Controlador de acceso de reconocimiento facial

Manual de usuario

V1.0.0

Prefacio

General

Este manual presenta la instalación y las operaciones básicas del controlador de acceso de reconocimiento facial (en lo sucesivo, "controlador de acceso").

Las instrucciones de seguridad

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

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

Revisión histórica

Versión	Contenido de revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento.	agosto 2020

Sobre el Manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por las operaciones que no cumplen con el manual.
- El manual se actualizaría de acuerdo con las últimas leyes y reglamentos de las regiones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Todavía puede haber desviación en los datos técnicos, descripción de funciones y operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final. Actualice el software del lector o
- pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).

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

Medidas de seguridad y advertencias importantes

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

Requisito de operación

- No coloque ni instale el controlador de acceso en un lugar expuesto a la luz solar o cerca de una fuente de calor.
- Mantenga el controlador de acceso alejado de la humedad, el polvo o el hollín.
- Mantenga el controlador de acceso instalado horizontalmente en un lugar estable para evitar que se caiga.
- No deje caer ni salpique líquido sobre el controlador de acceso y asegúrese de que no haya ningún objeto lleno de líquido sobre el controlador de acceso para evitar que el líquido fluya hacia el controlador de acceso.
- Instale el controlador de acceso en un lugar bien ventilado y no bloquee la ventilación del controlador de acceso.
- Opere el controlador de acceso dentro del rango nominal de entrada y salida de
- energía. No desmonte el controlador de acceso al azar.
- Transporte, utilice y almacene el controlador de acceso en las condiciones de humedad y temperatura permitidas.
- Para el controlador de acceso con una unidad de monitoreo de temperatura:
  - ◇ Instale la unidad de control de temperatura en un entorno interior sin viento y mantenga la temperatura ambiente interior entre 10 °C y 40 °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 usar el mismo modelo.
- Utilice los cables de alimentación recomendados en la región y cumpla con la especificación de potencia nominal.
- Utilice el adaptador de corriente proporcionado con el controlador de acceso; de lo contrario, podría provocar lesiones personales y daños en el dispositivo.
- La fuente de alimentación debe cumplir con los requisitos del estándar de seguridad de voltaje extra bajo (SELV) y suministrar energía con un voltaje nominal que cumpla con el requisito de fuente de alimentación limitada de acuerdo con IEC60950-1. Tenga en cuenta que el requisito de fuente de alimentación está sujeto a la etiqueta del dispositivo.
- Conecte el dispositivo (estructura tipo I) a la toma de corriente con puesta a tierra de protección. El acoplador
- del aparato es un dispositivo de desconexión. Cuando use el acoplador, mantenga el ángulo para facilitar la operación.

Tabla de contenido

1. Información general

1.1 Introducción

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

1.2 Características

- Pantalla LCD, la resolución del controlador de acceso de 7 pulgadas es de 1024 × 600. Admite desbloqueo
- facial, desbloqueo de tarjeta IC y desbloqueo de contraseña; desbloquear por período
- Con caja de detección de rostros; la cara más grande entre las caras que aparecen al mismo tiempo se reconoce primero; el tamaño máximo de cara se puede configurar en la web
- Lente WDR gran angular de 2MP; con iluminador automático/manual
- Con el algoritmo de reconocimiento facial, el controlador de acceso puede reconocer más de 360 posiciones en el rostro humano
- Precisión de verificación facial > 99,5 %; baja tasa de reconocimiento falso
- Admite reconocimiento de perfil; el ángulo del perfil es de 0° a 90° Admite
- detección de vida
- Admite alarma de coacción, alarma de manipulación, alarma de intrusión, alarma de tiempo de espera de contacto de puerta y alarma de umbral de superación de tarjeta ilegal
- Admite usuarios generales, 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
- Admite el control de la temperatura corporal a través de la unidad de control de la temperatura periférica

2 conexiones de cables

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

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

Tabla 2-1 Descripción del puerto

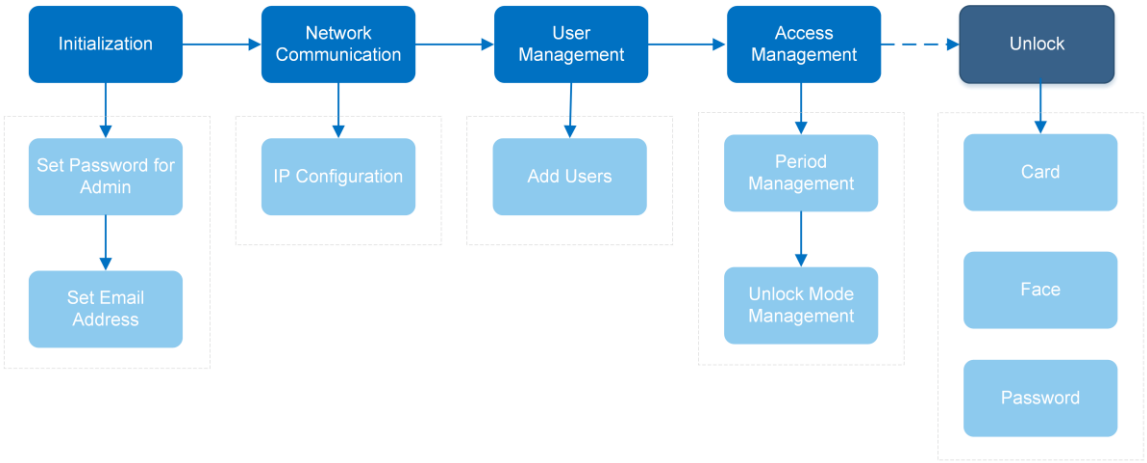
Puerto	Color de los cables	Nombre del cable	Descripción
CON1	Negro	RD–	Electrodo negativo del lector de tarjetas externo.
	Rojo	RD+	Electrodo positivo de lector de tarjetas externo.
	Azul	CASO	Entrada de alarma de sabotaje del lector de tarjetas externo.
	Blanco	D1	Entrada/salida Wiegand D1 (conectada al lector de tarjetas externo) (conectada al controlador).
	Verde	D0	Entrada Wiegand D0 (conectada al lector de tarjetas externo)/salida (conectada al controlador).
	Marrón	DIRIGIÓ	Conectado a indicador de lector externo en
	Amarillo	B	Entrada/salida del electrodo negativo RS-485 (conectado al lector de tarjetas externo) (conectado al controlador o conectado al módulo de seguridad del 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 separada para proporcionar energía. - Una vez que el módulo de seguridad está habilitado, el botón de salida, el control de bloqueo, el enlace de extinción de incendios y el monitor de temperatura no serán válidos.
	Púrpura	UN	Entrada/salida de electrodo positivo RS-485 (conectado al lector de tarjetas externo) (conectado al controlador o conectado al módulo de seguridad del 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 separada para proporcionar energía. - Una vez que el módulo de seguridad está habilitado, el botón de salida, el control de bloqueo, el enlace de extinción de incendios y el monitor de temperatura no serán válidos.
CON2	Blanco y rojo	ALARMA1_NO	La alarma 1 normalmente abre el puerto de salida.
	Blanco y naranja	ALARMA1_COM	Puerto de salida común de alarma 1.

Puerto	Color de los cables	Nombre del cable	Descripción
	Blanco y azul	ALARMA2_NO	La alarma 2 normalmente abre el puerto de salida.
	Blanco y gris	ALARMA2_COM	Puerto de salida común de alarma 2.
	Blanco y verde	TIERRA	Conectado al puerto GND común.
	marrón blanco	ALARMA1	Puerto de entrada de alarma 1.
	Blanco y amarillo	TIERRA	Conectado al puerto GND común.
	Blanco y púrpura	ALARMA2	Puerto de entrada de alarma 2.
CON3	Negro y rojo	RX	Puerto de recepción RS-232.
	Negro y naranja	Texas	Puerto de envío RS-232.
	Negro y azul	TIERRA	Conectado al puerto GND común.
	Negro y gris	SR1	Se utiliza para la detección de contacto de puerta.
	Negro y verde	EMPUJAR1	Botón de apertura de puerta de la puerta No.1
	Negro y marrón	PUERTA1_COMETRO	Puerto común de control de bloqueo.
	Negro y amarillo	PUERTA1_NO	El control de bloqueo normalmente abre el puerto.
	Negro y púrpura	PUERTA1_NC	Control de bloqueo puerto normalmente cerrado.

