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 significado definido pueden aparecer en el manual.

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

Revisión histórica

Versión	Contenido de la revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento.	Septiembre de 2020

Acerca del manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No nos hacemos responsables de ninguna pérdida ocasionada por las operaciones que no cumplan con
- el manual. El manual se actualizaría de acuerdo con las últimas leyes y regulaciones de las regiones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si existe 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 desviaciones en los datos técnicos, las funciones y la descripción de las operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final.

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

Advertencias y medidas de seguridad importantes

Este capítulo describe el contenido que cubre el manejo adecuado del terminal, la prevención de peligros y la prevención de daños a la propiedad. Lea estos contenidos detenidamente antes de utilizar el terminal, cúmplalos al utilizarlos y guárdelos en un lugar seguro 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 el 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 en 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.
- Para el terminal con unidad de control de temperatura:
  - ◇ Instale la unidad de control de temperatura en un entorno interior sin viento y mantenga la temperatura ambiente interior entre 15 ° C y 32 ° C.
  - ◇ Caliente la unidad de control de temperatura durante más de 20 minutos después del encendido para permitir que la unidad de control de temperatura alcance el equilibrio térmico.

Seguridad ELECTRICA

- El uso inadecuado de la batería puede provocar un incendio, una explosión o una inflamación.
- Cuando reemplace la batería, asegúrese de que se use el mismo modelo.
- Utilice los cables de alimentación recomendados en la región y cumpla con la especificación de potencia nominal.
- Utilice el adaptador de corriente que se proporciona con el terminal; de lo contrario, podrían producirse lesiones personales y daños al dispositivo.
- La fuente de alimentación debe cumplir con el requisito de la norma de seguridad de voltaje muy bajo (SELV) y suministrar energía con un voltaje nominal que cumpla con el requisito de fuente de energía limitada de acuerdo con IEC60950-1. Tenga en cuenta que el requisito de suministro de energía está sujeto a la etiqueta del dispositivo.
- Conecte el dispositivo (estructura tipo I) a la toma de corriente con toma de tierra de protección. El acoplador
- del aparato es un dispositivo de desconexión. Cuando utilice el acoplador, mantenga el ángulo para facilitar la operación.

Tabla de contenido

Prólogo I
Salvaguardias y advertencias importantes ..... III 1
Resumen 1
1.1 Introducción 1
1.2 Características 1
1.3 Solicitud 1
1.4 Dimensión y componente 2
2 Conexión e instalación 4
2.1 Conexiones de cable 4
2.2 Notas de instalación 6
2.3 Dibujos de instalación 8
2.4 Instalación 8
3 Operaciones del sistema 10
3.1 Procedimiento de configuración básica 10
3.2 Iconos comunes 10
3.3 Inicialización 10
3.4 Interfaz de espera 11
3.5 Menú principal 12
3.6 Métodos de desbloqueo 14
3.6.1 Rostro 14
3.6.2 Contraseña de usuario 14
3.6.3 Contraseña de administrador 15
3.7 Gestión de usuarios 15
3.7.1 Agregar nuevos usuarios 15
3.7.2 Visualización de la información del usuario ..... dieciséis
3.8 Gestión de Acceso 17
3.8.1 Gestión de períodos 17
3.8.2 Desbloquear 18
3.8.3 Configuración de alarma 21
3.8.4 Estado de la puerta 22
3.8.5 Bloqueo de tiempo de retención 22
3.9 Red de comunicacion 22
3.9.1 Dirección IP 22
3.9.2 Configuración del puerto serie 24
3.9.3 Configuración Wiegand 25
3.10 Sistema 26
3.10.1 Hora 26
3.10.2 Parámetro de cara 26
3.10.3 Modo de imagen 28
3.10.4 Configuración del modo de luz de relleno 28
3.10.5 Ajuste del brillo de la luz de relleno 28
3.10.6 Ajuste de volumen 28
3.10.7 Ajuste del brillo de la luz IR 28
3.10.8 Restaurar la configuración de fábrica 28

3.10.9 Reiniciar 29
3.11 USB 29
3.11.1 Exportación USB 29
3.11.2 Importación USB 30
3.11.3 Actualización USB 31
3.11.4 Características 31
3.11.5 Comentarios de resultados 34
3.12 Registro 36
3.13 Auto prueba 37
3.14 Información del sistema 37
4 Operaciones web 38
4.1 Inicialización 38
4.2 Acceso 40
4.3 Restablecimiento de la contraseña 40
4.4 Enlace de alarma 42
4.4.1 Configuración del enlace de alarma 42
4.4.2 Registro de alarmas 43
4.5 Configuración de llamada 44
4.5.1 Configuración del controlador de acceso 44
4.5.2 Servidor SIP 45
4.5.3 Gestión de videoporteros 47
4.5.4 Gestión del monitor interior 49
4.5.5 Configuración del dispositivo de gestión 51
4.5.6 Estado en línea 52
4.5.7 Registros de llamadas 53
4.6 Capacidad de datos 54
4.7 Configuración de vídeo 54
4.7.1 Velocidad de datos 54
4.7.2 Imagen 55
4.7.3 Exposición 56
4.7.4 Detección de movimiento 57
4.7.5 Ajuste de volumen 59
4.7.6 Modo de imagen 59
4.7.7 Codificación local 59
4.8 Detección de rostro 60
4.9 Configuración de red 63
4.9.1 TCP / IP 63
4.9.2 Puerto 64
4.9.3 Registrarse ..... sesenta y cinco
4.9.4 P2P ..... sesenta y cinco
4.10 Administración de Seguridad 66
4.10.1 Autoridad de propiedad intelectual 66
4.10.2 Sistemas 67
4.11 Gestión de usuarios 67
4.11.1 Agregar usuarios 68
4.11.2 Modificación de la información del usuario 68
4.12 Mantenimiento 68

4.13 Gestión de la configuración 69
4.14 Potenciar 69
4.15 Información de versión 69
4.16 Usuario en línea 69
4.17 Registro del sistema 70
4.17.1 Consulta de registros 70
4.17.2 Copia de seguridad de registros 71
4.17.3 Registro de administración 71
4.18 Salida 71
5 Preguntas frecuentes 72
Appendix 1 Notas de monitoreo de temperatura 73
Appendix 2 Notas de comparación / grabación facial 74
Appendix 3 Recomendaciones de ciberseguridad 77

1. Información general

1.1 Introducción

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

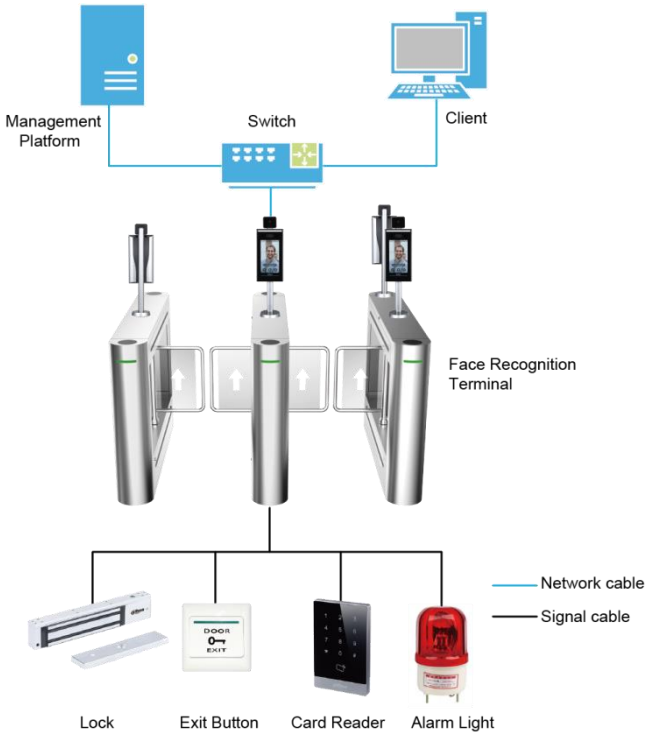
1.2 Características

- Pantalla LCD, la resolución del terminal de 7 pulgadas es de 1024 × 600 Admite
- desbloqueo facial y desbloqueo de contraseña; desbloquear por período
- Con caja de detección de rostros; se reconoce primero el rostro más grande entre los rostros que aparecen al mismo tiempo; el tamaño máximo de la cara se puede configurar en la web
- Lente WDR gran angular de 2MP; con iluminador automático / manual
- Con el algoritmo de reconocimiento facial, el terminal puede reconocer más de 360 posiciones en el rostro humano
- Precisión de verificación facial> 99,5%; baja tasa de falso reconocimiento
- Reconocimiento de perfil de soporte; 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 especiales
- Varios modos de visualización del estado de desbloqueo protegen la privacidad del usuario
- Apoyar el control de la temperatura corporal a través de la unidad de control de temperatura periférica

1.3 Solicitud

La terminal es aplicable a parques, edificios de oficinas, escuelas, fábricas, áreas residenciales y otros lugares. La identidad se verifica mediante reconocimiento facial para lograr el paso sin percepción.

Figure 1-1 Redes



1.4 Dimensión y componente

Figure 1-2 Dimensiones y componentes del modelo X (mm [pulgadas])

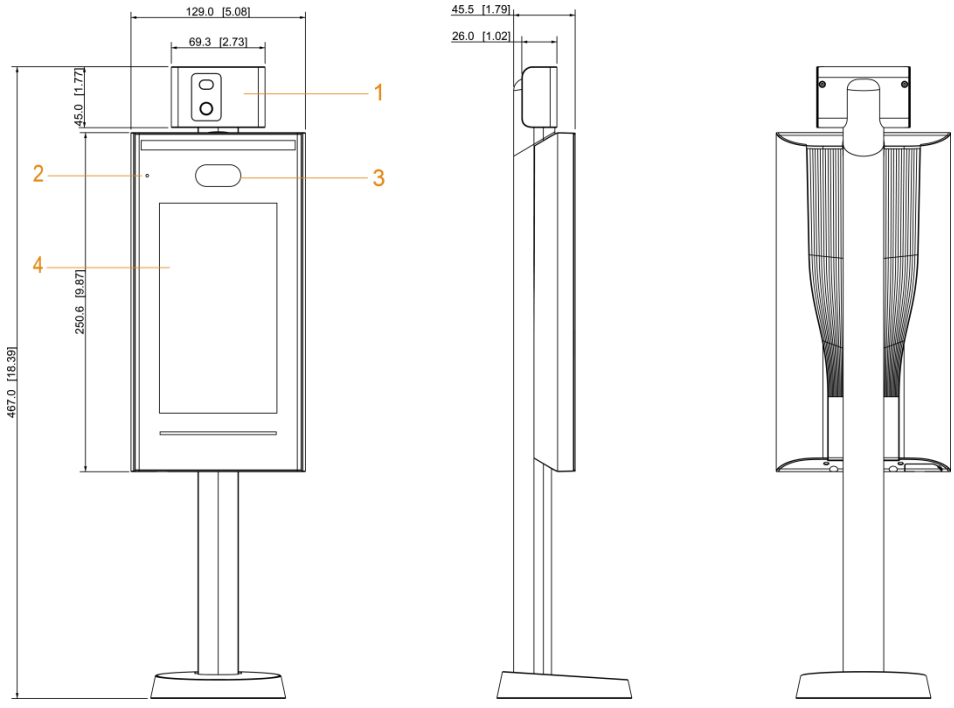


Tabla 1-1 Descripción de los componentes (1)

No.	Nombre	No.	Nombre
1	Unidad de control de temperatura	3	Cámaras duales
2	MIC	4	Monitor

Figure 1-3 Dimensiones y componentes del modelo Y (mm [pulgadas])

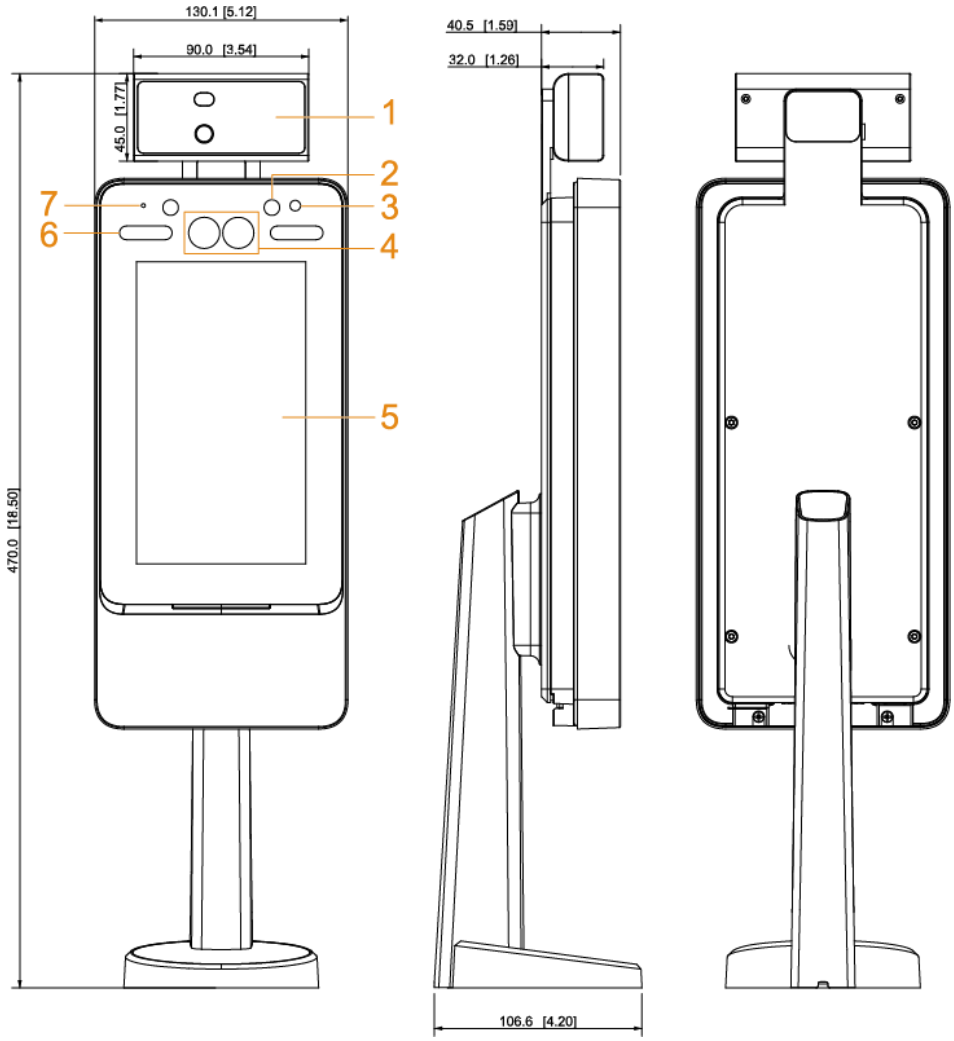


Tabla 1-2 Descripción de los componentes (2)

No.	Nombre	No.	Nombre
1	Unidad de control de temperatura	5	Monitor
2	Luz infrarroja	6	Iluminador LED blanco
3	Fototransistor	7	Micrófono
4	Cámaras duales	-	-

2 Conexión e instalación

2.1 Conexiones de cable

La conexión del cable del modelo X y el modelo Y es la misma. Esta sección toma el modelo X como ejemplo.

⚠

- Compruebe si el módulo de seguridad de control de acceso está habilitado en **Función> 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 independiente para proporcionar energía. Una vez que el
- módulo de seguridad está habilitado, el botón de salida, el control del torniquete y el enlace de extinción de incendios no serán válidos.

Figure 2-1 Conexiones de cable

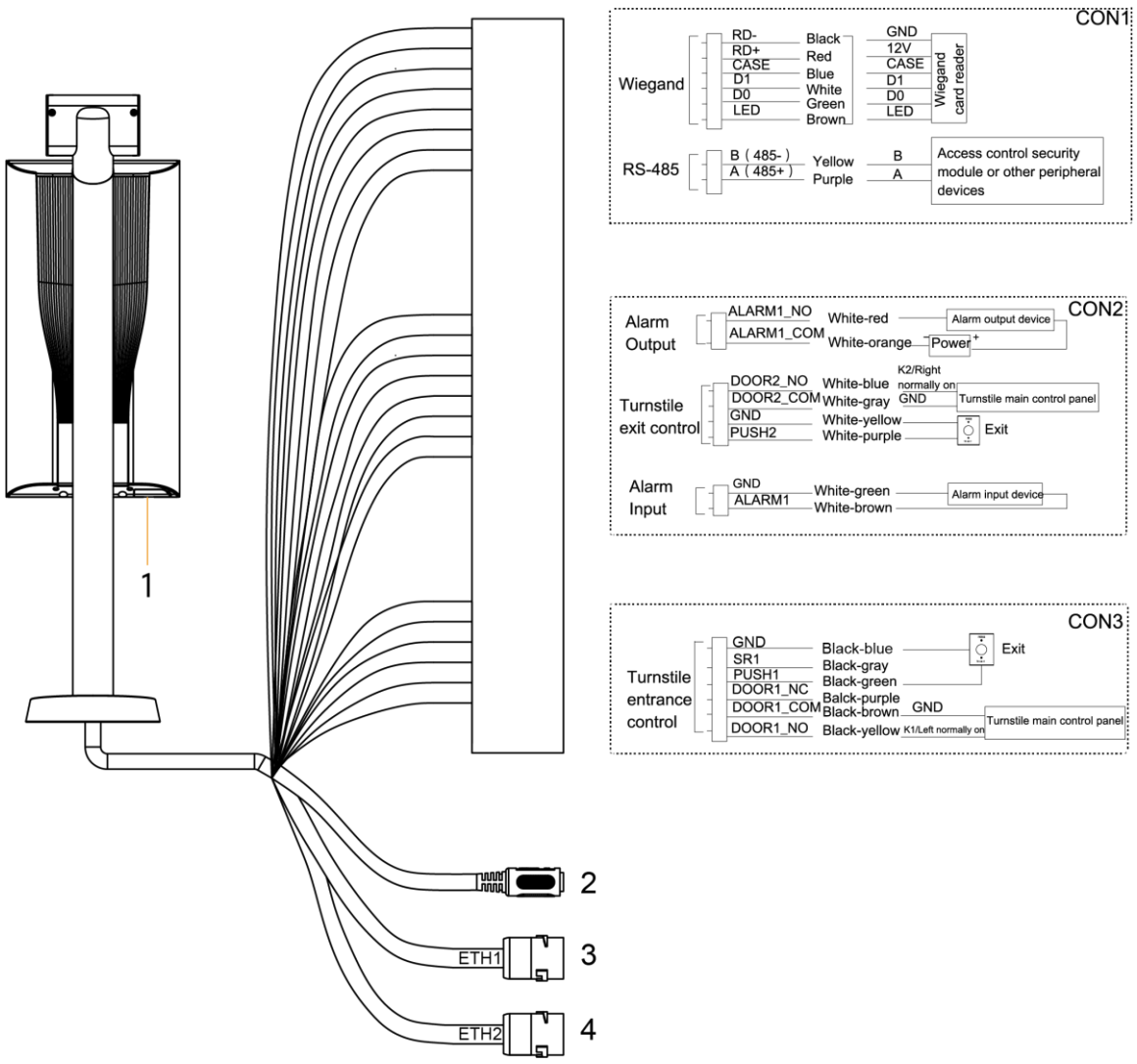


Tabla 2-1 Descripción de los componentes

No.	Nombre
1	Puerto USB
2	Puerto de alimentación

No.	Nombre
3	Puerto Ethernet
4	Puerto Ethernet (solo compatible con controladores de acceso modelo B de 7 pulgadas)

Tabla 2-2 Descripción del puerto

Puerto	Color del cable	Nombre del cable	Descripción
CON1	Negro	RD–	Electrodo negativo de lector de tarjetas externo.
	rojo	RD +	Electrodo positivo de lector de tarjetas externo.
	Azul	CASO	Entrada de alarma de sabotaje del lector de tarjetas externo.
	blanco	D1	Entrada Wiegand D1 (conectada al lector de tarjetas externo) / salida (conectada al controlador).
	Verde	D0	Entrada Wiegand D0 (conectada al lector de tarjetas externo) / salida (conectada al controlador).
	marrón	DIRIGIÓ	Conectado al indicador de lector externo en
	Amarillo	B	Entrada de electrodo negativo RS-485 (conectado al lector de tarjetas externo) / salida (conectado al controlador o conectado al módulo de seguridad de control de la 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 independiente 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 de electrodo positivo RS-485 (conectado al lector de tarjetas externo) / salida (conectado al controlador o conectado al módulo de seguridad de control de la 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 independiente 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.
CON2	blanco y rojo	ALARM1_NO	Alarma 1 puerto de salida normalmente abierto.
	blanco y naranja	ALARM1_COM	Puerto de salida común de alarma 1.
	blanco y azul	DOOR2_NO	Bloqueo de control puerto normalmente abierto.
	blanco y gris	DOOR2_COM	Bloquear el puerto común de control.
	blanco y amarillo	GND	Conectado al puerto GND común.

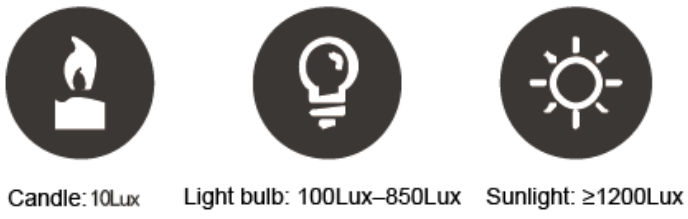
Puerto	Color del cable	Nombre del cable	Descripción
	blanco y púrpura	PUSH2	Botón de apertura de puerta de la puerta No 2
	blanco y verde	GND	Conectado al puerto GND común.
	blanco y marrón	ALARMA1	Puerto de entrada de alarma 1.
CON3	Negro y azul	GND	Conectado al puerto GND común.
	Negro y gris	SR1	Se utiliza para la detección de contactos de puertas.
	Negro y verde	PUSH1	Botón de apertura de puerta de la puerta No 1
	Negro y púrpura	DOOR1_NC	Bloqueo de control puerto normalmente cerrado.
	Negro y marrón	DOOR1_COM	Bloquear el puerto común de control.
	Negro y amarillo	DOOR1_NO	Bloqueo de control puerto normalmente abierto.

2.2 Notas de instalación

- Si hay una fuente de luz a 0,5 metros del dispositivo, la iluminación mínima no debe ser inferior a 100 Lux.
- Se recomienda que el dispositivo se instale en interiores, al menos a 3 metros de las ventanas y puertas y a 2 metros de las luces.
- Evite la luz de fondo y la luz solar directa.

Requisito de iluminación ambiental

Figure 2-2 Requisito de iluminación ambiental



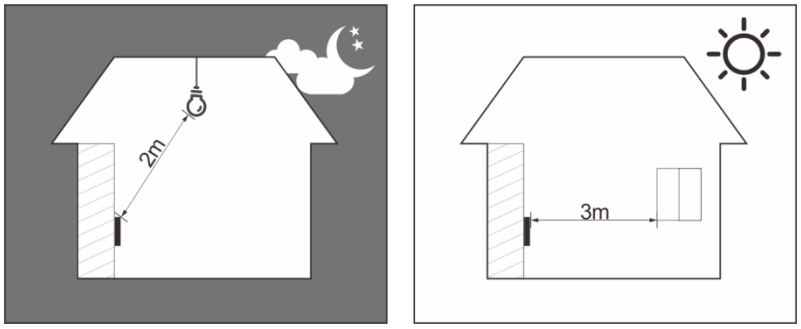
Requisito de monitoreo de temperatura

- Se recomienda instalar la unidad de control de temperatura en un entorno interior sin viento (un área relativamente aislada del exterior) y mantener la temperatura ambiente entre 15 ° C y 32 ° C.

- Caliente la unidad de control de temperatura durante más de 20 minutos después del encendido para permitir que la unidad de control de temperatura alcance el equilibrio térmico.
- Si no hay un entorno interior adecuado (incluidas las áreas que dan directamente a las áreas interiores y exteriores y las puertas exteriores), configure un pasaje temporal con temperatura ambiente estable para el control de la temperatura.
- Los factores como la luz solar, el viento, el aire frío y el aire acondicionado frío y caliente pueden afectar fácilmente la temperatura de la superficie del cuerpo humano y el estado de funcionamiento de la terminal, lo que provocará la desviación de temperatura entre la temperatura monitoreada y la temperatura real.
- Factores que influyen en el control de la temperatura
  - ◇ Viento: el viento quitará el calor de la frente, lo que afectará la precisión del control de la temperatura.
  - ◇ Sudoración: la sudoración es una forma en que el cuerpo se enfría y disipa el calor automáticamente. Cuando el cuerpo suda, la temperatura también disminuirá.
  - ◇ Temperatura ambiente: si la temperatura ambiente es baja, la temperatura de la superficie del cuerpo humano disminuirá. Si la temperatura de la habitación es demasiado alta, el cuerpo humano comenzará a sudar, lo que afectará la precisión del control de temperatura.
  - ◇ La unidad de control de temperatura es sensible a las ondas de luz con una longitud de onda de 10 um a 15 um. Evite usarlo al sol, fuentes de luz fluorescente, salidas de aire acondicionado, calefacción, salidas de aire frío y superficies de vidrio.

