de gestión.

3.8.1.3 Wifi

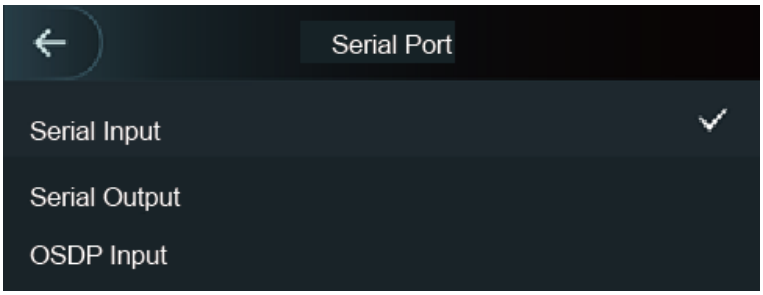
Puede conectar el controlador de acceso a la red a través de Wi-Fi si el controlador de acceso tiene función Wi-Fi.

3.8.2 Configuración del puerto serie

Seleccione la entrada en serie o la salida en serie de acuerdo con la dirección de entrada y la dirección de salida.

Seleccione**Conexión > Puerto Serie**, y luego el**Puerto serial**se muestra la interfaz. Consulte la Figura 3-12.

Figura 3-12 Puerto serie



- Seleccione**Entrada en serie**cuando se conectan al terminal dispositivos externos con funciones de lectura y escritura de tarjetas.**Entrada en serie**se selecciona para permitir el envío de la información de la tarjeta de acceso al terminal ya la plataforma de gestión.
- Cuándo**Entrada en serie**está seleccionado para que el terminal se conecte al lector en el torniquete, debe seleccionar Puerta 1 o Puerta 2 según sea necesario.
  - Puerta 1: si se selecciona Puerta 1, el lector y el terminal controlan la misma dirección de apertura de la puerta. Por ejemplo, tanto el lector como el terminal controlan la dirección de entrada a un lugar o todos controlan la dirección de salida de un lugar.
  - Puerta 2: si se selecciona Puerta 2, el lector y el terminal controlan diferentes direcciones de apertura de la puerta. Por ejemplo, la terminal controla la dirección de entrada a un lugar y el lector controla la dirección de salida de un lugar.
- Para terminales con funciones de reconocimiento facial, reconocimiento de huella, lectura y escritura de tarjetas, si seleccionas**Salida en serie**, el terminal enviará información de bloqueo/desbloqueo al terminal. Hay dos tipos de información de bloqueo/desbloqueo:
  - ID de usuario
  - número de tarjeta
- Seleccione Entrada OSDP cuando el lector de tarjetas del protocolo OSDP esté conectado al terminal. El terminal puede enviar información de la tarjeta a la plataforma de gestión.

3.8.3 Configuración Wiegand

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

Seleccione**Conexión > Wiegand**y luego se muestra la interfaz Wiegand. Consulte la Figura 3-13.

Figura 3-13 Wiegand

- Seleccione**Entrada Wiegand**cuando se conecta un mecanismo de lector de tarjeta externo al terminal.
- Cuándo**Entrada en serie**está seleccionado para que el terminal se conecte al lector en el torniquete, debe seleccionar Puerta 1 o Puerta 2 según sea necesario.
  - Puerta 1: si se selecciona Puerta 1, el lector y el terminal controlan la misma dirección de apertura de la puerta. Por ejemplo, tanto el lector como el terminal controlan la dirección de entrada a un lugar o todos controlan la dirección de salida de un lugar.
  - Puerta 2: si se selecciona Puerta 2, el lector y el terminal controlan diferentes direcciones de apertura de la puerta. Por ejemplo, la terminal controla la dirección de entrada a un lugar y el lector controla la dirección de salida de un lugar.
- Seleccione**Salida Wiegand**cuando el terminal funciona como un lector que se puede conectar al controlador. Consulte la Tabla 3-8.

Tabla 3-8 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 reconocer el terminal. - Wiegand26, tres bytes, seis dígitos. - Wiegand34, cuatro bytes, ocho dígitos. - Wiegand66, ocho bytes, dieciséis dígitos.
Ancho de pulso	Puede establecer 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 generará la ID de usuario. - Nº de tarjeta: si se selecciona Nº de tarjeta, se emitirá el número de tarjeta.

3.9 Sistema

3.9.1 Tiempo

Puede realizar la configuración de formato de fecha, configuración de fecha, configuración de hora, configuración de horario de verano, verificación de NTP, configuración de zona horaria.

- Cuando selecciona Network Time Protocol (NTP), necesita configurar lo siguiente parámetros Primero debe habilitar la función NTP Check. Dirección IP del servidor: introduzca la Dirección IP del servidor de tiempo, la hora del terminal se sincronizará con el servidor de tiempo.
- Puerto: Introduzca el número de puerto del servidor horario.
- Intervalo (min): intervalo de verificación NPT. Toque el icono de guardar para guardar.

3.9.2 Parámetro de cara

Figura 3-14 Parámetro de cara

Toque un parámetro y realice la configuración, y luego toque .

Tabla 3-9 Parámetro de cara

Nombre	Descripción
Reconocimiento facial Límite	La precisión del reconocimiento facial se puede ajustar. Cuanto mayor sea el valor, mayor será la precisión.
máx. Ángulo de reconocimiento facial	Puede establecer el ángulo de disparo de los perfiles del panel de control. Cuanto mayor sea el valor, se reconocerá una gama más amplia de perfiles.
Tiempo de espera de reconocimiento	Cuando una persona que no tiene la autoridad de acceso se para frente a la terminal y se le reconoce el rostro, el controlador indicará que el reconocimiento de rostro falló. El intervalo de solicitud se denomina tiempo de espera de reconocimiento.
Distancia pupilar	La distancia pupilar es el valor de píxel de la imagen entre los centros de las pupilas de cada ojo. Debe establecer un valor apropiado para que el controlador de acceso pueda reconocer las caras según sea necesario. El valor cambia según el tamaño de la cara y la distancia entre las caras y la lente. Cuanto más cerca esté la cara de la lente, mayor debe ser el valor. Si un adulto está a 1,5 metros de la lente, el valor de la distancia pupilar puede estar entre 50 y 70.
Intervalo de reconocimiento	Cuando una persona que tiene la autoridad de acceso se para frente a la terminal y obtiene el reconocimiento facial, el controlador indicará que el reconocimiento facial se realizó correctamente. El intervalo de indicación es el intervalo de reconocimiento.

Nombre	Descripción
Umbral anti-falsificación	Esta función evita que las personas se desbloqueen mediante imágenes de rostros humanos o modelos de rostros. Cuanto mayor sea el valor, las imágenes de rostros más difíciles pueden abrir la puerta. El rango de valores recomendado es superior a 80.

3.9.3 Configuración del modo de luz de relleno

Puede seleccionar modos de luz de relleno según sus necesidades. Hay tres modos:

- Automático: cuando el fotosensor detecta que el entorno ambiental no está oscuro, la luz de relleno normalmente está apagada; de lo contrario, la luz de llenado estará encendida.
- NO: La luz de llenado normalmente está abierta. NC:
- La luz de llenado normalmente está cerrada.

3.9.4 Configuración del brillo de la luz de relleno

Puede seleccionar el brillo de la luz de relleno según sus necesidades.

3.9.5 Ajuste de volumen

Grifo  o  para ajustar el volumen.

3.9.6 Ajuste del brillo de la luz IR

Cuanto mayor sea el valor, más claras serán las imágenes; de lo contrario, menos claras serán las imágenes.

3.9.7 Restaurar a la configuración de fábrica

- Los datos se perderán si restaura el controlador de acceso a la configuración de fábrica.
- Después de restaurar el controlador de acceso a la configuración de fábrica, la dirección IP no se cambió.

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

- Puede seleccionar restaurar el terminal a la configuración de fábrica con toda la información del usuario y del dispositivo eliminada.
- Puede seleccionar restaurar el terminal a la configuración de fábrica con la información del usuario y la información del dispositivo retenida.

3.9.8 Reiniciar

Seleccione**Configuración > Reiniciar**, grifo**Reiniciar**, y el terminal se reiniciará.

USB 3.10

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

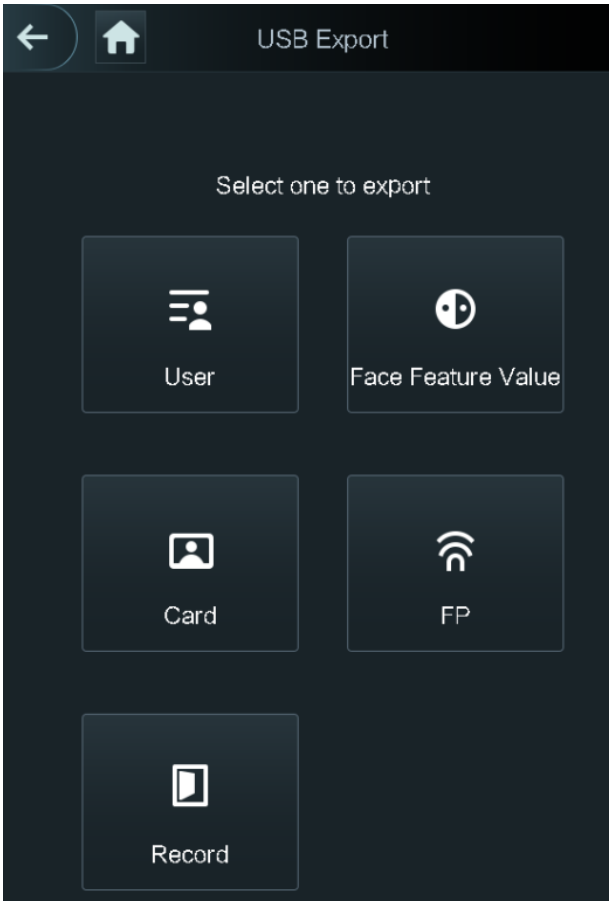
3.10.1 Exportación USB

Puede exportar datos desde el terminal al USB después de insertar el USB. Los datos exportados están encriptados y no se pueden editar.

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

los**Exportación USB**se muestra la interfaz. Consulte la Figura 3-15.

Figura 3-15 Exportación USB



Paso 2 Seleccione el tipo de datos que desea exportar.

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

Paso 3 Grifo**OK**.

Los datos exportados se guardarán en el USB.

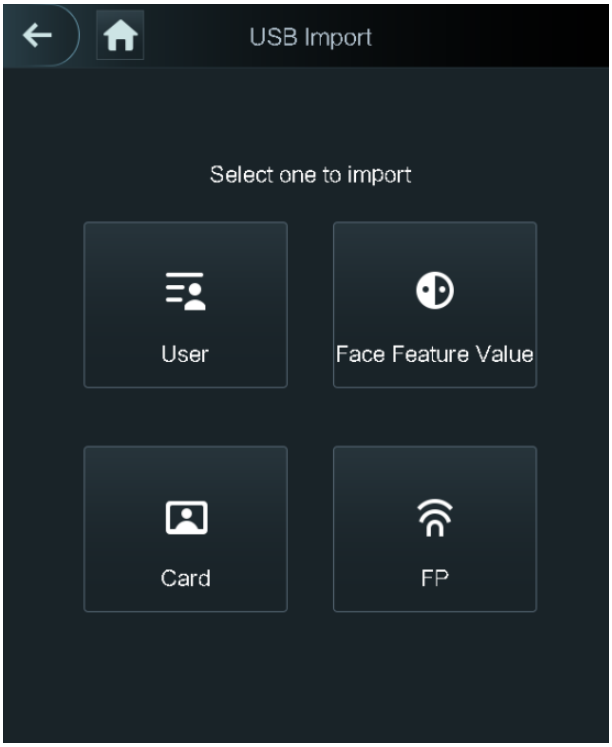
3.10.2 Importación USB

Solo los datos en el USB que se exportaron desde un terminal se pueden importar a otro terminal.

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

los**Importación USB**se muestra la interfaz. Consulte la Figura 3-16.

Figura 3-16 Importación USB



Paso 2 Seleccione el tipo de datos que desea importar.

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

Paso 3 Grifo**OK**.

Los datos del USB se importarán al terminal.

3.10.3 Actualización USB

El USB se puede utilizar 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 Grifo**OK**.

La actualización comienza y el terminal se reinicia después de que finaliza la actualización.

3.10.4 Características

Puede realizar configuraciones sobre privacidad, reversión del número de tarjeta, módulo de seguridad, tipo de sensor de puerta y retroalimentación de resultados. Para detalles de las funciones mencionadas, vea la Figura 3-17 y la Tabla 3-10.

Figura 3-17 Características

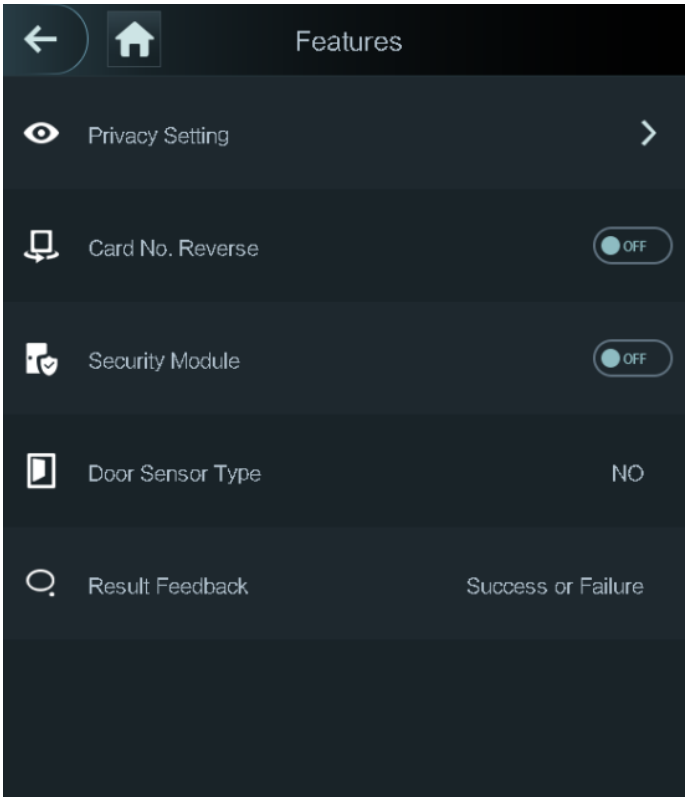


Tabla 3-10 Descripción de funciones

Parámetro	Descripción
Configuración de privacidad	Consulte "3.10.4.2 Configuración de privacidad" para obtener más información.
Número de tarjeta Reverso	Si el lector de tarjetas de terceros debe conectarse al terminal a través del puerto de salida wiegand, debe habilitar la función Invertir 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.
Módulo de seguridad	- Si el módulo de seguridad está habilitado, debe comprar el módulo de seguridad de control de acceso por separado. El módulo de seguridad necesita una fuente de alimentación separada para proporcionar energía. - Una vez que el módulo de seguridad está habilitado, el botón de salida, el control de bloqueo y el enlace de extinción de incendios no serán válidos.
Tipo de sensor de puerta	Hay dos opciones:**NO**y**CAROLINA DEL NORTE**.
Comentarios sobre los resultados	Muestra si el desbloqueo tuvo éxito o falló.

3.10.4.2 Configuración de privacidad

Figura 3-18 Configuración de privacidad

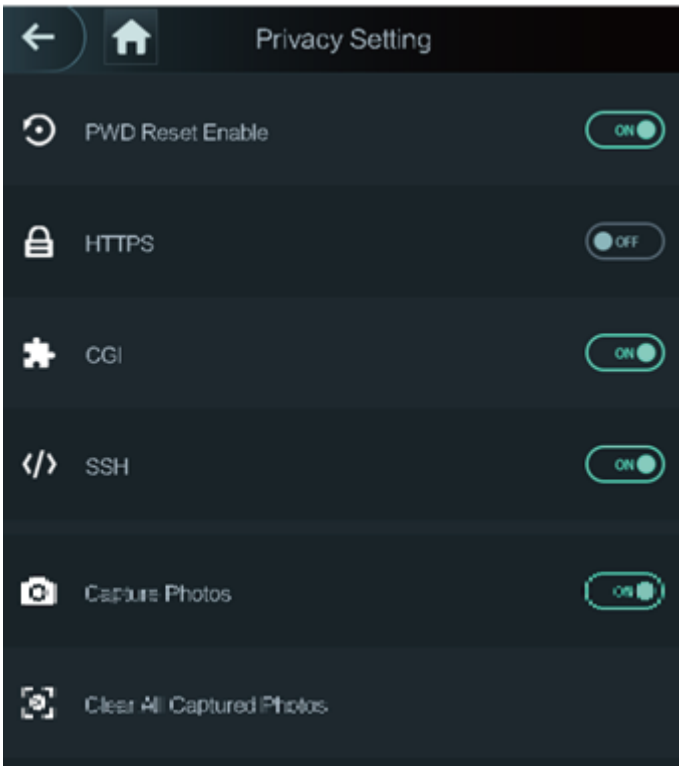


Tabla 3-11 Características

Parámetro	Descripción
Restablecimiento de PCD Habilitar	Si el**Habilitar restablecimiento de PWD**está habilitada, puede restablecer la contraseña. La función Restablecer PWD está habilitada de forma predeterminada.
HTTPS	Hypertext Transfer Protocol Secure (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 dinámicamente. 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 en una red no segura. Cuando SSH está habilitado, SSH proporciona un servicio criptográfico para la transmisión de datos.
Capturar foto	Si selecciona ON, cuando un usuario abre la puerta, la foto del usuario se tomará automáticamente. Esta función está activada de forma predeterminada.
Limpiar todo capturado fotos	Toque el icono y podrá eliminar todas las fotos capturadas.