3 Operaciones del sistema

3.1 Procedimiento de configuración básica

Figure 3-1 Procedimiento básico de configuración



3.2 Iconos comunes

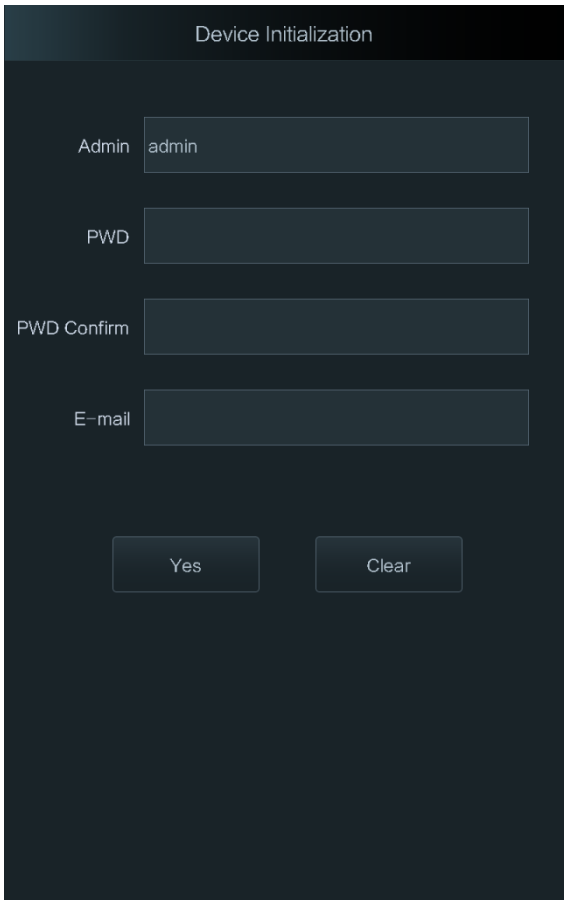
Tabla 3-1 Descripción del icono

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

3.3 Inicialización

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

Figure 3-2 Inicialización



- El administrador y la contraseña establecidos en esta interfaz se utilizan para iniciar sesión en la administración web plataforma.
- La contraseña de administrador se puede restablecer a través de la dirección de correo electrónico que ingresó si el el administrador olvida la contraseña.
- 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 caras, contraseñas y tarjetas. Consulte la Tabla 3-2.

- Si no hay operaciones en 30 segundos, el controlador de acceso pasará al modo de espera.
- La interfaz de espera puede variar con las versiones y prevalecerá la interfaz real.

Figure 3-3 Página principal

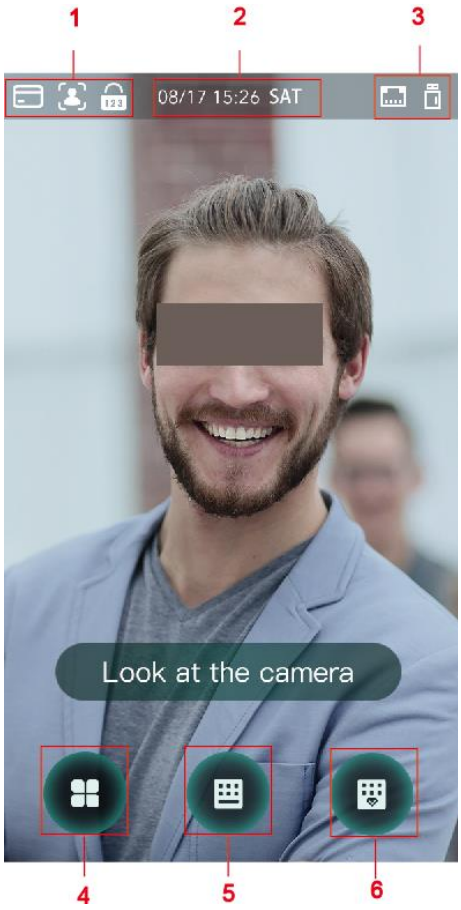


Tabla 3-2 Descripción de la página de inicio

No.	Descripción
1	Métodos de desbloqueo: Tarjeta, rostro y contraseña. Cuando la tarjeta, el rostro y la contraseña están configurados como modo de desbloqueo, el ícono de la contraseña no se mostrará en la esquina superior izquierda del controlador de acceso.
2	Fecha y hora. Muestra la fecha y hora actual.
3	Muestra el estado de la red y el estado del USB.
4	Icono del menú principal. Solo los usuarios con permiso de administrador pueden ingresar al menú principal.
5	Icono de desbloqueo de contraseña.
6	Icono de desbloqueo de contraseña de administrador.

3.5 Menú principal

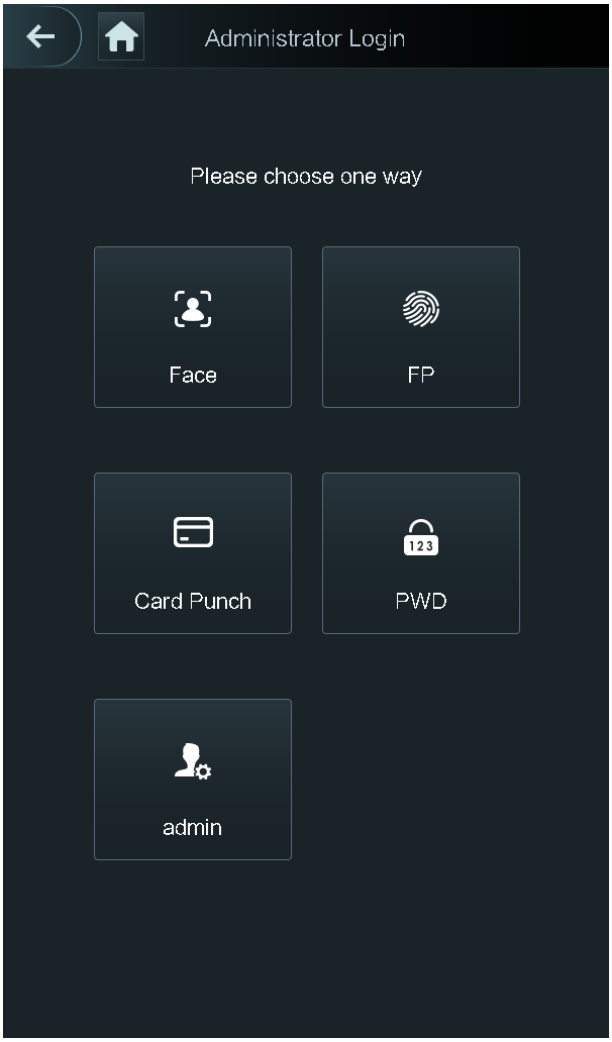
Los administradores pueden agregar usuarios de diferentes niveles, establecer parámetros relacionados con el acceso, configurar la red, ver registros de acceso e información del sistema, y más en el menú principal.

Step 1 Tocar en la interfaz de espera.

Step 2 Seleccione un método de entrada del menú principal.

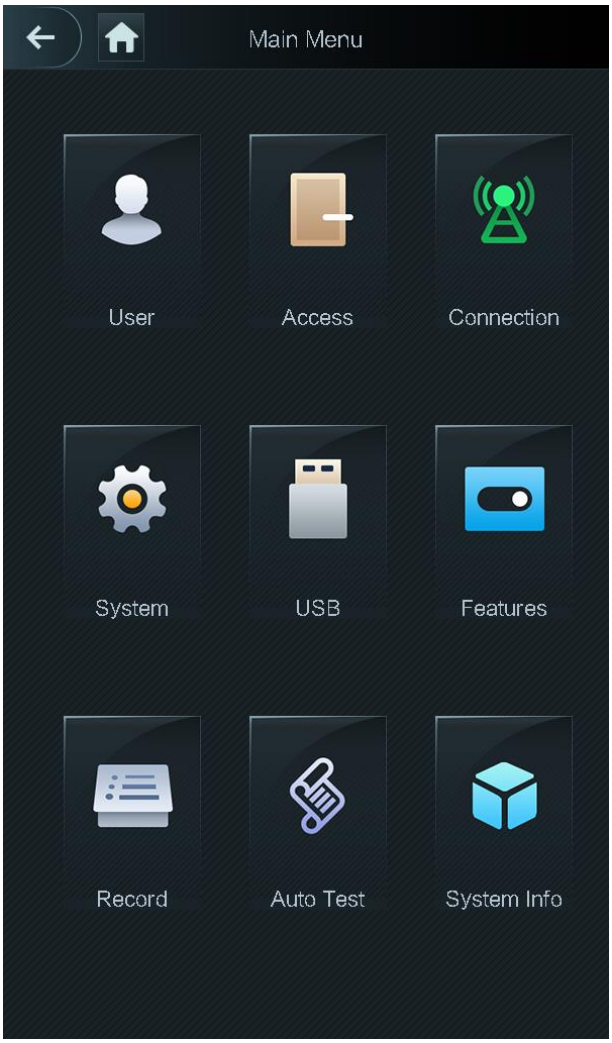
Los diferentes modos admiten diferentes métodos de desbloqueo y prevalecerá la interfaz real.

Figure 3-4 Inicio de sesión del administrador



Se muestra la interfaz del menú principal.

Figure 3-5 Menú principal



3.6 Métodos de desbloqueo

Puede desbloquear la puerta a través de caras, contraseñas y tarjetas.

3.6.1 Tarjetas

Coloque la tarjeta en el área de deslizamiento de la tarjeta para desbloquear la puerta.

3.6.2 Cara

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

3.6.3 Contraseña de usuario

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

Step 1 Tocar  en la página de inicio.

Step 2 Ingrese la ID de usuario y luego toque Ingrese la

Step 3 contraseña de usuario y luego toque La puerta está desbloqueada.

3.6.4 Contraseña de administrador

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

La contraseña de administrador no se puede utilizar cuando se selecciona NC en "3.8.1.5 Período NC".

Step 1 Tocar  en la página de inicio.

Step 2 Toque Ingrese el PWD del administrador. Ingrese la

Step 3 contraseña de administrador y luego toque La puerta está desbloqueada.

3.7 Gestión de usuarios

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

3.7.1 Adición de nuevos usuarios

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

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

Step 1 Seleccione Usuario > Nuevo usuario.

Figure 3-6 Información de nuevo usuario

Step 2 Configure los parámetros en la interfaz.