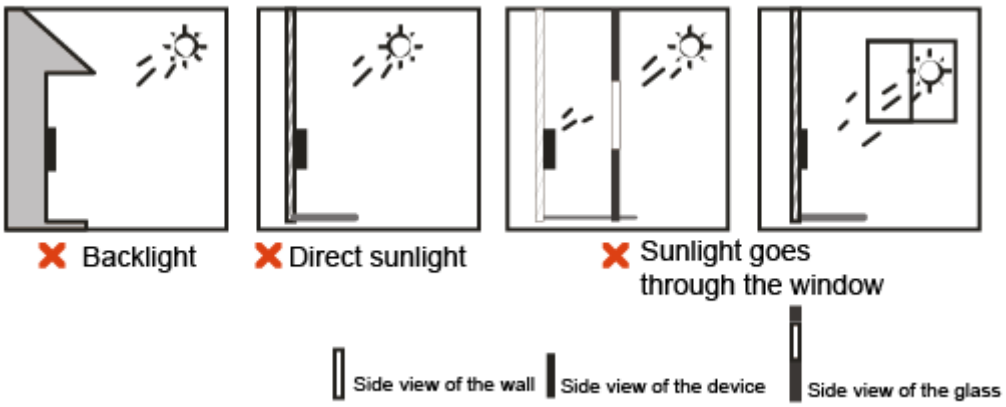
Lugares recomendados

Figure 2-3 Lugares recomendados



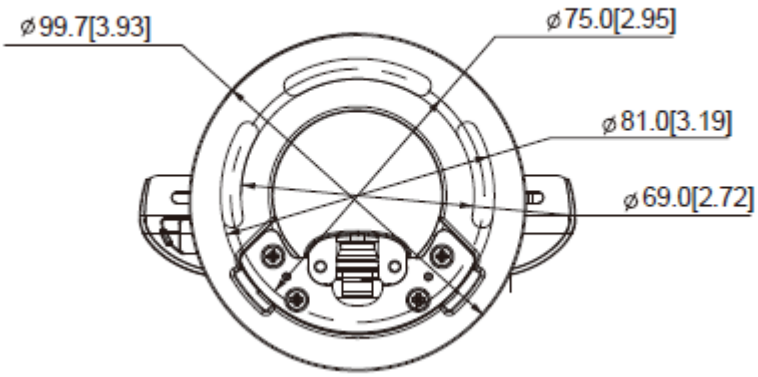
Lugares no recomendados

Figure 2-4 Lugares no recomendados



2.3 Dibujos de instalación

Figure 2-5 Dibujos de instalación (mm [pulgadas])



2.4 Instalación

La instalación del modelo X y del modelo Y es la misma. Esta sección toma el modelo X como ejemplo.

Figure 2-6 Instalación de la terminal

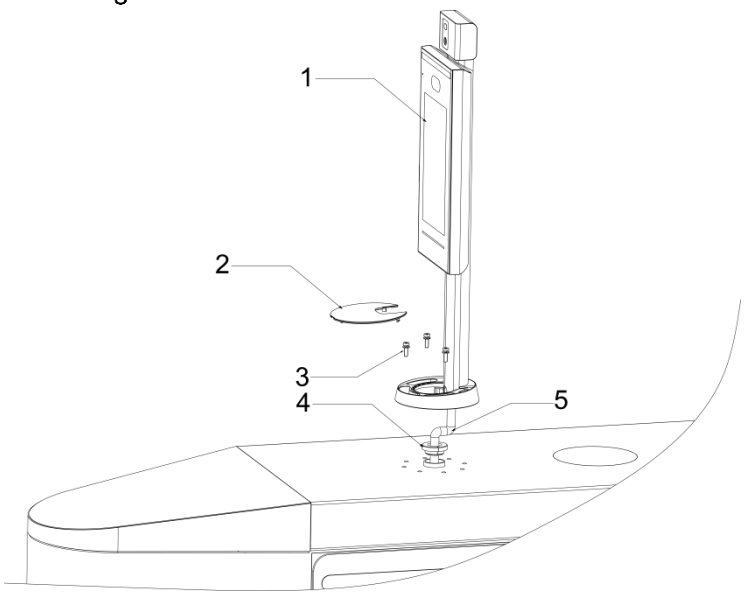


Figure 2-7 Aplicar sellador de silicona al terminal

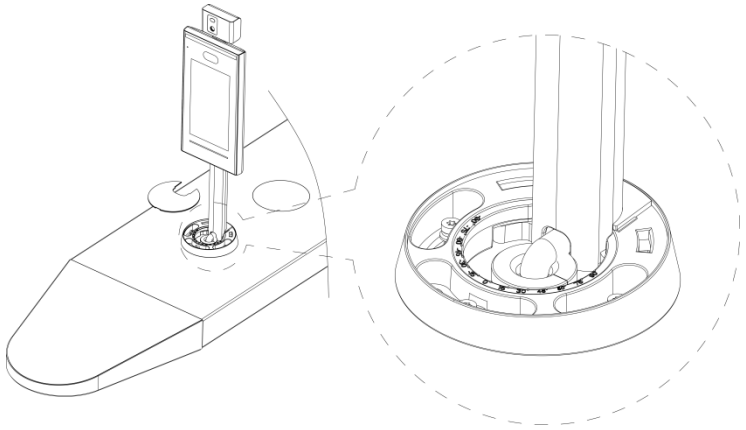


Tabla 2-3 Descripción de los componentes

No.	Nombre
1	Terminal
2	Cubierta ornamental
3	Tornillo M5
4	Tapón de gel de sílice impermeable
5	Cable

Procedimiento de instalación

Step 1 Pase el cable a través del torniquete.

Step 2 Coloque el enchufe de gel de sílice impermeable en el cable. Fije el

Step 3 terminal al torniquete con tornillos M5. Conecte los cables para el

Step 4 terminal. Consulte "2.1 Conexiones de cables".

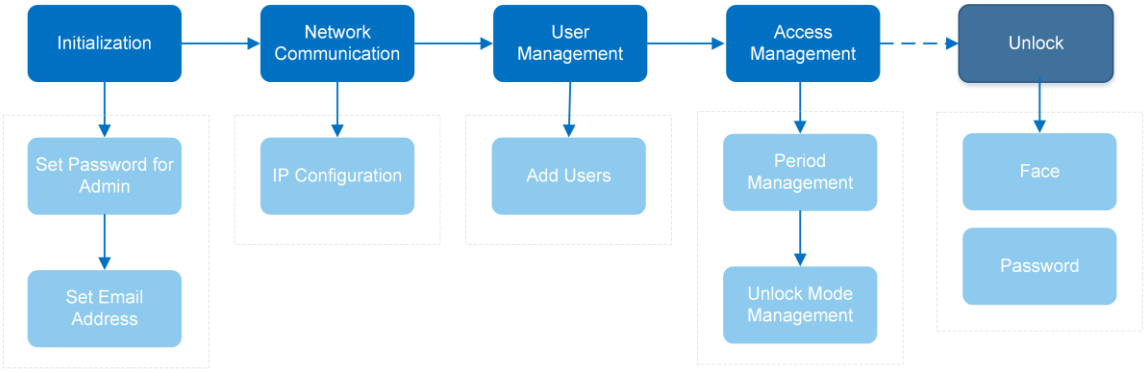
Step 5 Aplique sellador en los espacios entre el tapón de gel de sílice impermeable y el torniquete. Vea la Figura 2-7.

Step 6 Instale la cubierta ornamental en la base del terminal.

3 Operaciones del sistema

3.1 Procedimiento de configuración básica

Figure 3-1 Procedimiento de configuración básico



3.2 Iconos comunes

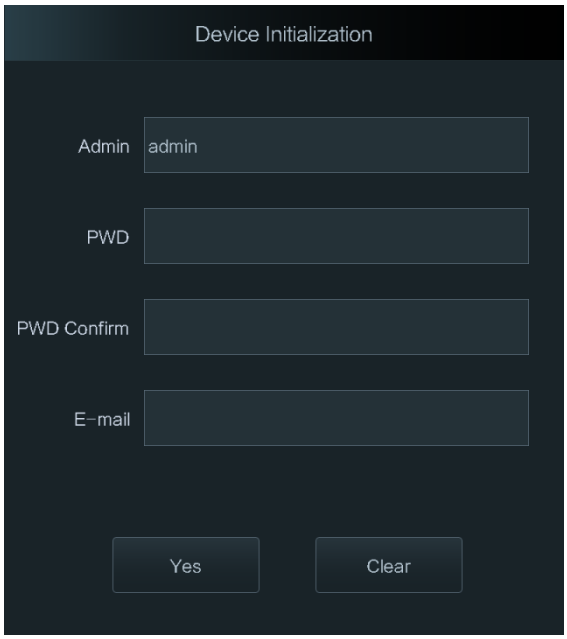
Tabla 3-1 Descripción de los iconos

Icono	Descripción
	Icono del menú principal.
	Confirmar icono.
	Pase a la primera página de la lista.
	Pase a la última página de la lista.
	Pasa a la página anterior de la lista.
	Pase a la siguiente página de la lista.
	Vuelve al menú anterior.
	Habilitar.
	Desactivar.

3.3 Inicialización

La contraseña de administrador y un correo electrónico deben establecerse la primera vez que se enciende el terminal o después de restablecerlo; de lo contrario, no se podrá utilizar el terminal.

Figure 3-2 Inicialización



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

3.4 Interfaz de espera

Puede desbloquear la puerta a través de rostros y contraseñas.

- Si no hay operaciones en 32 segundos, el terminal pasará al modo de espera. Las
- siguientes figuras son solo de referencia y prevalecerá la interfaz real.

Figure 3-3 Página principal

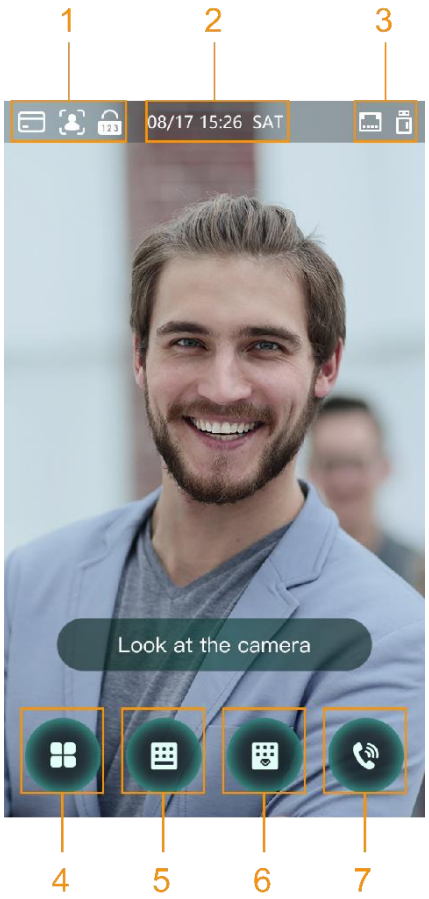


Tabla 3-2 Descripción de la página de inicio

No.	Descripción
1	Métodos de desbloqueo: tarjeta, rostro, huella digital y contraseña. Cuando la tarjeta, el rostro, la huella digital y la contraseña están configurados como modo de desbloqueo, el icono de contraseña no se mostrará en la esquina superior izquierda del controlador de acceso.
2	Fecha y hora: fecha y hora actuales.
3	Estado de la red y estado del USB.
4	Menú principal. Solo los administradores pueden ingresar al menú principal.
5	Desbloqueo de contraseña.
6	Desbloqueo de contraseña de administrador.
7	Toque para llamar a otros dispositivos.

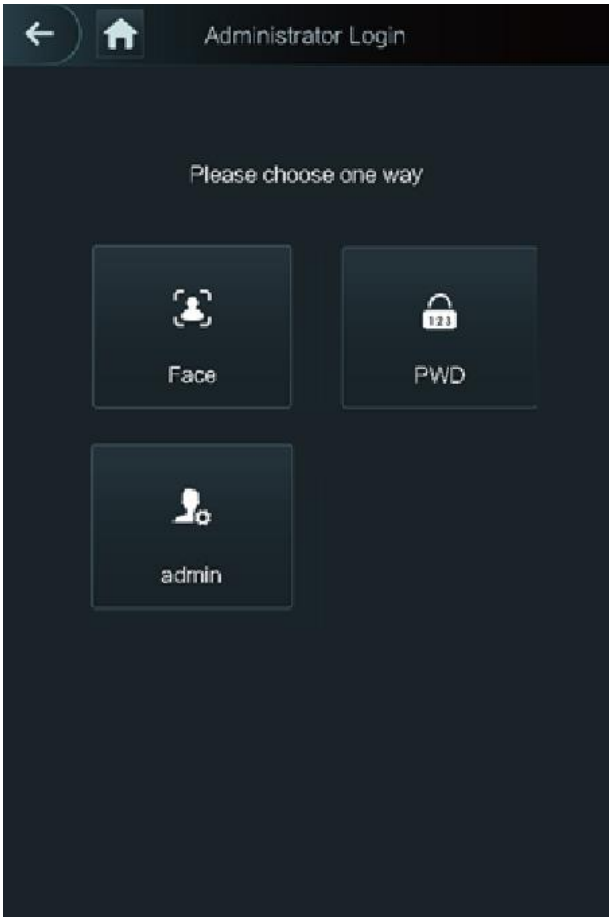
3.5 Menú principal

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

Step 1 Grifo en la interfaz de espera.

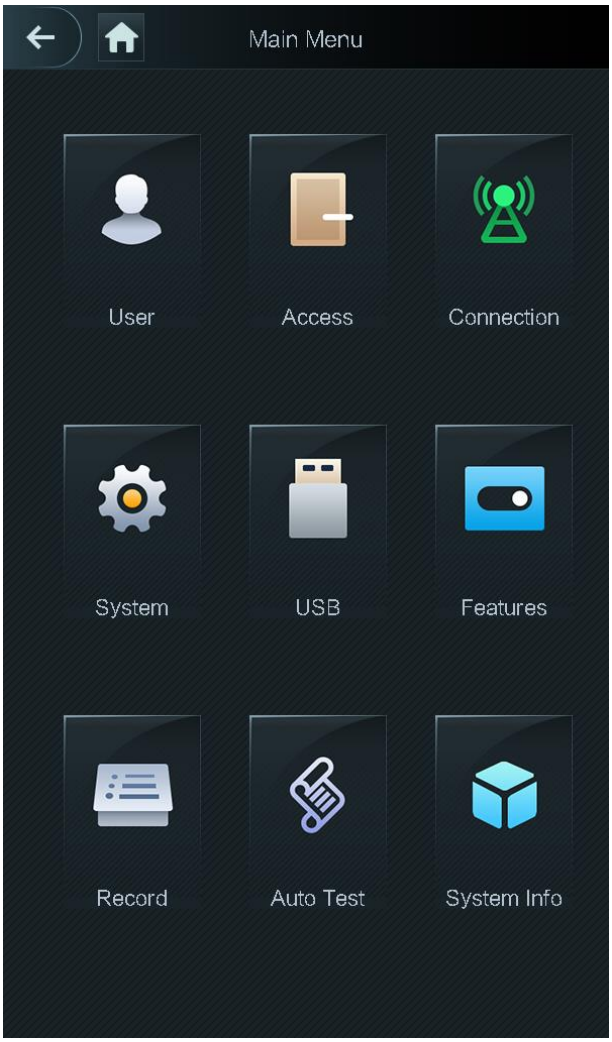
Los diferentes modos admiten diferentes métodos de desbloqueo, y prevalecerá la interfaz real.

Figure 3-4 Inicio de sesión de administrador



Step 2 Seleccione un método de entrada al menú principal.

Figure 3-5 Menú principal



3.6 Métodos de desbloqueo

Puede desbloquear la puerta a través de rostros y contraseñas.

3.6.1 Rostro

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

3.6.2 Contraseña de usuario

Ingrese la contraseña de usuario y luego podrá desbloquear la puerta.

Step 1 Grifo en la página de inicio.

Step 2 Ingrese la ID de usuario y luego toque .

Step 3 Ingrese la contraseña de usuario y luego toque .

3.6.3 Contraseña de administrador

Ingrese la contraseña de administrador y luego podrá desbloquear la puerta. Solo hay una contraseña de administrador para un terminal. La contraseña de administrador puede desbloquear la puerta sin estar sujeta a los 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".

Step 1 Grifo  en la página de inicio.

Step 2 Grifo **Ingrese la contraseña del administrador**.

Step 3 Ingrese la contraseña de administrador y luego toque. ☑

3.7 Gestión de usuarios

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

3.7.1 Agregar nuevos usuarios

Puede agregar nuevos usuarios ingresando sus ID de usuario, nombres, importando imágenes de caras, contraseñas, seleccionando sus niveles de usuario y más.

Step 1 Seleccione **Usuario> Nuevo usuario**.

La siguiente figura es solo para referencia y prevalecerá la interfaz real.

Figure 3-6 Nuevo Usuario

Step 2 Configure los parámetros en la interfaz.

Tabla 3-3 Descripción del nuevo parámetro de usuario

Parámetro	Descripción
ID de usuario	Ingrese los ID de usuario. Las identificaciones pueden ser números, letras y sus combinaciones, y la longitud máxima de la identificación es de 32 caracteres. Cada identificación es única.
Nombre	Ingrese nombres con un máximo de 32 caracteres (incluidos números, símbolos y letras).
Cara	Asegúrese de que su rostro esté centrado en el marco de captura de la imagen, y luego se capturará automáticamente una imagen de su rostro.
PWD	La contraseña de desbloqueo de la puerta. La longitud máxima de la contraseña es de 8 caracteres.
Nivel	Puede seleccionar un nivel de usuario para nuevos usuarios. Hay dos opciones. ● Usuario: los usuarios solo tienen permiso de desbloqueo de puertas. ● Administrador: los administradores no solo pueden desbloquear la puerta, sino que también tienen permiso de configuración de parámetros. En caso de que olvide la contraseña de administrador, será mejor que cree más de un administrador.
Período	Puede establecer un período en el que el usuario puede desbloquear la puerta. Para conocer la configuración detallada del período, consulte el manual de configuración.
Fiesta Plan	Puede establecer un plan de vacaciones en el que el usuario puede abrir la puerta. Para conocer la configuración detallada del plan de vacaciones, consulte el manual del usuario.
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 de la lista negra abren la puerta, el personal de servicio recibirá un aviso. ● Invitado: los invitados pueden abrir la puerta en determinados momentos en determinados períodos. Una vez que superan los tiempos y períodos máximos, no pueden volver a desbloquear la puerta. ● Patrulla: los usuarios de patrulla pueden hacer un seguimiento de su asistencia, pero no tienen permiso de desbloqueo. ● VIP: cuando VIP abre la puerta, el personal de servicio recibirá un aviso. Especial: ● cuando personas especiales desbloquean 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.

Step 3 Grifo ☑ para guardar la configuración.

3.7.2 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.

3.8 Gestión de Acceso

Puede realizar la gestión de acceso en 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 administración de acceso.

3.8.1 Gestión de períodos

Puede establecer períodos, períodos de vacaciones, períodos de planes de vacaciones, períodos de puerta normalmente abierta, períodos de puerta normalmente cerrada y períodos de verificación remota.

3.8.1.1 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.

3.8.1.2 Grupo de vacaciones

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

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

3.8.1.3 Plan de vacaciones

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

3.8.1.4 Periodo NO

Si se agrega un punto al **NO** período, entonces la puerta permanece abierta durante ese período.

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

3.8.1.5 Periodo NC

Si se agrega un punto al **CAROLINA DEL NORTE** período, entonces la puerta permanece cerrada durante ese período. Los usuarios no pueden desbloquear la puerta en este período.

3.8.1.6 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.

Necesita habilitar el **Período de verificación remota**.

-  significa habilitado.
-  significa no habilitado.

3.8.2 Desbloquear

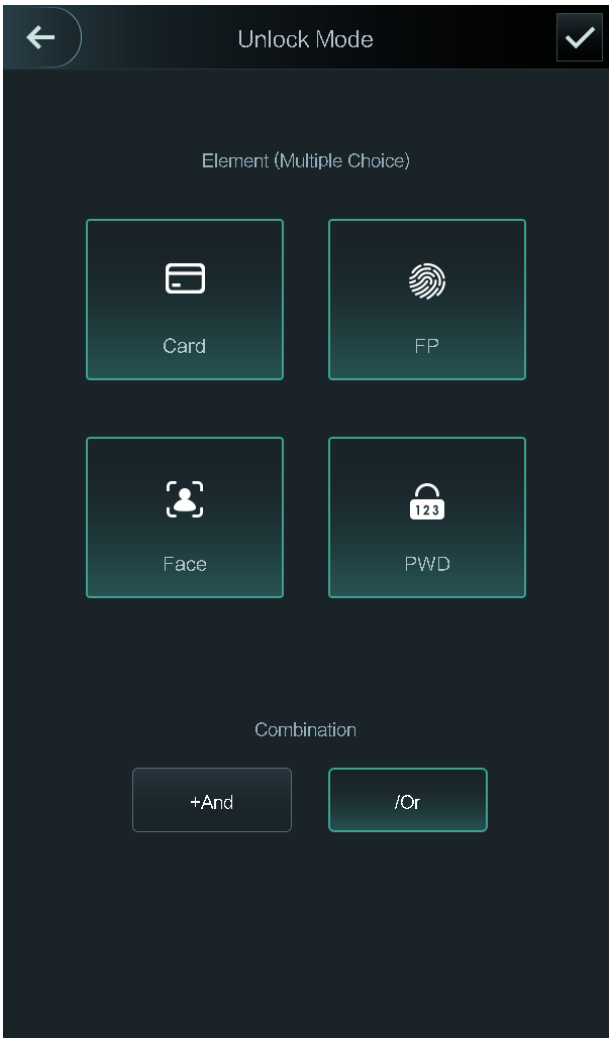
Hay tres modos de desbloqueo: modo de desbloqueo, desbloqueo por período y combinación de grupo. Los modos de desbloqueo varían según el modelo de terminal, y prevalecerá el terminal real.

3.8.2.1 Modo de desbloqueo

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

Step 1 Seleccione **Acceso> Modo de desbloqueo> Modo de desbloqueo**.

Figure 3-7 Elemento (opción múltiple)



Step 2 Seleccione uno o más modos de desbloqueo.

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

Step 3 Seleccione un modo de combinación.

- **+ Y** significa "y". Por ejemplo, si selecciona tarjeta + PWD, significa que para desbloquear la puerta, primero debe deslizar su tarjeta y luego obtener la contraseña.
- **/ O** significa "o". Por ejemplo, si selecciona tarjeta / PWD, significa que para desbloquear la puerta, puede deslizar su tarjeta o ingresar la contraseña.

Step 4 Grifo para guardar la configuración.

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

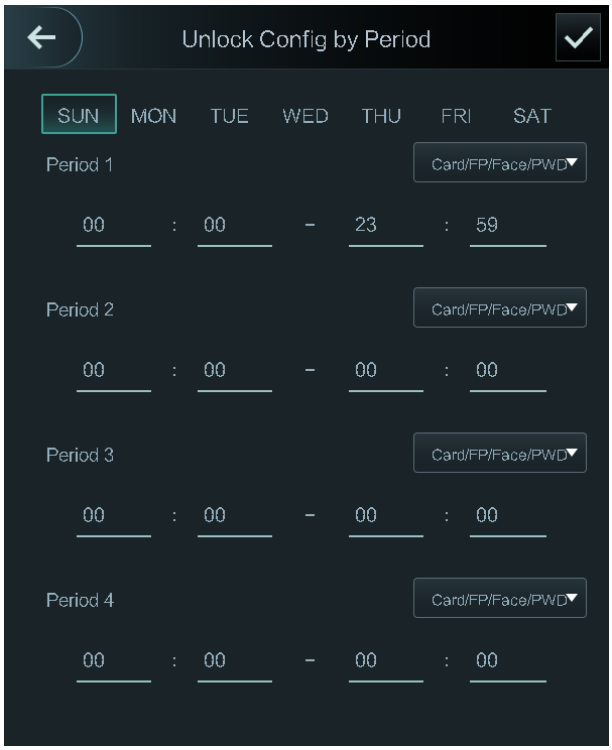
- significa habilitado.
- significa no habilitado.

3.8.2.2 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 mediante tarjeta; y en el período 2, las puertas solo se pueden desbloquear mediante contraseña.

Step 1 Seleccione **Acceso> Modo de desbloqueo> Desbloqueo por período**.

Figure 3-8 Desbloquear por período



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

Step 3 Toque para guardar la configuración.

Step 4 Habilite el **Desbloquear por período** función.

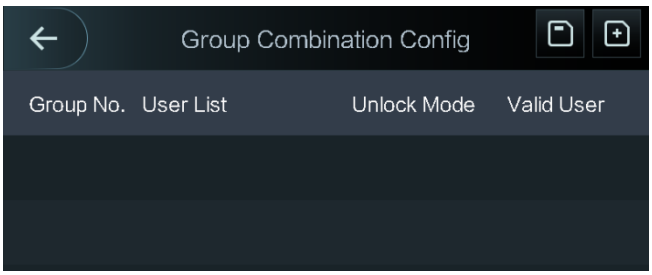
- ON significa habilitado.
- OFF significa no habilitado.

3.8.2.3 Combinación de grupos

Las puertas solo pueden ser desbloqueadas por un grupo o grupos que constan de más de dos usuarios si el **Combinación de grupo** está habilitado.

Step 1 Seleccione **Acceso> Modo de desbloqueo> Combinación de grupo**.

Figure 3-9 Combinación de grupo



Step 2 Grifo para crear un grupo.