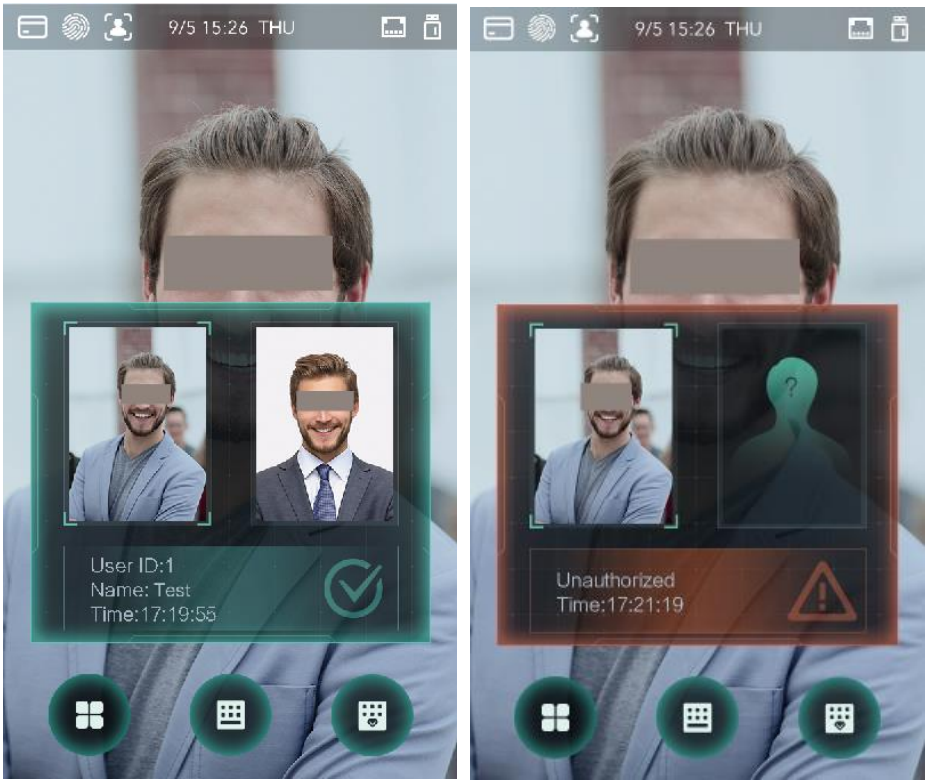
Cuando HTTPS está habilitado, la terminal se reiniciará automáticamente.

3.10.5 Comentarios sobre los resultados

Puede seleccionar un modo de retroalimentación de resultados según sea necesario.

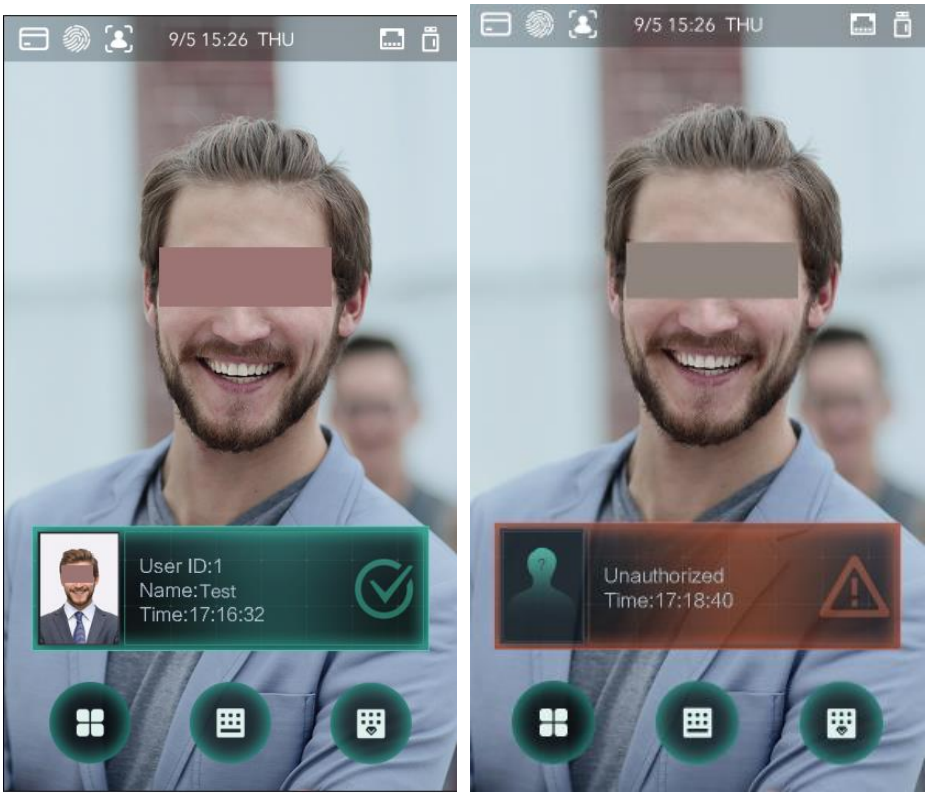
Modo 1

Figura 3-19 Modo 1



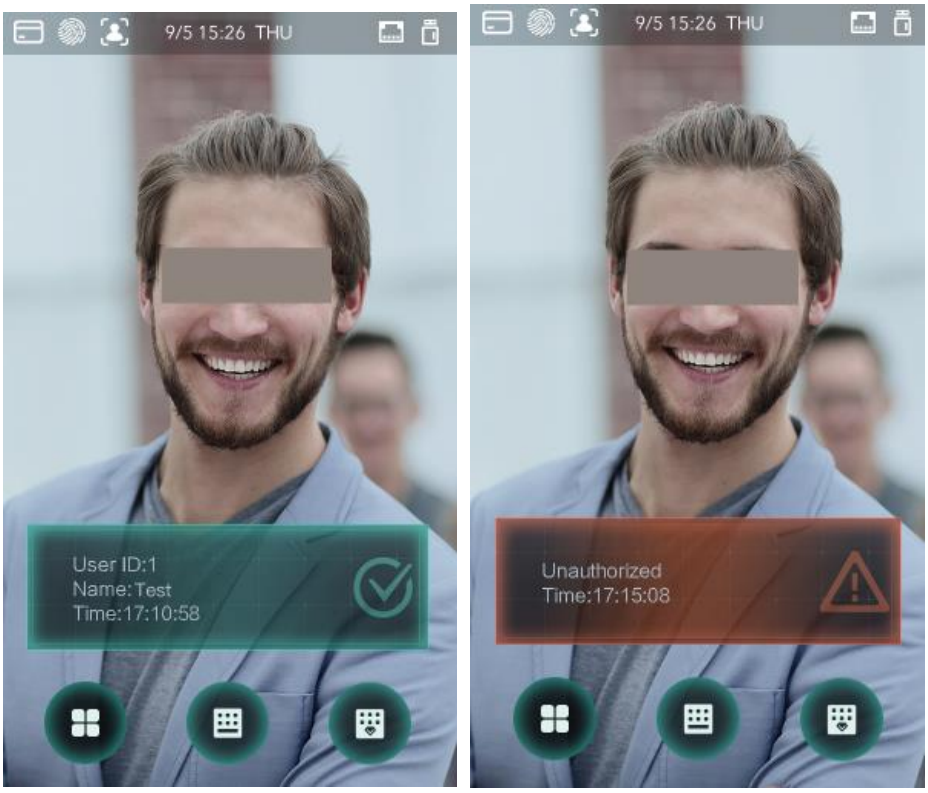
Modo 2

Figura 3-20 Modo 2



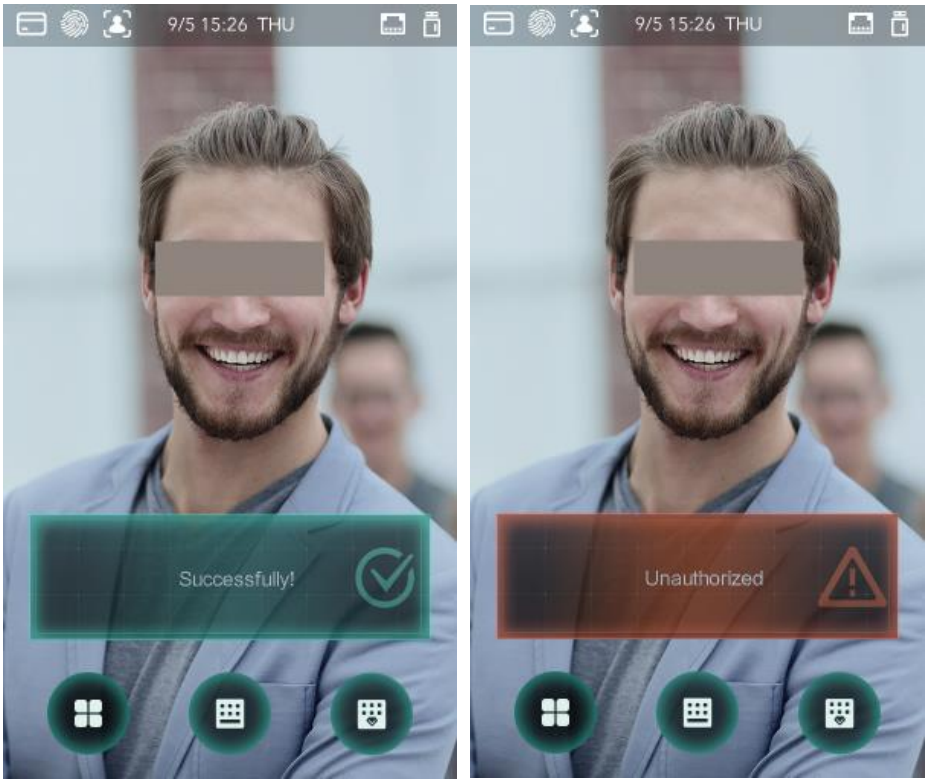
Modo 3

Figura 3-21 Modo 3



Modo 4

Figura 3-22 Modo 4



3.11 Registro

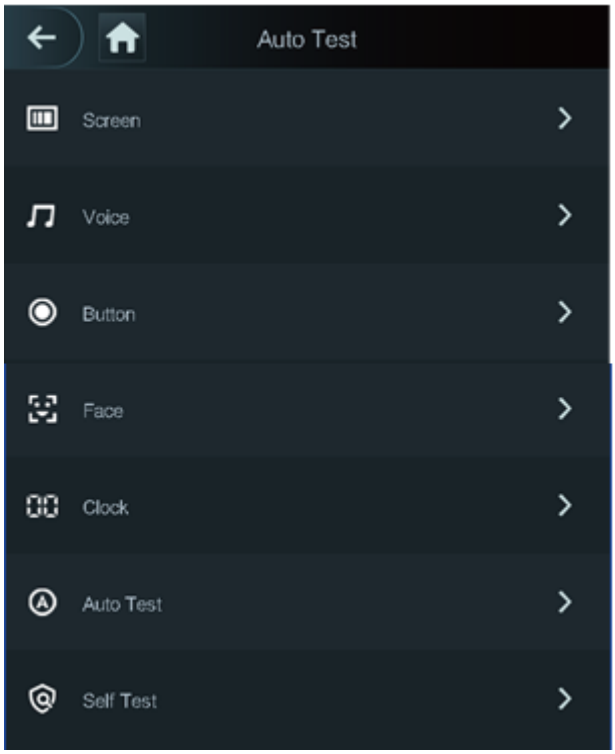
Puede consultar todos los registros de desbloqueo.

Figura 3-23 Registros de punzones de búsqueda

3.12 Prueba automática

Cuando usa el terminal por primera vez o cuando el terminal funciona mal, puede usar la función de prueba automática para verificar si el terminal puede funcionar normalmente. Realice las acciones de acuerdo con las indicaciones.

Figura 3-24 Prueba automática



cuando seleccionas**Auto prueba**, el terminal lo guiará para realizar todas las pruebas automáticas.

3.13 Información del sistema

Puede ver la capacidad de datos, la versión del dispositivo y la información del firmware del terminal en la **Información del sistema**interfaz.

4 Operación web

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

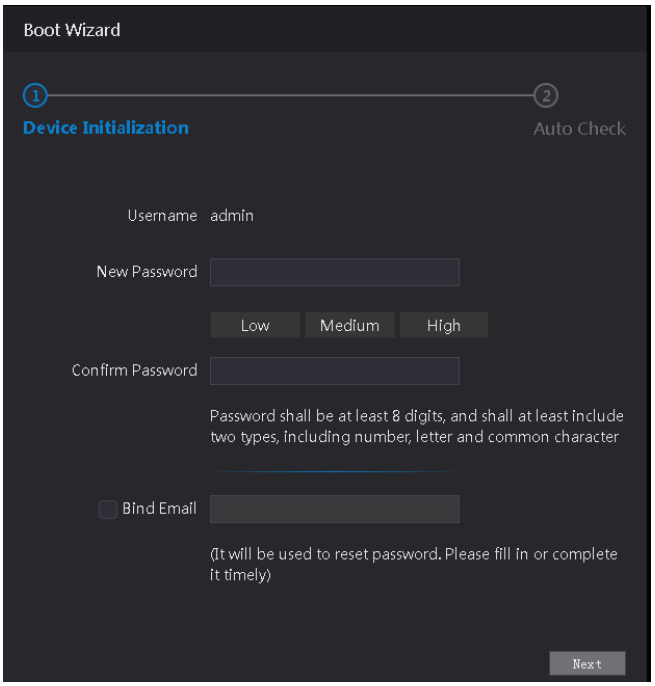
4.1 Inicialización

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 e ingrese la dirección IP (la dirección predeterminada es 192.168.1.108) del terminal en la barra de direcciones y luego presione Entrar.

los**Inicialización**se muestra la interfaz. Consulte la Figura 4-1.

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

Figura 4-1 Inicialización



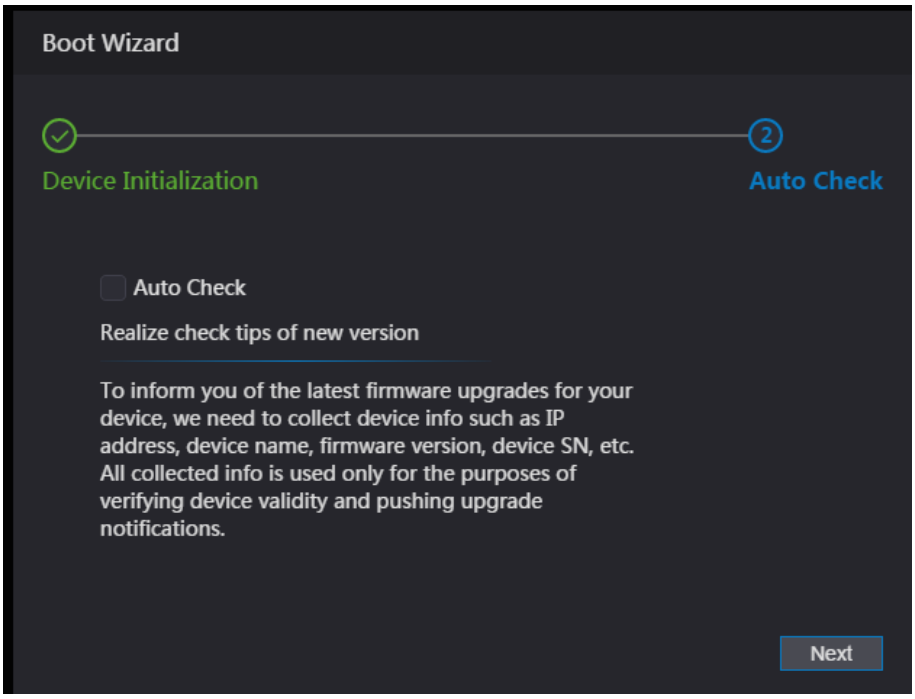
Paso 2 Ingrese la nueva contraseña, confirme la contraseña, ingrese una dirección de correo electrónico y luego toque**Próximo**.

- Por seguridad, mantenga la contraseña correctamente después de la inicialización y cambie la contraseña regularmente.
- 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 especiales carácter (excluyendo ' " ; : &). Establezca una contraseña de alto nivel de seguridad de acuerdo con 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 Hacer clic**Próximo**.

los**Verificación automática**se muestra la interfaz. Consulte la Figura 4-2.