Tabla 3-3 Descripción del nuevo parámetro de usuario

Parámetro	Descripción
ID de usuario	Introduzca los ID de usuario. Los ID pueden ser números, letras y sus combinaciones, y la longitud máxima del ID es de 32 caracteres. Cada identificación es única.
Nombre	Introduzca nombres con un máximo de 32 caracteres (incluidos números, símbolos y letras).
Rostro	Asegúrese de que su cara esté centrada en el marco de captura de imágenes y el controlador de acceso tomará una foto de la cara del nuevo usuario automáticamente.
Tarjeta	Puede registrar cinco tarjetas como máximo para cada usuario. En la interfaz de registro de la tarjeta, ingrese su número de tarjeta o deslice su tarjeta, y luego el controlador de acceso leerá la información de la tarjeta. Puede habilitar el**Tarjeta de coacción**función en la interfaz de registro de la tarjeta. Las alarmas se activarán si se utiliza una tarjeta de coacción para desbloquear la puerta. Solo ciertos modelos admiten el desbloqueo de tarjetas.
PCD	La contraseña de desbloqueo de la puerta. La longitud máxima de la contraseña es de 8 dígitos. Si el controlador de acceso no tiene pantalla táctil, debe conectar el acceso

Parámetro	Descripción
	controlador a un lector de tarjetas periférico. Hay botones en el lector de tarjetas.
Nivel de usuario	Puede seleccionar un nivel de usuario para los nuevos usuarios. Hay dos opciones: ● Usuario: los usuarios solo tienen permiso para abrir puertas. ● Admin: los administradores pueden desbloquear la puerta y también tener permiso de configuración de parámetros. No importa si hay un administrador en el controlador de acceso, se necesita la autenticación de identidad del administrador.
Período	Puede establecer un período en el que el usuario puede desbloquear la puerta.
Fiesta Plan	Puede establecer un plan de vacaciones en el que el usuario puede desbloquear la puerta.
Fecha válida	Puede establecer un período durante el cual la información de desbloqueo del usuario es válida.
Nivel de usuario	Hay seis niveles: ● General: los usuarios generales pueden desbloquear la puerta normalmente. ● Lista negra: cuando los usuarios en la lista negra abren la puerta, el personal de servicio recibirá un aviso. ● Invitado: los invitados pueden desbloquear la puerta en ciertos momentos. Una vez que superan los tiempos máximos, no pueden volver a desbloquear la puerta. ● Patrulla: los usuarios de libertad condicional 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 abren la puerta, habrá un retraso de 5 segundos antes de que se cierre la puerta.
tiempo de uso	Cuando el nivel de usuario es Invitado, puede establecer el número máximo de veces que el usuario puede desbloquear la puerta.

Step 3 Tocar  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 administrar el acceso según el período, el modo de desbloqueo, la alarma, el estado de la puerta y el tiempo de retención de la cerradura.

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

3.8.1 Gestión de períodos

Puede establecer periodos, periodos de vacaciones, periodos de plan de vacaciones, periodos de puerta normalmente encendida, periodos de puerta normalmente cerrada y periodos 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 grupales y luego puede establecer planes para grupos de vacaciones. Puede configurar 128 grupos cuyo rango de números es 0–127. Puede agregar 16 días festivos a un grupo. 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). Tocar para guardar el nombre del grupo de vacaciones.

3.8.1.3 Plan de vacaciones

Puede agregar grupos de vacaciones a los planes de vacaciones. Puede usar planes de vacaciones para administrar el permiso 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 SIN

Si se agrega un período al período NO, la puerta normalmente está abierta en ese período.

Los permisos del período NO/NC son más altos que los permisos en otros períodos.

3.8.1.5 Período NC

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

3.8.1.6 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.

Debe habilitar el Período de verificación remota.

-  significa habilitado.
-  significa no habilitado.

3.8.2 Desbloquear

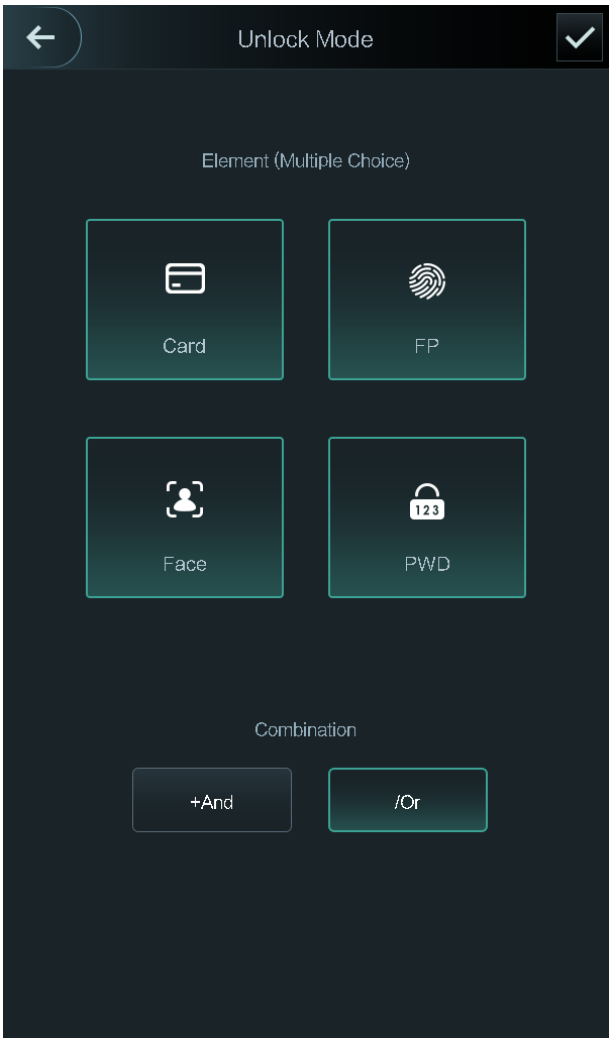
Hay cuatro modos de desbloqueo: modo de desbloqueo, desbloqueo por período, combinación de grupo y modo de control de temperatura. Los modos de desbloqueo varían según los modelos de acceso al controlador y prevalecerá el acceso real al controlador.

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 1 Seleccione el(los) modo(s) de desbloqueo.

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

Step 2 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 ingresar 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 3 Tocar  para guardar la configuración.

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

Step 4 el modo de desbloqueo.

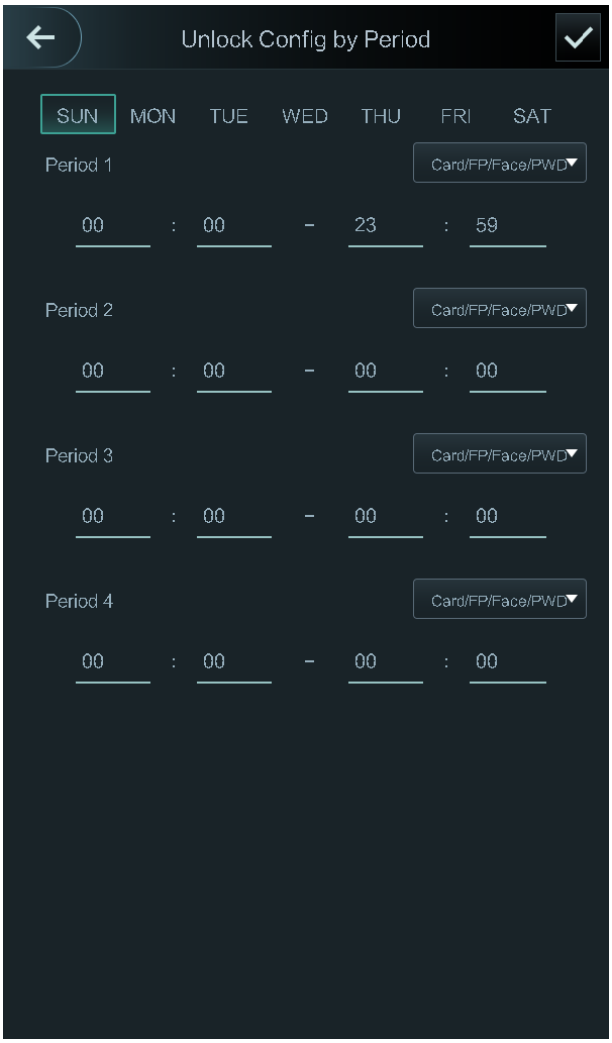
-  significa habilitado.
-  significa no habilitado.

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 tarjetas; y en el período 2, las puertas solo se pueden bloquear a través de las caras.

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

Figure 3-8 Desbloqueo 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 Tocar  para guardar la configuración.

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

Step 4 Habilite la función Desbloquear por período.

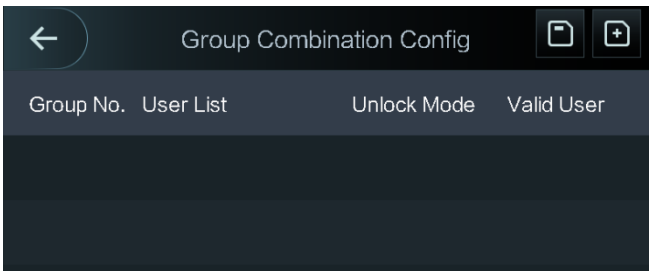
-  significa habilitado.
-  significa no habilitado.

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 la combinación de grupos está habilitada.

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

Figure 3-9 Combinación de grupos



Step 2 Tocar  para crear un grupo.