Figure 3-10 Agregar un grupo

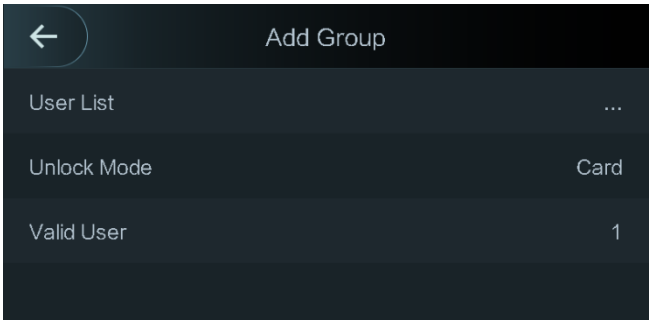


Tabla 3-4 Parámetro de grupo

Parámetro	Descripción
Lista de usuarios	Agregue usuarios al grupo recién creado. 1. Toque **Lista de usuarios**. 2. Toque y luego ingrese una ID de usuario. para 3. Grifo guardar la configuración.
Modo de desbloqueo	Hay dos opciones: **PWD** y **Cara**.
Usuario válido	Los usuarios válidos son los que tienen permiso de desbloqueo. Las puertas se pueden desbloquear solo cuando el número de usuarios para abrir 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, las puertas solo pueden ser desbloqueadas por todos los usuarios del grupo. ● Si los usuarios válidos son menores que el número total de usuarios en un grupo, las puertas pueden ser desbloqueadas por cualquier usuario cuyo número sea igual al número de usuario válido.

Step 3 Grifo para volver a la interfaz anterior.

Step 4 Grifo para guardar la configuración.

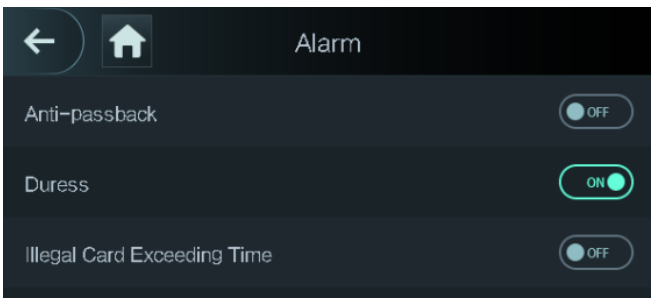
Step 5 Habilite la combinación de grupos.

- significa habilitado.
- significa no habilitado.

3.8.3 Configuración de alarma

Los administradores pueden gestionar el permiso de desbloqueo de visitantes a través de la configuración de alarmas. Seleccione**Acceso> Alarma**.

Figure 3-11 Alarma



- significa habilitado.

-  significa no habilitado.

Tabla 3-5 Parámetros en la interfaz de alarma

Parámetro	Descripción
Anti-passback	Una vez habilitado el anti-passback, los usuarios deben verificar las identidades tanto para la entrada como para la salida; de lo contrario, se activará una alarma. ● Si una persona entra con la identidad verificada y sale sin la identidad verificada, se activará una alarma cuando la persona intente ingresar nuevamente y la persona ya no tendrá permiso para abrir la puerta. Si una persona ingresa sin verificar la identidad, se activará una alarma. cuando la persona intente salir con la identidad verificada, y la persona ya no tendrá permiso para abrir la puerta.
Coacción	Después de habilitar la función de coacción, se activará una alarma cuando se utilice una tarjeta de coacción o una contraseña de coacción para desbloquear la puerta.
Tarjeta ilegal Excesivo Tiempo	Después de que se utilice una tarjeta no autorizada para desbloquear la puerta más de 5 veces en 50 segundos, se activará una alarma.

3.8.4 Estado de la puerta

Hay tres opciones: **NO**, **CAROLINA DEL NORTE**, y **Normal**.

- NO: Si **NO** está seleccionado, la puerta permanece abierta, lo que significa que la puerta nunca se cerrará. NC: Si
- **CAROLINA DEL NORTE** está seleccionado, la puerta permanece cerrada, lo que significa que la puerta no se
- desbloqueará. Normal: si se selecciona Normal, la puerta se desbloqueará y bloqueará según su configuración.

3.8.5 Bloqueo de tiempo de retención

Bloquear tiempo de espera es la duración en la que se desbloquea la cerradura. Si el candado se ha desbloqueado por un período que excede la duración, el candado se bloqueará automáticamente.

3.9 Red de comunicacion

Para que el terminal funcione con normalidad, debe configurar los parámetros para la red, los puertos serie y los puertos Wiegand.

3.9.1 Dirección IP

3.9.1.1 Configuración de IP

Configure una dirección IP para que el terminal se conecte a la red.

Figure 3-12 Configuración de la dirección IP

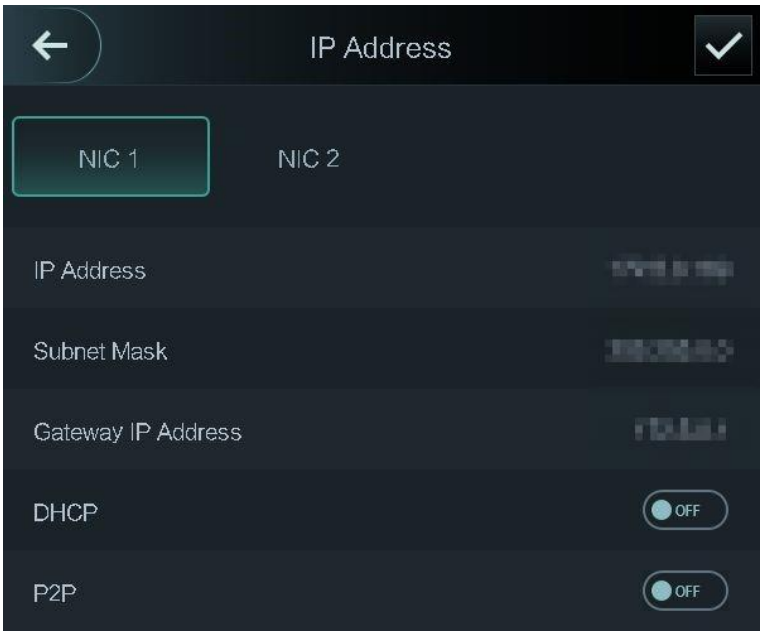


Tabla 3-6 Parámetros de configuración de IP

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

- Asegúrese de que la computadora utilizada para iniciar sesión en la web esté en la misma LAN que el dispositivo. Los
- terminales del modelo X de 7 pulgadas tienen NIC duales. La dirección de administración predeterminada para ETH1 es 192.168.1.108 y para ETH2 es 192.168.2.108.

3.9.1.2 Registro activo

Al registrarse activamente, 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 administración y el terminal se puede inicializar; debe proteger el permiso de administración de la plataforma en caso de pérdida de datos causada por un funcionamiento incorrecto.

Tabla 3-7 Parámetro de registro activo

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

3.9.1.3 Wi-Fi

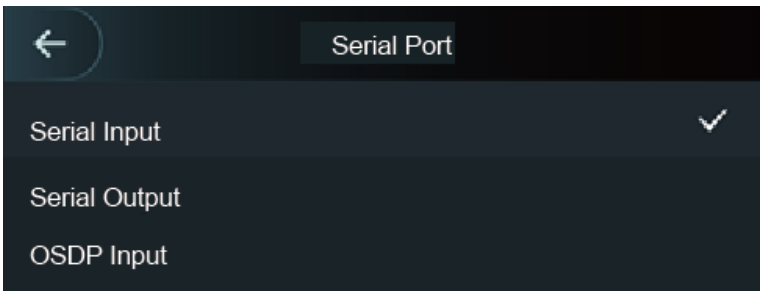
Puede conectar el terminal a la red a través de Wi-Fi si el terminal tiene función Wi-Fi.

3.9.2 Configuración del puerto serie

Seleccione la entrada en serie o la salida en serie de acuerdo con el uso de los dispositivos externos.

Seleccione**Conexión> Puerto serie**.

Figure 3-13 Puerto serial



- Seleccione **Entrada serial** cuando los dispositivos externos que tienen funciones de lectura y escritura de tarjetas están conectados al terminal. **Entrada serial** se selecciona para permitir que la información de la tarjeta de acceso se envíe al terminal y la plataforma de gestión.
- Cuando **Entrada serial** se selecciona 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, el 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, lectura y escritura de tarjetas, si selecciona **Salida serial**, el terminal enviará información de bloqueo / desbloqueo al terminal. Hay dos tipos de información de bloqueo / desbloqueo:
  - ◇ ID de usuario
  - ◇ Tarjeta No.
- 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.

3.9.3 Configuración Wiegand

Seleccione **Entrada Wiegand** o **Salida Wiegand**

respectivamente. Seleccione**Conexión> Wiegand**.

Figure 3-14 Wiegand

- Seleccione **Entrada Wiegand** cuando un mecanismo de deslizamiento de tarjeta externo está conectado al terminal.
- Cuando **Entrada serial** se selecciona 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, el 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 terminal.

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 configurar el ancho de pulso y el intervalo de pulso.
Intervalo de pulso	
Tipo de datos de salida	Puede seleccionar los tipos de datos de salida. ● ID de usuario: si se selecciona ID de usuario, se generará la ID de usuario. Número ● de tarjeta: si se selecciona el número de tarjeta, se emitirá el número de tarjeta.

3.10 Sistema

3.10.1 Hora

Puede realizar la configuración del formato de fecha, la configuración de la fecha, la configuración de la hora, la configuración de DST, la verificación de NTP, la configuración de la zona horaria.

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

3.10.2 Parámetro de cara

Figure 3-15 Parámetro de cara

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

Tabla 3-9 Parámetro de cara

Nombre	Descripción
Reconocimiento facial Umbral	Se puede ajustar la precisión del reconocimiento facial. Cuanto mayor sea el valor, mayor será la precisión.
Max. Ángulo de la cara	Configure el ángulo de disparo de los perfiles del panel de control. Cuanto mayor sea el valor

Nombre	Descripción
Reconocimiento	es decir, se reconocerá la gama más amplia de perfiles.
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 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.
Tiempo de espera de reconocimiento (S)	Cuando una persona que no tiene el permiso de acceso se para frente al controlador de acceso y consigue que se reconozca la cara, el controlador indicará que el reconocimiento facial falló. El intervalo de solicitud se denomina tiempo de espera de reconocimiento.
Mensaje de rostro no válido Intervalo (S)	Cuando un rostro no tiene permiso de acceso se coloca frente al controlador de acceso, el controlador indicará que el rostro no es válido. El intervalo de aviso es un intervalo de aviso de rostro no válido.
Umbral anti-falsificación	Esta función evita que las personas se desbloqueen mediante imágenes de rostros humanos o modelos de rostros.
Parámetros de temperatura	Establezca si desea habilitar la monitorización de la temperatura corporal. ● Unidad de temperatura: seleccione una unidad de temperatura. ● Temp Rect: establezca si se muestra el cuadro de control de temperatura o no. ● Distancia de monitorización de temperatura (cm): el valor predeterminado es 0. Configure otros valores para habilitar el monitoreo de temperatura dentro de una distancia definida. Se recomiendan 80 cm. ● Umbral de temperatura (° C): establezca el umbral de temperatura. La temperatura corporal monitoreada se considerará alta si es mayor o igual al valor establecido. ● Valor de corrección de temperatura: este parámetro es para pruebas. La diferencia del entorno de monitoreo de temperatura puede causar la desviación de temperatura entre la temperatura monitoreada y la temperatura real. Puede seleccionar varias muestras monitoreadas para la prueba y luego corregir la desviación de temperatura con este parámetro de acuerdo con la comparación entre la temperatura monitoreada y la temperatura real. Por ejemplo, si la temperatura monitoreada es 0.5 ° C más baja que la temperatura real, el valor de corrección se establece en 0.5 ° C; si la temperatura monitoreada es 0.5 ° C más alta que la temperatura real, el valor de corrección se establece en -0.5 ° C. Solo el controlador de acceso con una unidad de monitoreo de temperatura admite este parámetro.
Parámetros de máscara	● Sin detección: la máscara no se detecta durante el reconocimiento facial. ● Recordatorio de máscara: la máscara se detecta durante el reconocimiento facial. Si la persona es detectada sin usar una máscara, el sistema le recordará la máscara y se permitirá el paso. ● Intercepción de máscara: la máscara se detecta durante el reconocimiento facial. Si el

Nombre	Descripción
	La persona es detectada sin usar una máscara, el sistema le avisará como recordatorio de la máscara y no se permitirá el paso.

3.10.3 Modo de imagen

Hay tres opciones:

- Interior: Seleccionar **Interior** cuando el controlador de acceso está instalado en el interior;
- Exterior: Seleccionar**Exterior** cuando el controlador de acceso está instalado al aire libre;
- Otro: Seleccione **Otro** cuando el controlador de acceso se instala en lugares con luz de fondo como pasillos y pasillos.

3.10.4 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 es oscuro, la luz de relleno permanece apagada; de lo contrario, la luz de relleno estará encendida.
- NO: La luz de relleno permanece abierta. NC:
- La luz de relleno permanece cerrada.

3.10.5 Ajuste de brillo de la luz de relleno

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

3.10.6 Ajuste de volumen

Puede ajustar los pitidos y el volumen de la voz.

Step 1 Seleccione **Sistema> Volumen**.

Step 2 Seleccione **Volumen del pitido** o **Volumen del micrófono** según sea necesario.

Step 3 Grifo  o  para ajustar el volumen.

3.10.7 Ajuste del brillo de la luz IR

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

3.10.8 Restaurar la configuración de fábrica

- Los datos se perderán si restaura el terminal a la configuración de fábrica.
- Una vez que el terminal se restaure a la configuración de fábrica, la dirección IP no se cambiará.

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

3.10.9 Reiniciar

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

3.11 USB

⚠

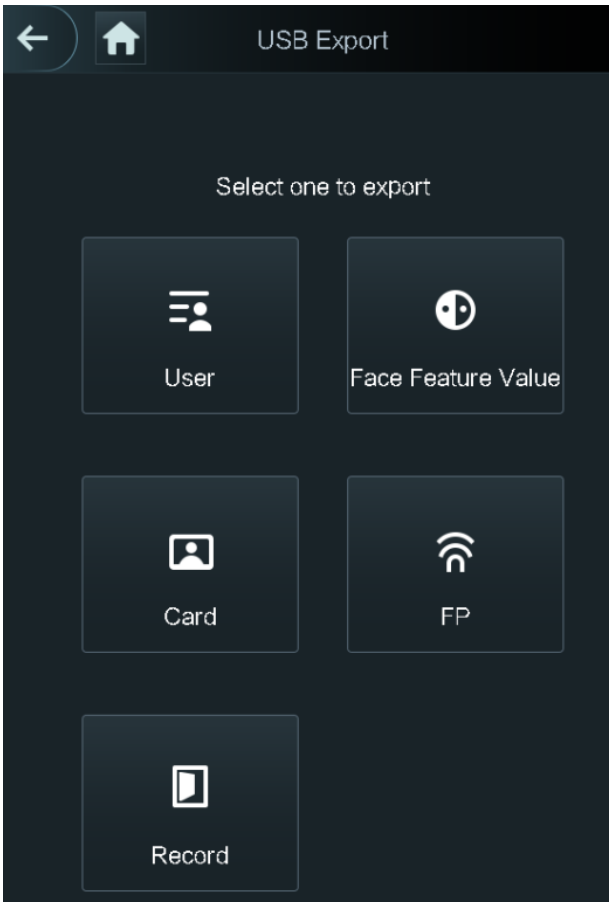
- Asegúrese de que el USB esté insertado antes de exportar la información del usuario y actualizar. Durante la exportación o actualización, no extraiga el USB ni realice otras operaciones; de lo contrario, la exportación o la actualización fallarán.
- Debe importar información de un terminal al USB antes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

3.11.1 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.

Step 1 Seleccione **USB> Exportación USB**.

Figure 3-16 Exportación USB



Step 2 Seleccione el tipo de datos que desea exportar.

Step 3 Grifo**OK**.

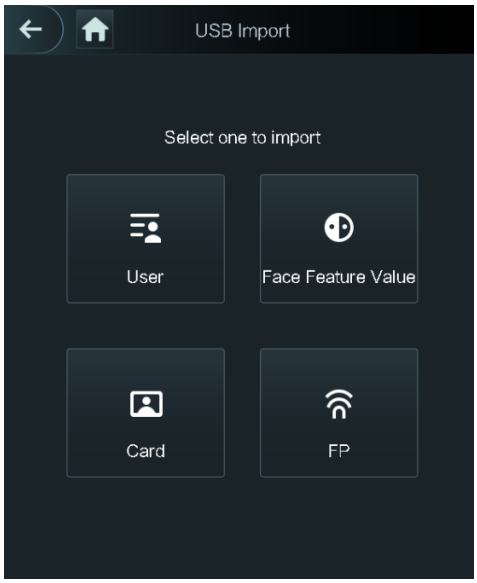
Los datos exportados se guardarán en el USB.

3.11.2 Importación USB

Solo los datos de la unidad flash USB que se exportaron desde un terminal se pueden importar a otro terminal.

Step 1 Seleccione **USB> Importación USB**.

Figure 3-17 Importación USB



Step 2 Seleccione el tipo de datos que desea importar.

Step 3 Grifo**OK**.

Los datos de la unidad flash USB se importarán al terminal.

3.11.3 Actualización USB

Se puede utilizar una unidad flash USB para actualizar el sistema.

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

Step 2 Seleccione **USB> Actualización USB**.

Step 3 Grifo**OK**.

La actualización comienza y el terminal se reiniciará después de que finalice la actualización.

3.11.4 Funciones

Puede realizar configuraciones sobre privacidad, número de tarjeta inverso, módulo de seguridad, tipo de sensor de puerta y retroalimentación de resultados. Para obtener detalles de las funciones mencionadas.

Figure 3-18 Características

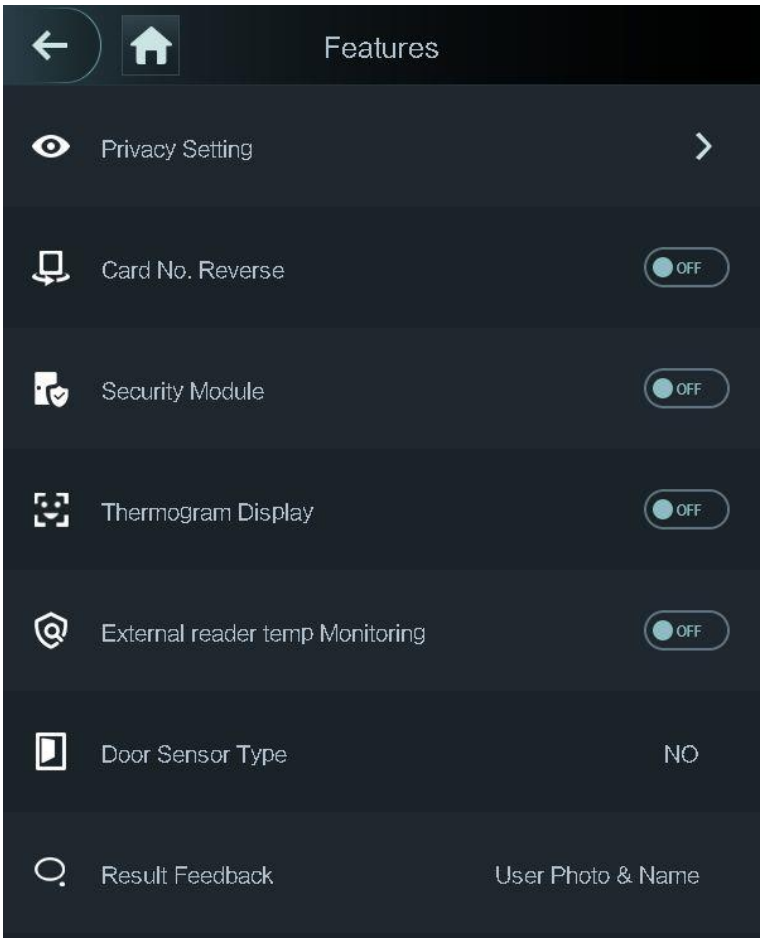


Tabla 3-10 Descripción de funciones

Parámetro	Descripción
Configuración de privacidad	Consulte la Figura 3-19 para obtener más detalles.
Número de tarjeta reverso	Si el lector de tarjetas de terceros debe conectarse al controlador de acceso a través del puerto de salida wiegand, debe habilitar la función de reverso de número de tarjeta; de lo contrario, la comunicación entre el controlador de acceso 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 independiente 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.
Pantalla de termograma	Muestre un mapa de calor en la esquina superior izquierda.
Lector externo Monitoreo de temperatura	Enciéndalo y se controlará la temperatura de la persona cuando pase la tarjeta.
Tipo de sensor de puerta	Hay dos opciones: **NO** y **CAROLINA DEL NORTE**.
Comentarios de resultados	Muestra si el desbloqueo se realizó correctamente o no.

Figure 3-19 Configuración de privacidad

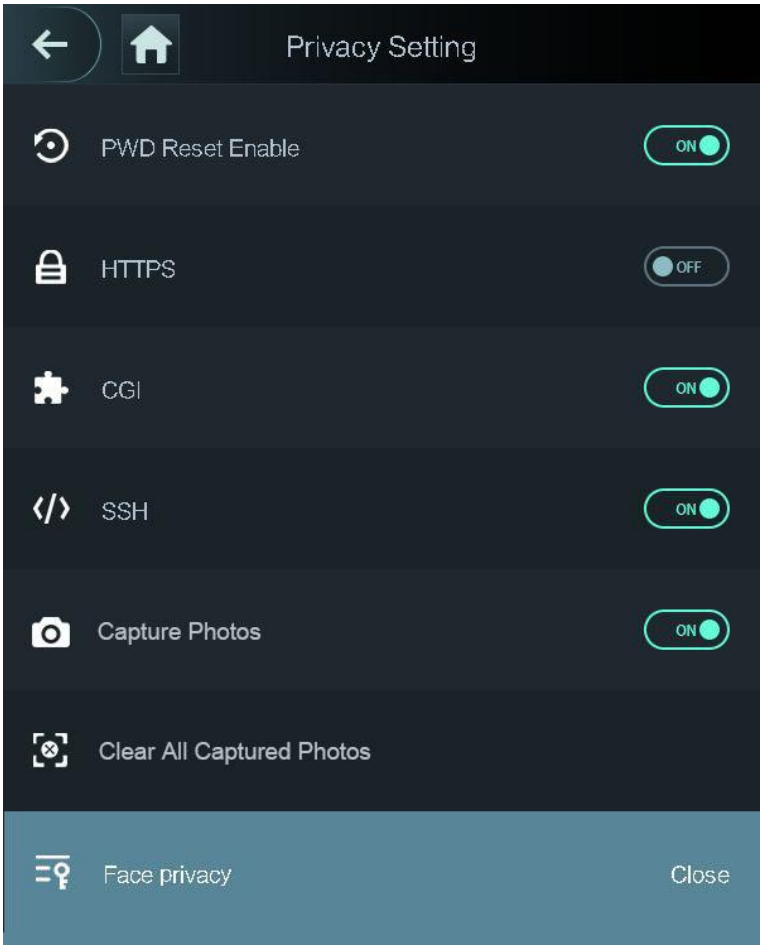


Tabla 3-11 Características

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

Parámetro	Descripción
FP	Si selecciona APAGADO para Huella dactilar (FP), la información de la huella dactilar de los usuarios no se mostrará cuando se registren las huellas dactilares o cuando usen huellas dactilares para desbloquear la puerta.
Capturar Foto	Si selecciona ON, cuando un usuario desbloquea 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.
Privacidad facial	Establezca diferentes niveles para difuminar la interfaz de espera.

Cuando HTTPS está habilitado, el terminal se reiniciará automáticamente.

3.11.5 Comentarios de resultados

Puede seleccionar un modo de retroalimentación de resultados según sea necesario. Seleccione**Funciones> Comentarios de resultados**.