Figura 4-2 Prueba automática



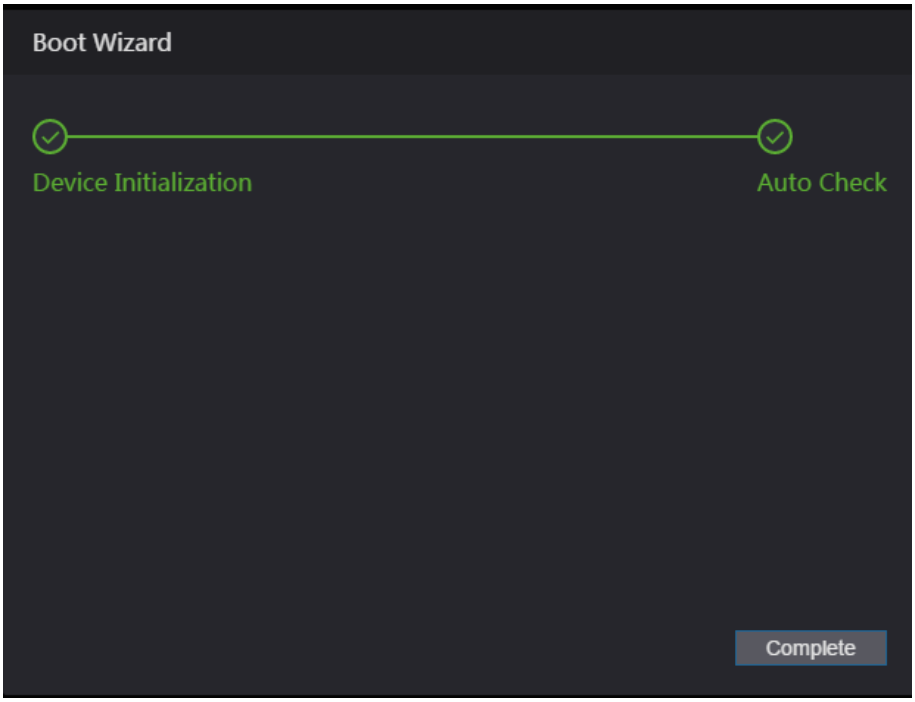
Etapa 4 Puede decidir si seleccionar**Verificación automática**O no.

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

Paso 5 Hacer clic**Próximo**.

La configuración ha terminado. Consulte la Figura 4-3.

Figura 4-3 Configuración finalizada



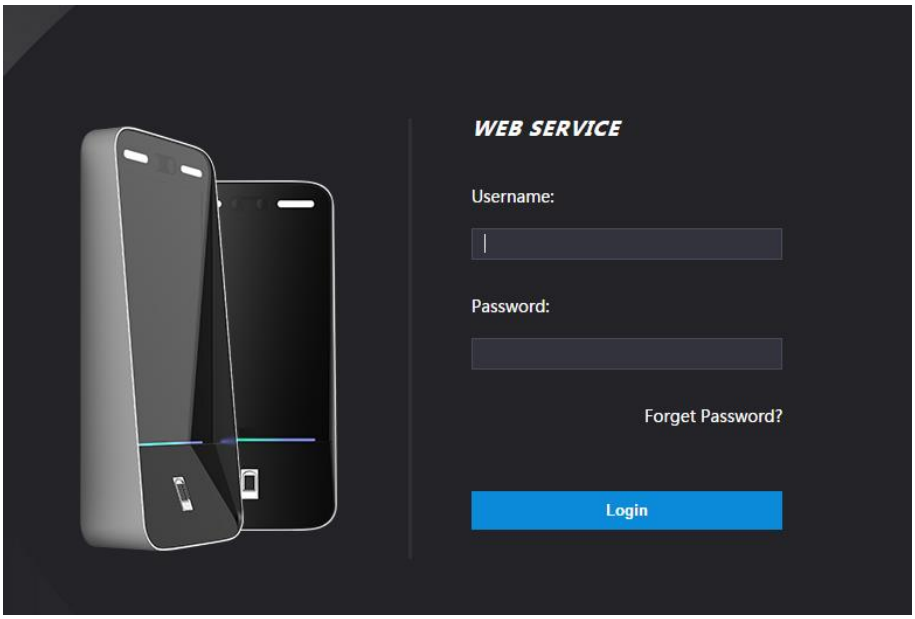
Paso 6 Hacer clic**Completo**y se completa la inicialización. Se muestra la interfaz de inicio de sesión web.

4.2 Iniciar sesión

Paso 1 Abra el navegador web IE, ingrese la dirección IP del terminal en la barra de direcciones y

presione Entrar.

Figura 4-4 Inicio de sesión



Paso 2 Introduzca 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 Terminal . Modificar el administrador regularmente y mantenerlo correctamente por motivos de seguridad.
- Si olvida la contraseña de inicio de sesión del administrador, puede hacer clic en**¿Contraseña olvidada?**para reinicialo. Ver " 4.3 Restablecer la contraseña ."

Paso 3 Hacer clic**Acceso**.

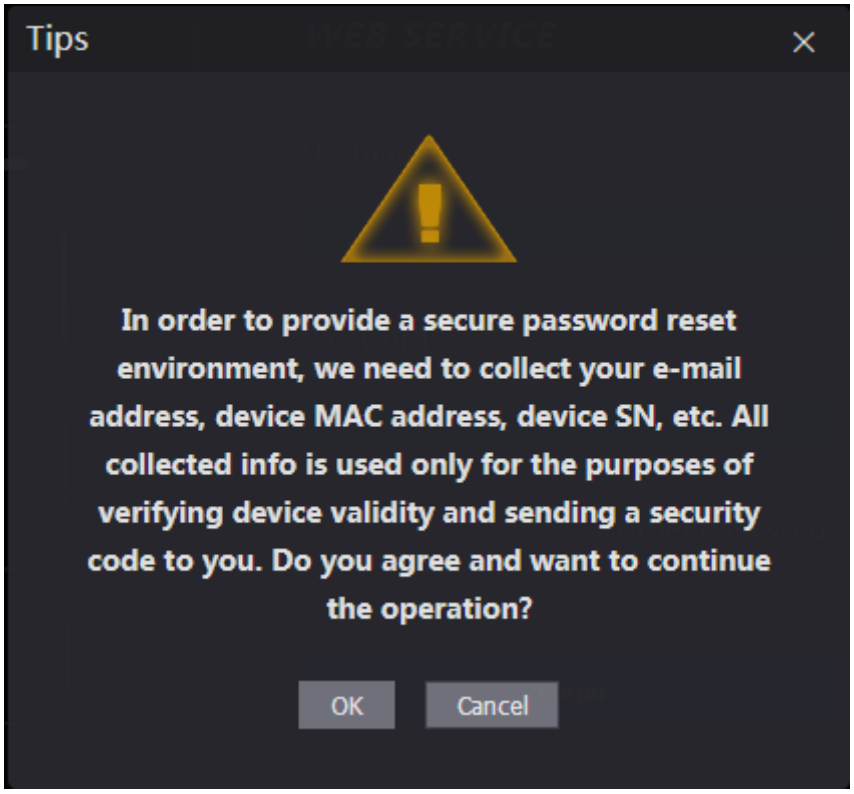
Se ha iniciado sesión en la interfaz web.

4.3 Restablecer la contraseña

Al restablecer la contraseña de la cuenta de administrador, se necesitará su dirección de correo electrónico. Paso 1

Hacer clic**¿Contraseña olvidada?**en la interfaz de inicio de sesión. los**Consejos**se muestra la interfaz.

Figura 4-5 Consejos

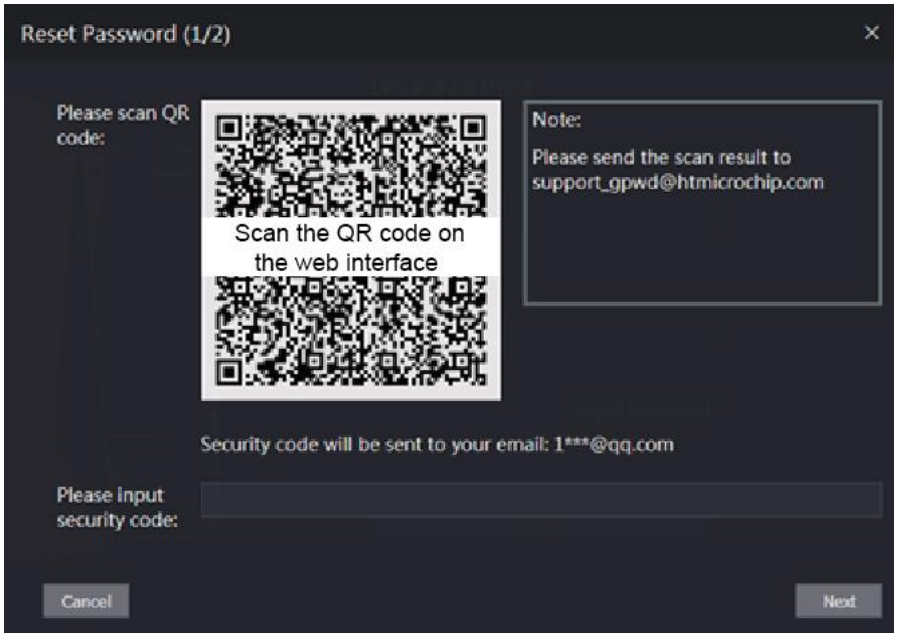


Paso 2 Lea los consejos.

Paso 3 Hacer clic**OK**.

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

Figura 4-6 Restablecer contraseña



Etapa 4 Escanee el código QR en la interfaz y obtendrá el código de seguridad.

- Como máximo se generarán dos códigos de seguridad escaneando el mismo código QR. Para obtenga más código de seguridad, actualice el código QR.
- Debe enviar el contenido que obtiene después de escanear el código QR al 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, será convertirse en inválido.
- Si se ingresan códigos de seguridad incorrectos cinco veces consecutivas, el administrador se congelará durante cinco minutos.

Paso 5 Introduzca el código de seguridad que ha recibido. Hacer clic

Paso 6 **Próximo**.

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

Paso 7 Restablece y confirma 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 8 Hacer clic**OK**, y el restablecimiento se completa.

4.4 Enlace de alarma

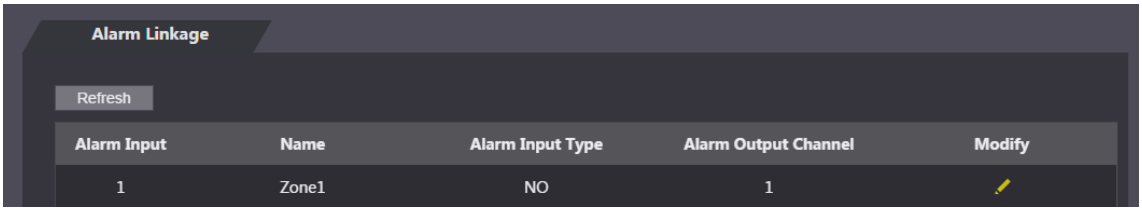
4.4.1 Configuración de enlace de alarma

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

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

los**Enlace de alarma**se muestra la interfaz. Consulte la Figura 4-7.

Figura 4-7 Enlace de alarma



Paso 2 Hacer clic , y luego puede modificar los parámetros de enlace de alarma. Consulte la Figura 4-8

Figura 4-8 Modificación del parámetro de enlace de alarma

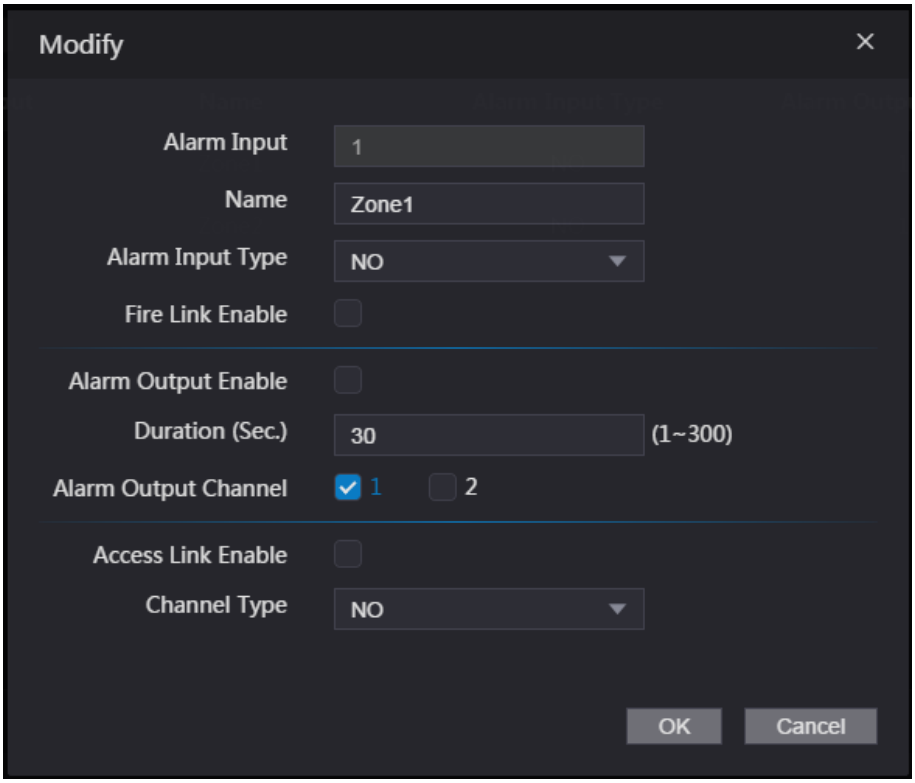


Tabla 4-1 Descripción del parámetro de enlace de alarma

Parámetro	Descripción
Entrada de alarma	No puede modificar el valor. Manténgalo predeterminado.
Nombre	Introduzca un nombre de zona.
Tipo de entrada de alarma	Hay dos opciones: NO y NC. Si el tipo de entrada de alarma del dispositivo de alarma que compró es NO, entonces debe seleccionar NO; de lo contrario, debe seleccionar NC.
Habilitar enlace de fuego	Si el enlace de incendio está habilitado, el terminal 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 por defecto si el enlace de incendio está habilitado.
Salida de alarma Habilitar	El relé puede emitir información de alarma (se enviará a la plataforma de gestión) si el**Salida de alarma**está habilitado.
Duración (seg.)	La duración de la alarma y el rango es de 1 a 300 segundos.
Salida de alarma Canal	Puede seleccionar un canal de salida de alarma según el dispositivo de alarma que haya instalado. Cada dispositivo de alarma se puede considerar como un canal.
Enlace de acceso Habilitar	Una vez habilitado el enlace de acceso, el terminal estará normalmente abierto o normalmente cerrado cuando haya señales de alarma de entrada.
Tipo de canal	Hay dos opciones: NO y NC.

Paso 3 Hacer clic**OK**y luego se completa la configuración.

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

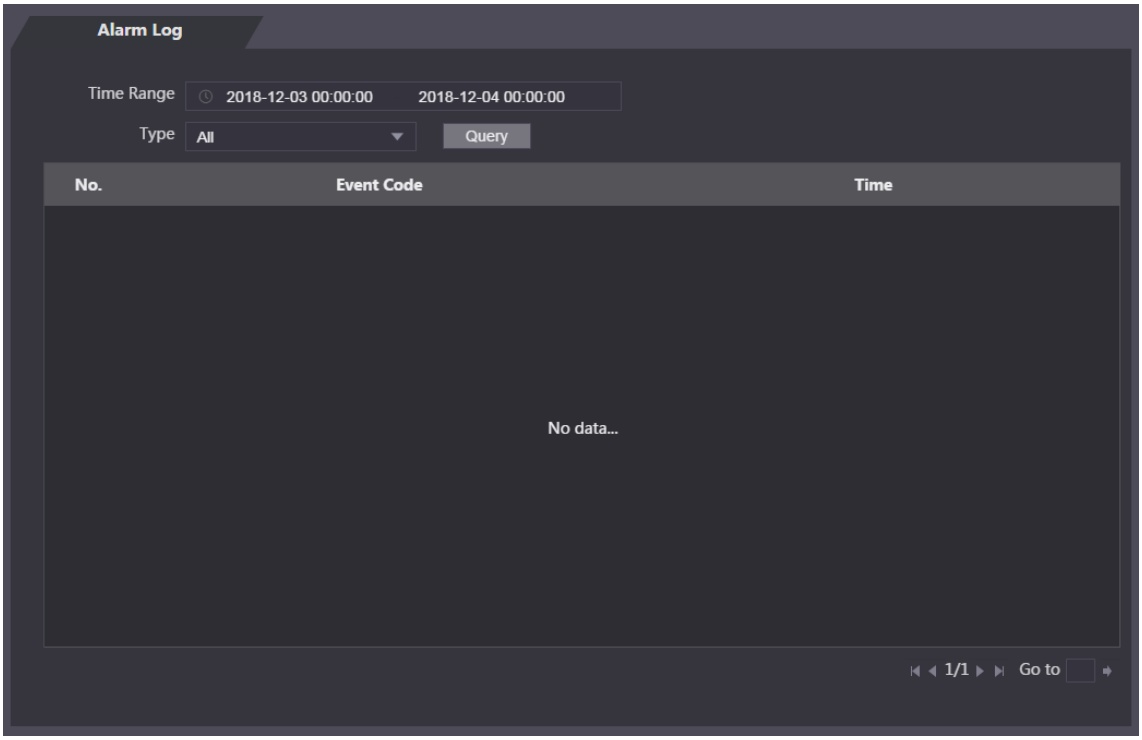
4.4.2 Registro de alarmas

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

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

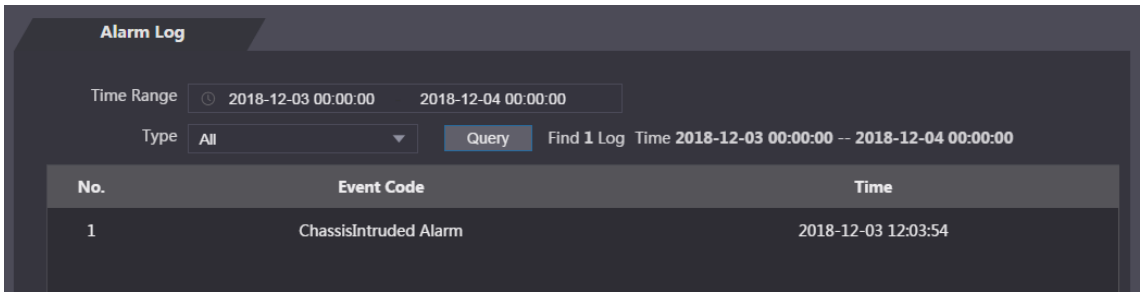
los**Registro de alarmas**se muestra la interfaz. Consulte la Figura 4-9.