Figure 3-10 Agregar un grupo

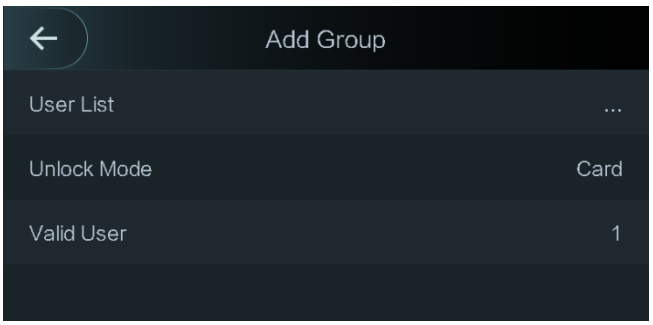


Tabla 3-4 Parámetro de grupo

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

Step 3 Tocar  para volver a la interfaz anterior.

Step 4 Tocar  para guardar la configuración.

Step 5 Habilite la combinación de grupos.

-  significa habilitado.

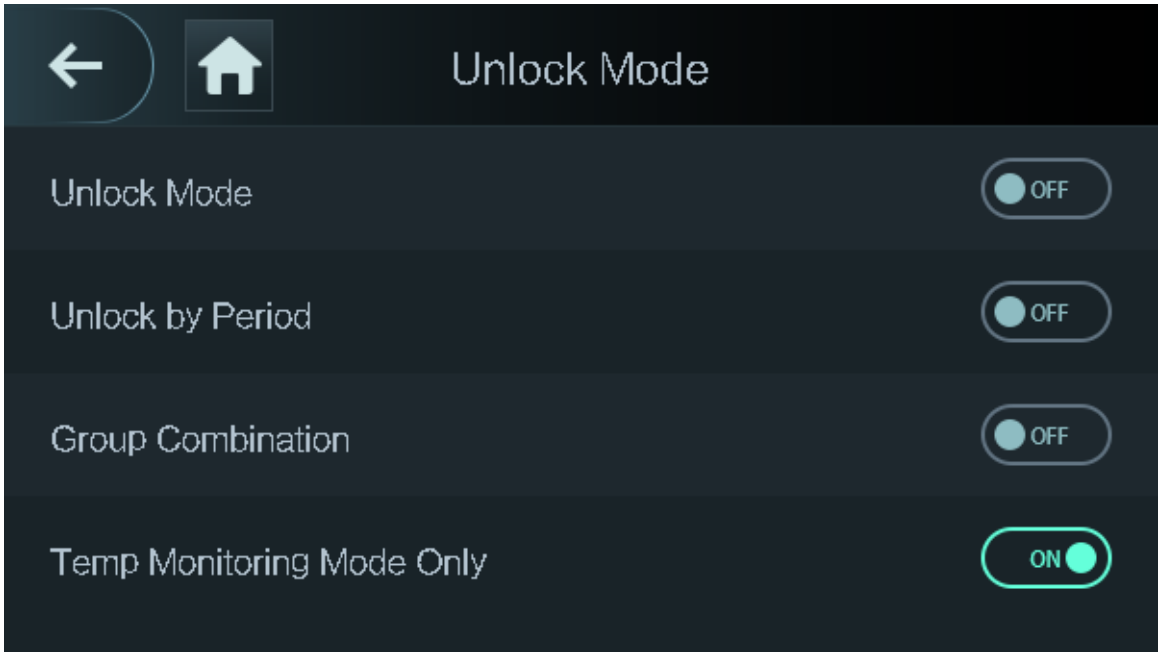
-  significa no habilitado.

3.8.2.4 Desbloqueo por control de temperatura

Las puertas se pueden desbloquear controlando la temperatura. Para desbloquear la puerta, primero se debe controlar la temperatura de la muñeca.

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

Figure 3-11 Desbloquear mediante el control de la temperatura



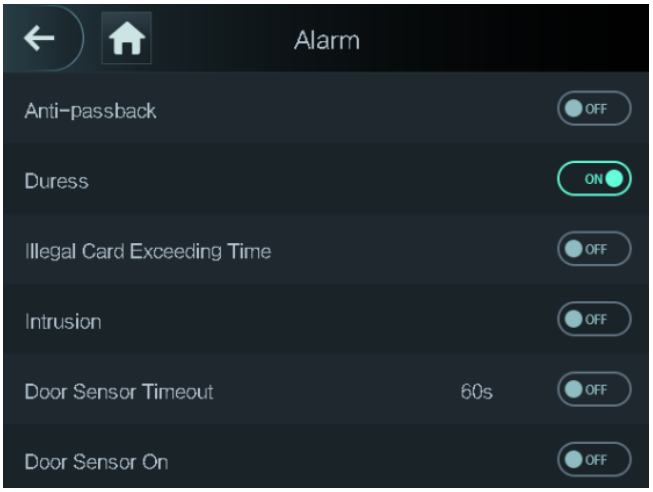
Step 2 Permitir**Solo modo de monitoreo de temperatura**función.

-  significa habilitado.
-  significa no habilitado.

3.8.3 Configuración de alarmas

Los administradores pueden administrar el permiso de desbloqueo de los visitantes a través de la configuración de alarmas. Seleccione**Acceso > Alarma**. Se muestra la interfaz de alarma.

Figure 3-12 Alarma



-  significa habilitado.

-  significa no habilitado.

Tabla 3-5 Parámetros en la interfaz de alarma

Parámetro	Descripción
Anti-passback	Después de habilitar 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 ingresa 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 desbloquear 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 desbloquear la puerta.
Coacción	Se activará una alarma cuando se use una tarjeta de coacción o una contraseña de coacción para desbloquear la puerta.
Tarjeta ilegal Excesivo Tiempo	Después de usar una tarjeta no autorizada para desbloquear la puerta más de 5 veces en 50 segundos, se activará una alarma.
Intrusión	Se activará una alarma de intrusión si se desbloquea una puerta sin que se haya liberado el contacto de la puerta.
sensor de puerta Se acabó el tiempo	Se activará una alarma de tiempo de espera si el tiempo que tarda un usuario en desbloquear la puerta supera el tiempo de espera del sensor de puerta. El intervalo de tiempo de espera del sensor de puerta es de 1 a 9999 segundos.
sensor de puerta Sobre	Solo cuando el**Sensor de puerta activado**está habilitado puede activarse la alarma de intrusión y la alarma de tiempo de espera del sensor de puerta.

3.8.4 Estado de la puerta

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

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

3.8.5 Tiempo de retención de bloqueo

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

3.9 Red de comunicacion

Para que el controlador de acceso funcione con normalidad, debe configurar los parámetros de red, puertos serie y puertos Wiegand.

3.9.1 Dirección IP

3.9.1.1 Configuración IP

Configure una dirección IP para el controlador de acceso para que se conecte a la red. Consulte la Figura 3-13 y la Tabla 3-6.

Figure 3-13 configuración de dirección IP

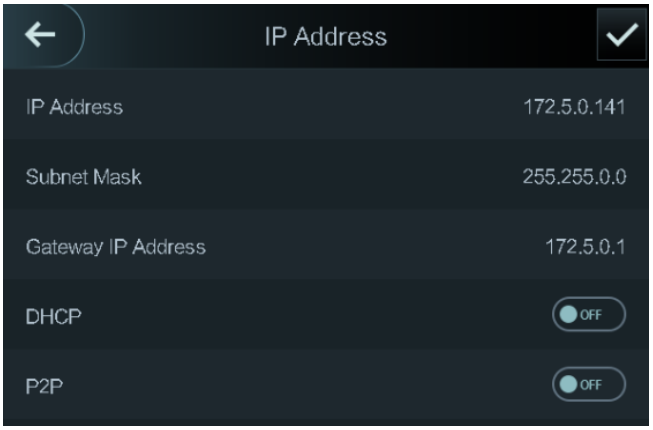


Tabla 3-6 Parámetros de configuración de IP

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 activadas. el mismo segmento de red. Después de la configuración, toque para salvar el configuraciones
DHCP	DHCP (Protocolo de configuración dinámica de host).

Parámetro	Descripción
	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 controladores de acceso modelo X de 7 pulgadas tienen NIC dobles. La dirección de administración predeterminada para El puerto de red de 1000M es 192.168.1.108 y el puerto de red de 100M es 192.168.2.108.

3.9.1.2 Registro activo

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

Las configuraciones que ha realizado se pueden borrar en la plataforma de gestión y el acceso El controlador se puede inicializar, debe proteger el permiso de administración de la plataforma en caso de pérdida de datos causada por una operación incorrecta.

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

Tabla 3-7 Registro activo

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

3.9.1.3 WiFi

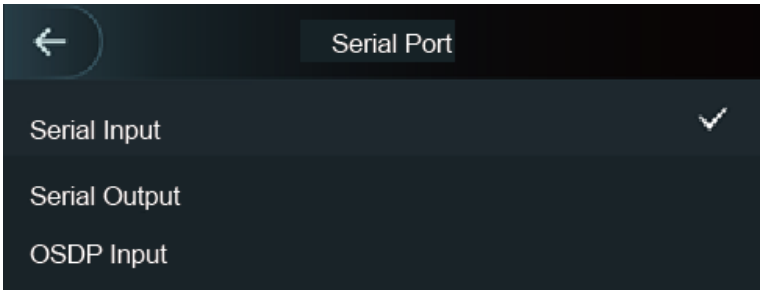
Puede conectar el controlador de acceso a la red a través de Wi-Fi si el controlador de acceso tiene función Wi-Fi.

3.9.2 Configuración del puerto serie

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

Seleccione**Conexión > Puerto Serie**, y luego el**Puerto serial**se muestra la interfaz.