Foto y nombre

Figure 3-20 Foto y nombre

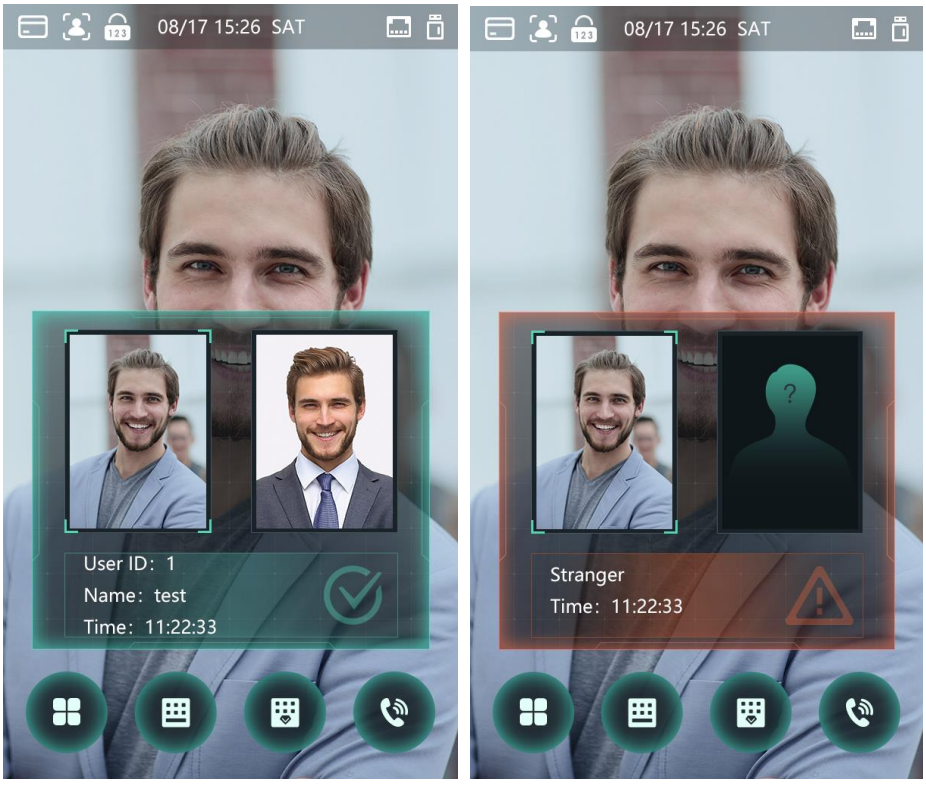
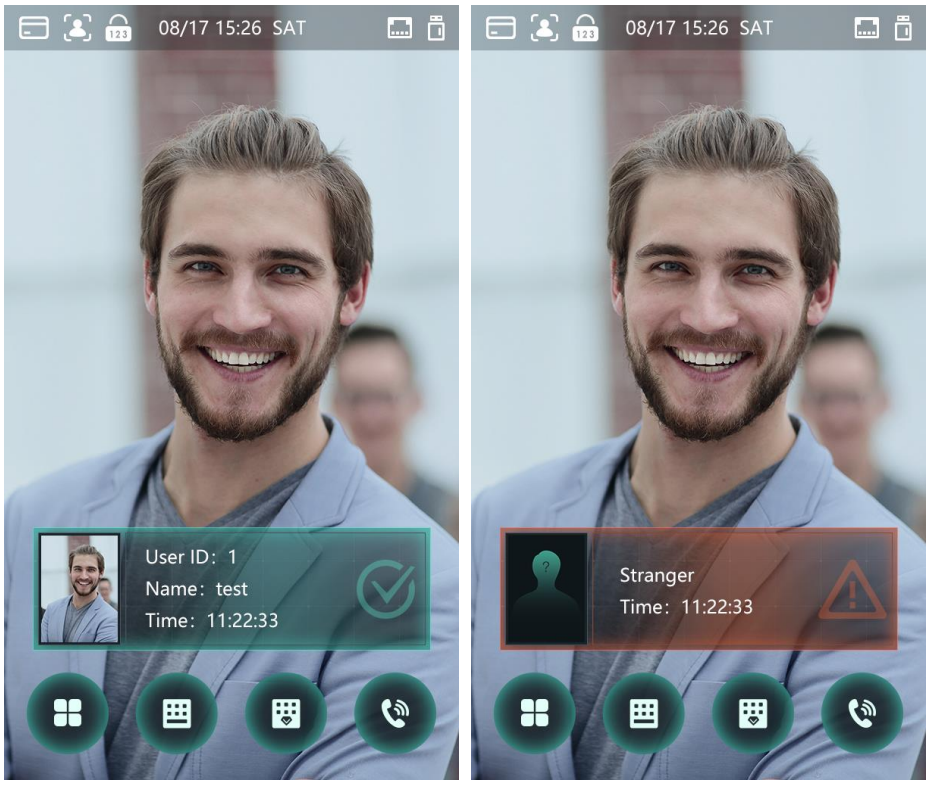


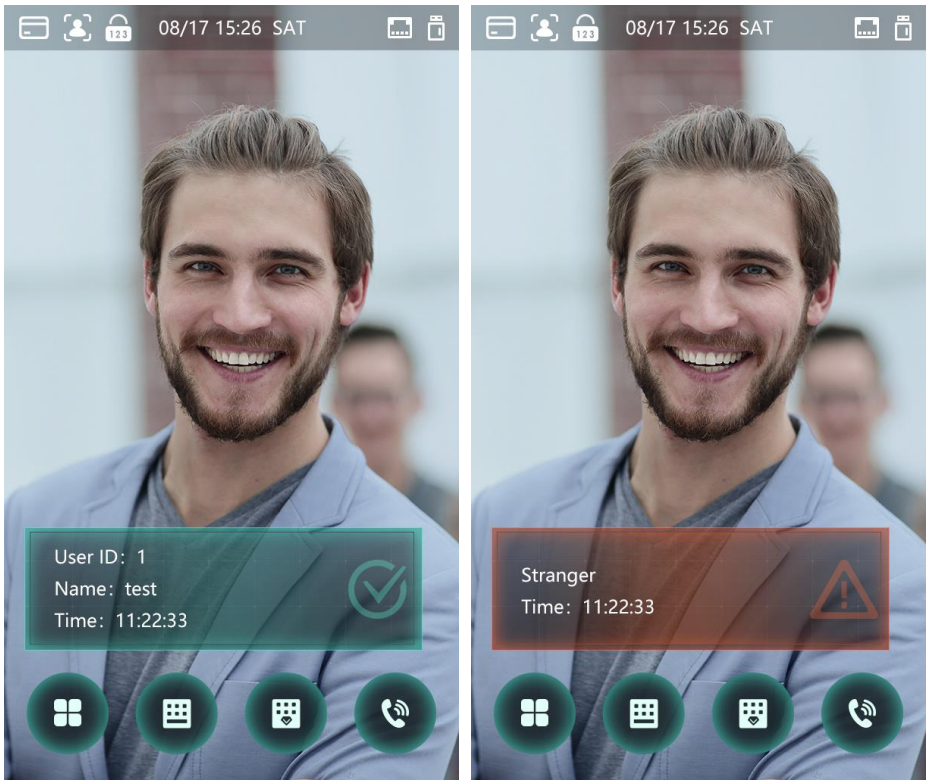
Foto y nombre de usuario

Figure 3-21 Nombre y foto de usuario



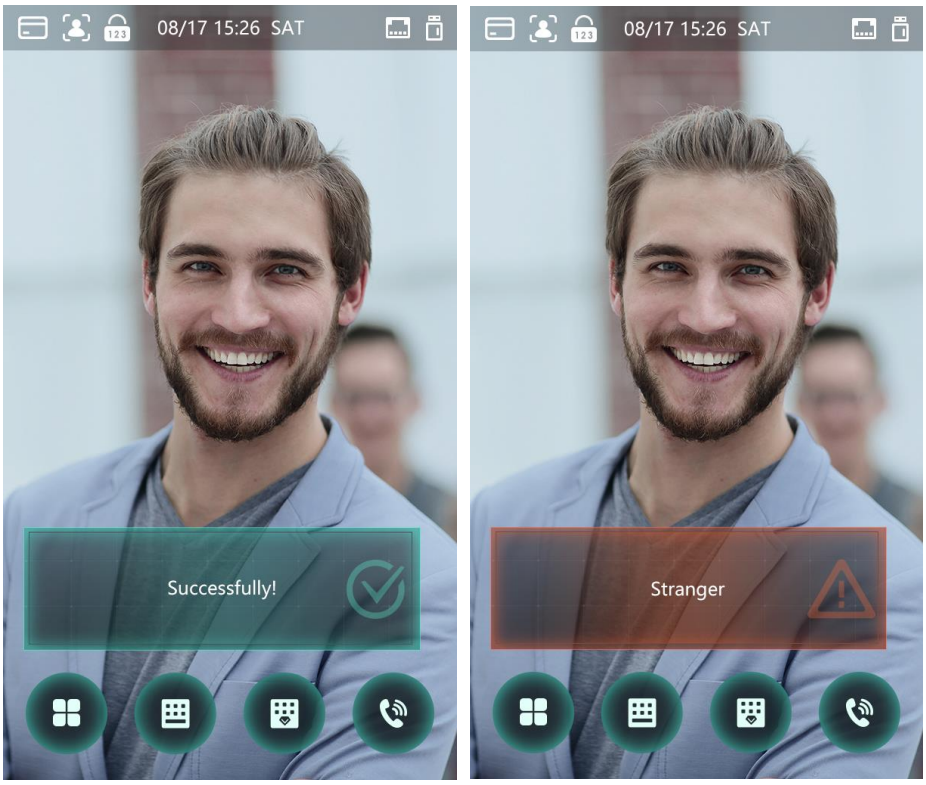
Solo nombre

Figure 3-22 Solo nombre



Éxito o fracaso

Figure 3-23 Éxito o fracaso



3.12 Registro

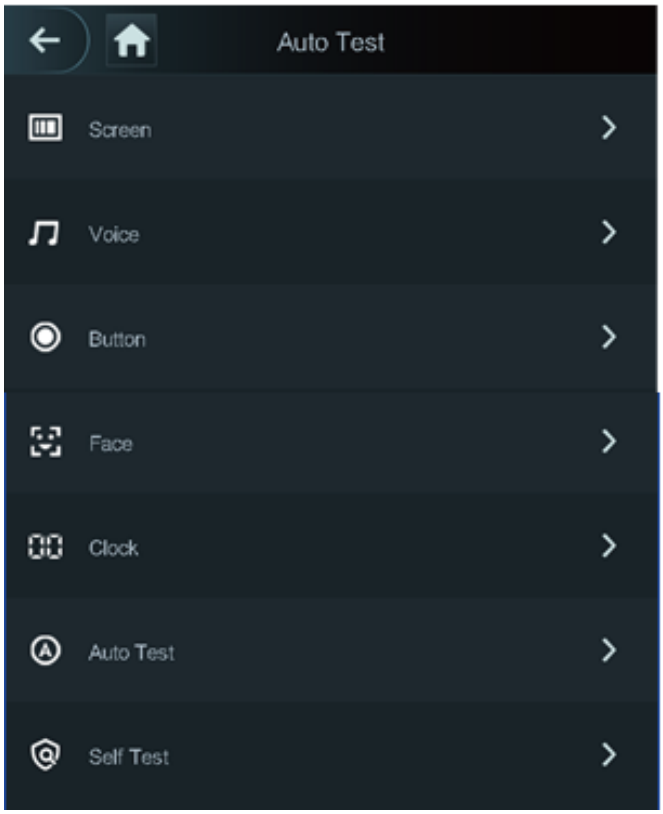
Puede consultar todos los registros de desbloqueo.

Figure 3-24 Buscar registros de perforaciones

3.13 Auto prueba

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

Figure 3-25 Auto prueba



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

3.14 Información del sistema

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

4 Operaciones web

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

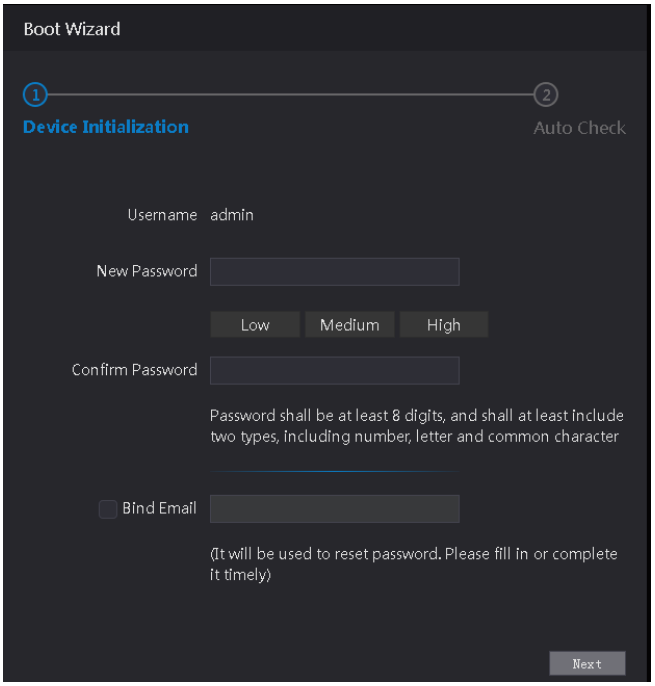
4.1 Inicialización

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

Step 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.

- Utilice un navegador más reciente que IE 8; de lo contrario, es posible que no inicie sesión en la web. Asegúrese de
- que la computadora utilizada para iniciar sesión en la web esté en la misma LAN que el dispositivo.
- Los terminales modelo X de 7 pulgadas tienen dos NIC. La dirección IP predeterminada para ETH1 es 192.168.1.108 y para ETH2 es 192.168.2.108.

Figure 4-1 Inicialización



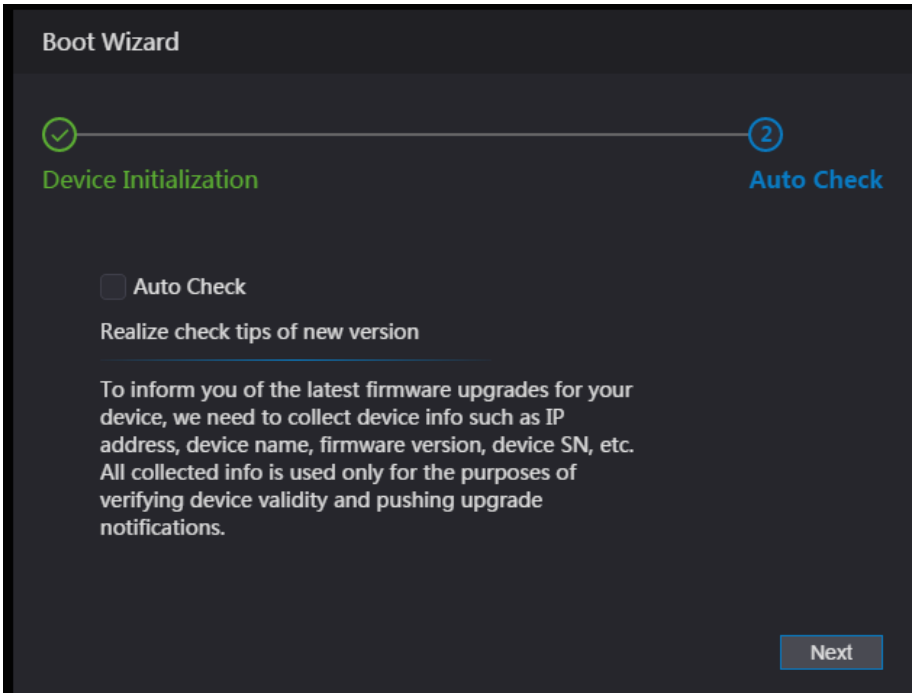
Step 2 Ingrese la nueva contraseña, confirme la contraseña, ingrese una dirección de correo electrónico y luego haga clic en **próximo**.

- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo '";: &). Establezca una contraseña de alto nivel de seguridad según la solicitud de seguridad de la contraseña.
- Por seguridad, mantenga la contraseña correctamente después de la inicialización y cámbiela con regularidad.

- Cuando necesite restablecer la contraseña de administrador escaneando el código QR, necesita una dirección de correo electrónico para recibir el código de seguridad.

Step 3 Hacer clic **próximo**.

Figure 4-2 Verificación automática

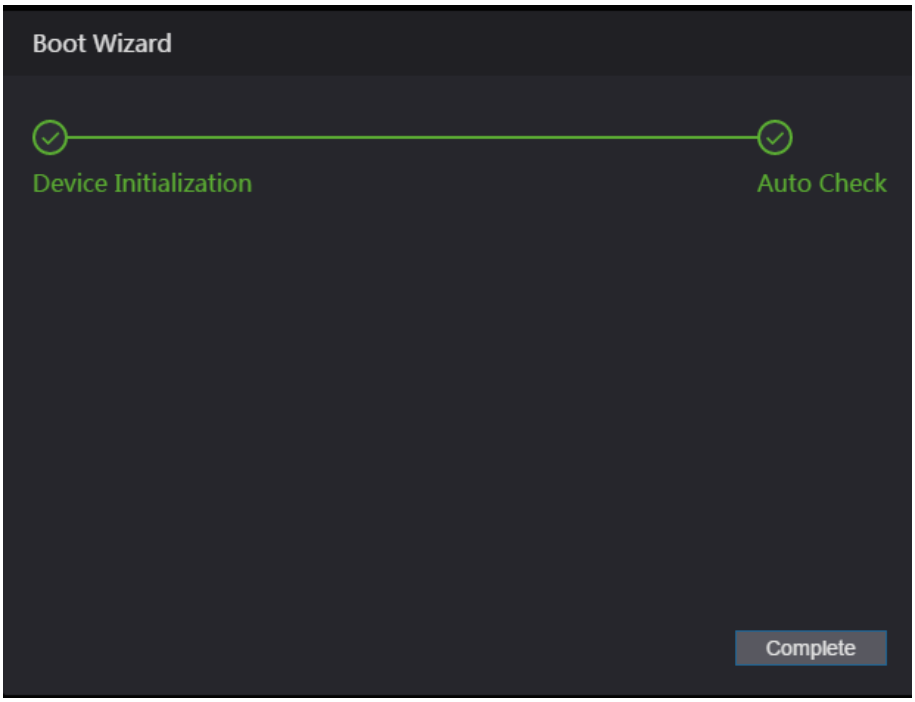


Step 4 Puede decidir si desea seleccionar **Verificación automática** o no.

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

Step 5 clic**próximo**.

Figure 4-3 Verificación automática completada



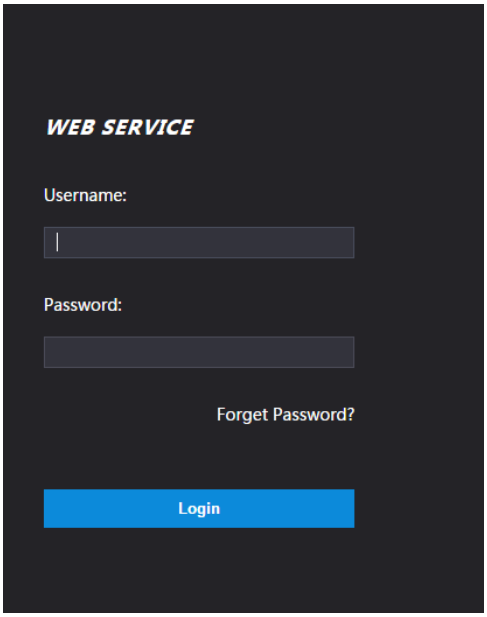
Step 6 Hacer clic **Completo**y se completa la inicialización.

4.2 Acceso

Step 1 Abra el navegador web IE, ingrese la dirección IP del terminal en la barra de direcciones y presione Enter.

- Utilice un navegador más reciente que IE 8; de lo contrario, es posible que no inicie sesión en la web. Asegúrese de
- que la dirección IP de la computadora utilizada para iniciar sesión en la web esté en la misma LAN que el terminal.
- Los terminales modelo X de 7 pulgadas tienen dos NIC. La dirección IP predeterminada para ETH1 es 192.168.1.108 y para ETH2 es 192.168.2.108.

Figure 4-4 Acceso



Step 2 Ingrese el nombre de usuario y la contraseña.

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

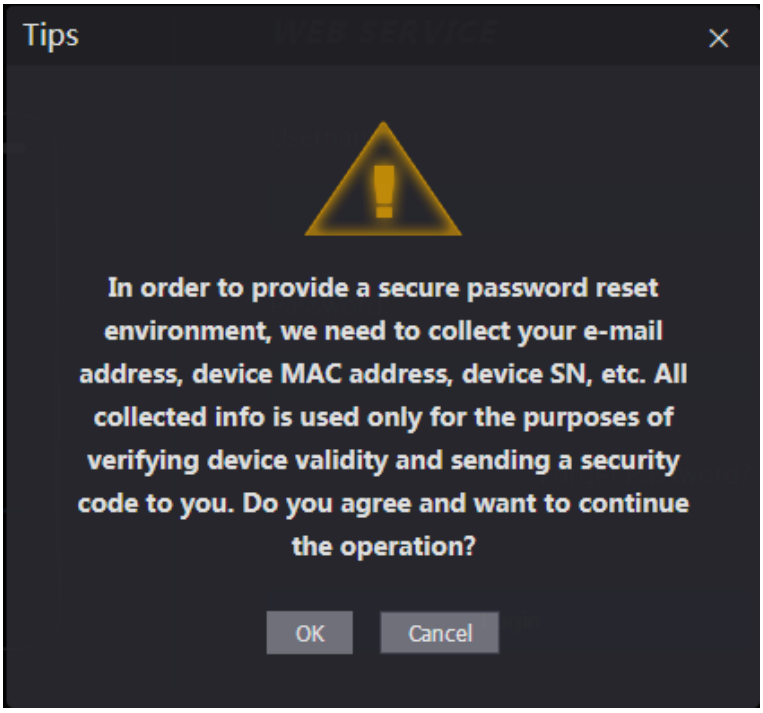
Step 3 Hacer clic **Acceso**.

4.3 Restablecimiento de la contraseña

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

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

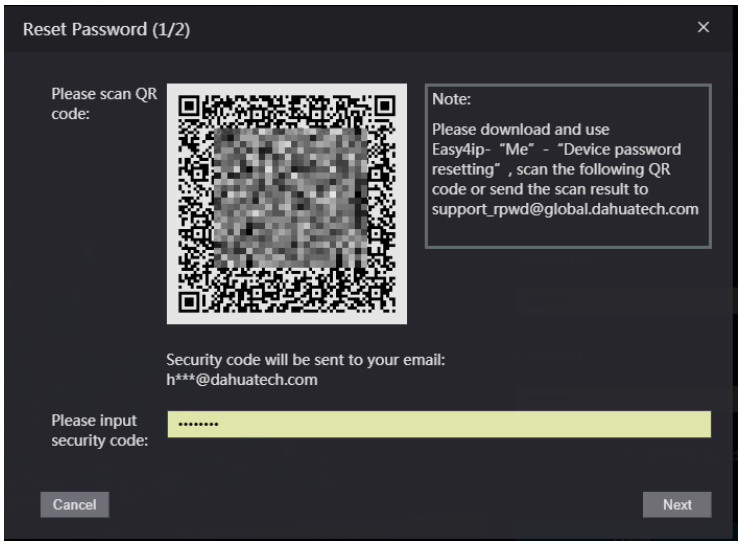
Figure 4-5 Consejos



Step 2 Lea los consejos.

Step 3 Hacer clic **OK**.

Figure 4-6 Restablecer la contraseña



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

- Se generarán como máximo dos códigos de seguridad escaneando el mismo código QR. Para obtener más código de seguridad, actualice el código QR.
- Debe enviar el contenido que obtiene después de escanear el código QR a la dirección de correo electrónico designada, y luego obtendrá el código de seguridad.
- Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, dejará de ser válido.
- Si se ingresan códigos de seguridad incorrectos cinco veces consecutivas, el administrador quedará congelado durante cinco minutos.

Step 5 Ingrese el código de seguridad que ha recibido. Hacer

Step 6 clic**próximo**.

Step 7 Restablezca y confirme la nueva contraseña.

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

Step 8 Hacer clic **OK**y se completa el reinicio.

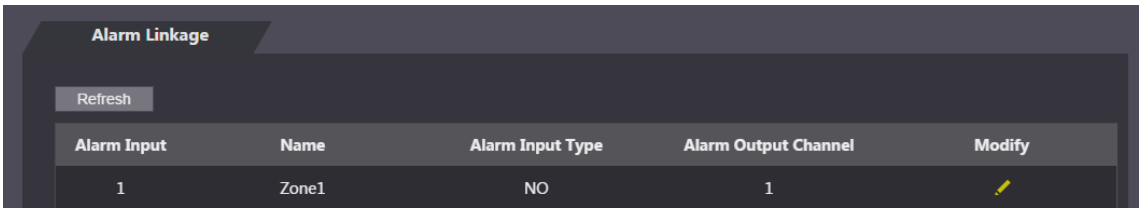
4.4 Enlace de alarma

4.4.1 Configuración del enlace de alarma

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

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

Figure 4-7 Enlace de alarma



Step 2 Hacer clic y, a continuación, puede modificar los parámetros de vinculación de alarmas.

Figure 4-8 Modificación del parámetro de vinculación de alarmas

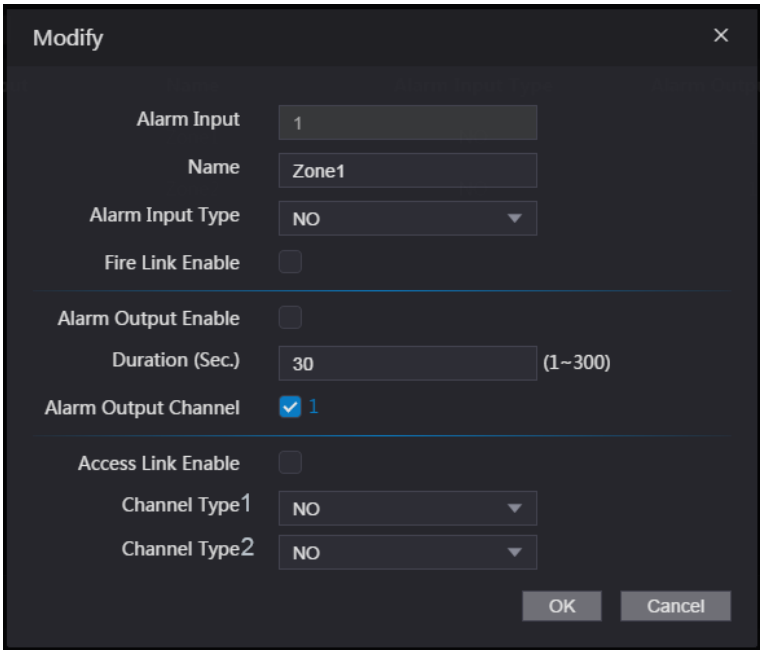


Tabla 4-1 Descripción de los parámetros de vinculación de alarmas

Parámetro	Descripción
Entrada de alarma	No puede modificar el valor. Manténgalo predeterminado.
Nombre	Ingrese un nombre de zona.
Tipo de entrada de alarma	Hay dos opciones: NO y NC.