Figura 4-9 Registro de alarmas



Paso 2 Seleccione un intervalo de tiempo y un tipo de alarma y, a continuación, haga clic en **Consulta**. Se muestran los resultados de la consulta. Consulte la Figura 4-10.

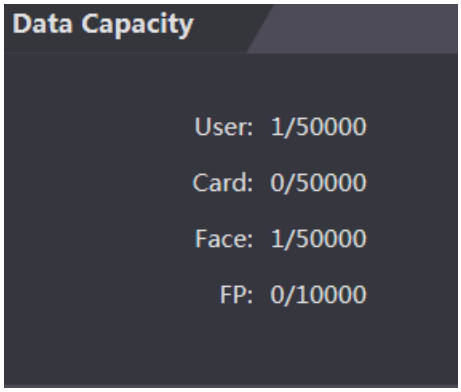
Figura 4-10 Resultados de la consulta



4.5 Capacidad de datos

Puede ver cuántos usuarios, tarjetas, imágenes de rostros y huellas dactilares puede contener el terminal en el **Capacidad de datos**interfaz.

Figura 4-11 Capacidad de datos



4.6 Configuración de vídeo

Puede configurar parámetros que incluyen velocidad de datos, parámetros de imagen (brillo, contraste, tono, saturación, etc.) y exposición en el**Configuración de vídeo**interfaz.

4.6.1 Velocidad de datos

Para obtener descripciones de la velocidad de datos, consulte la Tabla 4-2.

Figura 4-12 Velocidad de datos

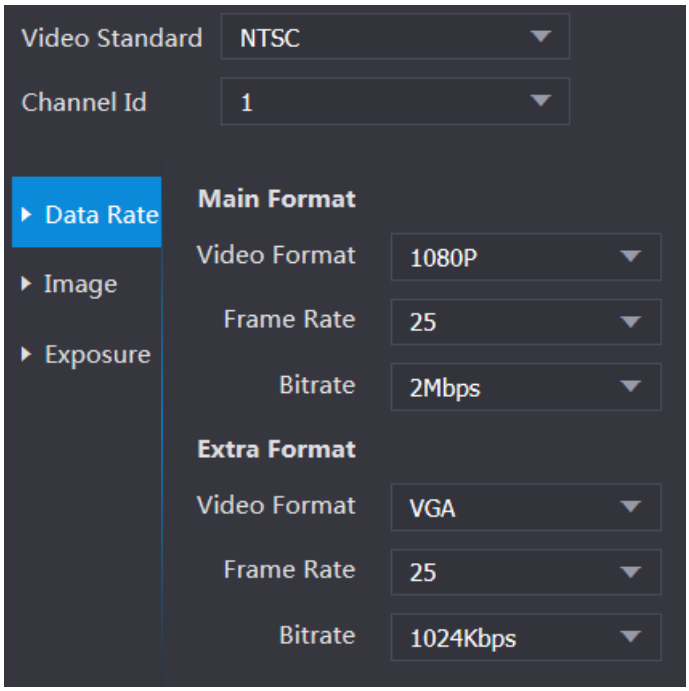


Tabla 4-2 Descripción del parámetro de velocidad de datos

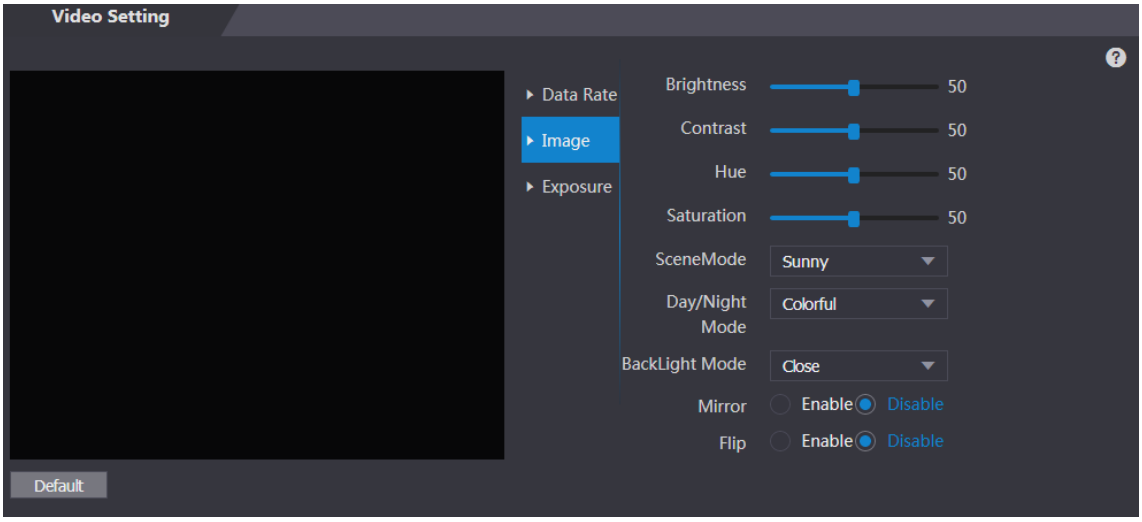
Parámetro		Descripción
Estándar de vídeo		Hay dos opciones: NTSC y PAL. Seleccione un estándar de acuerdo con el estándar de video de su región.
Canal		Hay dos opciones: 1 y 2. 1 es cámara de luz blanca y 2 es cámara de luz IR.
Principal Formato	Formato de video	Hay cuatro opciones: D1, VGA, 720p y 1080p. Seleccione una opción de acuerdo con la calidad de video que desee.

Parámetro		Descripción
	Cuadros por segundo	La velocidad a la que aparecen fotogramas consecutivos en una pantalla. los el rango de velocidad de fotogramas es de 1 a 25 fps.
	Tasa de bits	El número de bits que se transmiten o procesan por unidad de tiempo. Hay cinco opciones: 1,75 Mbps, 2 Mbps, 4 Mbps, 6 Mbps y 8 Mbps.
Extra Formato	Formato de video	Hay tres opciones: D1, VGA y QVGA.
	Cuadros por segundo	La velocidad a la que aparecen fotogramas consecutivos en una pantalla. los el rango de velocidad de fotogramas es de 1 a 25 fps.
	Tasa de bits	El número de bits que se transmiten o procesan por unidad de tiempo. Hay opciones: 256 Kbps, 320 Kbps, 384 Kbps, 448 Kbps, 512 Kbps, 640 Kbps, 768 Kbps, 896 Kbps, 1024 Kbps, 1,25 Mbps, 1,5 Mbps y 1,75 Mbps.

4.6.2 Imagen

Hay dos canales, y necesita configurar parámetros para cada canal. Paso 1 Seleccione **Configuración de video> Configuración de video> Imagen**.

Figura 4-13 Imagen



Paso 2 Seleccione**Amplia dinámica**en el modo de luz de fondo.

Tabla 4-3 Descripción del parámetro de imagen

Parámetro	Descripción
Brillo	Cuanto mayor sea el valor, más brillantes serán las imágenes.
Contraste	El contraste es la diferencia de luminancia o color que hace que un objeto sea distinguible. Cuanto mayor sea el valor de contraste, mayor será el brillo y el contraste de color.
Matiz	Cuanto mayor sea el valor, más profundo será el color.
Saturación	Cuanto mayor sea el valor, más brillantes serán los colores. El valor no cambia el brillo de la imagen.

Parámetro	Descripción
Modo escena	- Cerrar: sin modos. - Automático: el sistema ajusta automáticamente los modos de escena. - Soleado: en este modo, se reducirá el tono de la imagen. Noche: en - este modo, se aumentará el tono de la imagen. Soleado está seleccionado de forma predeterminada.
Modo Día/Noche	El modo Día/Noche decide el estado de funcionamiento de la luz de relleno. - Auto: El sistema ajusta automáticamente los modos día/noche. - Colorido: en este modo, las imágenes tienen colores. - Blanco y negro: en este modo. Las imágenes están en blanco y negro.
Modo de luz de fondo	- Cierre: Sin retroiluminación. - BLC: la compensación de contraluz corrige regiones con niveles de luz extremadamente altos o bajos para mantener un nivel de luz normal y utilizable para el objeto enfocado. - WDR: en el modo de amplio rango dinámico, el sistema atenúa las áreas brillantes y compensa las áreas oscuras para garantizar la definición de los objetos en las áreas brillantes y oscuras. Cuando los rostros humanos están en la luz de fondo, debe habilitar Wide Dynamic. - HLC: la compensación de altas luces es necesaria para compensar la sobreexposición de altas luces o fuentes de luz potentes como focos, faros, luces de porches, etc. para crear una imagen que se pueda utilizar y que no sea superada por una luz brillante.
Espejo	Cuando la función está habilitada, las imágenes se mostrarán con los lados izquierdo y derecho invertidos.
Dar la vuelta	Cuando esta función está habilitada, los videos se pueden voltear.

4.6.3 Exposición

Para ver las descripciones de los parámetros de exposición, consulte la Tabla 4-4.

Tabla 4-4 Descripción de los parámetros de exposición

Parámetro	Descripción
Contra parpadeo	- 50 Hz: cuando la frecuencia de servicio de la corriente alterna es de 50 Hz, la exposición se ajusta automáticamente para asegurarse de que no haya rayas en las imágenes. - 60 Hz: cuando la frecuencia de servicio de la corriente alterna es de 60 Hz, la exposición se ajusta automáticamente para asegurarse de que no haya rayas en las imágenes. - Exterior: Cuando**Exterior**está seleccionado, se puede cambiar el modo de exposición.

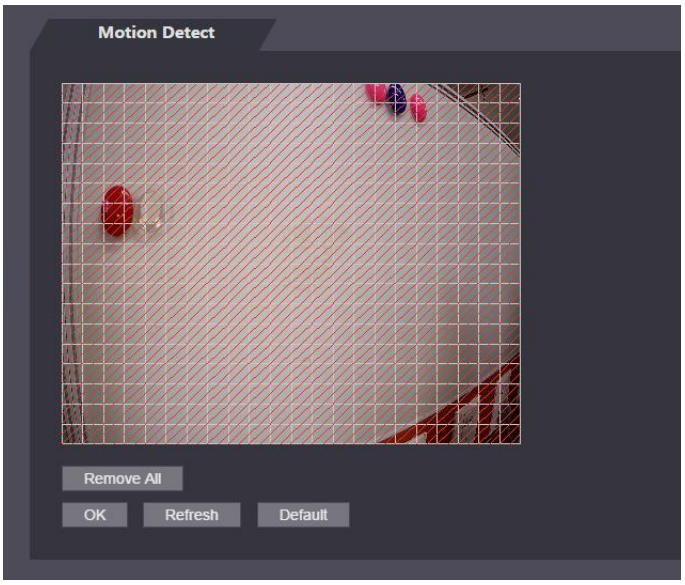
Parámetro	Descripción
Modo de exposición	- cuando seleccionas**Exterior**en el**Contra parpadeo**lista desplegable, puede seleccionar**Prioridad de obturador**como el modo de exposición. - Los modos de exposición de diferentes dispositivos pueden variar, y prevalecerá el producto real. Puede seleccionar entre: - Automático: el terminal ajustará automáticamente el brillo de las imágenes. - Prioridad de obturador: el terminal ajustará el brillo de la imagen de acuerdo con el rango de valores de exposición del obturador. Si el brillo de la imagen no es suficiente y el valor del obturador ha alcanzado el límite superior o inferior, el terminal ajustará el valor de ganancia automáticamente para obtener el brillo ideal. - Manual: puede configurar la ganancia y el valor del obturador manualmente para ajustar el brillo de la imagen.
Obturador	Cuanto mayor sea el valor del obturador y menor el tiempo de exposición, más oscuras serán las imágenes.
Valor del obturador Rango	Si selecciona**Gama personalizada**, puede personalizar el rango de valores del obturador.
Rango de valor de ganancia	Cuando se establece el rango de valores de ganancia, se mejorará la calidad del video.
Exposición Compensación	Puede aumentar el brillo del video ajustando el valor de compensación de exposición.
NR 3D	Cuando se habilita la Reducción de ruido 3D (RD), se puede reducir el ruido de video y se producirán videos de alta definición.
Calificación	Puede ajustar el valor de 3D NR cuando 3D NR está activado. Cuanto mayor sea el valor, menor será el ruido.

4.6.4 Detección de movimiento

Establezca un rango en el que se puedan detectar objetos en movimiento.

Paso 1 Seleccione**Configuración de video > Configuración de video > Detección de movimiento**. los **Detección de movimiento**se muestra la interfaz. Consulte la Figura 4-14.

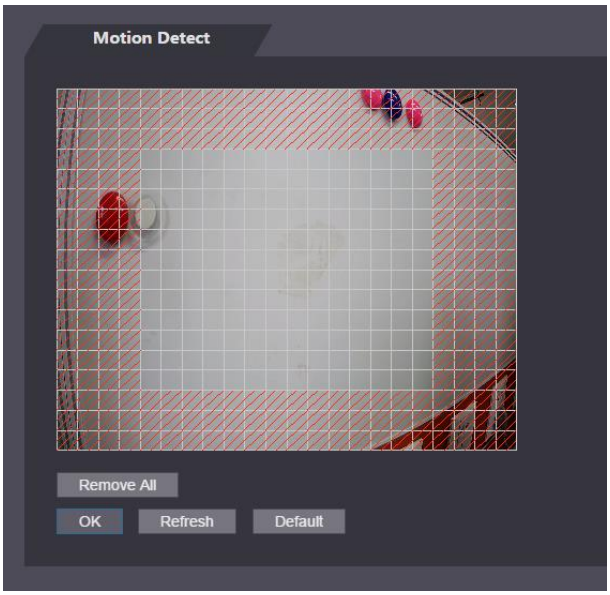
Figura 4-14 Detección de movimiento



Paso 2 Mantenga presionado el botón izquierdo del mouse y luego arrastre el mouse en el área roja. los **Detección de movimiento**se muestra el área. Consulte la Figura 4-15.

- Los rectángulos rojos son el área de detección de movimiento. El rango de detección de movimiento predeterminado son todos los rectángulos.
- Para dibujar un área de detección de movimiento, debe hacer clic en**Eliminar todo**primero.
- El área de detección de movimiento que dibuje será un área sin detección de movimiento si dibujar en el área de detección de movimiento predeterminada.

Figura 4-15 Área de detección de movimiento

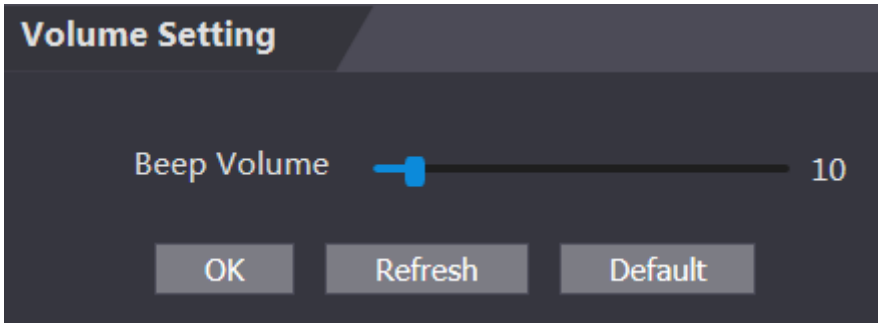


Paso 3 Hacer clic**OK**para terminar el ajuste.

4.6.5 Configuración de volumen

Puede ajustar el volumen del altavoz del terminal.

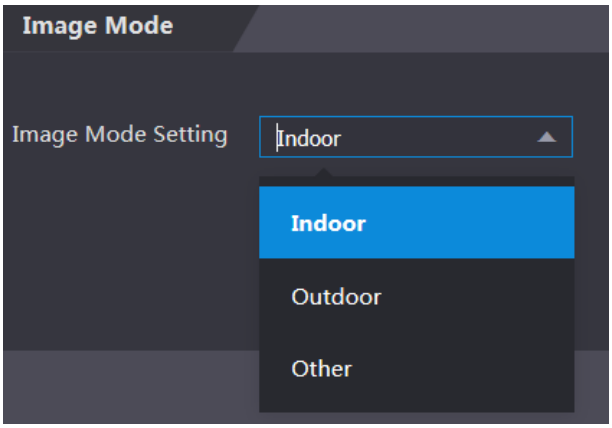
Figura 4-16 Ajuste de volumen



4.6.6 Modo de imagen

Hay tres opciones: interior, exterior y otros. Seleccione**Interior**cuando el terminal se instala en interiores; Seleccione**Exterior**cuando el terminal se instala al aire libre; y seleccione**Otro**cuando la terminal se instala en lugares con retroiluminación como corredores y pasillos.