Figure 3-14 Puerto serial



- Seleccione**Entrada en serie**cuando los dispositivos externos que tienen funciones de lectura y escritura de tarjetas están conectados al controlador de acceso.**Entrada en serie**se selecciona para permitir que la información de la tarjeta de acceso se envíe al controlador de acceso y la plataforma de gestión.
- Para controladores de acceso con funciones de reconocimiento facial, lectura y escritura de tarjetas, si selecciona**Salida en serie**, el controlador de acceso enviará información de bloqueo/desbloqueo al controlador de acceso. Hay dos tipos de información de bloqueo/desbloqueo:
  - ◇ ID de usuario
  - ◇ número de tarjeta
- Seleccione Entrada OSDP cuando el lector de tarjetas del protocolo OSDP esté conectado al controlador de acceso. El controlador de acceso 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**y luego se muestra la interfaz Wiegand.

Figure 3-15 Wiegand

- Seleccione**Entrada Wiegand**cuando se conecta un mecanismo externo de pase de tarjeta al controlador de acceso.
- Seleccione**Salida Wiegand**cuando el controlador de acceso funciona como un lector que se puede conectar al controlador. Consulte la Tabla 3-8.

Tabla 3-8 Salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	Él**Tipo de salida Wiegand**determina el número de tarjeta o el dígito del número que puede ser reconocido por el controlador de acceso. ● Wiegand26, tres bytes, seis dígitos. ● Wiegand34, cuatro bytes, ocho dígitos. ● Wiegand66, ocho bytes, dieciséis dígitos.
Ancho de pulso	Puede establecer el ancho de pulso y el intervalo de pulso.

Parámetro	Descripción
Intervalo de pulso	
Tipo de datos de salida	Puede seleccionar los tipos de datos de salida. ● ID de usuario: si se selecciona ID de usuario, se generará la ID de usuario. ● Nº de tarjeta: si se selecciona Nº de tarjeta, se emitirá el número de tarjeta.

3.10 Sistema

3.10.1 Hora

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

- cuando seleccionas**Protocolo de tiempo de red**(NTP), debe habilitar NTP Check función primero. Dirección IP del servidor: ingrese la dirección IP del servidor de tiempo, hora del acceso El controlador se sincronizará con el servidor horario.
- Puerto: Introduzca 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 3-16 Parámetro de cara

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

Tabla 3-9 Parámetro de cara

Nombre	Descripción
Reconocimiento facial Límite	La precisión del reconocimiento facial se puede ajustar. Cuanto mayor sea el valor, mayor será la precisión.

Nombre	Descripción
máx. Ángulo de reconocimiento facial	Configure el ángulo de disparo del panel de control de los perfiles. Cuanto mayor sea el valor, se reconocerá una 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 las caras según sea necesario. El valor cambia según el tamaño de la cara y la distancia entre las caras y la lente. Cuanto más cerca esté la cara de la lente, mayor debe ser el valor. Si un adulto está a 1,5 metros de la lente, el valor de la distancia pupilar puede estar entre 50 y 70.
Tiempo de espera de reconocimiento	Cuando una persona que no tiene el permiso de acceso se para frente al controlador de acceso y obtiene el reconocimiento facial, el controlador indicará que el reconocimiento facial falló. El intervalo de solicitud se denomina tiempo de espera de reconocimiento.
Intervalo de reconocimiento	Cuando una persona que tiene el permiso de acceso se para frente al controlador de acceso y obtiene el reconocimiento facial, el controlador indicará que el reconocimiento facial se realizó correctamente. El intervalo de indicación es el intervalo de reconocimiento.
Indicación de cara no válida Intervalo	Cuando una cara sin permiso de acceso se para frente al controlador de acceso, el controlador indicará que la cara no es válida. El intervalo de solicitud es un intervalo de solicitud de cara no válido.
Umbral anti-falsificación	Esta función evita que las personas se desbloqueen mediante imágenes de rostros humanos o modelos de rostros. Cuanto mayor sea el valor, las imágenes de rostros más difíciles pueden abrir la puerta. El rango de valores recomendado es superior a 80.
Temperatura Vigilancia	Establezca si habilitar el control de la temperatura corporal. ● Unidad de temperatura: Seleccione una unidad de temperatura. ● Distancia de control de temperatura (cm): el valor predeterminado es de 5 cm. Establezca otros valores para permitir el control de la temperatura dentro de una distancia definida que oscila entre 2 cm y 5 cm. ● Umbral de temperatura alta: establezca el umbral de temperatura alta. La temperatura corporal monitoreada se considerará alta si es mayor o igual que el valor establecido. ● Umbral de temperatura baja: establece el umbral de temperatura baja. La temperatura corporal no se controlará si es inferior al valor establecido. ● Valor de corrección de temperatura: este parámetro es para realizar 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 múltiples muestras monitoreadas para la prueba y luego corregir la desviación de temperatura por 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 inferior a 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.

Nombre	Descripción
	● Tiempo de espera de monitoreo de temperatura: establezca la duración del monitoreo de temperatura. Si el tiempo de monitoreo es más largo que este valor, la pantalla le pedirá que inicie el siguiente monitoreo de temperatura. Solo el controlador de acceso con una unidad de monitoreo de temperatura admite este parámetro.
Modo máscara	● Sin detección: la máscara no se detecta durante el reconocimiento facial. ● Recordatorio de máscara: la máscara se detecta durante el reconocimiento facial. Si se detecta a la persona sin usar una máscara, el sistema le indicará un recordatorio de máscara y se le permitirá el paso. ● Intercepción de máscara: la máscara se detecta durante el reconocimiento facial. Si la persona es detectada sin usar una máscara, el sistema le indicará un recordatorio de la máscara y no se le permitirá el paso.

3.10.3 Modo de imagen

Hay tres opciones:

- Interior: Seleccione**Interior**cuando el controlador de acceso se instala en interiores;
- Exterior: Seleccionar**Exterior**cuando el controlador de acceso se instala al aire libre;
- Otro: Seleccionar**Otro**cuando el controlador de acceso se instala en lugares con retroiluminación como corredores 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 está oscuro, la luz de relleno normalmente está apagada; de lo contrario, la luz de llenado estará encendida.
- NO: La luz de llenado normalmente está encendida. NC:
- La luz de llenado normalmente está cerrada.

3.10.5 Configuración del brillo de la luz de relleno

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

3.10.6 Ajuste de volumen

Tocar  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, menos claras serán las imágenes.

3.10.8 Restaurar a la configuración de fábrica

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

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

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

3.10.9 Reiniciar

Seleccione**Configuración > Reiniciar**, tocar**Reiniciar**y el controlador de acceso se reiniciará.

3.11 USB

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

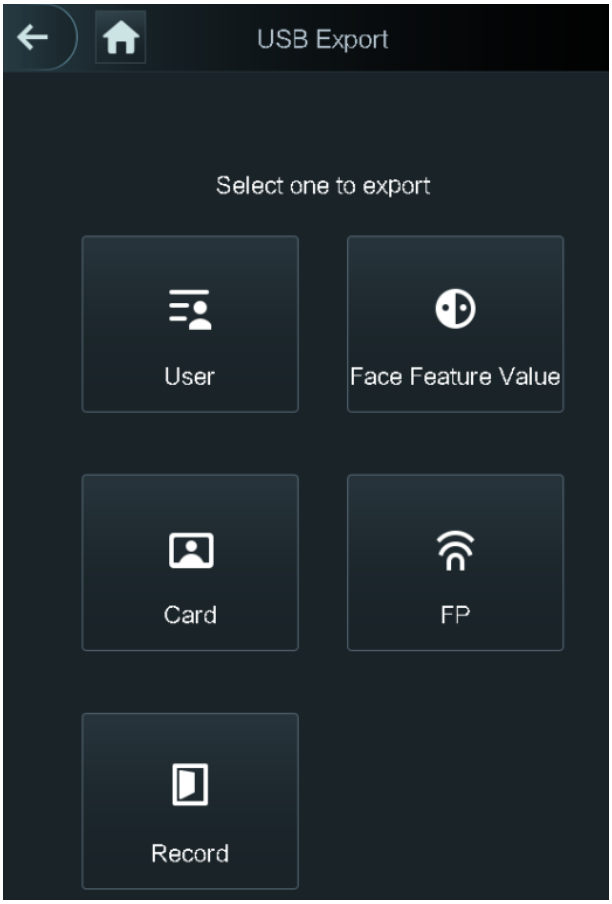
3.11.1 Exportación USB

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

Step 1 Seleccione USB > Exportar USB.

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

Figure 3-17 Exportación USB



Step 2 Seleccione el tipo de datos que desea exportar. Se muestra el mensaje Confirmar para exportar. Tocar**DE**

Step 3 **ACUERDO**.

Los datos exportados se guardarán en el USB.

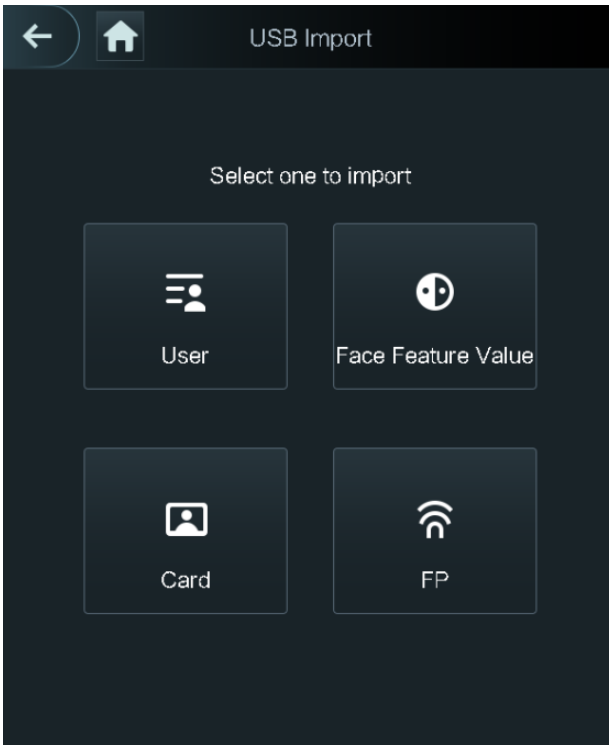
3.11.2 Importación USB

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

Step 1 Seleccione USB > Importar USB.