Parámetro	Descripción
	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.
Activar 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 de forma predeterminada 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.
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 **CAROLINA DEL NORTE**.

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

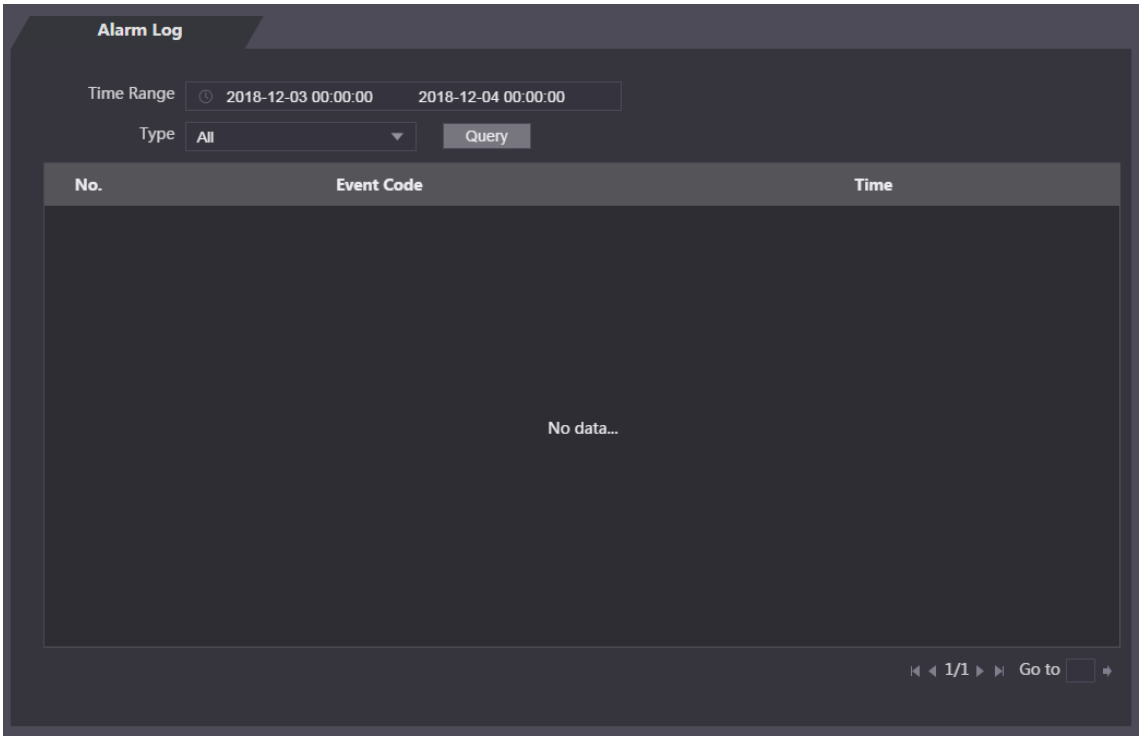
La configuración en la web se sincronizará con la configuración en el cliente si el terminal se agrega a un cliente.

4.4.2 Registro de alarmas

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

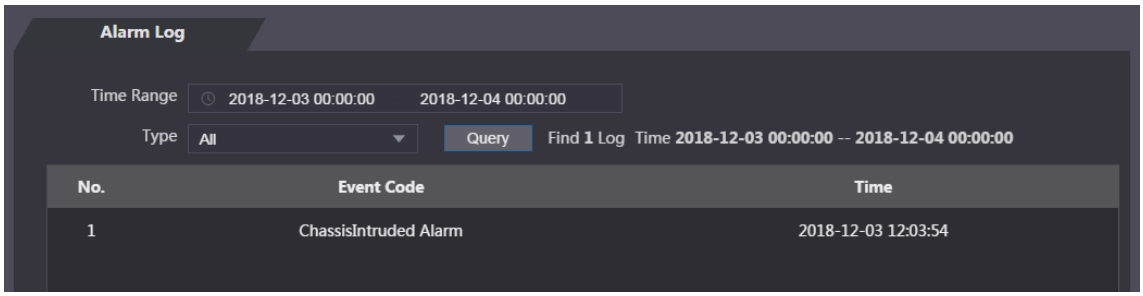
Step 1 Seleccione **Enlace de alarmas> Registro de alarmas**.

Figure 4-9 Registro de alarmas



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

Figure 4-10 Resultados de la consulta



4.5 Configuración de llamada

El controlador de acceso puede funcionar como una estación de puerta y llamar a otros dispositivos.

4.5.1 Configuración del controlador de acceso

Configure el tipo y número de dispositivo.

4.5.1.1 Controlador de acceso como servidor SIP

Step 1 Inicie sesión en la web.

Step 2 Seleccione **Configuración de Talkback>**

Step 3 **Local**. Configure los parámetros.

Figure 4-11 Local (1)

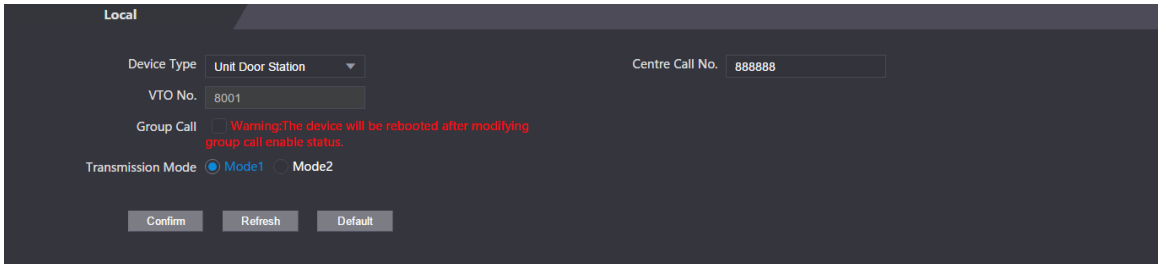


Tabla 4-2 Descripción de los parámetros

Parámetro	Descripción
Tipo de dispositivo	El controlador de acceso solo puede funcionar como una estación de puerta de unidad.
Número de llamada del centro	Ingrese un número para ser identificado por el centro de gestión. Debe ser "888888" más tres números.
VTO No.	No se puede configurar.
Llamada grupal	Cuando está habilitado, también se enviará una llamada desde el controlador de acceso a una estación interior maestra a todas sus estaciones interiores de extensión.
Transmisión Modo	● Mode1: Llamada en tiempo real, pero el video y el sonido pueden estar retrasados con una red deficiente. ● Mode2: No es una llamada en tiempo real, pero garantiza un video y sonido fluidos.

Step 4 Hacer clic **Confirmar**.

4.5.1.2 Otro dispositivo como servidor SIP

Step 1 Inicie sesión en la web.

Step 2 Seleccione **Configuración de Talkback>**

Step 3 **Local**. Configure los parámetros.

Figure 4-12 Local (2)

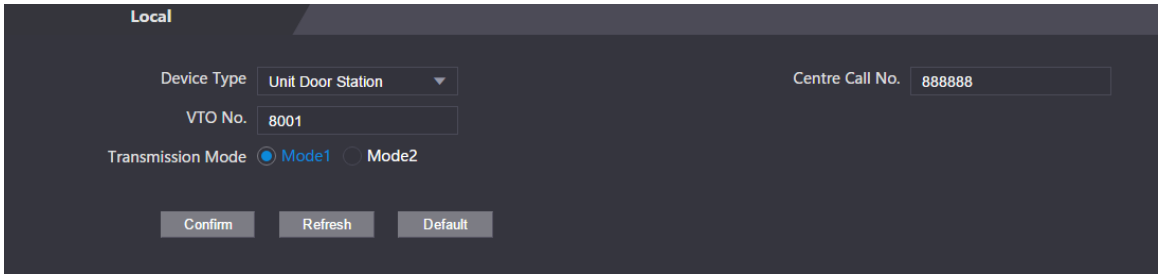


Tabla 4-3 Descripción de los parámetros

Parámetro	Descripción
Tipo de dispositivo	El controlador de acceso puede funcionar como una estación de puerta de la unidad o una estación de cerca.
Número de llamada del centro	Ingrese un número para ser identificado por el centro de gestión. Debe ser "888888" más tres números.
VTO No.	Ingrese un número para el controlador de acceso. - Debe tener cuatro dígitos. Los dos primeros deben ser 80 y los dos últimos comienzan con 01, como 8001. - Si hay varias estaciones de puerta, los números de VTO no pueden ser los mismos.
Transmisión Modo	● Mode1: Llamada en tiempo real, pero el video y el sonido pueden estar retrasados con una red deficiente. ● Mode2: No es una llamada en tiempo real, pero garantiza un video y sonido fluidos.

4.5.2 Servidor SIP

En la web, puede agregar estaciones de puerta y estaciones interiores al servidor SIP para que puedan comunicarse entre sí. El servidor SIP puede ser el controlador de acceso u otras estaciones de puerta.

Cuando el controlador de acceso funciona como servidor SIP, puede conectar hasta 50 controladores de acceso y monitores interiores combinados.

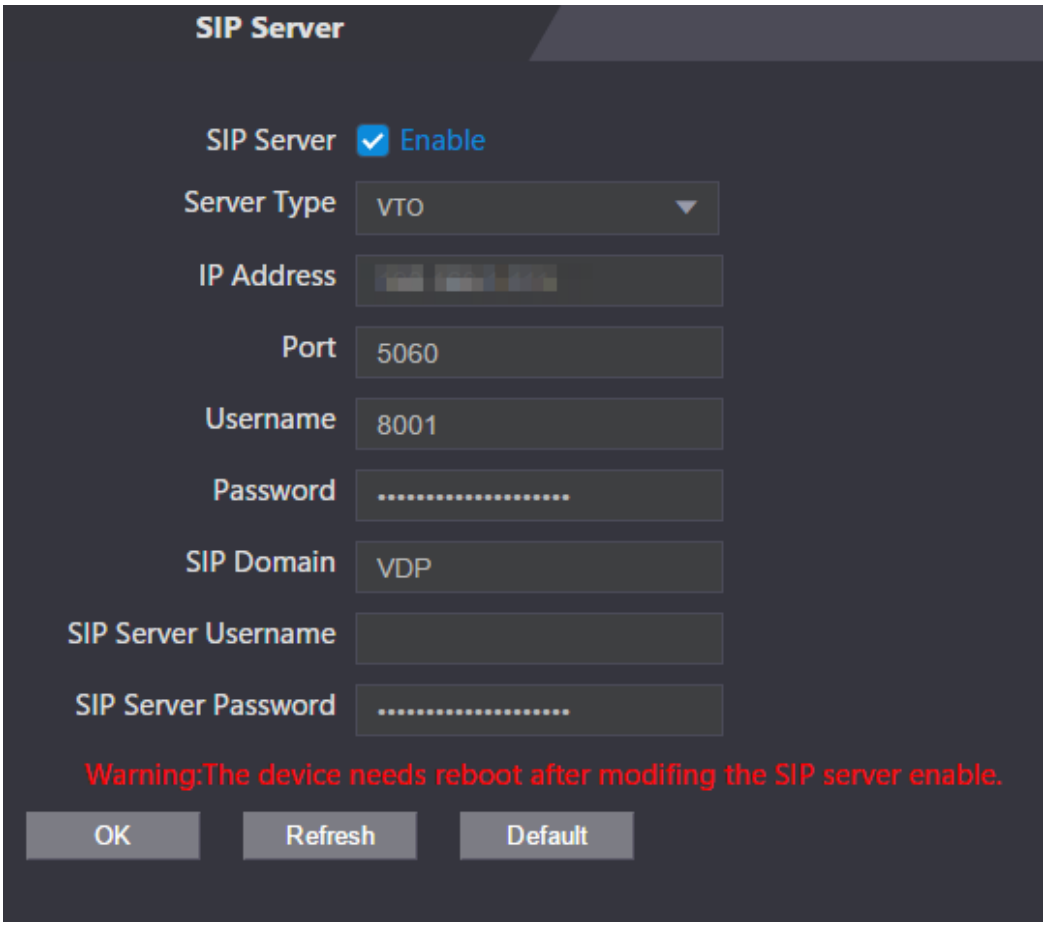
4.5.2.1 Controlador de acceso como servidor SIP

Step 1 Inicie sesión en la web.

Step 2 Seleccione **Configuración de Talkback> Servidor SIP**.

Step 3 Habilitar **Servidor SIP** y mantener otros parámetros por defecto.

Figure 4-13 Servidor SIP (1)



Step 4 Hacer clic **OK** y el controlador de acceso se reiniciará.

4.5.2.2 Otro dispositivo como servidor SIP

Step 1 Inicie sesión en la web.

Step 2 Seleccione **Configuración de Talkback> Servidor SIP**.

Step 3 No actives **Servidor SIP** y seleccione **Tipo de servidor** como VTO.

Step 4 Configure los parámetros.

Figure 4-14 Servidor SIP (2)

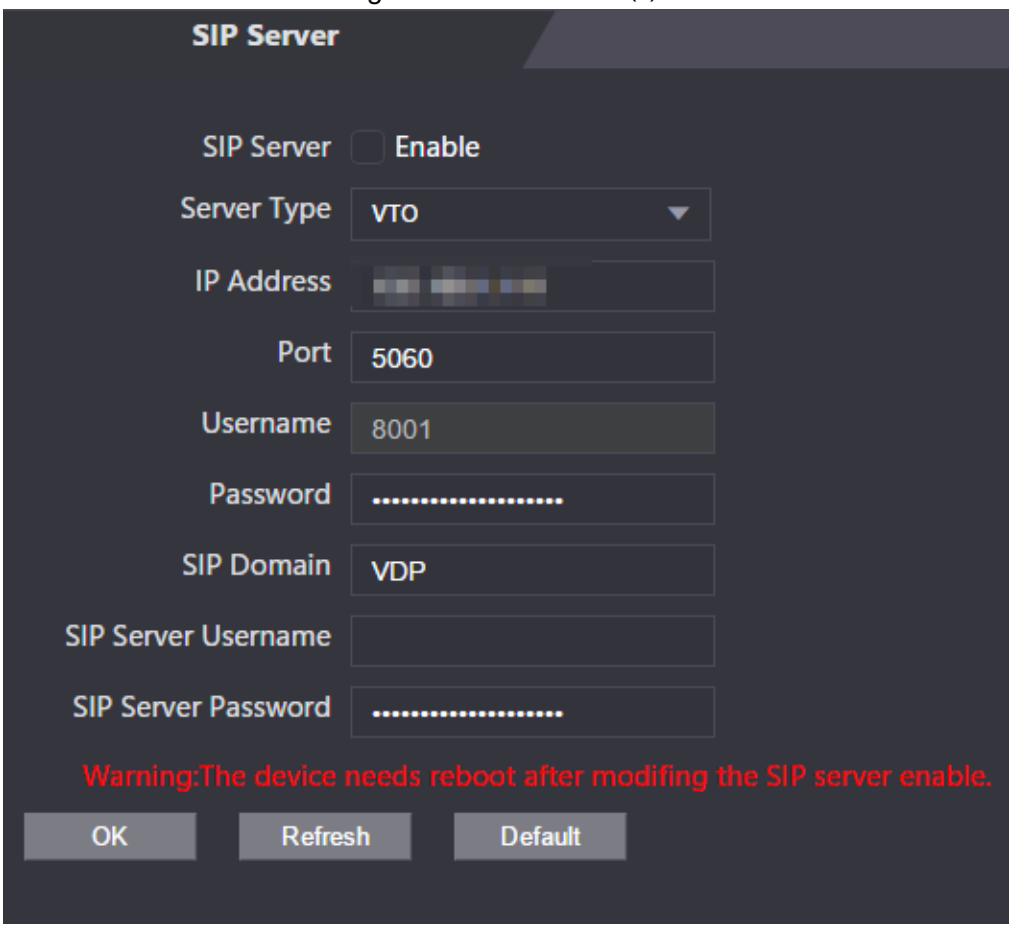


Tabla 4-4 Descripción de los parámetros del servidor SIP (1)

Parámetro	Descripción
Dirección IP	La dirección IP de la estación de puerta que funciona como servidor SIP.
Puerto	5060 por defecto.
Nombre de usuario	Mantenga los valores predeterminados.
Contraseña	
Dominio SIP	Debe ser VDP.
Servidor SIP Nombre de usuario	Nombre de usuario y contraseña de inicio de sesión del servidor SIP.
Servidor SIP Contraseña	

Step 5 Hacer clic **OK**.

4.5.3 Gestión de videoporteros

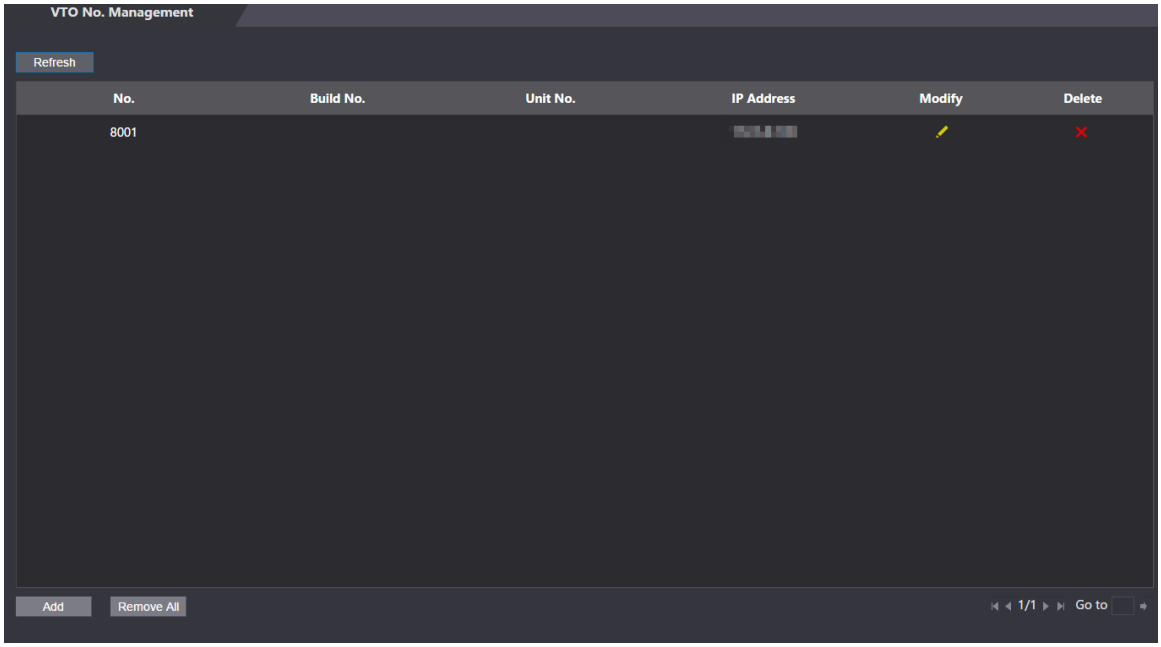
Cuando el controlador de acceso funciona como servidor SIP, agregue otras estaciones de puerta para llamarlos.

Step 1 Inicie sesión en la web.

Step 2 Seleccione **Configuración de Talkback> Gestión de números de VTO**. Hacer

Step 3 clic**Agregar**.

Figure 4-15 Gestión del número de VTO



Step 4 Configure los parámetros.

Figure 4-16 Agregar una estación de puerta

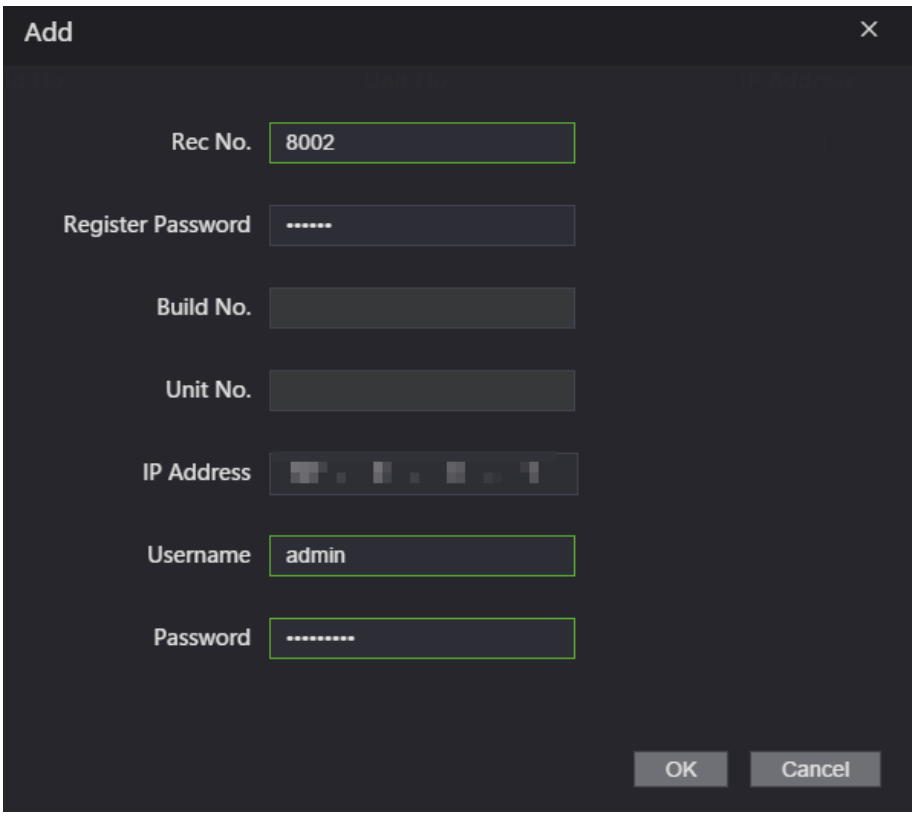


Tabla 4-5 Descripción de los parámetros

Parámetro	Descripción
Rec No.	Número de la estación de puerta.
Registrar contraseña	Conserva el valor predeterminado.
Construir No.	No se puede configurar.
Numero de unidad.	No se puede configurar.
Dirección IP	Dirección IP de la estación de puerta.

Parámetro	Descripción
Nombre de usuario	Nombre de usuario y contraseña de inicio de sesión web para la estación de puerta.
Contraseña	

Step 5 Hacer clic **OK**.

4.5.4 Gestión del monitor interior

Cuando el controlador de acceso funciona como servidor SIP, agregue todos los monitores interiores relevantes para llamarlos.

Cuando hay monitores interiores principales y de extensión, primero debe habilitar la función de llamada de grupo antes de agregarlos.

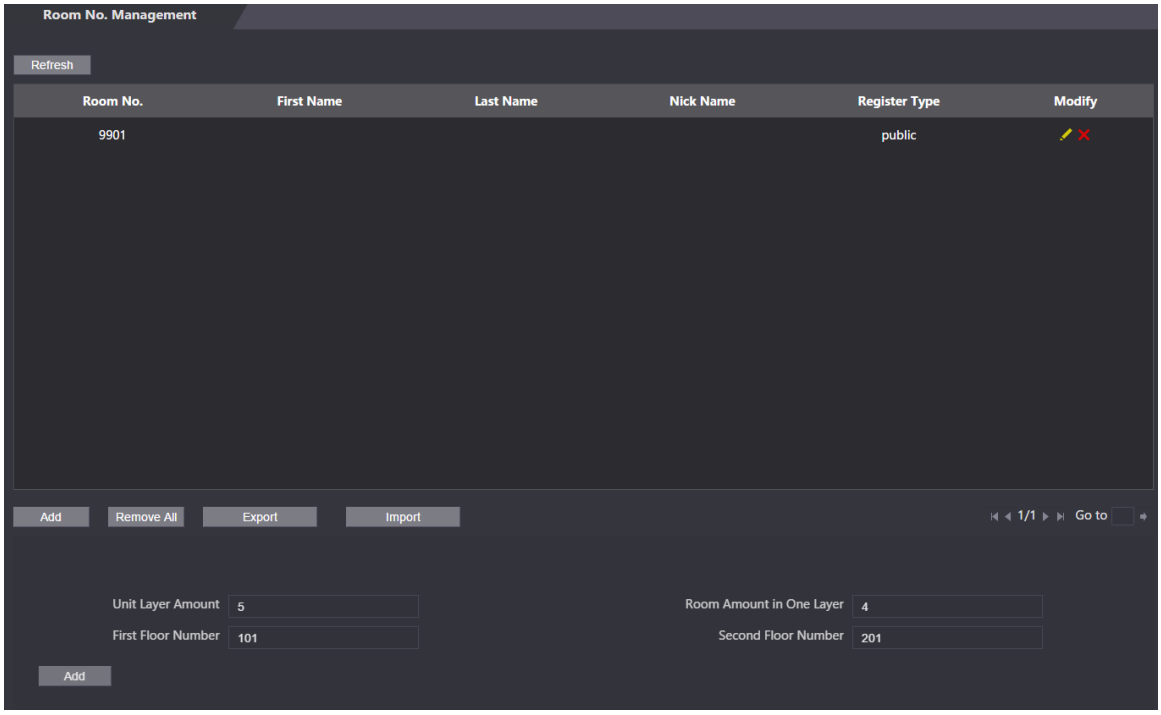
4.5.4.1 Agregar un monitor interior

Step 1 Inicie sesión en la web.

Step 2 Seleccione **Configuración de Talkback> Gestión de número de habitación**. Hacer clic

Step 3 **Agregar**.

Figure 4-17 Gestión de número de habitación



Step 4 Ingrese la información.