Figura 4-17 Modo de imagen



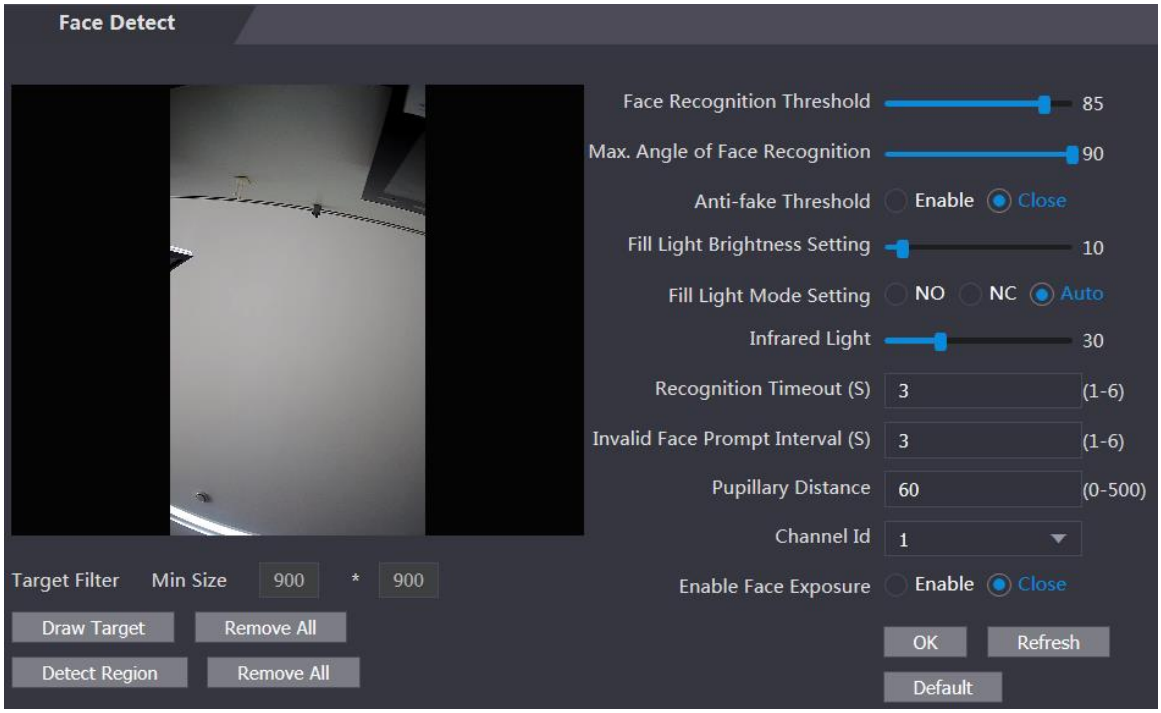
4.7 Detección de rostros

Puede configurar parámetros relacionados con el rostro humano en esta interfaz para aumentar la precisión del reconocimiento facial.

Paso 1 Seleccione**Detección de rostro**.

los**Detección de rostro**se muestra la interfaz. Consulte la Figura 4-18.

Figura 4-18 Detección de rostros



Paso 2 Configurar parámetros. Consulte la Tabla 4-5.

Tabla 4-5 Descripción del parámetro de detección de rostros

Parámetro	Descripción
Rostro Reconocimiento Límite	Cuanto mayor sea el valor, mayor será la precisión.
máx. Ángulo de reconocimiento facial	Cuanto mayor sea el ángulo, se reconocerá una gama más amplia de perfiles.
Umbral anti-falsificación	Esta función evita que las personas se desbloqueen mediante imágenes de rostros humanos o modelos de rostros humanos. Cuanto mayor sea el valor, más difíciles serán las imágenes de rostros o los modelos de rostros humanos que pueden abrir la puerta.
Brillo de luz de relleno Ajuste	Puede configurar el brillo de la luz de relleno.
Ajuste del modo de luz de relleno	Hay tres modos de luz de relleno. - NO: La luz de llenado normalmente está abierta. - NC: La luz de llenado normalmente está cerrada. - Automático: la luz de relleno se encenderá automáticamente cuando se active un evento de detección de movimiento. Cuándo**Auto**está seleccionado, la luz de relleno no estará encendida incluso si el valor de la luz infrarroja es superior a 19.
Luz infrarroja	Ajuste el brillo IR arrastrando la barra de desplazamiento.
Tiempo de espera de reconocimiento	Cuando una persona que no tiene la autoridad de acceso se para frente a la terminal y se le reconoce el rostro, el controlador indicará que el reconocimiento de rostro falló. El intervalo de solicitud se denomina tiempo de espera de reconocimiento.
Indicación de cara no válida Intervalo	Cuando una cara que no tiene autoridad de acceso se para frente a la terminal, el controlador indicará que la cara no es válida. El intervalo rápido

Parámetro	Descripción
	es un intervalo de solicitud de cara no válido.
Distancia pupilar	La distancia pupilar es el valor de píxel de la imagen entre los centros de las pupilas de cada ojo. Debe establecer un valor apropiado para que el controlador de acceso pueda reconocer las caras según sea necesario. El valor cambia según el tamaño de la cara y la distancia entre las caras y la lente. Cuanto más cerca esté la cara de la lente, mayor debe ser el valor. Si un adulto está a 1,5 metros de la lente, el valor de la distancia pupilar puede estar entre 50 y 70.
Habilitar exposición facial	Después de habilitar la exposición de la cara, la cara humana será más clara cuando la terminal se instale al aire libre.
Canal ID	Hay dos opciones: 1 y 2. 1 es cámara de luz blanca y 2 es cámara de luz IR.
Dibujar objetivo	Hacer clic**Dibujar objetivo**, y luego puede dibujar el marco mínimo de detección de rostros. Hacer clic**Eliminar todo**y puede eliminar todos los marcos que dibujó.
Detectar región	Hacer clic**Detectar región**, mueva el mouse y podrá ajustar la región de detección de rostros. Hacer clic**Eliminar todo**y puede eliminar todas las regiones de detección.

Paso 3 Hacer clic**OK**para terminar el ajuste.

4.8 Configuración de red

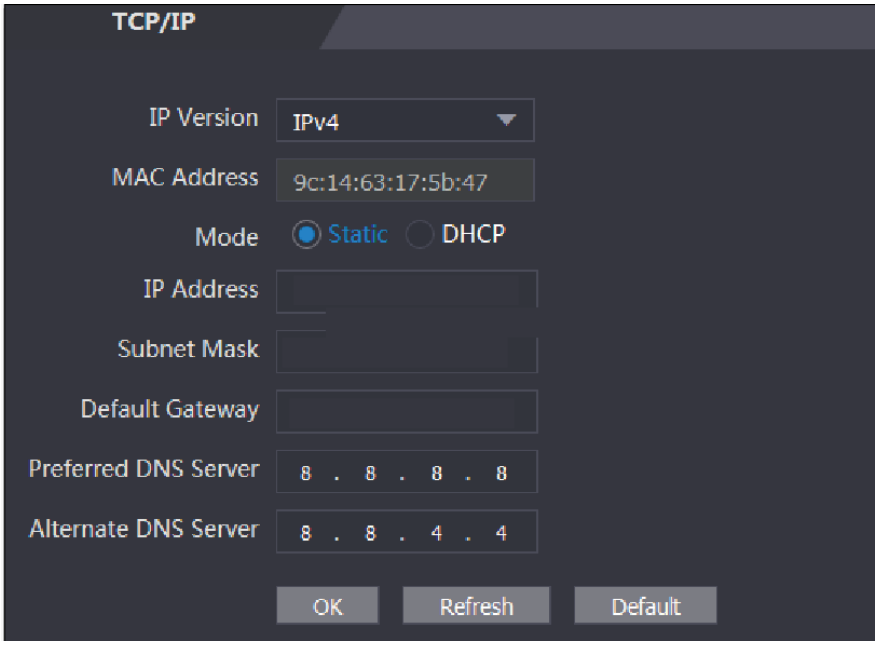
4.8.1 TCP/IP

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

Condición previa

Asegúrese de que el terminal esté conectado a la red correctamente. Paso 1
Seleccione**Configuración de red > TCP/IP**.

Figura 4-19 TCP/IP



Paso 2 Configurar parámetros.

Tabla 4-6 TCP/IP

Parámetro	Descripción
Versión IP	Hay una opción: IPv4.
MAC	dirección MAC de la**Terminal**se visualiza.
Modo	- Estático Establezca la dirección IP, la máscara de subred y la dirección de la puerta de enlace manualmente. - DHCP - Después de habilitar 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 cero. - Si desea ver la IP predeterminada cuando DHCP está activo, deshabilite DHCP.
Enlace local habla a	La dirección de enlace local solo está disponible cuando se selecciona IPv6 en la versión IP. Se asignarán direcciones locales de enlace únicas al controlador de interfaz de red en cada red de área local para permitir las comunicaciones. La dirección de enlace local no se puede modificar.
Dirección IP	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.
Máscara de subred	
Puerta	
Privilegiado DNS Servidor	Configure la dirección IP del servidor DNS preferido.
Alterno DNS Servidor	Establezca la dirección IP del servidor DNS alternativo.

Paso 3 Hacer clic**OK**para completar el ajuste.

4.8.2 Puerto

Establezca las conexiones máximas de clientes a los que se puede conectar el terminal y los números de puerto.

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

. los**Puerto**se muestra la interfaz.

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

Excepto conexión máxima, es necesario reiniciar el terminal para realizar la configuración efectivo después de modificar los valores.

Tabla 4-7 Descripción del puerto

Parámetro	Descripción
máx. conexión	Puede establecer las conexiones máximas de clientes a las que se puede conectar el terminal. Los clientes de la plataforma como Smartpss no se cuentan.
Puerto TCP	El valor 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.
Puerto HTTPS	El valor predeterminado es 443.
Puerto RTSP	El valor predeterminado es 554.

Paso 3 Hacer clic**OK**para completar el ajuste.

4.8.3 Registro

Cuando se conecta a una red externa, la terminal informará su dirección al servidor designado por el usuario para que los clientes puedan acceder a la terminal.

Paso 1 Seleccione**Configuración de red > Registro automático**.

los**Registro automático**se muestra la interfaz.

Paso 2 Seleccione**Habilitar**e ingrese la IP del host, el puerto y la ID del subdispositivo.

Tabla 4-8 Descripción del registro automático

Parámetro	Descripción
IP del anfitrión	Dirección IP del servidor o nombre de dominio del servidor.
Puerto	Puerto del servidor utilizado para el registro automático.
ID de dispositivo secundario	ID de terminal asignado por el servidor.

Paso 3 Hacer clic**OK**para completar el ajuste.

4.8.4 P2P

La computación o redes punto a punto 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 que se pueda administrar más de una terminal en el

aplicación movil. 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 terminal a una red externa; de lo contrario la terminal No puede ser usado.

Figura 4-20 P2P

Paso 1 Seleccione**Configuración de red > P2P**. los**P2P** se muestra la interfaz. Seleccione**Habilitar**para

Paso 2 habilitar la función P2P. Hacer clic**OK**para

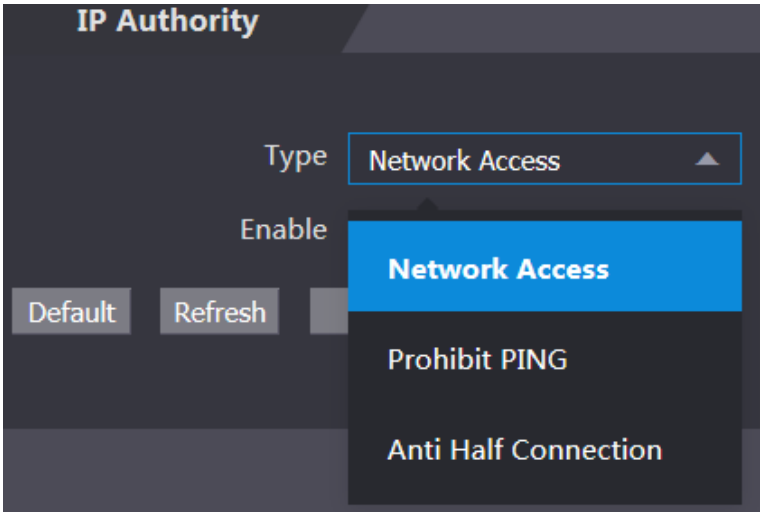
Paso 3 completar el ajuste.

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

4.9 Gestión de la seguridad

4.9.1 Autoridad de PI

Figura 4-21 Autoridad IP



Seleccione un modo de seguridad cibernética según sea necesario.

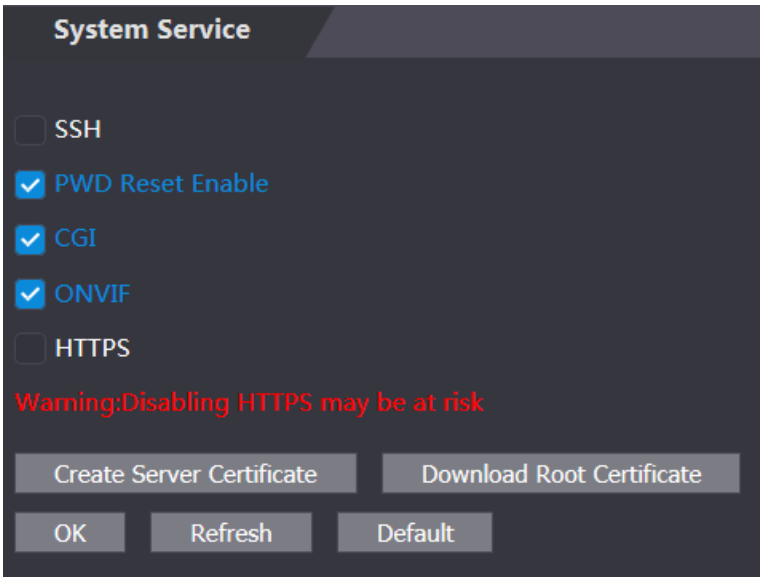
4.9.2 Sistemas

4.9.2.1 Servicio del sistema

Hay cuatro opciones: SSH, PWD Reset Enable, CGI y HTTPS. Consulte "3.10.4 Funciones" para seleccionar una o más de ellas.

La configuración del servicio del sistema realizada en la página web y la configuración en el**Características** La interfaz del terminal se sincronizará.

Figura 4-22 Servicio del sistema



4.9.2.2 Crear certificado de servidor

Hacer clic**Crear certificado de servidor**, ingrese la información necesaria, haga clic en**Salvar**, y luego la terminal se reiniciará.

4.9.2.3 Descargar certificado raíz

Paso 1 Hacer clic**Descargar certificado raíz**.

Seleccione una ruta para guardar el certificado en el**Guardar el archivo**caja de diálogo.

Paso 2 Haga doble clic**Certificado Raíz**que ha descargado para instalar el certificado. Instale el certificado siguiendo las instrucciones en pantalla.

4.9.3 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.

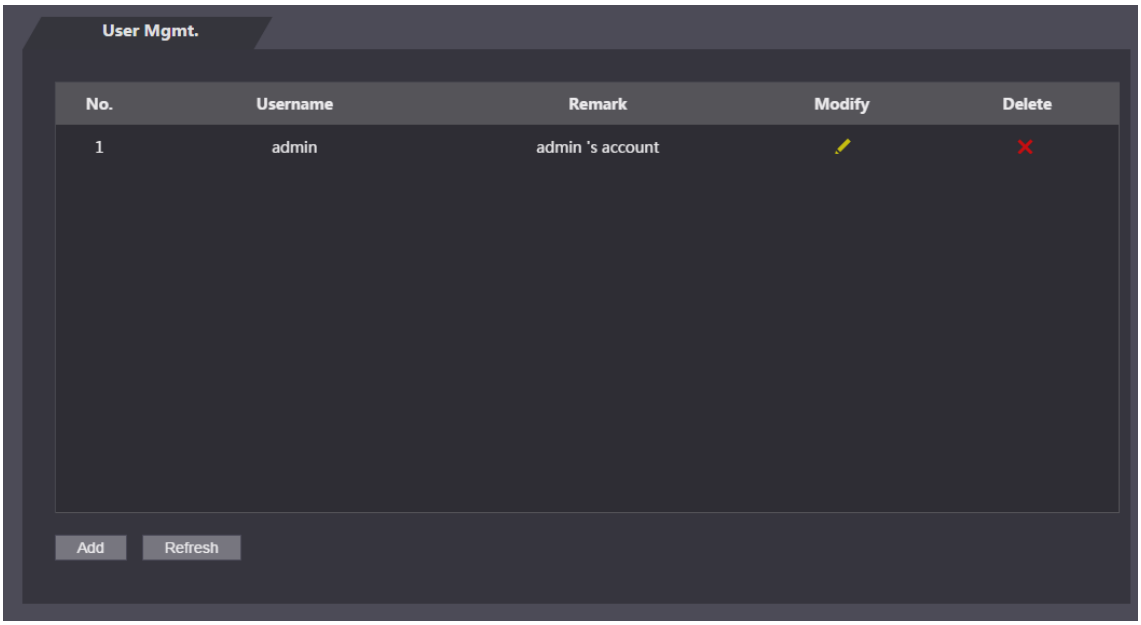
4.9.3.1 Agregar usuarios

Hacer clic**Agregar**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**OK**para completar la adición del usuario.

4.9.3.2 Modificar la información del usuario

Puede modificar la información del usuario haciendo clic en sobre el**Gestión de usuarios**interfaz. Consulte la Figura 4-23.