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

Figure 3-18 Importación USB



Step 2 Seleccione el tipo de datos que desea importar. el aviso**Confirmar para importar**se visualiza. Tocar**DE**

Step 3 **ACUERDO**.

Los datos de la unidad flash USB se importarán al controlador de acceso.

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 de la unidad flash USB.

- Asegúrese de que la computadora utilizada para iniciar sesión en la web esté en la misma LAN que el dispositivo .
- 7 pulgadas controladores de acceso modelo X de tener dos NIC . La gestión por defecto la dirección para el puerto de red de 1000M es 192.168.1.108, y para el puerto de red de 100M es 192.168.2.108.

Step 2 Seleccione USB > Actualización de USB.

el aviso**Confirmar para actualizar**se visualiza. Tocar**DE**

Step 3 **ACUERDO**.

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

3.12 Características

Puede realizar configuraciones sobre privacidad, reversión del número de tarjeta, módulo de seguridad, tipo de sensor de puerta y retroalimentación de resultados. Para detalles de las funciones mencionadas, vea la Figura 3-19 y la Tabla 3-10.

Figure 3-19 Características

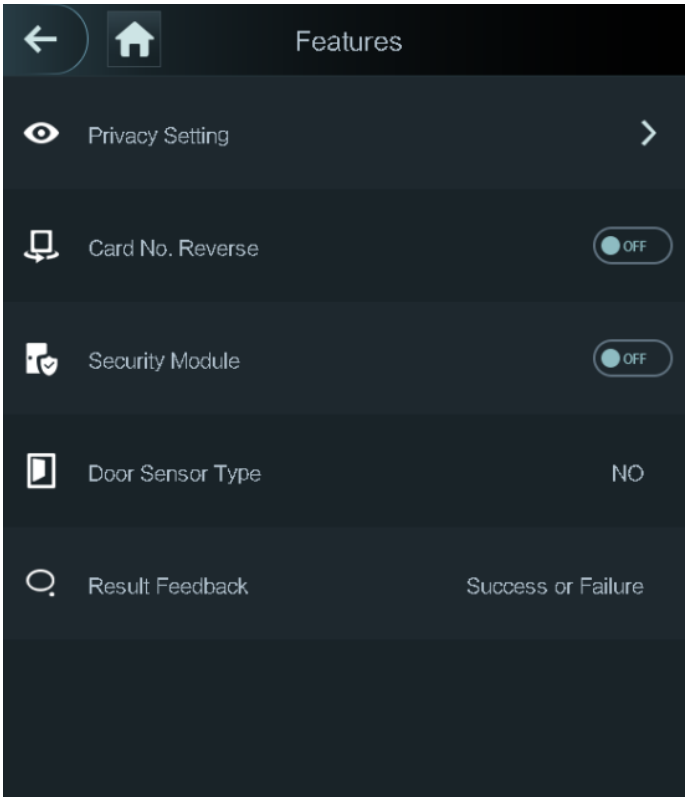


Tabla 3-10 Descripción de funciones

Parámetro	Descripción
Configuración de privacidad	Consulte "3.12.1 Configuración de privacidad" para obtener más detalles.
Número de tarjeta Reverso	Si el lector de tarjetas de terceros necesita conectarse al controlador de acceso a través del puerto de salida wiegand, debe habilitar la función Invertir 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 separada para proporcionar energía. ● Una vez que el módulo de seguridad está habilitado, el botón de salida, el control de bloqueo, el enlace de extinción de incendios y el monitor de temperatura no serán válidos.
Tipo de sensor de puerta	Hay dos opciones:**NO**y**CAROLINA DEL NORTE**.
Comentarios sobre los resultados	Muestra si el desbloqueo tuvo éxito o falló.

3.12.1 Configuración de privacidad

Figure 3-20 Configuración de privacidad

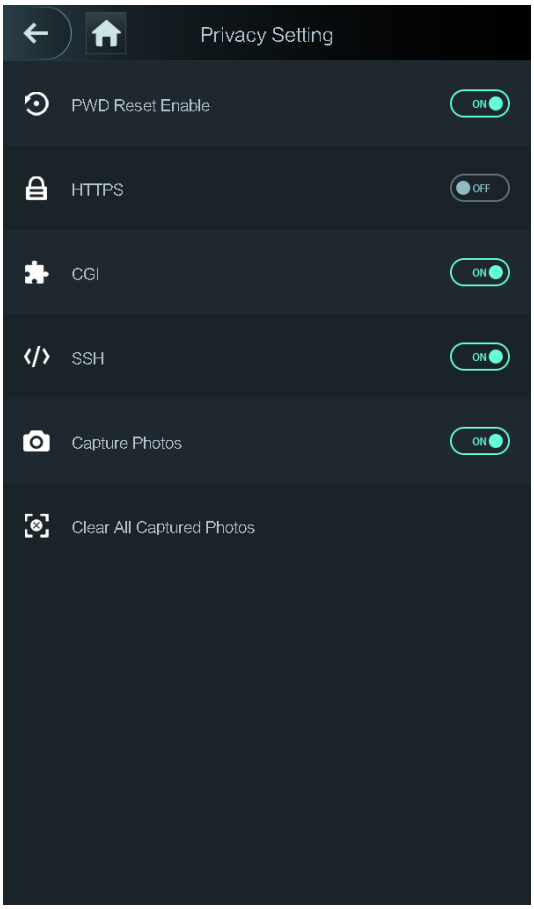


Tabla 3-11 Características

Parámetro	Descripción
Restablecimiento de PCD Permitir	Si el**Habilitar restablecimiento de PWD**está habilitada, puede restablecer la contraseña. La función Restablecer PWD está habilitada de forma predeterminada.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) es un protocolo para la comunicación segura a través de una red informática. Cuando HTTPS está habilitado, HTTPS se utilizará para acceder a los comandos CGI; de lo contrario, se utilizará HTTP. 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 dinámicamente. Cuando CGI está habilitado, se pueden usar comandos CGI. El CGI está habilitado de forma predeterminada.
SSH	Secure Shell (SSH) es un protocolo de red criptográfico para operar servicios de red de forma segura en una red no segura. Cuando SSH está habilitado, SSH proporciona un servicio criptográfico para la transmisión de datos.
Capturar foto	Si selecciona ON, cuando un usuario abre la puerta, la foto del usuario será

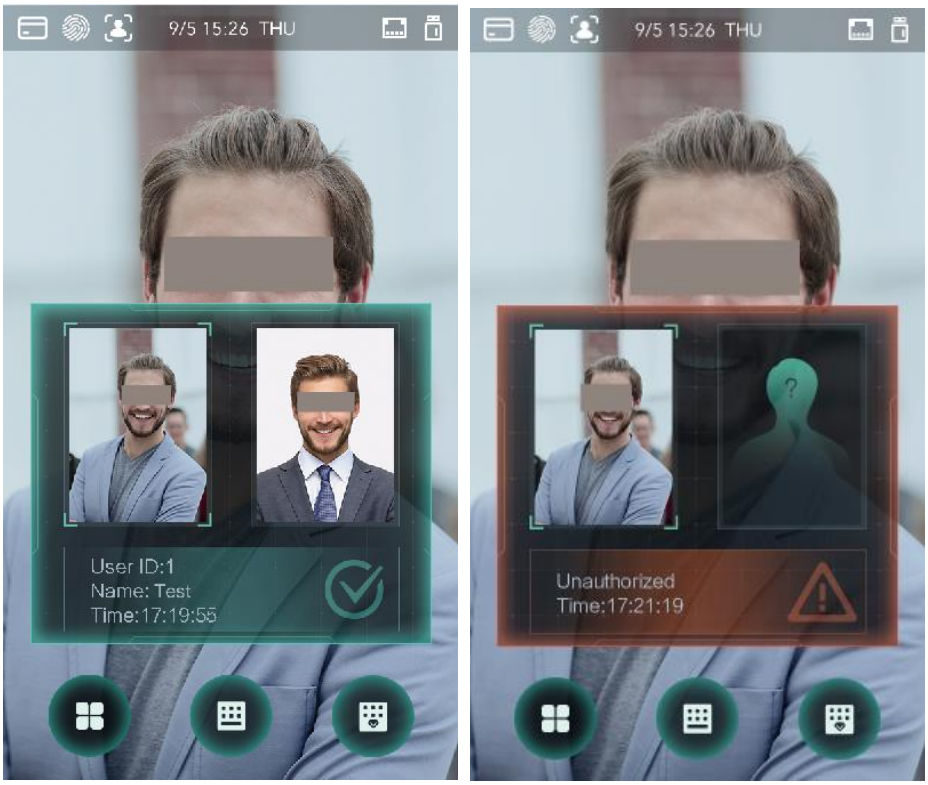
Parámetro	Descripción
	tomado automáticamente. Esta función está activada de forma predeterminada.
Limpiar todo capturado fotos	Toque el icono y podrá eliminar todas las fotos capturadas.