Figure 4-18 Agregue un monitor interior

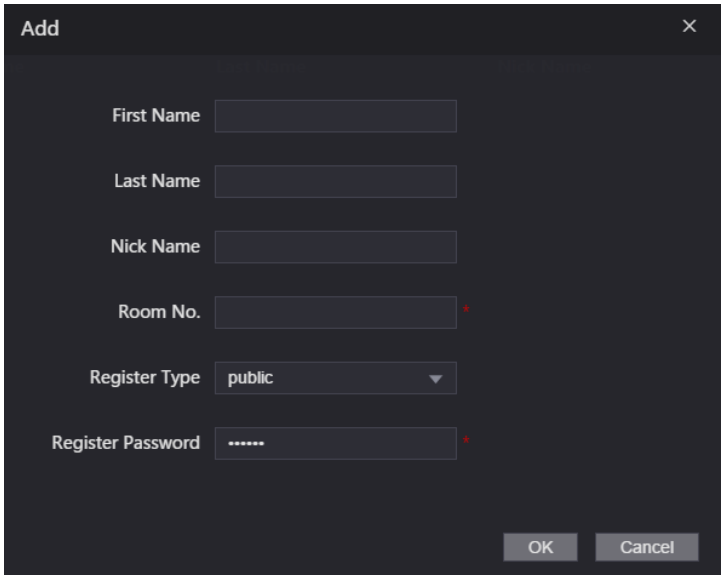


Tabla 4-6 Descripción de los parámetros

Parámetro	Descripción
Primer nombre	Para diferenciar cada monitor interior.
Apellido	
Apodo	
Habitación no.	Número de habitación del monitor interior. - Puede contener hasta cinco dígitos y debe ser el mismo que el configurado en el monitor interior. - Cuando hay monitores interiores principales y de extensión, el número de habitación del monitor interior principal debe terminar con "-0", y el de los monitores interiores de extensión con "-1", "-2", "-3" ... Por ejemplo, el el monitor interior principal es 101-0, los monitores de extensión son 101-1, 101-2 y 101-3.
Tipo de registro	Conserva el valor predeterminado.
Registrar contraseña	

Step 5 Hacer clic **OK**.

También puede hacer clic en **Exportar** para exportar el número de habitación e importarlo a otros dispositivos.

4.5.4.2 Agregar monitores interiores en lotes

Puede agregar hasta 1024 monitores de interior.

Step 1 Inicie sesión en la web.

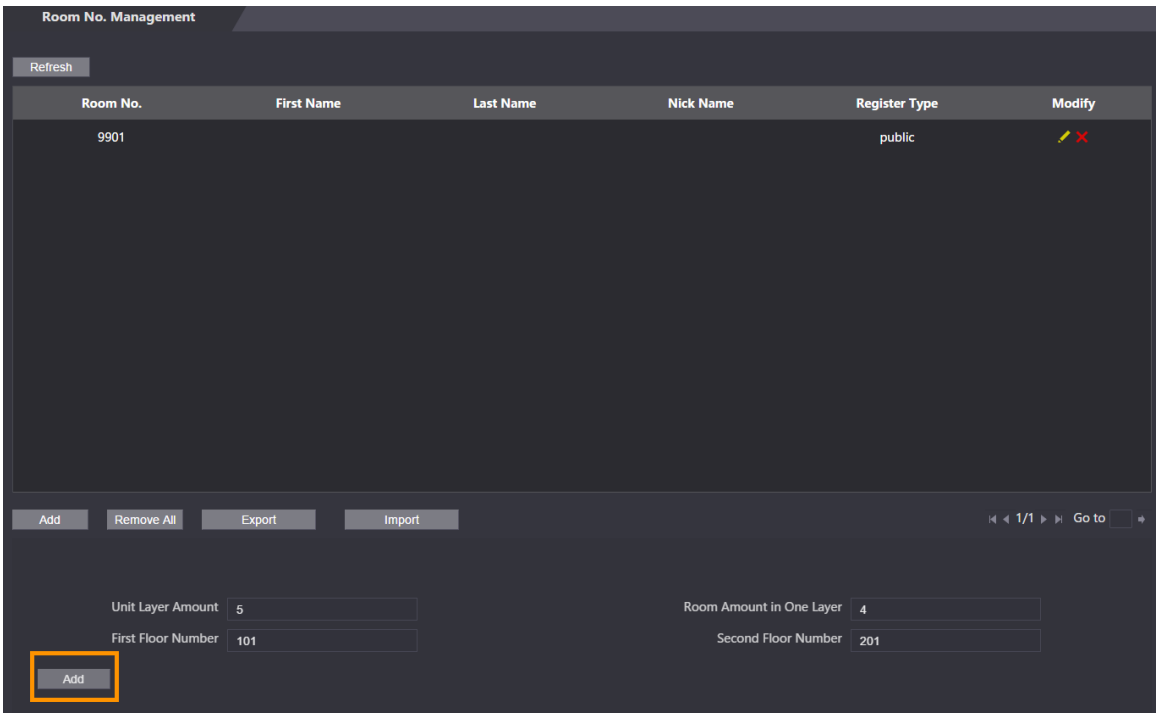
Step 2 Seleccione **Configuración de Talkback> Gestión de número de habitación**.

Step 3 En la parte inferior, ingrese los números para Cantidad de capa de unidad, Cantidad de habitación en una capa, Número de primer piso y Número de segundo piso.

- La cantidad de capa unitaria puede ser de 1 a 99, la cantidad de espacio en una capa de 1 a 99 y el número de piso 1 a 99999.

Step 4 Hacer clic **Agregar**.

Figure 4-19 Agregue monitores de interior en lotes



4.5.5 Configuración del dispositivo de gestión

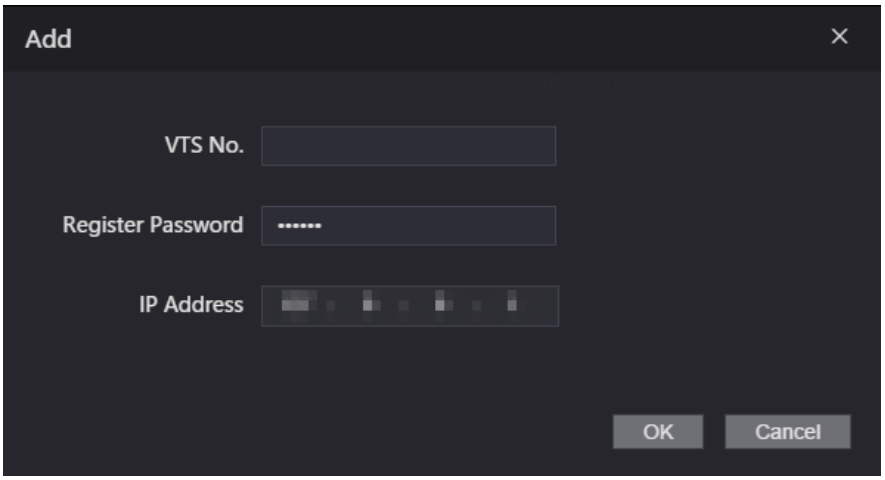
Cuando el controlador de acceso funciona como servidor SIP, agregue otros dispositivos de administración para llamarlos.

Step 1 Inicie sesión en la web.

Step 2 Seleccione **Configuración de Talkback> Administración de VTS**.

Step 3 Hacer clic**Agregar**.

Figure 4-20 Agregar dispositivos de administración

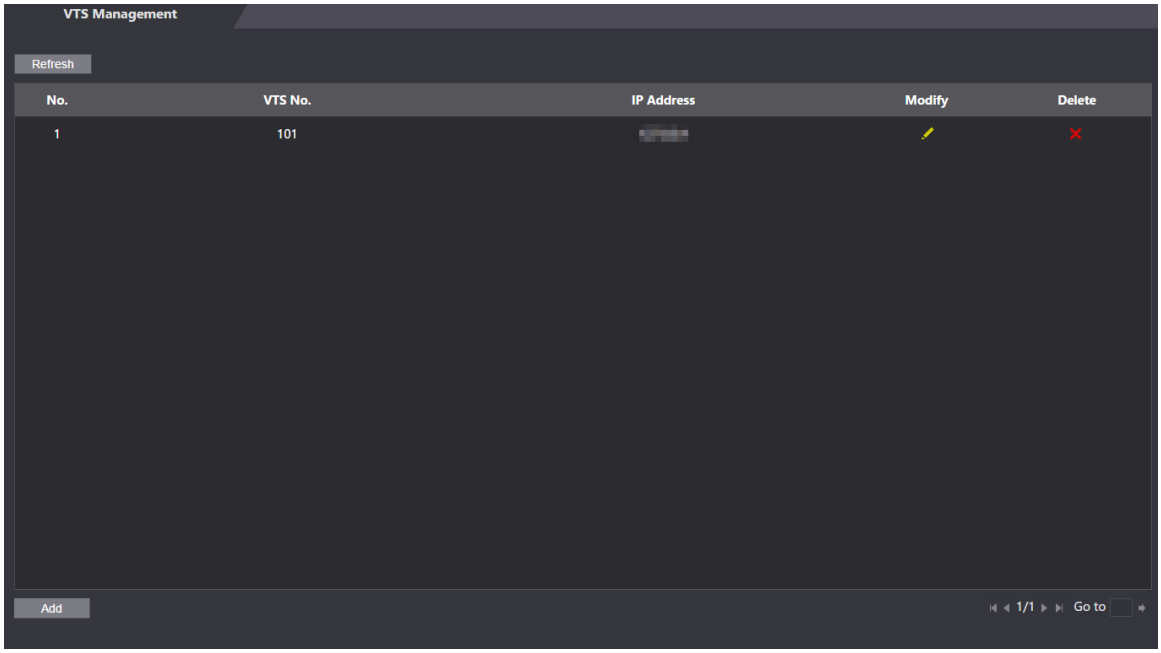


Step 4 Ingrese la información.

- El número de VTS puede contener hasta 9 dígitos.
- Contraseña de inicio de sesión para el dispositivo de gestión. Conserva el valor predeterminado.

Step 5 Hacer clic **OK**.

Figure 4-21 Se agregó un dispositivo de administración.



- Modificar un dispositivo de gestión.

  Necesita actualizar la información cuando la contraseña de registro o la dirección IP del gestionar los cambios de dispositivo. Hacer clic e ingrese la nueva contraseña o dirección IP, y luego hacer clic **OK**.

- Eliminar un dispositivo de gestión.

  Hacer clic .

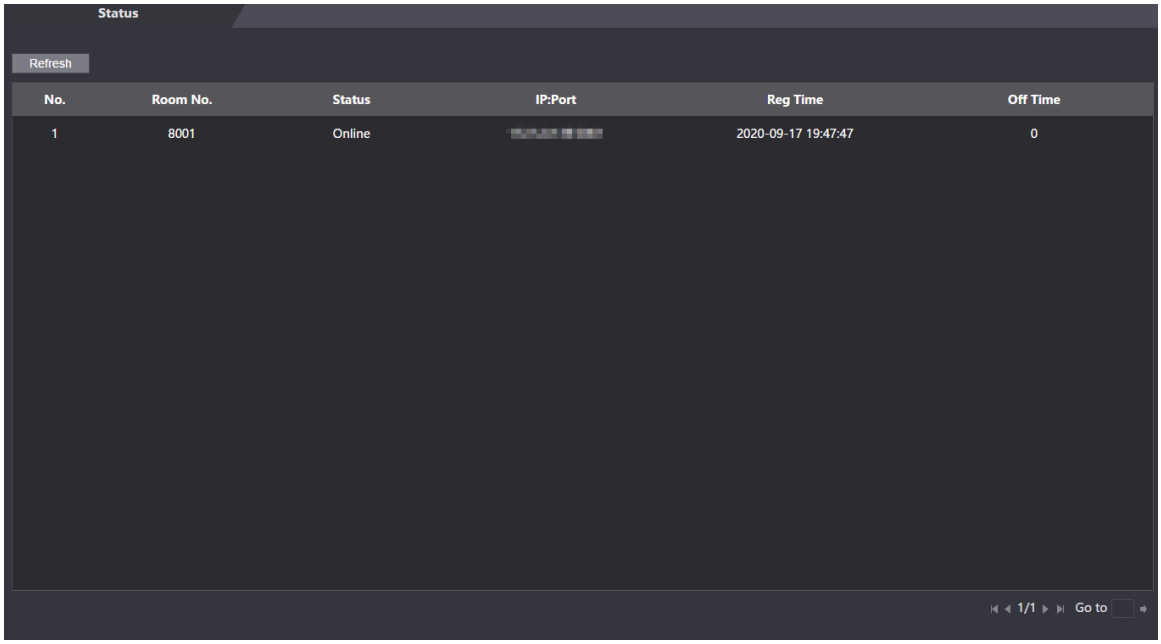
4.5.6 Estado en línea

Cuando el controlador de acceso funciona como servidor SIP, los administradores pueden iniciar sesión en la web y verificar la información de los dispositivos en línea.

Step 1 Inicie sesión en la web.

Step 2 Seleccione **Configuración de Talkback> Estado**.

Figure 4-22 Estado



4.5.7 Registros de llamadas

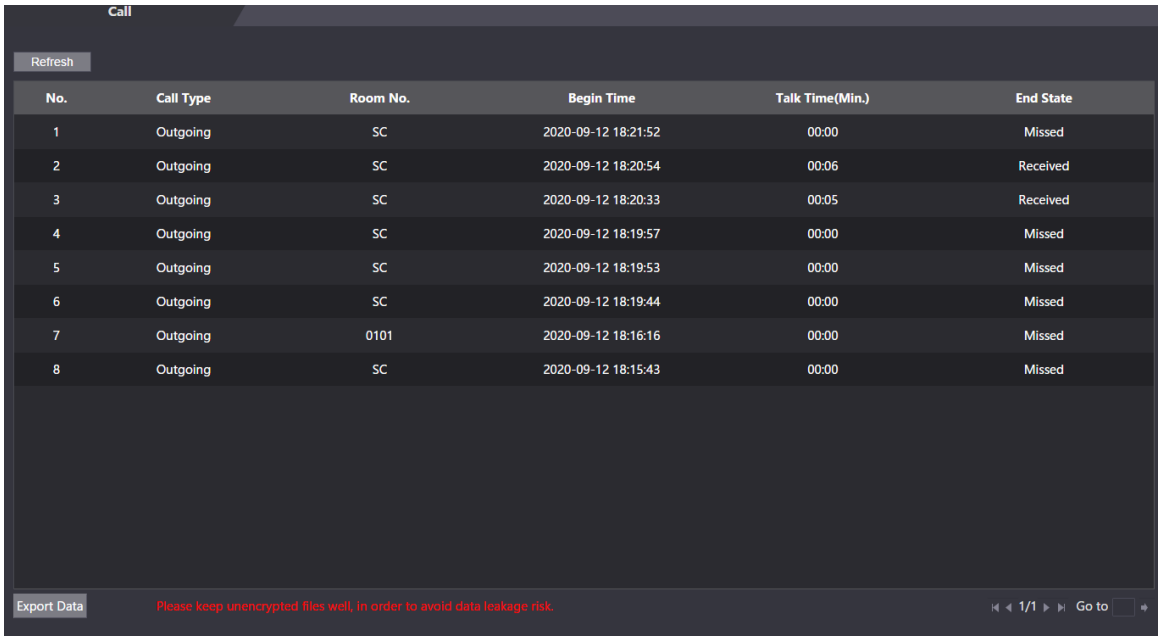
Puede consultar hasta 1024 registros de llamadas.

Step 1 Inicie sesión en la web.

Step 2 Seleccione **Configuración de Talkback> Llamada**.

Step 3 (Opcional) Haga clic en **Exportar datos** para exportar todos los registros.

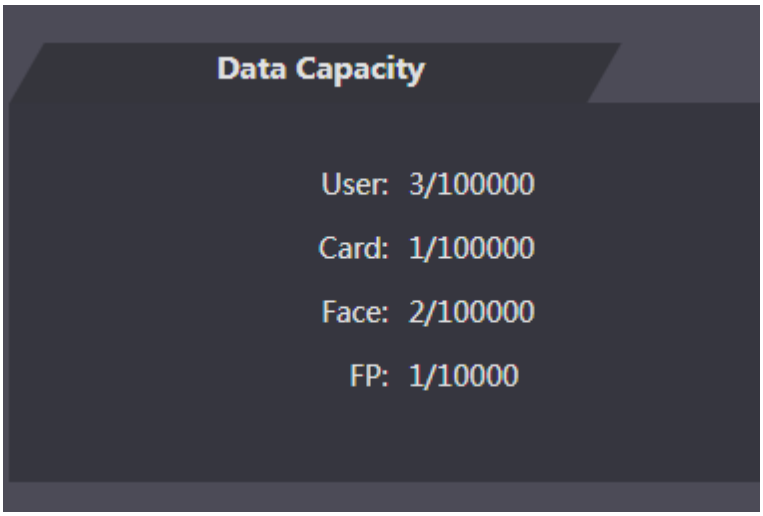
Figure 4-23 Registros de llamadas



4.6 Capacidad de datos

Puede ver cuántos usuarios, tarjetas e imágenes de caras puede contener el terminal en el **Capacidad de datos** interfaz.

Figure 4-24 Capacidad de datos



4.7 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.

4.7.1 Velocidad de datos

Figure 4-25 Velocidad de datos

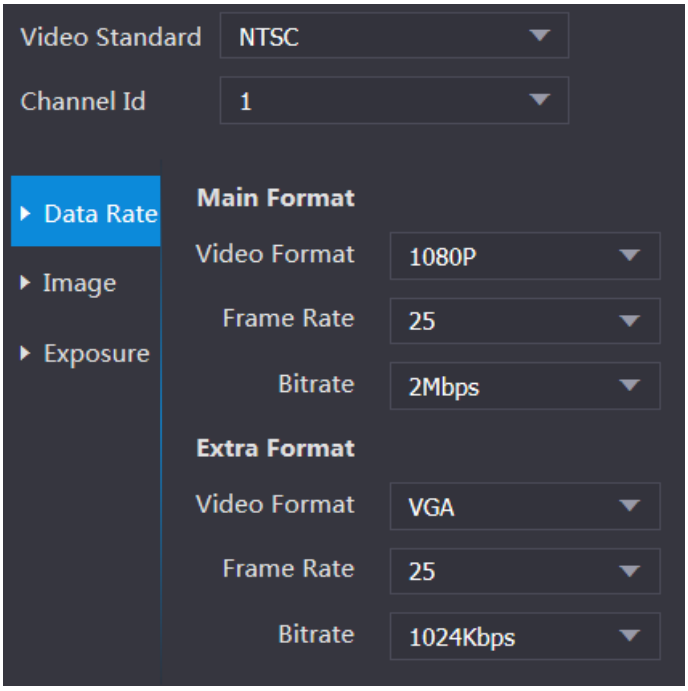


Tabla 4-7 Descripción del parámetro de velocidad de datos

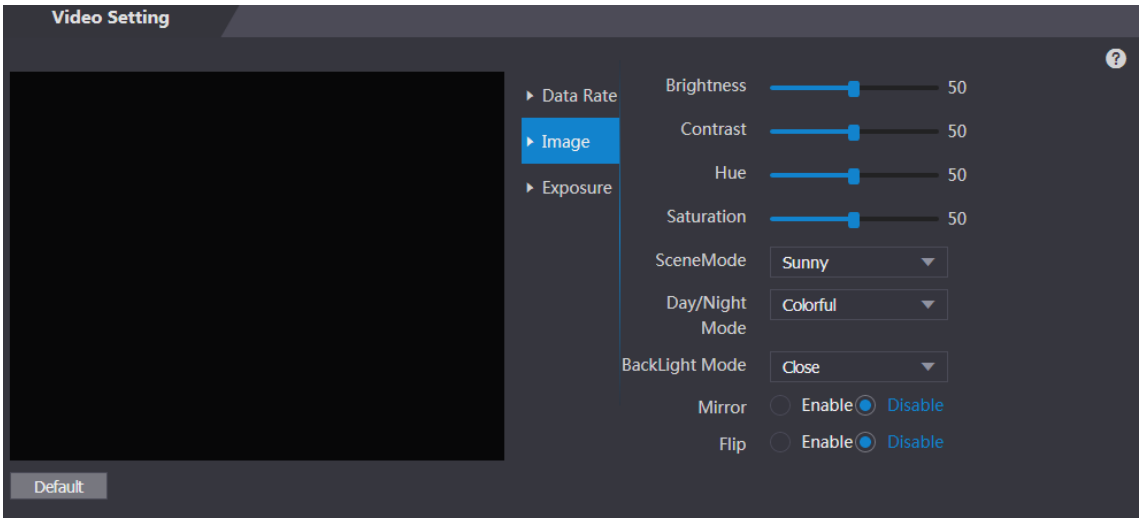
Parámetro		Descripción
Estándar de video		Hay dos opciones: NTSC y PAL. Seleccione un estándar de acuerdo con el estándar de video de su región.
Canal		Hay dos opciones: 1 y 2. 1 es una cámara de luz blanca y 2 es una cámara de luz IR.
Principal Formato	Formato de video	Hay cuatro opciones: D1, VGA, 720p y 1080p. Seleccione una opción de acuerdo con la calidad de video que desee. 720p está configurado de forma predeterminada. Si necesita la función de llamada, no la configure en 1080p.
	Cuadros por segundo	La velocidad a la que aparecen fotogramas consecutivos en una pantalla. El rango de velocidad de fotogramas es de 1 a 30 fps.
	Tasa de bits	El número de bits que se transportan o procesan por unidad de tiempo. Hay cinco opciones: 2 Mbps, 4 Mbps, 6 Mbps, 8 Mbps y 10 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. El rango de velocidad de fotogramas es de 1 a 30 fps.
	Tasa de bits	El número de bits que se transportan o procesan por unidad de tiempo. Hay opciones: 512 Kbps, 640 Kbps, 768 Kbps, 896 Kbps, 1024 Kbps, 1,25 Mbps, 1,5 Mbps, 1,75 Mbps y 2 Mbps.

4.7.2 Imagen

Hay dos canales y debe configurar los parámetros para cada canal.

Step 1 Seleccione **Configuración de video> Configuración de video> Imagen**.

Figure 4-26 Imagen



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

Tabla 4-8 Descripción de los parámetros de la 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.
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, aumentará el tono de la imagen. **Soleado** está seleccionado de forma predeterminada.
Día / noche Modo	El modo día / noche decide el estado de funcionamiento de la luz de relleno. ● Automático: el sistema ajusta automáticamente los modos día / noche. Colorido: ● en este modo, las imágenes se muestran con colores. ● Blanco y negro: en este modo, las imágenes se muestran en blanco y negro.
Luz de fondo Modo	● Cerrar: Sin retroiluminación. ● BLC: la compensación de luz de fondo corrige las 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 rango dinámico amplio, el sistema atenúa las áreas brillantes y compensa las áreas oscuras para asegurar la definición de los objetos en las áreas brillantes y oscuras. Cuando hay rostros humanos en la luz de fondo, debe habilitar el WDR. ● HLC: Se necesita compensación de altas luces para compensar la sobreexposición de altas luces o fuentes de luz fuertes como focos, faros, luces de porche, etc. para crear una imagen que sea utilizable y no superada por una luz brillante.
Espejo	Cuando la función está habilitada, las imágenes se mostrarán con los lados izquierdo y derecho invertidos.
Voltear	Cuando esta función está habilitada, las imágenes se pueden voltear.

4.7.3 Exposición

Tabla 4-9 Descripción de los parámetros de exposición

Parámetro	Descripción
Contra parpadeo	● 50Hz: cuando la frecuencia de servicio de la corriente alterna es 50Hz, la exposición se ajusta automáticamente para asegurarse de que no haya rayas en las imágenes. ● 60Hz: cuando la frecuencia de servicio de la corriente alterna es de 60Hz, la exposición se ajusta automáticamente para asegurarse de que no haya

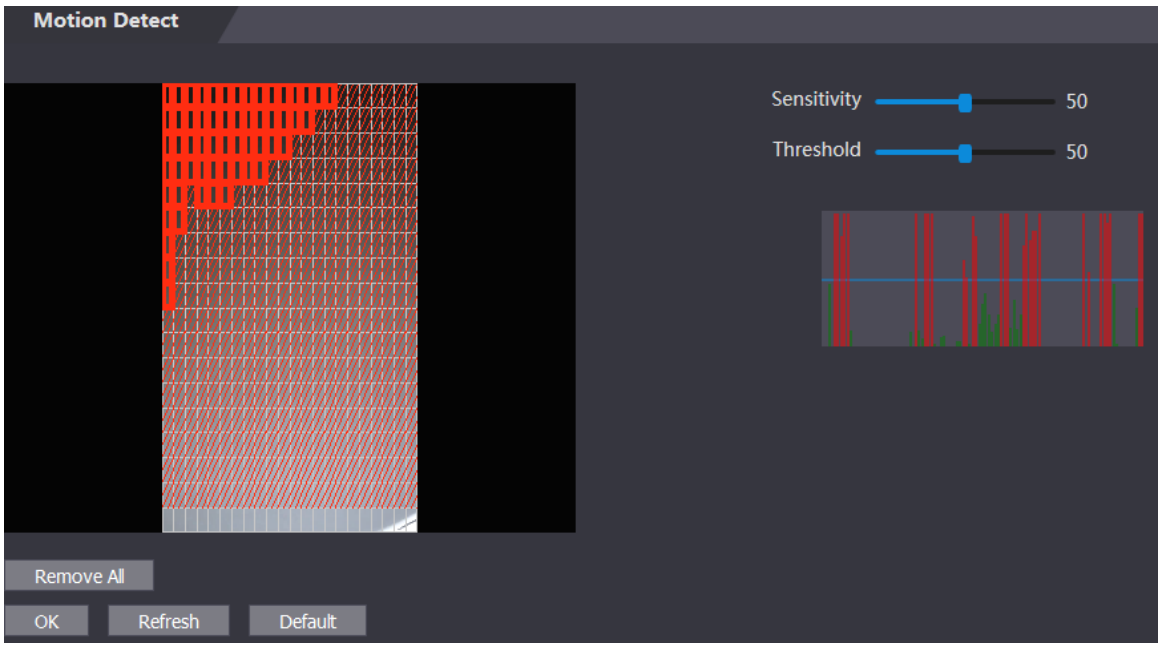
Parámetro	Descripción
	rayas en las imágenes. ● Al aire libre: cuando **Exterior** está seleccionado, se puede cambiar el modo de exposición.
Exposición Modo	 - Cuando seleccionas **Exterior** en el **Contra parpadeo** lista desplegable, puede seleccionar **Prioridad de obturador** como el modo de exposición. - Los modos de exposición de los diferentes dispositivos pueden variar y prevalecerá el producto real. Puede seleccionar entre: ● Auto: el terminal ajustará automáticamente el brillo de las imágenes. Prioridad del ● 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 Distancia	Si seleccionas **Gama personalizada**, puede personalizar el rango de valores del obturador.
Ganar valor Distancia	Cuando se establece el rango del valor de ganancia, se mejorará la calidad del video.
Exposición Compensación	Puede aumentar el brillo del video ajustando el valor de compensación de exposición.
3D NR	Cuando la reducción de ruido 3D (RD) está habilitada, se puede reducir el ruido del video y se producirán videos de alta definición.
Calificación	Puede ajustar el valor de 3D NR cuando 3D NR está habilitado. Cuanto mayor sea el valor, menos ruido habrá.