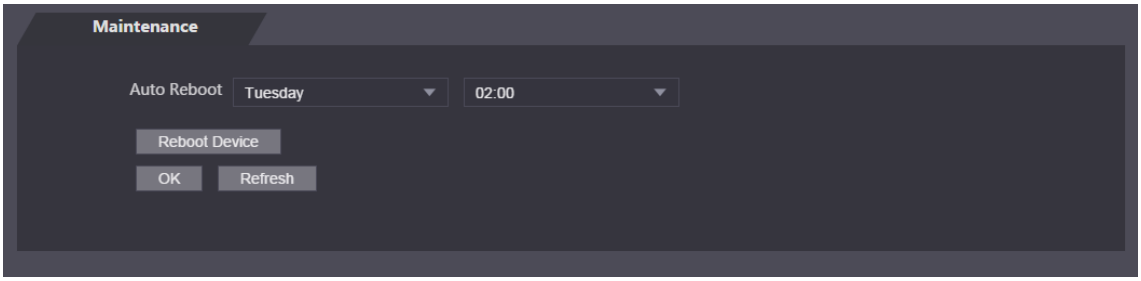
Figura 4-23 Gestión de usuarios



4.9.4 Mantenimiento

Puede hacer que el terminal se reinicie en tiempo de inactividad para mejorar la velocidad de ejecución del terminal. Consulte la Figura 4-24.

Figura 4-24 Mantenimiento

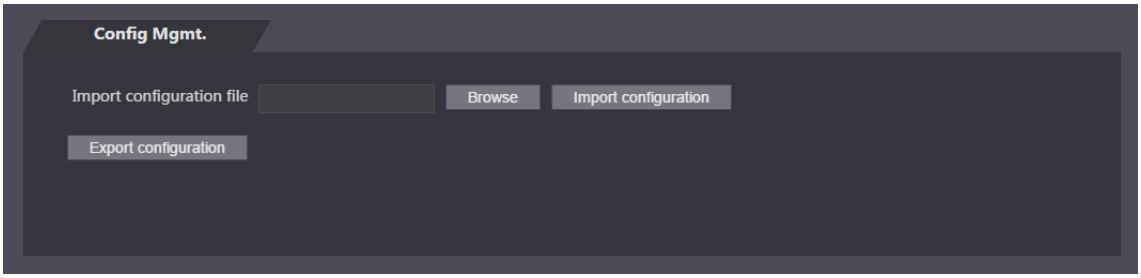


Seleccione la fecha y la hora de reinicio automático. La hora de reinicio predeterminada es a las 2 en punto de la mañana en Martes. Hacer clic**Reiniciar dispositivo**, el terminal se reiniciará inmediatamente. Hacer clic**OK**, la terminal reiniciar a las 2 en punto de la mañana todos los martes.

4.9.5 Gestión de la configuración

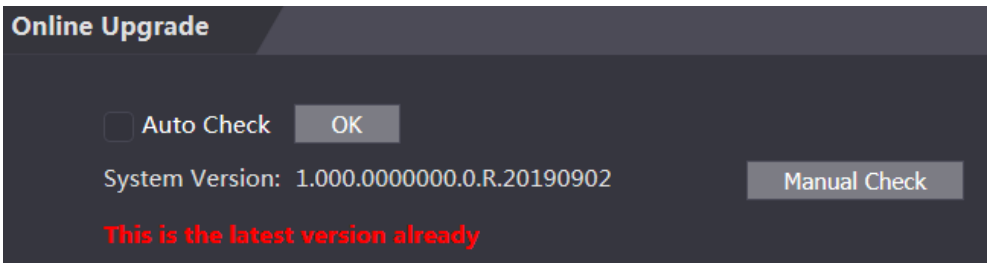
Cuando más de un terminal necesita la misma configuración, puede configurar sus parámetros importando o exportando archivos de configuración. Consulte la Figura 4-25.

Figura 4-25 Gestión de la configuración



4.9.6 Actualizar

Puedes elegir**Verificación automática**para actualizar el sistema automáticamente. También puede seleccionar**Comprobación manual**para actualizar el sistema manualmente.



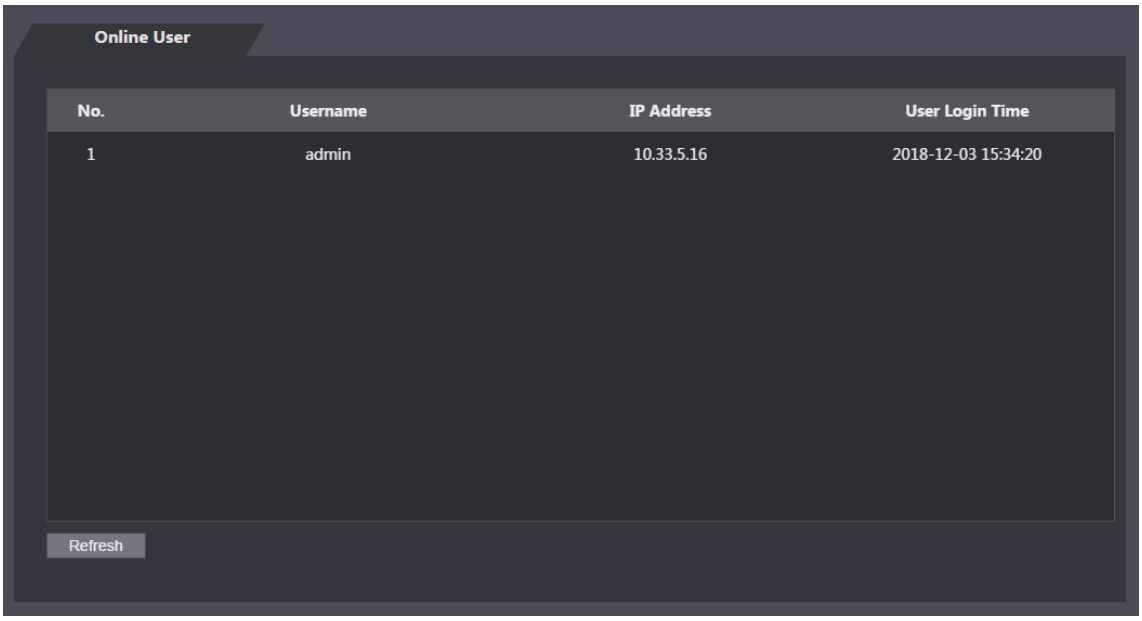
4.9.7 Información de la versión

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

4.9.8 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. Consulte la Figura 4-26.

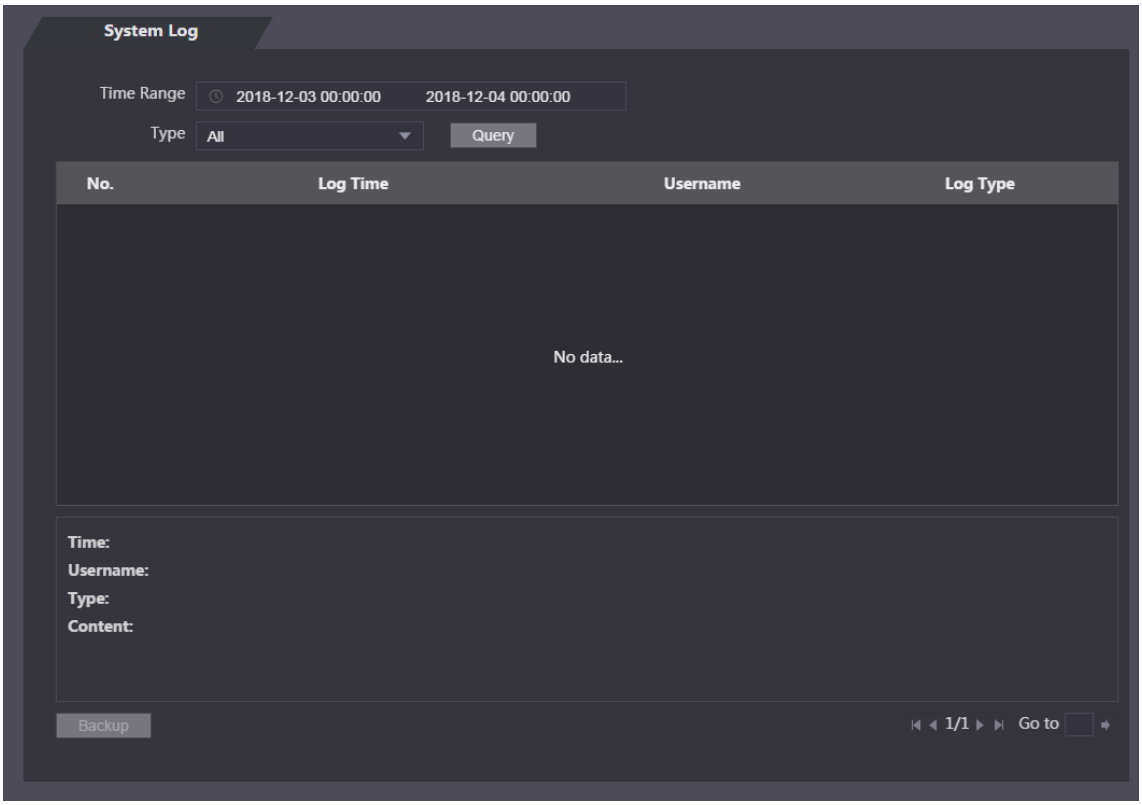
Figura 4-26 Usuario en línea



4.10 Registro del sistema

Puede ver y hacer una copia de seguridad del registro del sistema en el**Registro del sistema**interfaz. Consulte la Figura 4-27.

Figura 4-27 Registro del sistema



4.10.1 Registros de consultas

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

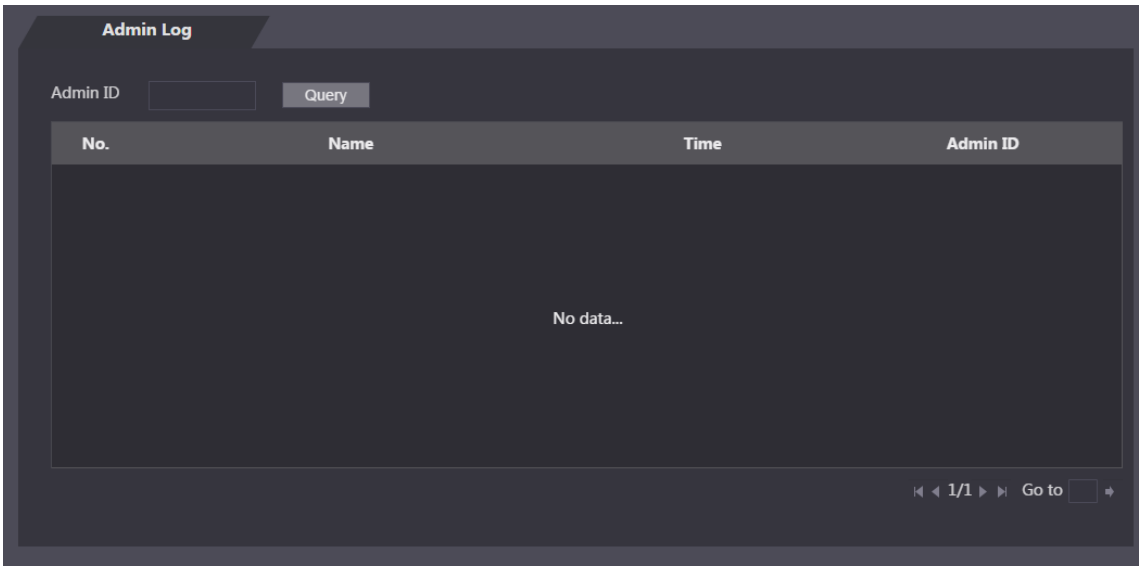
4.10.2 Registros de copia de seguridad

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

4.11 Registro de administración

Ingrese la identificación del administrador en el**Registro de administración**interfaz, haga clic**Consulta**, y luego verá los registros de operaciones del administrador. Consulte la Figura 4-28.

Figura 4-28 Registro de administración



Pase el cursor del mouse sobre , y luego puede ver información detallada de la actual usuario.

4.12 Salir

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

5 Configuración de SmartPSS

Puede realizar la configuración de permisos de acceso a una sola puerta o grupos de puertas a través del cliente Smart PSS. Para configuraciones detalladas, consulte el manual de usuario de SmartPSS.

Las interfaces de Smart PSS pueden variar según las versiones y prevalecerá la interfaz real.

5.1 Iniciar sesión

Instale Smart PSS (el nombre de usuario es admin y la contraseña es admin123 de forma predeterminada), haga doble clic  para operarlo. Siga las instrucciones para finalizar la inicialización e iniciar sesión.

5.2 Agregar dispositivos

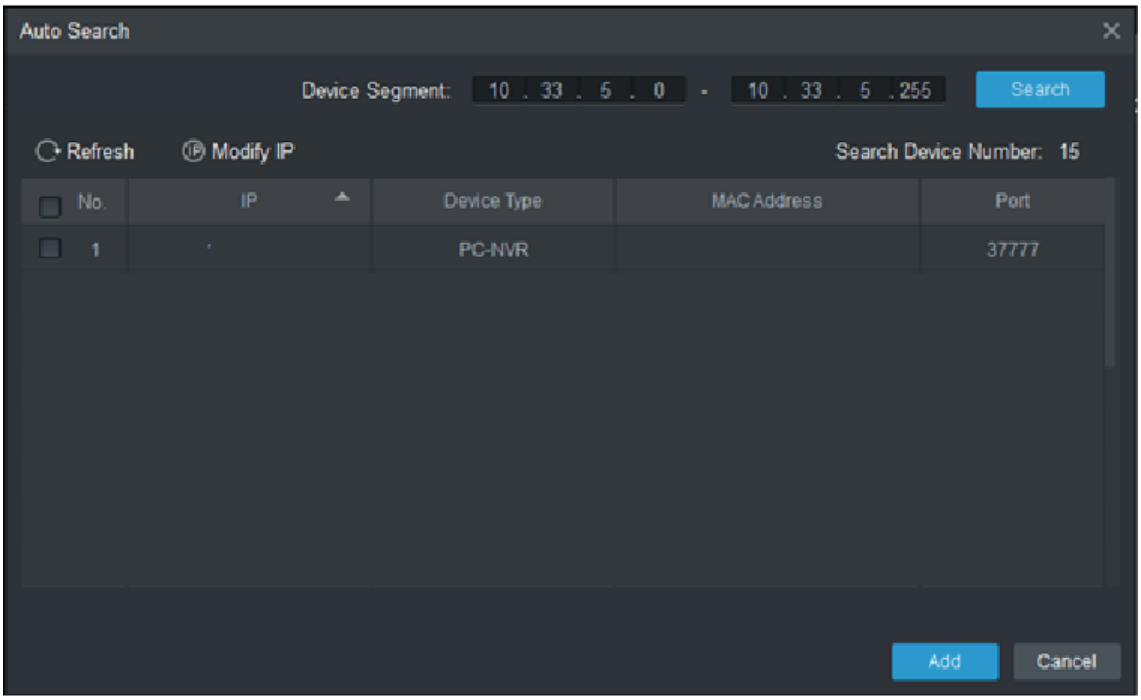
Debe agregar terminales al Smart PSS. Puedes hacer clic**Auto búsqueda**para agregar y hacer clic**Agregar** para agregar manualmente.

5.2.1 Búsqueda automática

Puede buscar y agregar terminales en el mismo segmento de red al SmartPSS. Consulte la Figura 5-1 y la Figura 5-2.

Figura 5-1 Dispositivos

Figura 5-2 Búsqueda automática



Paso 1 Hacer clic**Auto búsqueda**, ingrese el segmento de red y luego haga clic en**Búsqueda**. Se mostrará una lista.

Paso 2 Seleccione los terminales que desea agregar al Smart PSS y luego haga clic en**Agregar**, los **Información Entrar**se mostrará el cuadro de diálogo.

Paso 3 Ingrese el nombre de usuario y la contraseña de inicio de sesión para iniciar sesión.

Puede ver el terminal añadido en la**Dispositivos**interfaz.

Seleccione un terminal, haga clic en**Modificar IP**, y puede modificar la dirección IP del terminal. Para detalles sobre la modificación de la dirección IP, consulte el manual de usuario de Smart PSS.

5.2.2 Adición manual

Debe conocer las direcciones IP y los nombres de dominio de los terminales que desea agregar. Consulte la Figura 5-3 y la Figura 5-4.