3.12.2 Comentarios sobre los resultados

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

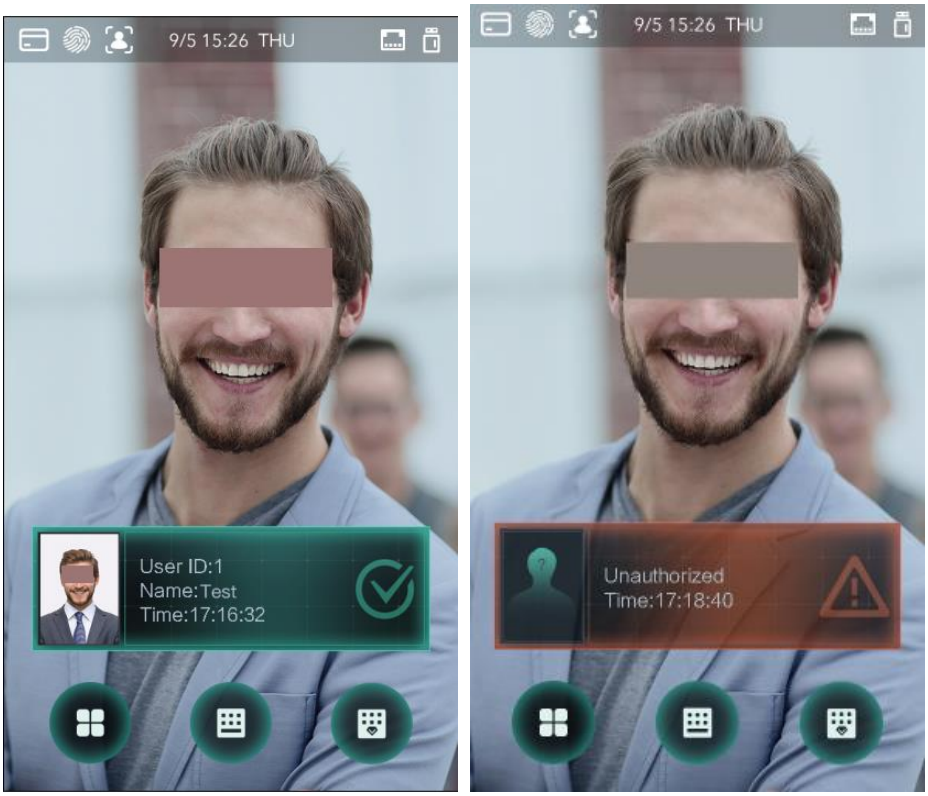
Modo 1

Figure 3-21 Modo 1



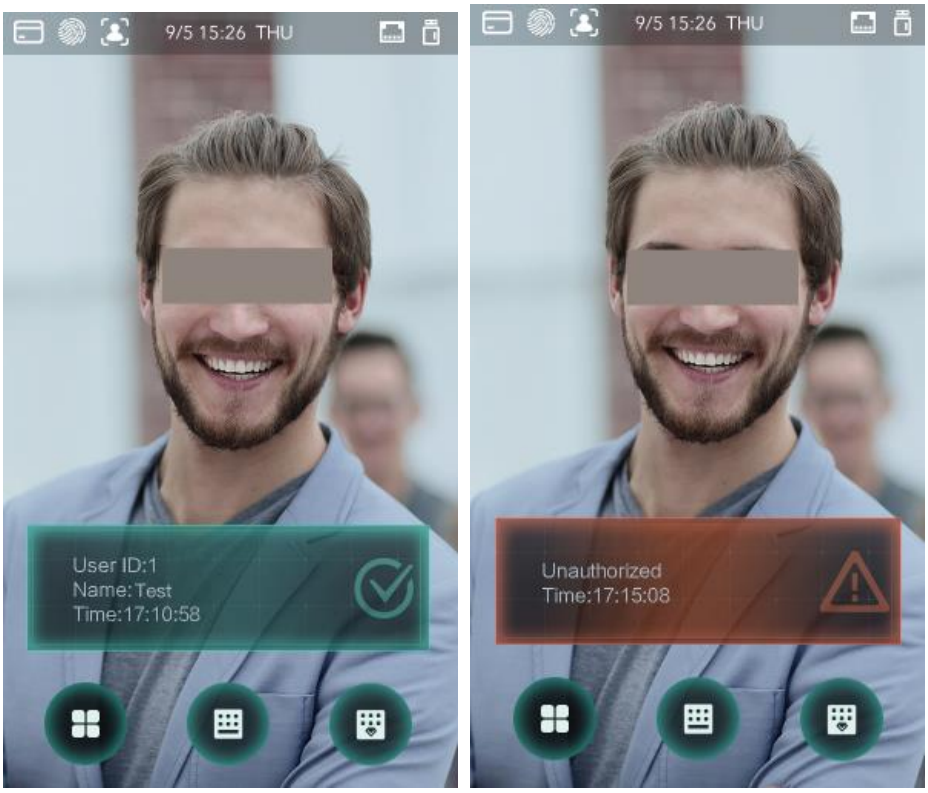
Modo 2

Figure 3-22 Modo 2



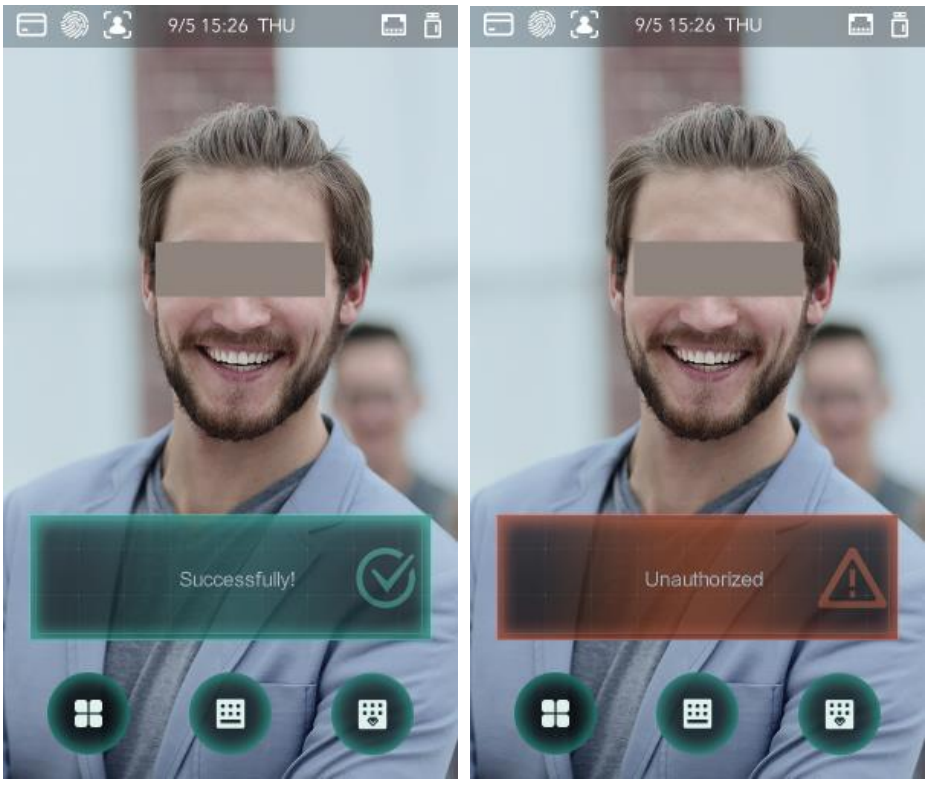
Modo 3

Figure 3-23 Modo 3



Modo 4

Figure 3-24 Modo 4



3.13 Registro

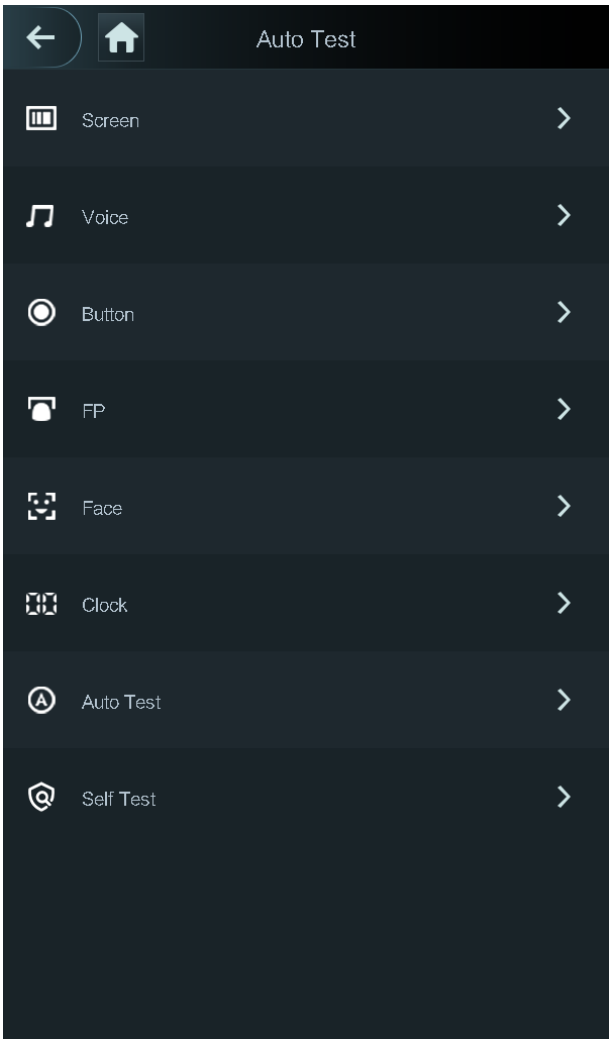
Puede consultar todos los registros de desbloqueo.