4.7.4 Detección de movimiento

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

Step 1 Seleccione **Configuración de video> Configuración de video> Detección de movimiento**.

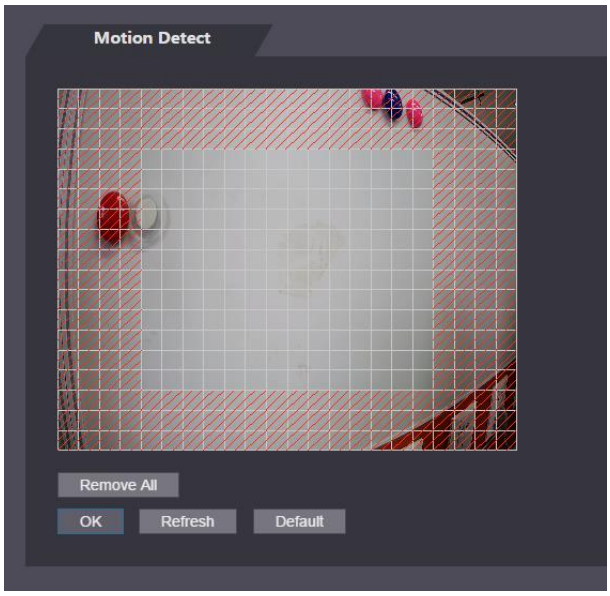
Figure 4-27 Detección de movimiento



Step 2 Mantenga presionado el botón izquierdo del mouse y luego arrastre el mouse en el área roja.

- 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 dibuja en el área de detección de movimiento predeterminada.

Figure 4-28 Área de detección de movimiento



Step 3 Configure la sensibilidad y el umbral.

- La sensibilidad representa la capacidad de cada cuadrícula para detectar el movimiento. Cuanto mayor sea el valor, mayor será la sensibilidad.
- El umbral es la condición de detección de movimiento. Cuando el número de cuadrícula alcanza el umbral, se activará la detección de movimiento. Cuanto menor sea el valor, es más probable que se active la detección de movimiento.

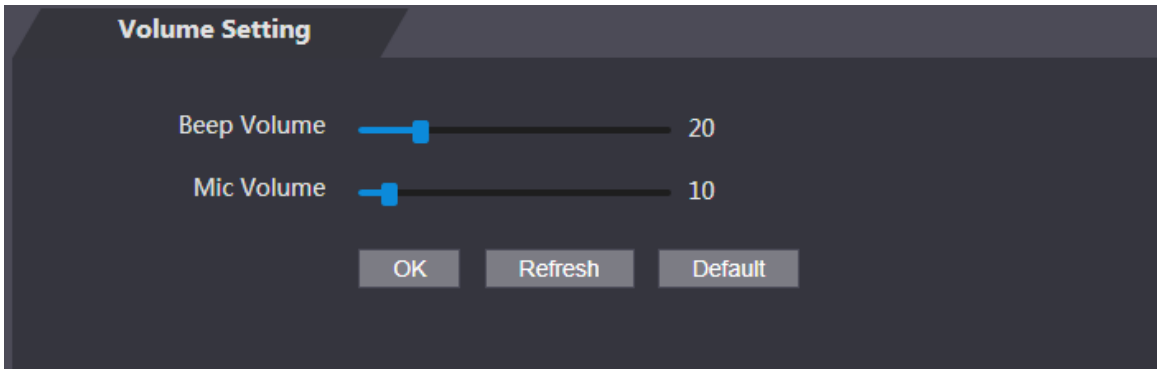
- Cuando el número de cuadrícula es menor que el umbral, aparecerá una línea verde; cuando el número de cuadrícula es mayor que el umbral, aparecerá una línea roja. Vea la Figura 4-27.

Step 4 Hacer clic **OK** para terminar el ajuste.

4.7.5 Ajuste de volumen

Puede ajustar el volumen del altavoz del terminal.

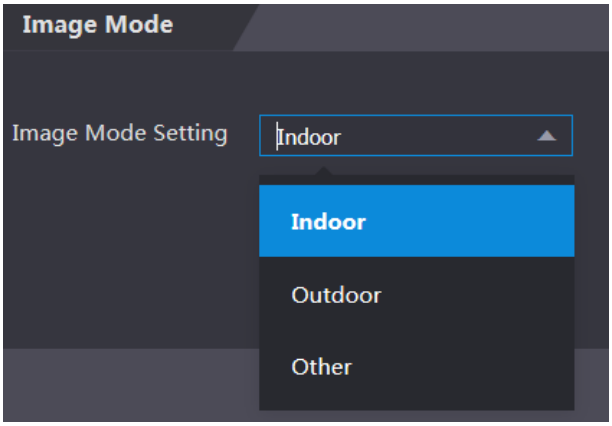
Figure 4-29 Ajuste de volumen



4.7.6 Modo de imagen

Hay tres opciones: interior, exterior y otras. Seleccione**Interior** cuando el terminal está instalado en interiores; Seleccione**Exterior** cuando el terminal se instala al aire libre; y seleccione**Otro** cuando la terminal se instala en lugares con luz de fondo como pasillos y pasillos.

Figure 4-30 Modo de imagen



4.7.7 Codificación local

Configure el área que se mostrará en los monitores interiores.

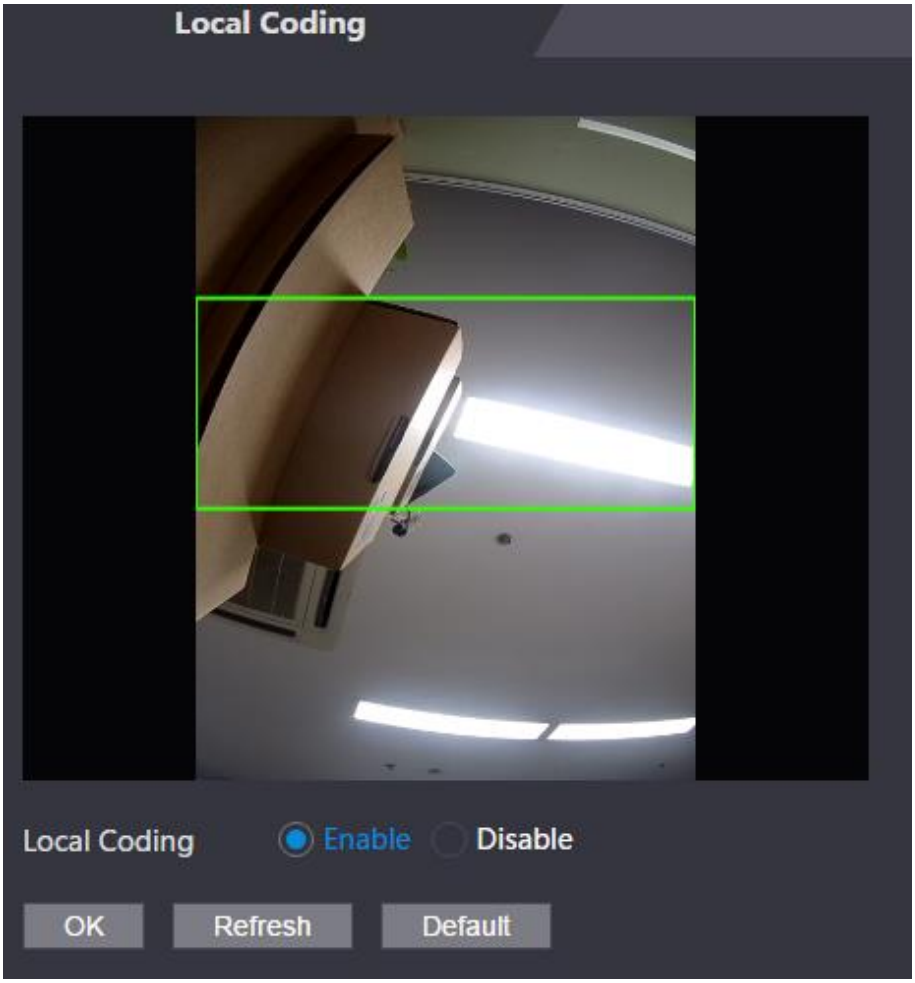
Step 1 Inicie sesión en la web.

Step 2 Seleccione **Configuración de video> Codificación**

Step 3 **local**. Habilite la función.

Step 4 Arrastre el cuadro según sea necesario.

Figure 4-31 Codificación local



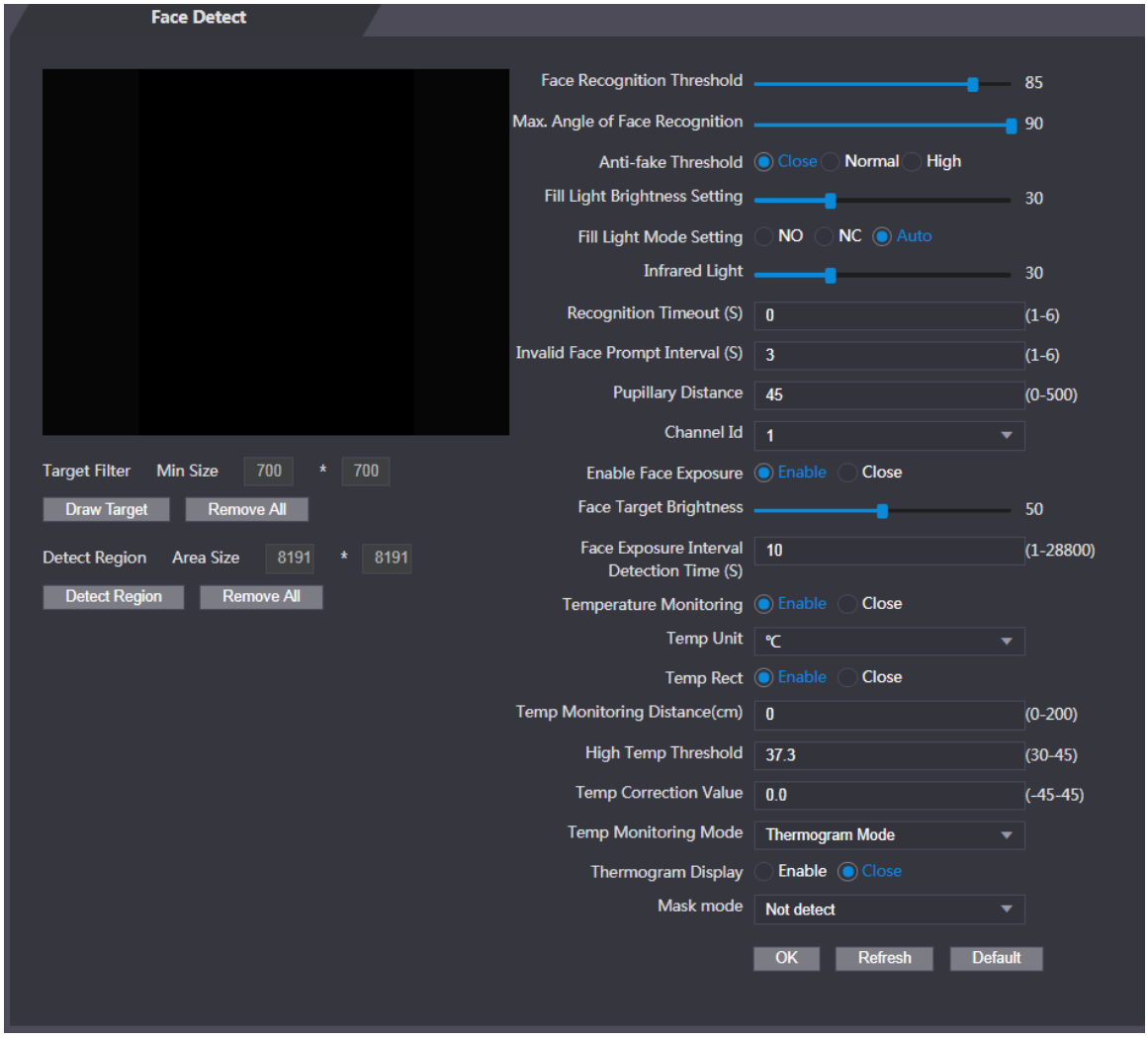
Step 5 Hacer clic **OK**.

4.8 Detección de rostro

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

Step 1 Seleccione **Detección de rostro**.

Figure 4-32 Detección facial



Step 2 Configure los parámetros.

Tabla 4-10 Descripción del parámetro de detección facial

Parámetro	Descripción
Cara Reconocimiento Umbral	Cuanto mayor sea el valor, mayor será la precisión.
Max. Ángulo de reconocimiento facial	Cuanto mayor sea el ángulo, se reconocerá la 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. Hay dos opciones: **Habilitar** y **Cerrar**.
Llenar el brillo de la luz Configuración	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 relleno permanece abierta. NC: ● La luz de relleno permanece cerrada. ● Automático: la luz de relleno se encenderá automáticamente cuando se active un evento de detección de movimiento. Cuando **Auto** está seleccionado, la luz de relleno no se encenderá incluso si

Parámetro	Descripción
	El valor de luz es superior a 19.
Luz infrarroja	Ajuste el brillo de infrarrojos arrastrando la barra de desplazamiento.
Tiempo de espera de reconocimiento	Cuando una persona que no tiene el permiso de acceso se para frente a la terminal y logra que se reconozca la cara, la terminal indicará que el reconocimiento facial falló. El intervalo de solicitud se denomina tiempo de espera de reconocimiento.
Mensaje de rostro no válido Intervalo	Cuando un rostro no tiene permiso de acceso se encuentra frente a la terminal, el terminal indicará que el rostro no es válido. El intervalo de aviso es un intervalo de aviso de rostro 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 terminal pueda reconocer 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 la exposición facial	Una vez habilitada la exposición facial, el rostro humano se verá más claro cuando el terminal se instale al aire libre.
Canal ID	Hay dos opciones: 1 y 2. 1 es una cámara de luz blanca y 2 es una 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.
Temperatura Vigilancia	Establezca si desea habilitar la monitorización de la temperatura corporal. ● Unidad de temperatura: seleccione una unidad de temperatura. ● Temp Rect: establezca si se muestra el cuadro de control de temperatura o no. ● Distancia de monitorización de temperatura (cm): el valor predeterminado es 0. Configure otros valores para habilitar el monitoreo de temperatura dentro de una distancia definida. Se recomiendan 80 cm. ● Umbral de temperatura (° C): establezca el umbral de temperatura. La temperatura corporal monitoreada se considerará alta si es mayor o igual al valor establecido. ● Valor de corrección de temperatura: este parámetro es para pruebas. La diferencia del entorno de monitoreo de temperatura puede causar la desviación de temperatura entre la temperatura monitoreada y la temperatura real. Puede seleccionar varias muestras monitoreadas para su análisis. De acuerdo con la comparación entre la temperatura monitoreada y la temperatura real, puede corregir la desviación de temperatura con este parámetro. Por ejemplo, si la temperatura monitoreada es 0.5 ° C más baja que la temperatura real, el valor de corrección se establece en 0.5 ° C; si la temperatura medida es de 0,5 ° C

Parámetro	Descripción
	más alta que la temperatura real, el valor de corrección se establece en -0,5 ° C. Solo el terminal con una unidad de control de temperatura admite este parámetro.
Modo de máscara	● Sin detección: la máscara no se detecta durante el reconocimiento facial. ● Recordatorio de máscara: la máscara se detecta durante el reconocimiento facial. Si la persona es detectada sin usar una máscara, el sistema le recordará la máscara y se permitirá el paso. ● Intercepción de máscara: la máscara se detecta durante el reconocimiento facial. Si se detecta a la persona sin usar una máscara, el sistema le recordará la máscara y no se permitirá el paso.

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

4.9 Configuración de red

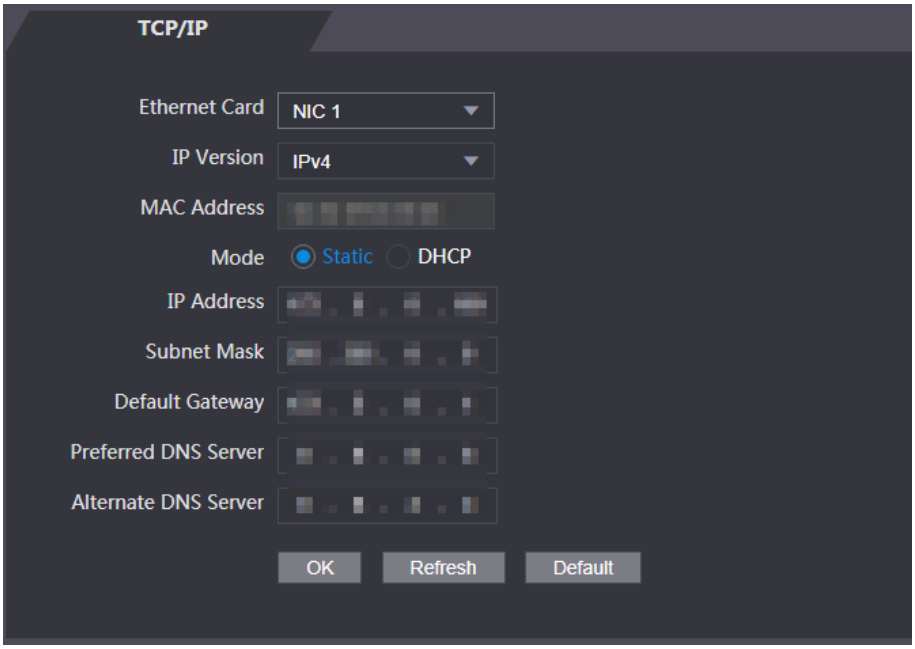
4.9.1 TCP / IP

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

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

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

Figure 4-33 TCP / IP



Step 2 Configure los parámetros.

Tabla 4-11 TCP / IP

Parámetro	Descripción
Tarjeta ethernet	Seleccione para configurar los parámetros de la tarjeta.
Versión de IP	Hay una opción: IPv4.
MAC	Dirección MAC del terminal.
Modo	● Estático Configure la dirección IP, la máscara de subred y la dirección de la puerta de enlace manualmente. ● DHCP - Una vez que se habilita DHCP, la dirección IP, la máscara de subred y la dirección de la puerta de enlace no se pueden configurar. - Si DHCP es efectivo, la dirección IP, la máscara de subred y la dirección de la puerta de enlace se mostrarán automáticamente; si DHCP no es efectivo, la dirección IP, la máscara de subred y la dirección de la puerta de enlace serán todas cero. - Si desea ver la IP predeterminada cuando DHCP es efectivo, deshabilite DHCP.
Enlace local Dirección	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	Configure la dirección IP del servidor DNS alternativo.

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

4.9.2 Puerto

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

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

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

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

Tabla 4-12 Descripción del puerto

Parámetro	Descripción
Max Conexión	Puede establecer las conexiones máximas de clientes a los que se puede conectar el terminal. Los clientes de plataforma como Smart PSS 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 cuando inicie sesión a través de navegadores.

Puerto HTTPS	El valor predeterminado es 443.
Puerto RTSP	El valor predeterminado es 554.

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

4.9.3 Registro

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

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

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

Tabla 4-13 Descripción del registro automático

Parámetro	Descripción
IP de host	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.

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

4.9.4 P2P

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

Si va a utilizar P2P, debe conectar el terminal a una red externa; de lo contrario, no se podrá utilizar el terminal.

Figure 4-34 P2P

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

Step 2 **Habilitar** para habilitar la función P2P. Hacer clic

Step 3 **OK** para completar el ajuste.

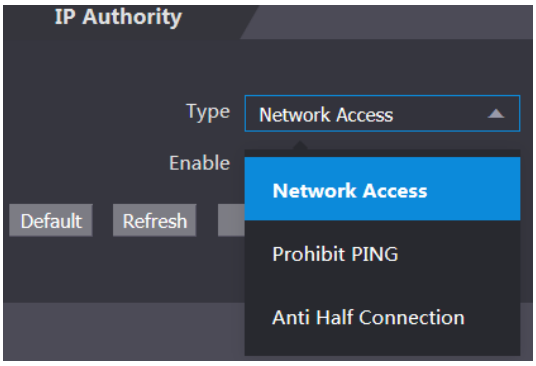
Escanee el código QR en su interfaz web para obtener el número de serie del terminal.

4.10 Administración de Seguridad

4.10.1 Autoridad de propiedad intelectual

Seleccione un modo de ciberseguridad según sea necesario.

Figure 4-35 Autoridad de propiedad intelectual



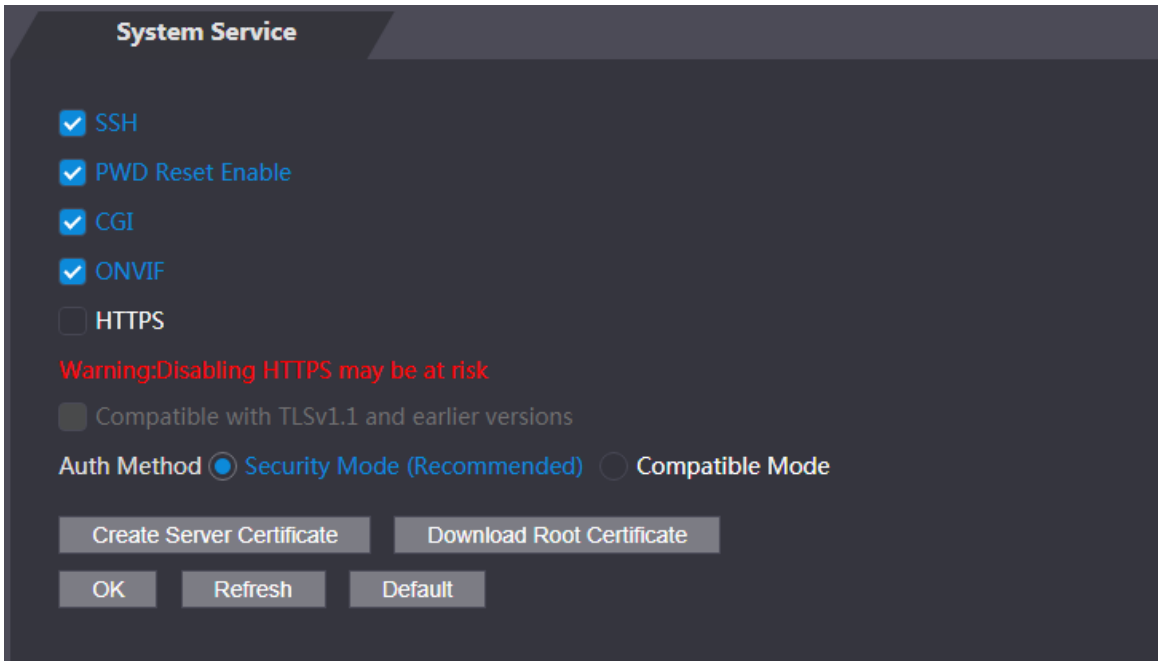
4.10.2 Sistemas

4.10.2.1 Servicio del sistema

Hay cuatro opciones: SSH, PWD Reset Enable, CGI y HTTPS. Consulte "3.11.4 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.

Figure 4-36 Servicio del sistema



4.10.2.2 Creación de certificado de servidor

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

4.10.2.3 Descarga del certificado raíz

Step 1 Haga clic en Descargar certificado raíz.