Figura 5-3 Dispositivos

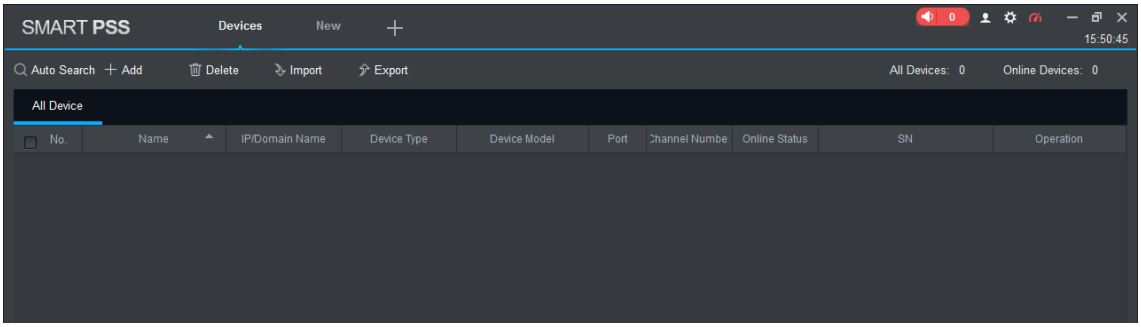
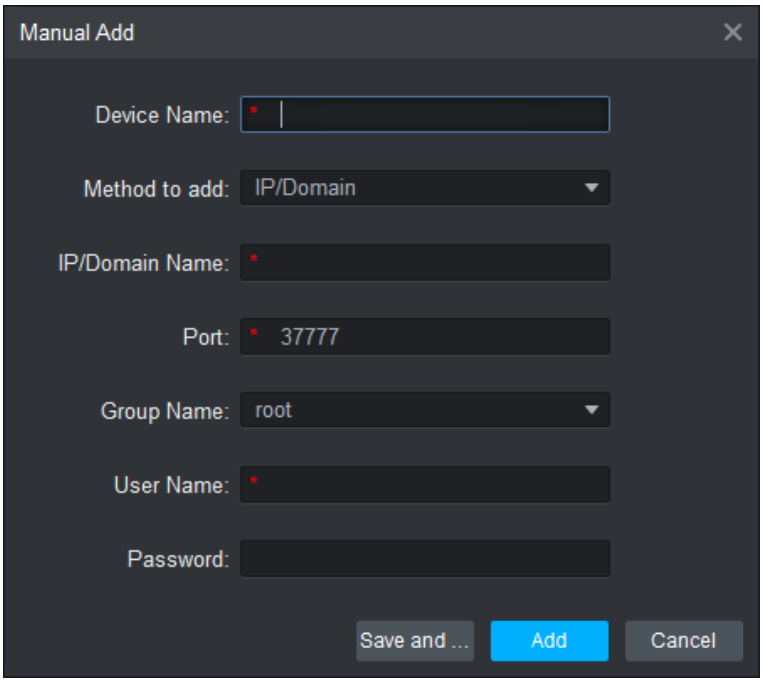


Figura 5-4 Adición manual



Paso 1 Hacer clic**Agregar**sobre el**Dispositivos**interfaz, y la**Adición manual**se mostrará la interfaz. Introducir el

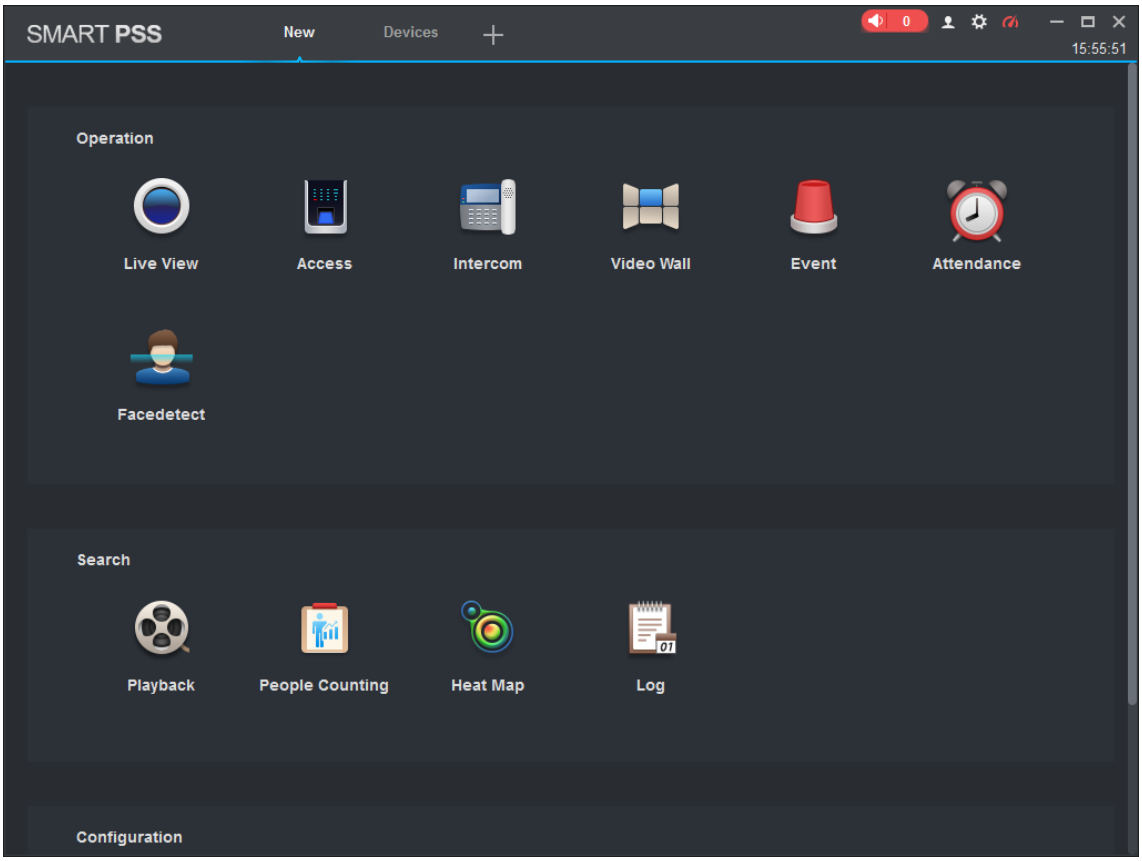
Paso 2 **Nombre del dispositivo**, seleccione un método para agregar, ingrese el**IP/Nombre de Dominio**,**Número de puerto**(37777 por defecto),**Nombre del grupo**,**Nombre de usuario**, y**Clave**. Hacer clic**Agregar**, y luego

Paso 3 puede ver el terminal agregado en el**Dispositivos**interfaz.

5.3 Adición de usuarios

Los usuarios están vinculados con tarjetas. Después de haber agregado usuarios al Smart PSS, puede configurar los permisos de acceso de los usuarios en el**Nuevo > Acceso**. Consulte la Figura 5-5.

Figura 5-5 Nuevo



5.3.1 Selección del tipo de tarjeta

Los tipos de tarjeta deben ser los mismos que los tipos de emisor de la tarjeta; de lo contrario, los números de tarjeta no se pueden leer.

Sobre el**Acceso**interfaz, haga clic  , luego haga clic en el icono de la tarjeta IC o ID, y luego seleccione una tarjeta escribe. Hay dos opciones: tarjeta de identificación y tarjeta IC. Consulte la Figura 5-6 y la Figura 5-7.

Figura 5-6 Acceso

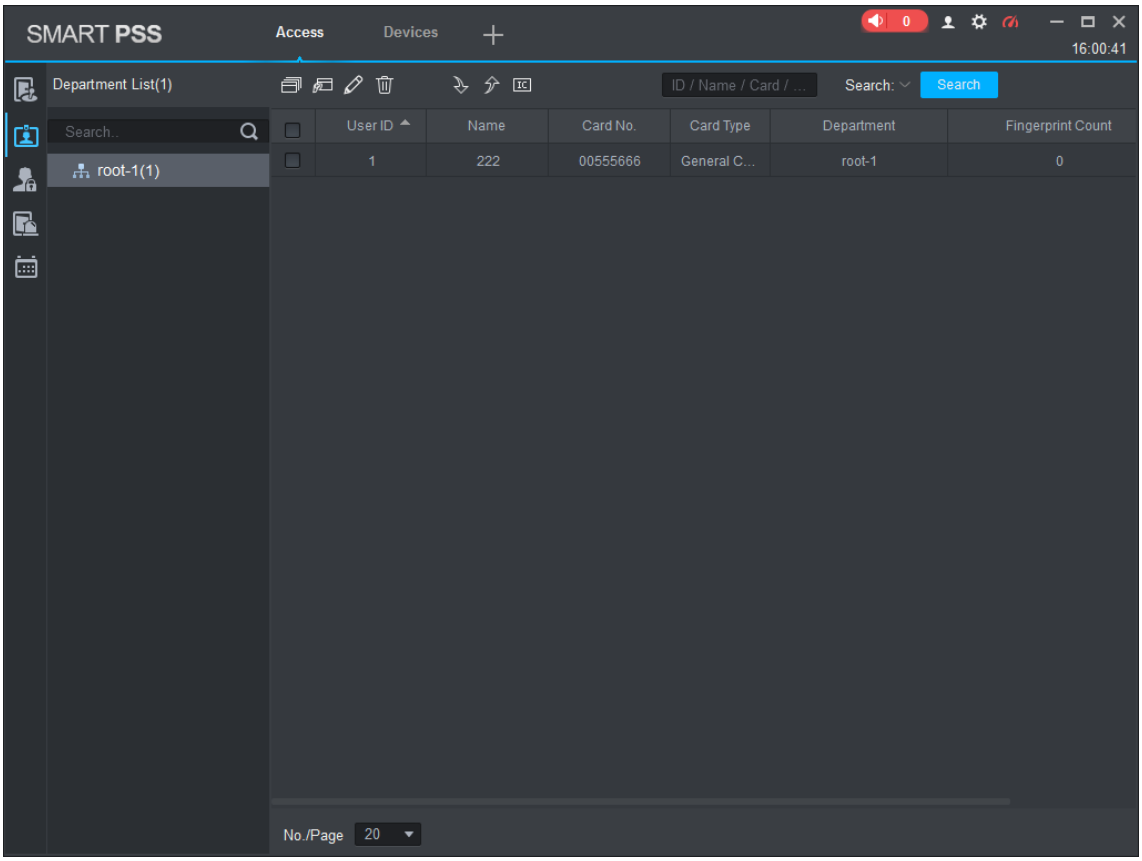
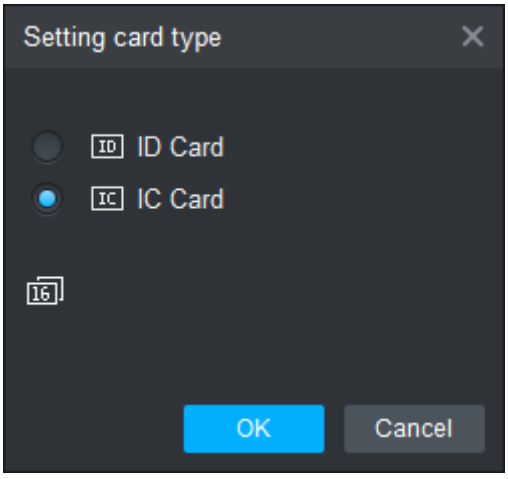


Figura 5-7 Configuración del tipo de tarjeta



5.3.2 Adición de un usuario

Puede agregar usuarios uno por uno.

Sobre el**Acceso**interfaz, haga clic  , luego haga clic  y luego ingrese la información del usuario. Hacer clic **Finalizar**para completar la adición del usuario. Consulte la Figura 5-8 y la Figura 5-9.

Figura 5-8 Acceso

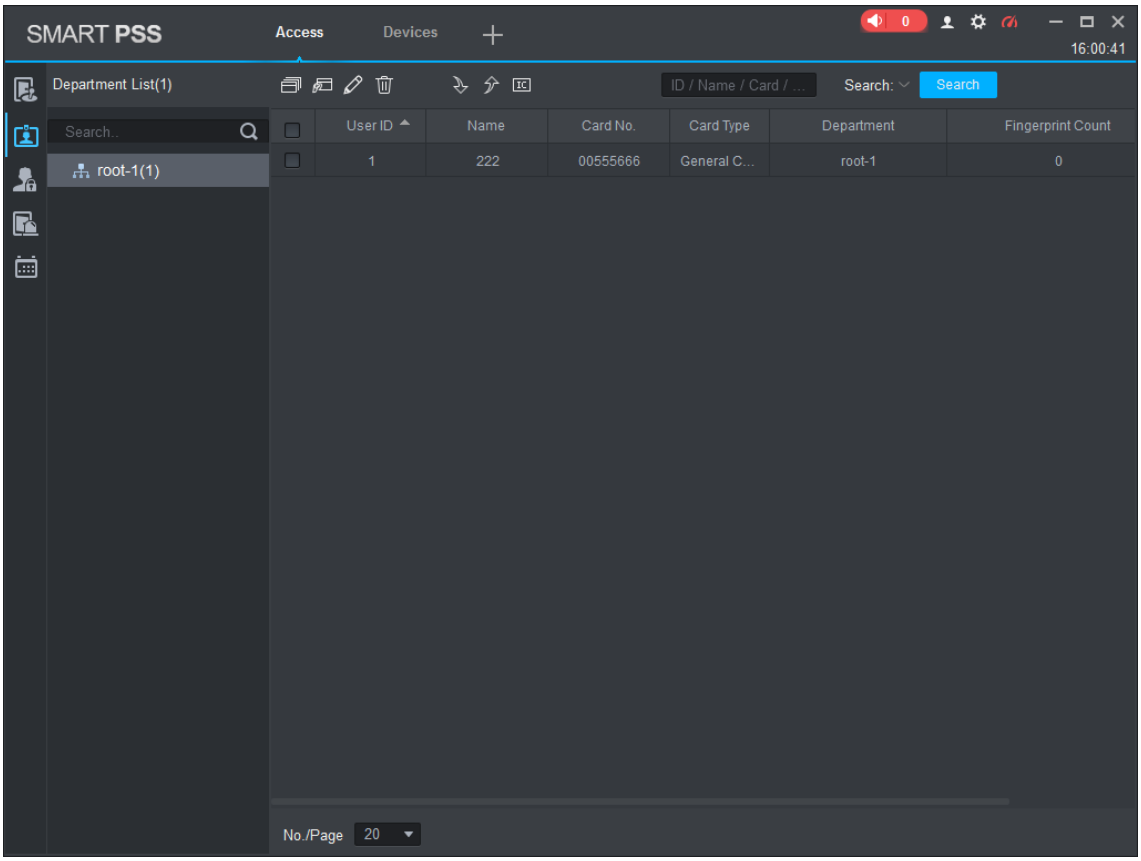
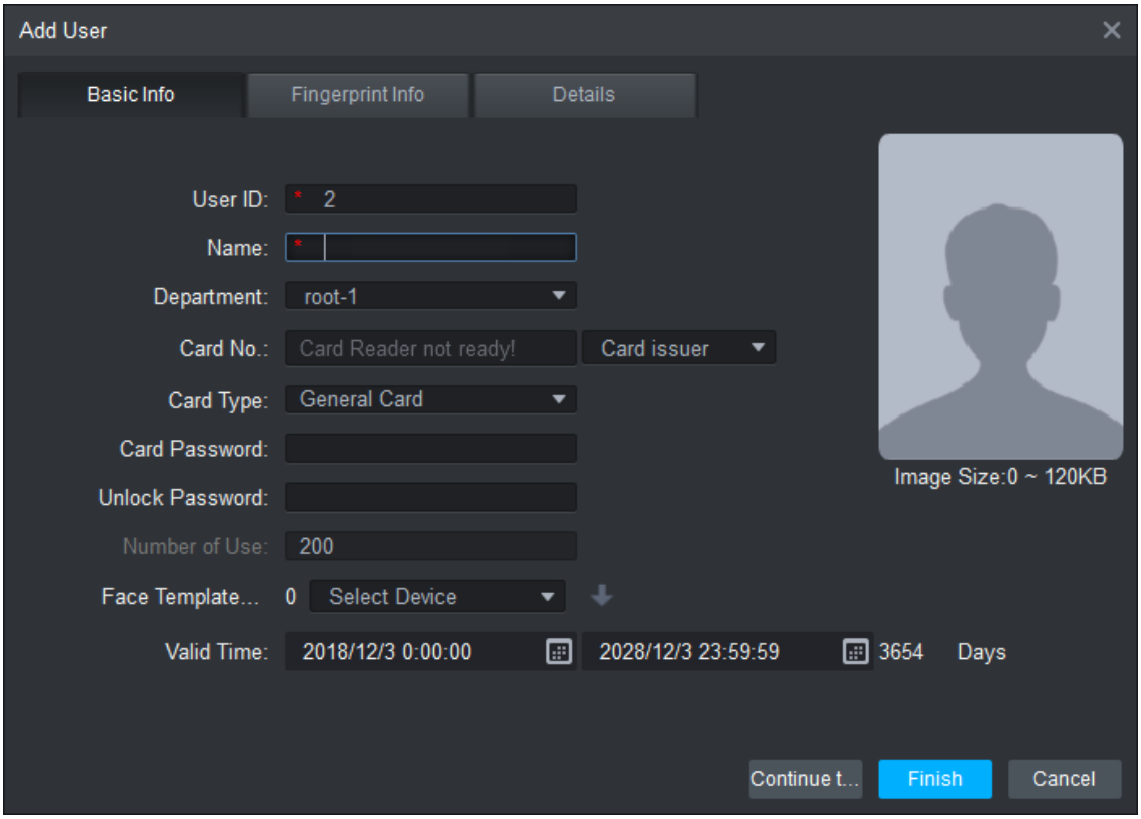


Figura 5-9 Agregar usuario



5.4 Adición de un grupo de puertas

Puede gestionar puertas agrupando puertas.

Sobre el**Acceso**interfaz, haga clic  , haga clic**Agregar**, ingrese el nombre del grupo de puertas, seleccione una zona horaria. Hacer clic**Finalizar**para completar la adición del usuario. Consulte la Figura 5-10 y la Figura 5-11.

Figura 5-10 Acceso

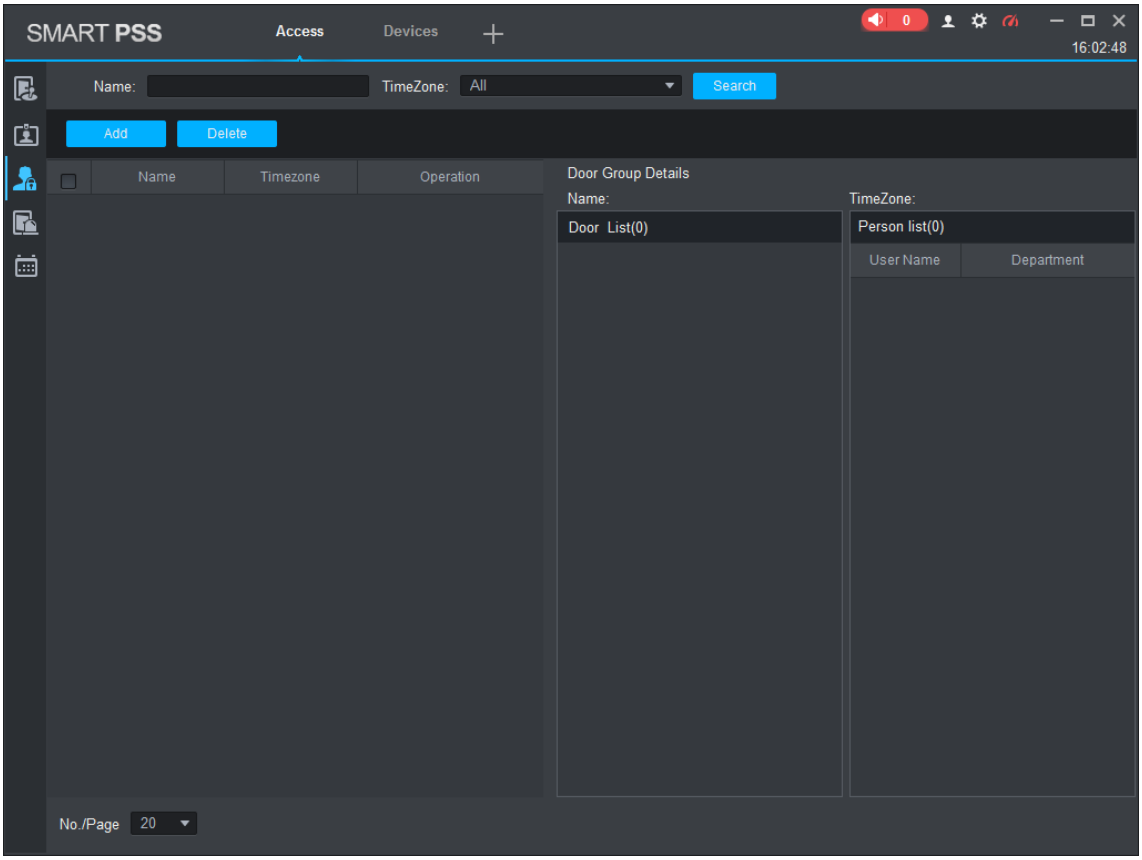
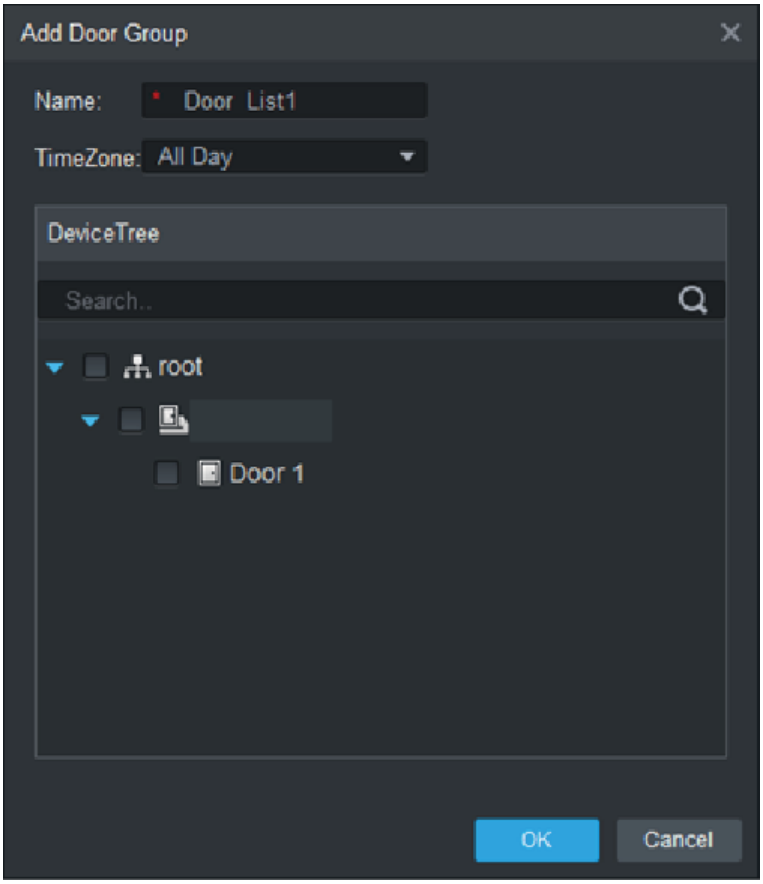


Figura 5-11 Agregar grupo de puertas



5.5 Configuración de permisos de acceso

Puede hacer la configuración de permisos de acceso. Hay dos opciones: permiso de acceso de grupo de puerta y permiso de acceso de usuario. Se sincronizará la información de los usuarios a los que se les da permiso de acceso en el Smart PSS y los terminales.

5.5.1 Dar permiso por grupo de puertas

Seleccione un grupo de puertas, agregue usuarios a la lista de puertas y, a continuación, los usuarios de la lista de puertas obtendrán permisos de acceso para todas las puertas de la lista de puertas. Consulte la Figura 5-12 y la Figura 5-13.

Figura 5-12 Acceso

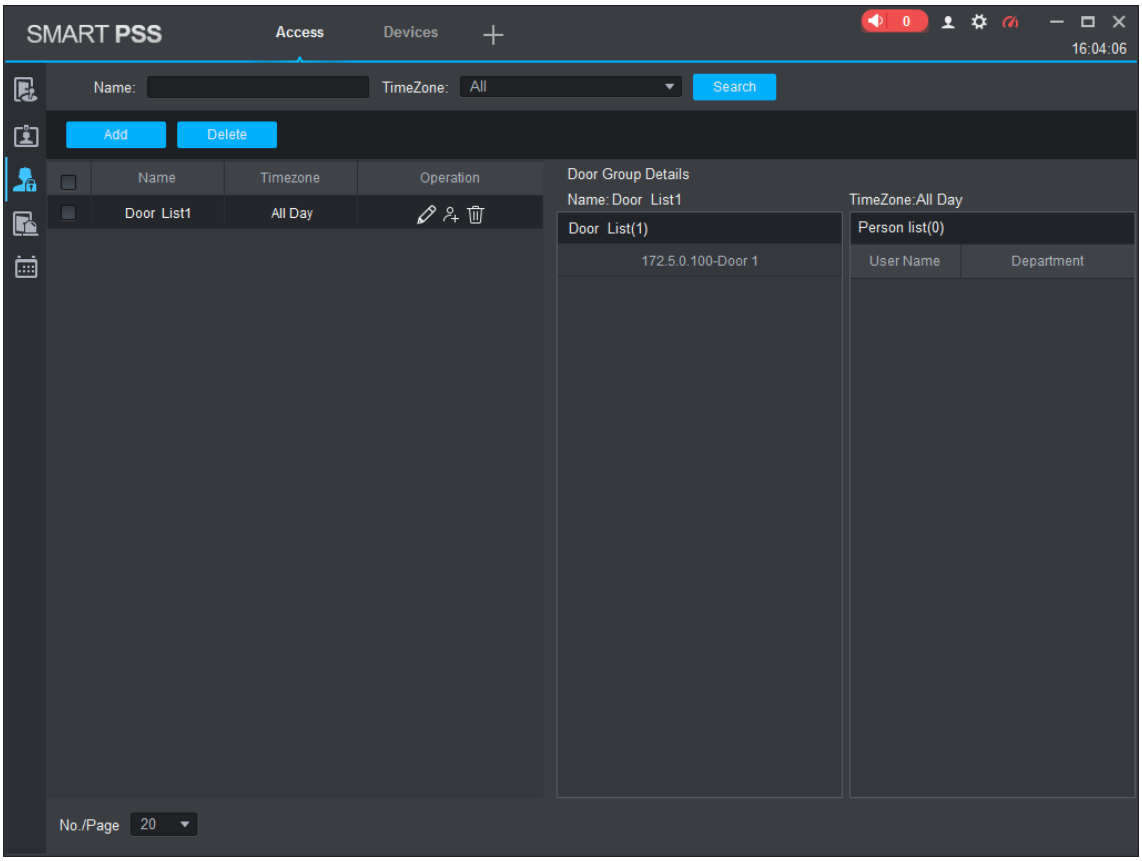
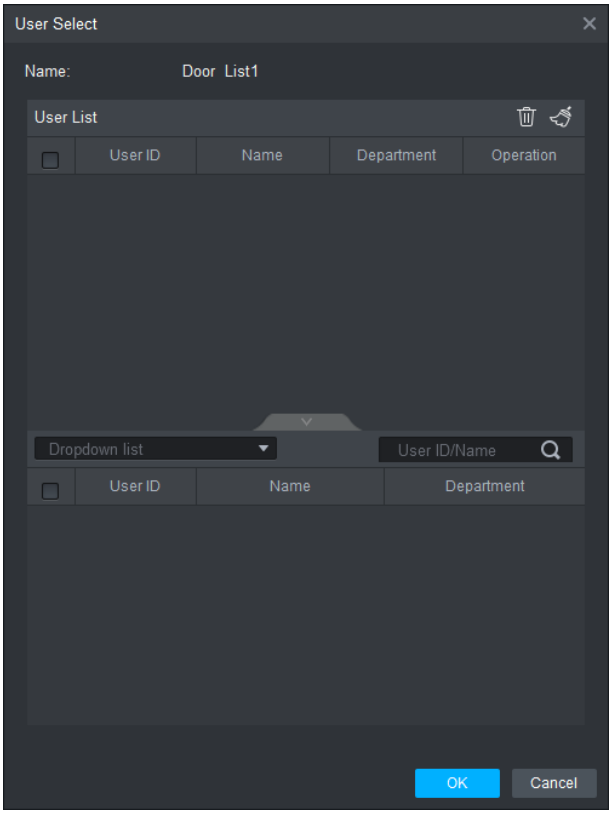


Figura 5-13 Selección de usuario



Paso 1 Sobre el**Acceso**interfaz, haga clic  , haga clic**Agregar**, haga clic**Permiso de grupo de puertas**.

Paso 2 Hacer clic  . Seleccione el departamento del usuario en la lista desplegable, o ingrese el usuario**Identificación/Nombre**, y

luego buscar usuarios. Seleccione usuarios de los usuarios que encontró.

Paso 3 Hacer clic**Finalizar**para completar la configuración.

No se pueden encontrar usuarios sin ID de usuario.

5.5.2 Dar permiso por ID de usuario

Puede otorgar permiso de acceso a un usuario seleccionando un usuario y luego seleccionando grupos de puertas para el usuario. Consulte la Figura 5-14 y la Figura 5-15.

Figura 5-14 Acceso

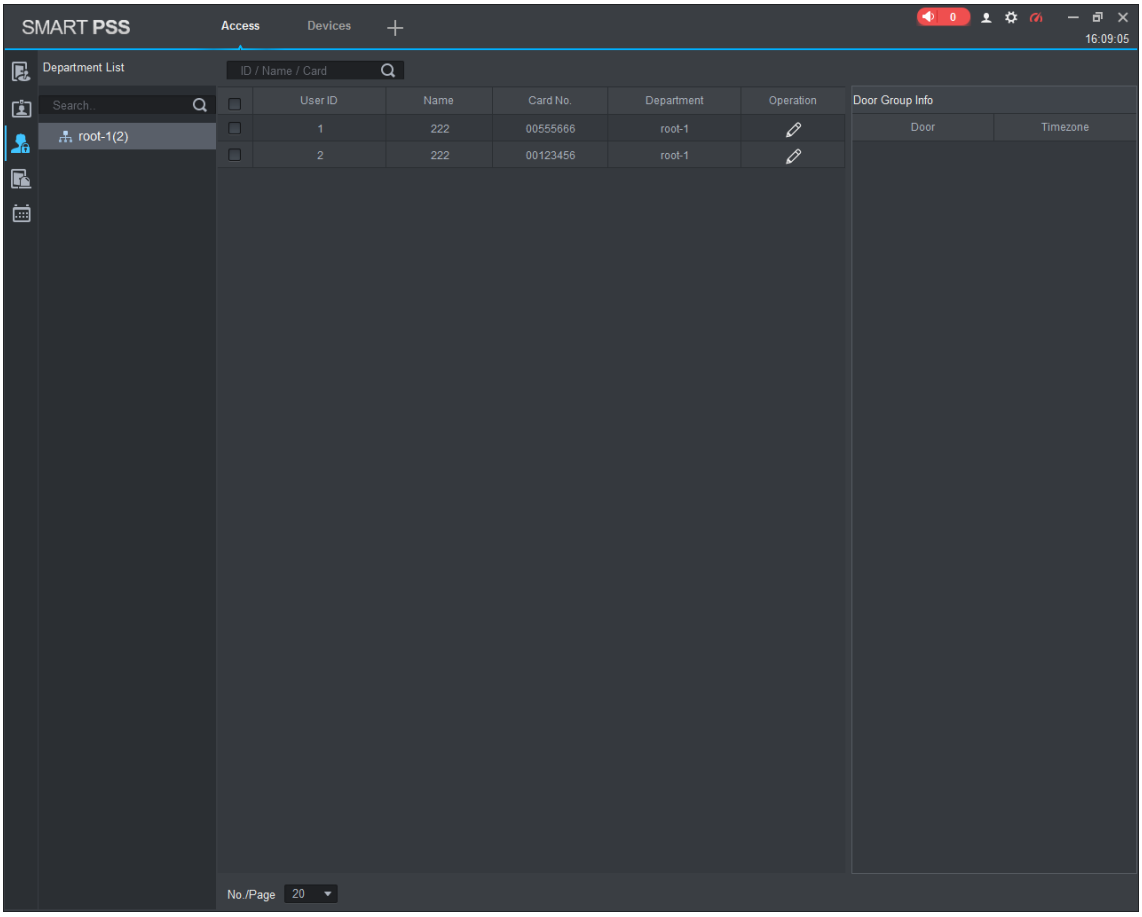
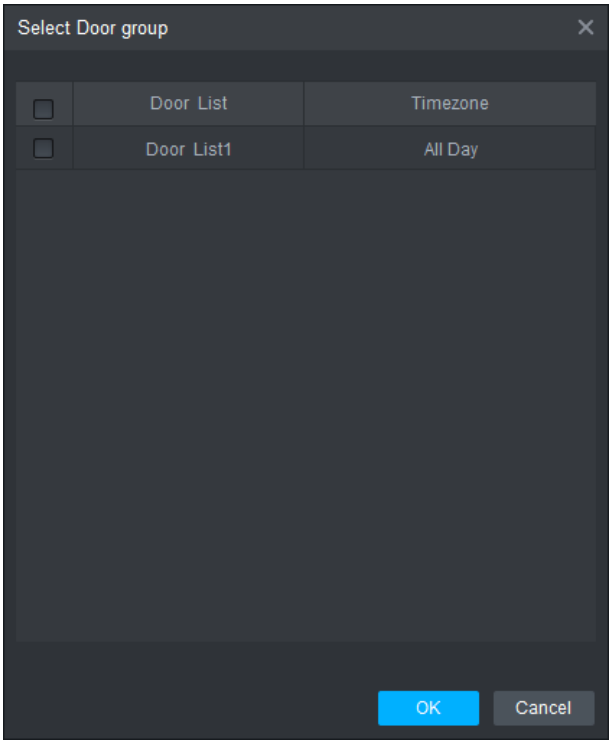


Figura 5-15 Seleccionar grupo de puertas



Paso 1 Sobre el**Acceso**interfaz, haga clic  .

Paso 2 Hacer clic  . los**Seleccionar grupo de puertas**se muestra la interfaz.

Paso 3 Seleccione el departamento del usuario en la lista desplegable, o ingrese el usuario**Identificación/Nombre**y luego seleccione una lista de puertas.

Etapa 4 Hacer clic**Finalizar**para completar la configuración.

Apéndice 1 Recomendaciones sobre 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 presentan algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias a tomar para la seguridad de la red de equipos básicos: 1.

Usar contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de caracteres; 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 del 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 "autoverificación de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones "agradables de tener" para mejorar la seguridad de su red de equipos: 1. Protección física

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

2. Cambie las contraseñas regularmente

Le sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinadas o descifradas.

3. Establezca y actualice la información de restablecimiento de contraseñas 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 de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección de contraseña, se sugiere no utilizar aquellas que se pueden 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 varias veces con la contraseña incorrecta, 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 a cualquier conjunto de números entre 1024 y 65535, lo que reduce el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.

6. Habilitar HTTPS

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

9. Asigne cuentas y privilegios de manera razonable

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios razonablemente 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 los riesgos.

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

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

11. Transmisión encriptada de audio y video

Si el contenido de sus datos de audio y video es muy importante o confidencial, 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 causará cierta pérdida en la eficiencia de la transmisión.

12. Auditoría segura

- Verifique a los usuarios en línea: le sugerimos que verifique a los usuarios en línea regularmente 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 usaron 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 habilitar la función de registro de red para asegurarse de que los registros críticos se sincronizan 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:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de 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, se sugiere usar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.