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

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

4.11 Gestión de usuarios

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

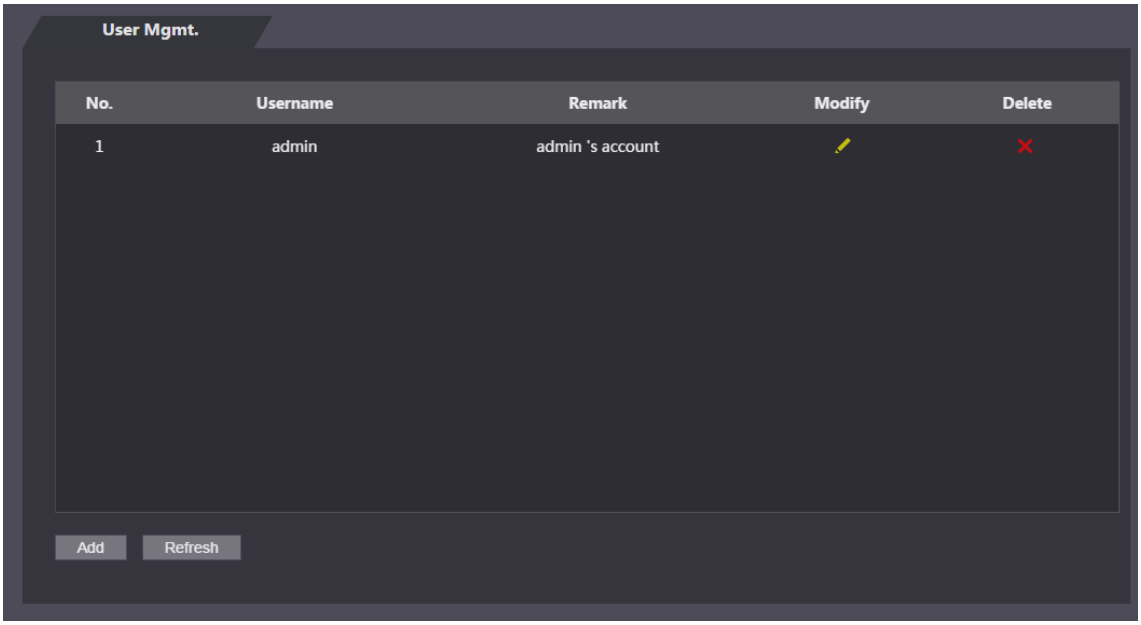
4.11.1 Agregar usuarios

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.

4.11.2 Modificación de la información del usuario

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

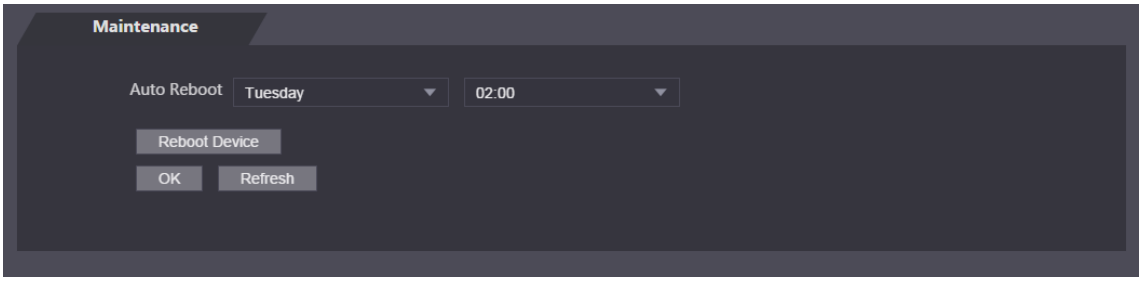
Figure 4-37 Gestión de usuarios



4.12 Mantenimiento

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

Figure 4-38 Mantenimiento

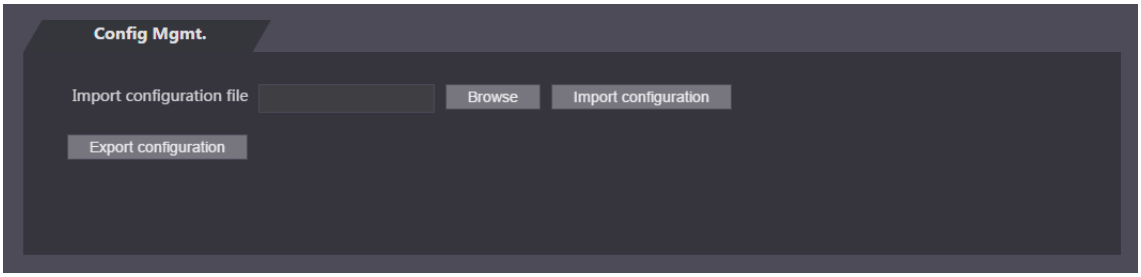


Seleccione la fecha y hora de reinicio automático. La hora de reinicio predeterminada es a las 2 de la mañana del martes. Hacer clic**Reiniciar dispositivo**, el terminal se reiniciará inmediatamente. Hacer clic**OK**, la terminal se reiniciará a las 2 de la mañana todos los martes.

4.13 Gestión de la configuración

Cuando más de un terminal necesita la misma configuración, puede configurar los parámetros para ellos importando o exportando archivos de configuración.

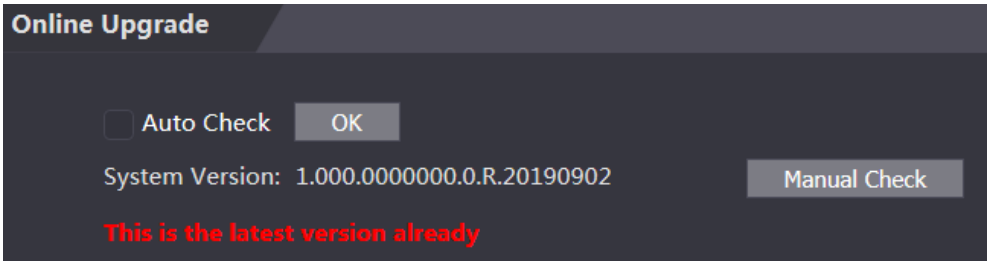
Figure 4-39 Gestión de la configuración



4.14 Potenciar

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

Figure 4-40 Potenciar



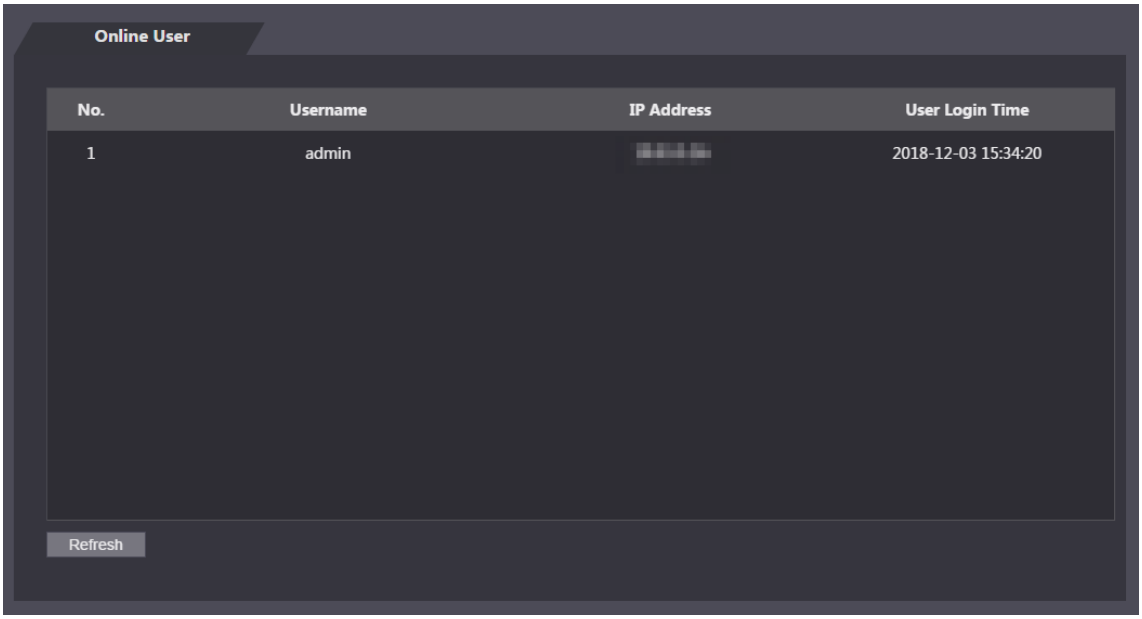
4.15 Información de versión

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.

4.16 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.

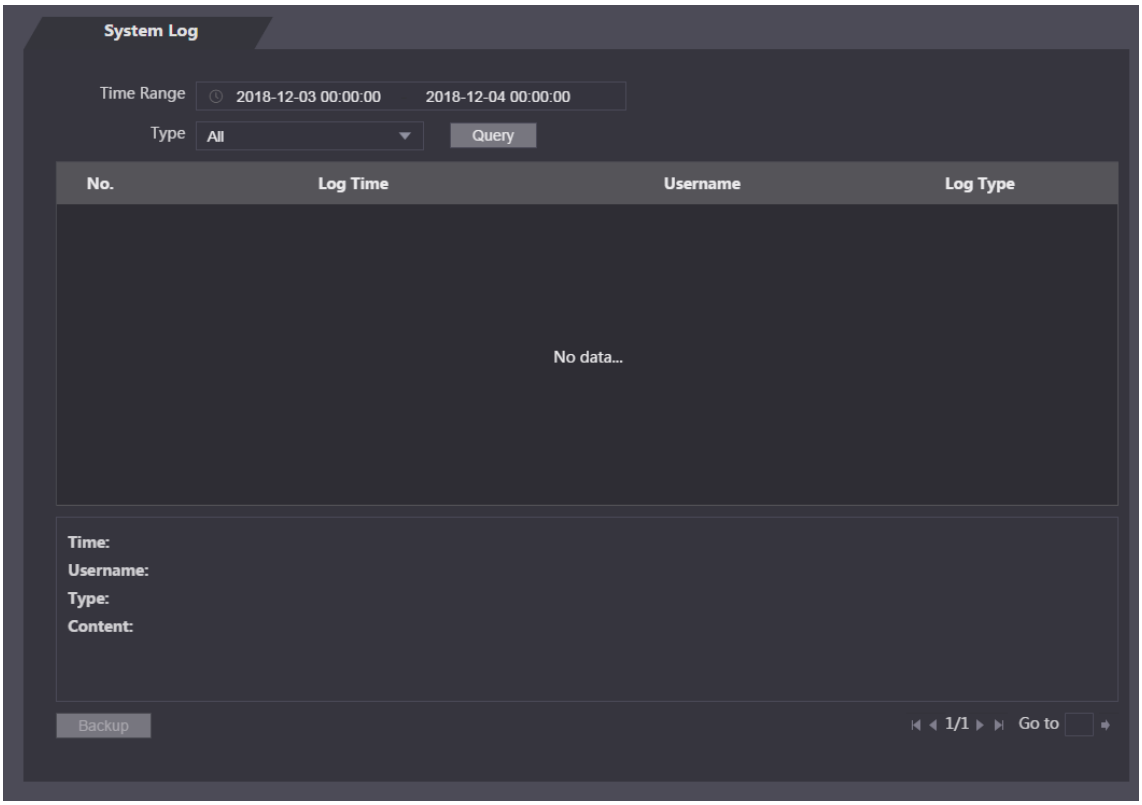
Figure 4-41 Usuario en línea



4.17 Registro del sistema

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

Figure 4-42 Registro del sistema



4.17.1 Consulta de registros

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

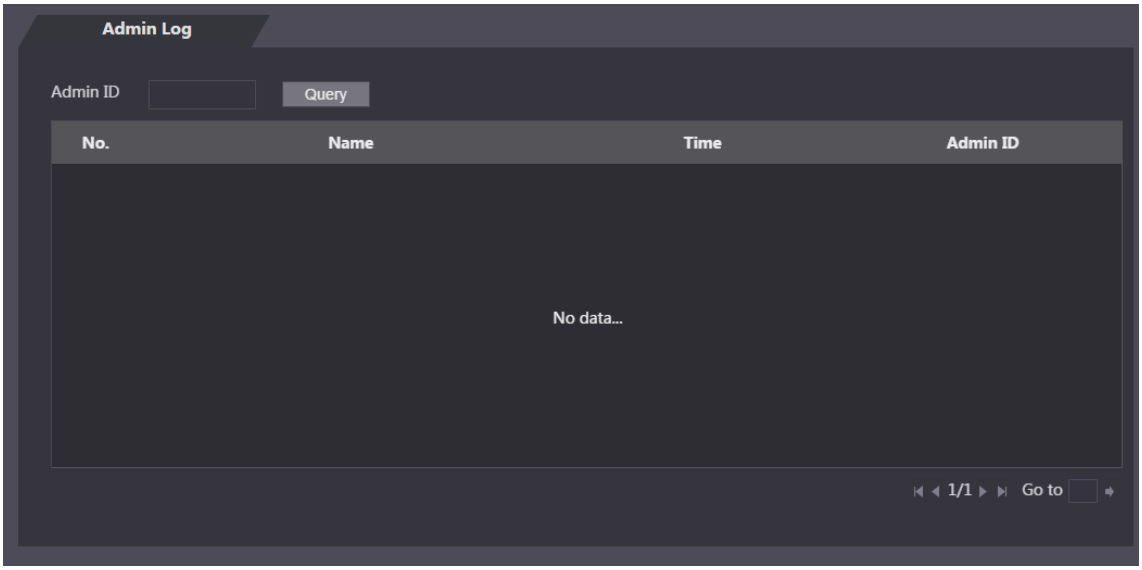
4.17.2 Copia de seguridad de registros

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

4.17.3 Registro de administración

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

Figure 4-43 Registro de administración



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

4.18 Salida

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

5 preguntas frecuentes

1 **El terminal no se inicia después del encendido.**

Compruebe si la fuente de alimentación de 12 V está conectada correctamente y si el botón de encendido está presionado.

2 **Las caras no se pueden reconocer después de que se enciende el terminal.**Asegúrese de que Cara esté seleccionado en el modo de desbloqueo. Consulte "3.8.2 Desbloqueo".

Asegúrese de que Cara esté seleccionada como modo de desbloqueo en **Acceso> Modo de desbloqueo> Combinación de grupo**. Consulte “3.8.2.3 Combinación de grupos”.

3 **No hay señal de salida cuando el terminal y el controlador externo están conectados al puerto Wiegand.**

Compruebe si el cable GND del terminal y el controlador externo están conectados.**No se pueden realizar**

4 **configuraciones después de olvidar el administrador y la contraseña.**Elimine administradores a través de la plataforma o comuníquese con el soporte técnico para desbloquear el terminal de forma remota.

5 **La información del usuario y las imágenes faciales no se pueden importar al terminal.**

Compruebe si se modificaron los nombres de los archivos XML y los títulos de las tablas porque el sistema identificará los archivos a través de sus títulos.

6 **Cuando se reconoce la cara de un usuario, pero se muestra la información de otros usuarios.**

Asegúrese de que al importar rostros humanos, no haya otras personas alrededor. Elimina la cara original e impórtala de nuevo.

Appendix 1 Notas de monitoreo de temperatura

- Caliente la unidad de control de temperatura durante más de 20 minutos después del encendido para permitir que la unidad de control de temperatura alcance el equilibrio térmico.
- Instale la unidad de control de temperatura en un entorno interior sin viento y mantenga la temperatura ambiente interior entre 15 ° C y 32 ° C.
- Evite la luz solar directa sobre la unidad de control de temperatura.
- Evite instalar la unidad de control de temperatura orientada hacia la fuente de luz y el vidrio.
- Mantenga la unidad de control de temperatura alejada de fuentes de interferencia térmica.
- Los factores como la luz solar, el viento, el aire frío y el aire acondicionado frío y caliente afectarán la temperatura de la superficie del cuerpo humano, lo que provocará la desviación de temperatura entre la temperatura monitoreada y la temperatura real.
- La sudoración también es una forma en que el cuerpo se enfría y disipa el calor automáticamente, lo que también provocará la desviación de temperatura entre la temperatura monitoreada y la temperatura real.
- Mantenga la unidad de control de temperatura con regularidad (cada 2 semanas). Utilice un paño suave sin polvo para limpiar suavemente el polvo de la superficie del sensor de temperatura y el sensor de distancia para mantenerlo limpio.

Appendix 2 Notas de la cara Grabación / comparación

Antes del registro

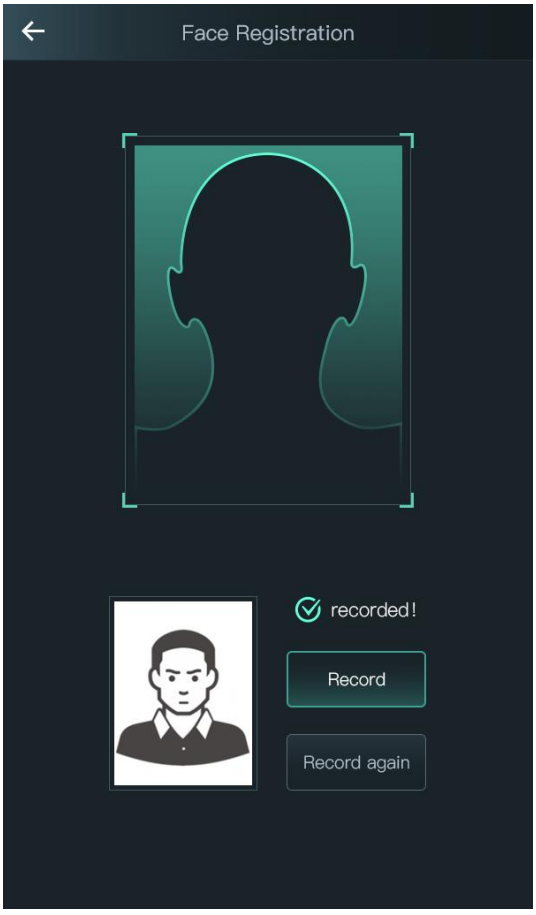
- Los anteojos, los sombreros y la barba pueden influir en el rendimiento del
- reconocimiento facial. No cubra sus cejas cuando use sombreros.
- No cambie mucho el estilo de su barba si va a utilizar el dispositivo; de lo contrario, el reconocimiento facial podría fallar.
- Mantén tu cara limpia.
- Mantenga el dispositivo al menos a dos metros de la fuente de luz y al menos a tres metros de las ventanas o puertas; de lo contrario, la luz de fondo y la luz solar directa pueden influir en el rendimiento del reconocimiento facial del dispositivo.

Durante el registro

Puedes registrar rostros a través del terminal o a través de la plataforma. Para registrarse a través de la plataforma, consulte el manual de usuario de la plataforma.

Haga que su cabeza se centre en el marco de captura de fotos. Se capturará automáticamente una imagen de su rostro.

Apéndice Figura 2-1 Registro

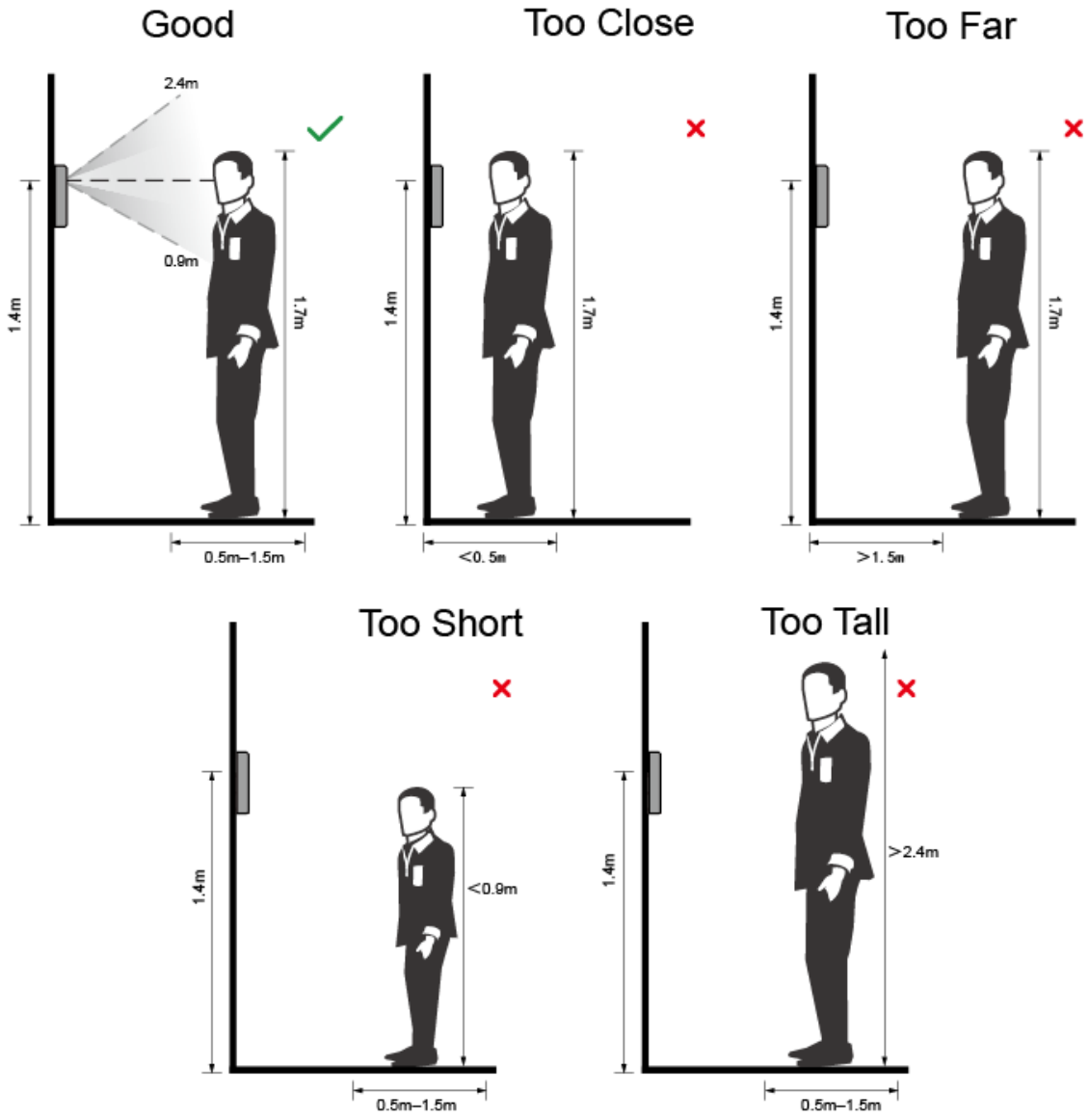


- No sacuda la cabeza o el cuerpo, o el registro podría fallar. Evite que
- aparezcan dos caras en el cuadro de captura al mismo tiempo.

Posición de la cara

Si su rostro no está en la posición adecuada, el efecto de reconocimiento facial podría verse afectado.

Apéndice Figura 2-2 Posición adecuada de la cara



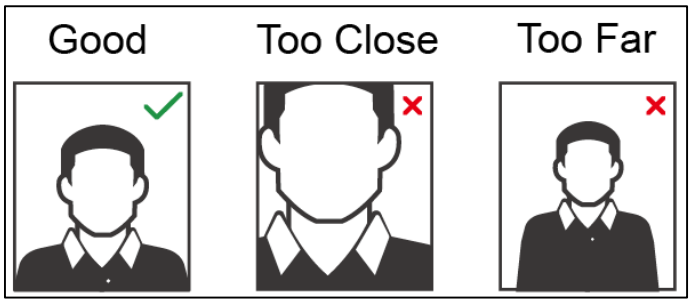
Requisitos de caras

- Asegúrese de que la cara esté limpia y la frente no esté cubierta de pelo.
- No use anteojos, sombreros, barbas espesas u otros adornos faciales que influyan en la grabación de imágenes faciales.
- Con los ojos abiertos, sin expresiones faciales, y dirija su rostro hacia el centro de la cámara.
- Cuando grabe su rostro o durante el reconocimiento facial, no mantenga su rostro demasiado cerca o

demasiado lejos de la cámara.

Apéndice Figura 2-3 Posición de la cabeza

Apéndice Figura 2-4 Distancia entre caras



- Al importar imágenes de rostros a través de la plataforma de administración, asegúrese de que la resolución de la imagen esté dentro del rango de 150 × 300–600 × 1200; los píxeles de la imagen son más de 500 × 500; el tamaño de la imagen es inferior a 75 KB y el nombre de la imagen y la identificación de la persona son
- iguales. Asegúrese de que la cara ocupe más de 1/3 pero no más de 2/3 de toda el área de la imagen y que la relación de aspecto no exceda 1: 2.

Appendix 3 Recomendaciones de ciberseguridad

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

Acciones obligatorias que se deben tomar para la seguridad básica de la red del dispositivo:

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Actualice el firmware y el software cliente a tiempo

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

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

Recomendaciones "Es bueno tener" para mejorar la seguridad de la red de su dispositivo: 1. Protección física

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

2. Cambie las contraseñas con regularidad

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

3. Establecer y actualizar la información de restablecimiento de contraseñas oportunamente

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

4. Habilite el bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilite HTTPS

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

7. Enlace de dirección MAC

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

8. Asignar cuentas y privilegios de forma razonable

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

9. Deshabilite los servicios innecesarios y elija modos seguros

Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir 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 de correo.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

10. Transmisión encriptada de audio y video

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

Recordatorio: la transmisión cifrada provocará una pérdida en la eficiencia de la transmisión.

11. Auditoría segura

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

12. Registro de red

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

13. Construya un entorno de red seguro

Para garantizar mejor la seguridad del dispositivo y reducir los posibles riesgos cibernéticos, recomendamos:

- Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde una red externa.
- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere usar VLAN, red GAP y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.

- Habilite la función de filtrado de direcciones IP / MAC para limitar el rango de hosts permitidos para acceder al dispositivo.