Figure 3-25 Buscar registros de perforaciones

3.14 Auto prueba

Cuando usa el controlador de acceso por primera vez o cuando el controlador de acceso no funciona correctamente, puede usar la función de prueba automática para verificar si el controlador de acceso puede funcionar normalmente. Realice las acciones de acuerdo con las indicaciones.

Figure 3-26 Auto prueba



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

3.15 Información del sistema

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

4 Operaciones Web

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

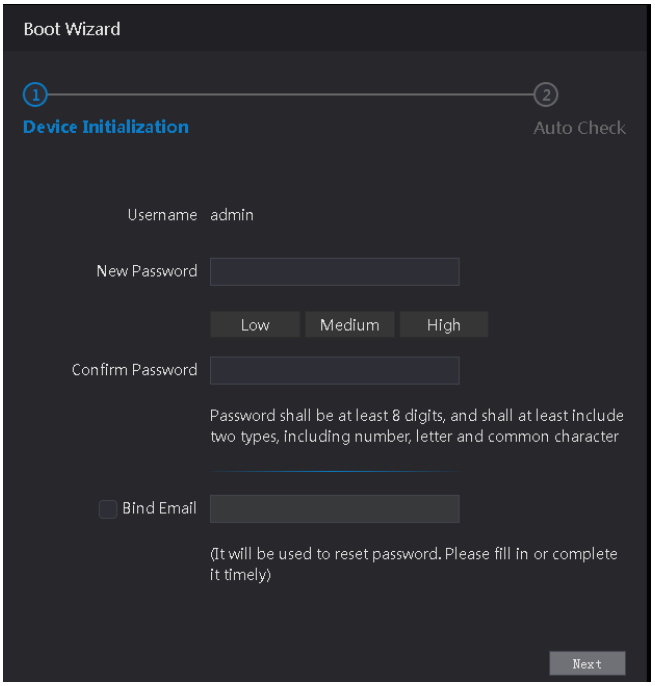
4.1 Inicialización

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 controlador de acceso 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 controladores de acceso modelo X de 7 pulgadas tienen NIC dobles. La dirección IP predeterminada para El puerto de red de 1000M es 192.168.1.108, y para el puerto de red de 100M es 192.168.2.108.

Figure 4-1 Inicialización



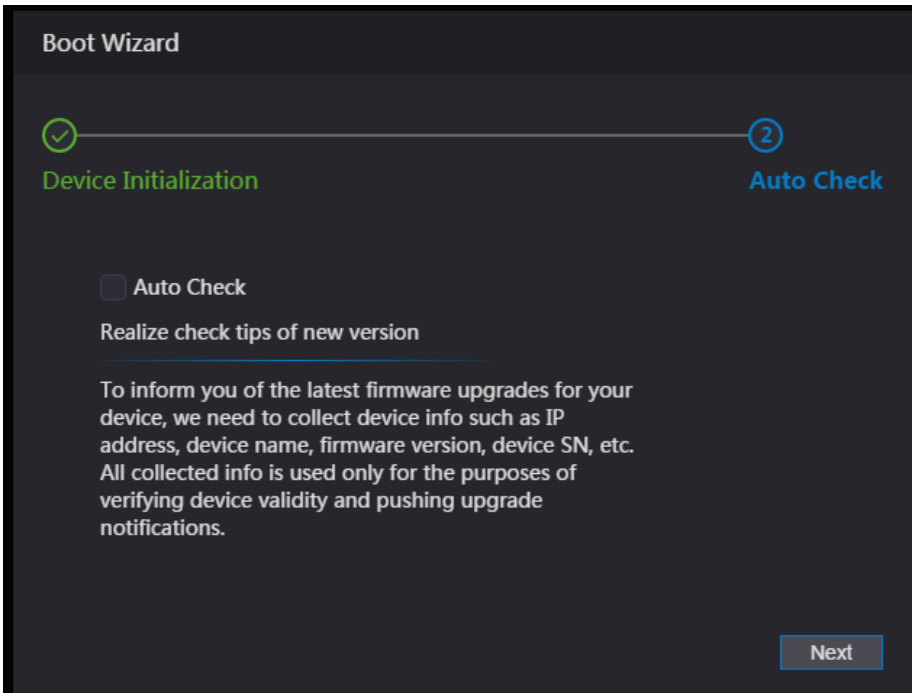
Step 2 Ingrese la nueva contraseña, confirme la contraseña, ingrese una dirección de correo electrónico y luego haga clic en **próximo**.

- 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 especiales carácter (excluyendo ' " ; : &). Establezca una contraseña de alto nivel de seguridad de acuerdo con la solicitud de seguridad de la contraseña.

- Por seguridad, mantenga la contraseña correctamente después de la inicialización y cambie la contraseña regularmente.
- 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

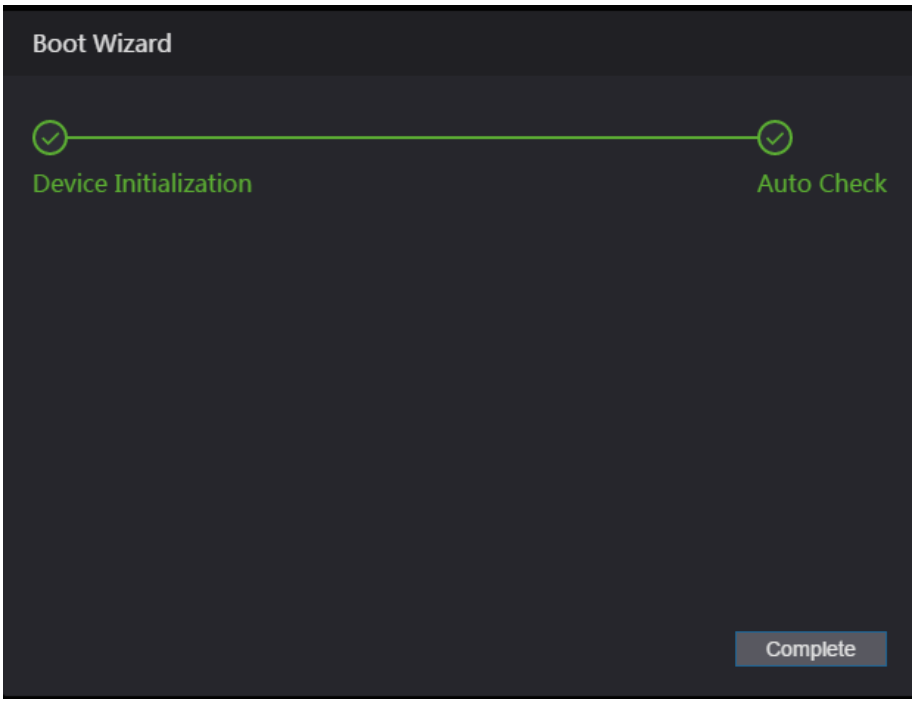


Step 4 Puede decidir si seleccionar**Verificación automática**o no.

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

Step 5 Hacer clic**próximo**.

Figure 4-3 Configuración finalizada



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

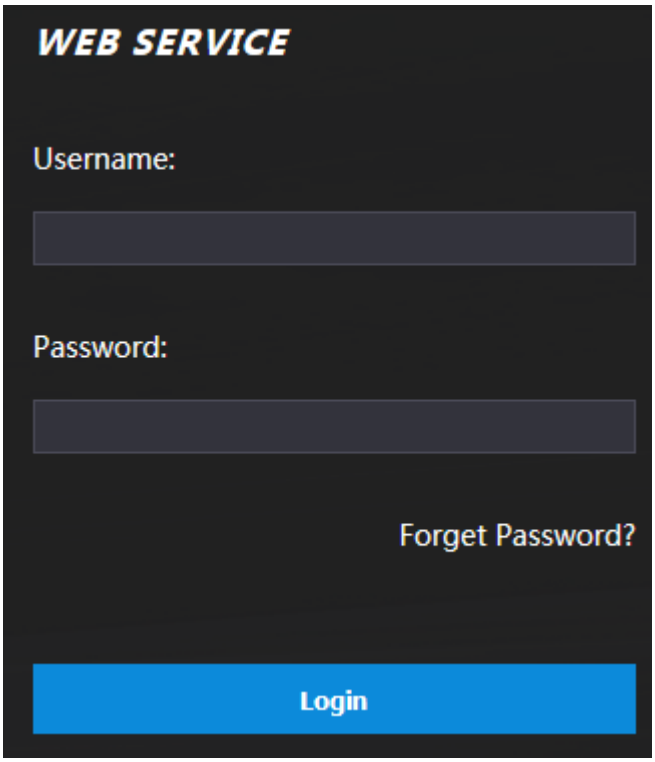
Se muestra la interfaz de inicio de sesión web.

4.2 Acceso

Step 1 Abra el navegador web IE, ingrese la dirección IP del controlador de acceso en la barra de direcciones y presione**Ingresar**.

- 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 .
- 7 pulgadas controladores de acceso modelo X de tener dos NIC . La gestión por defecto la dirección para el puerto de red de 1000M es 192.168.1.108, y para el puerto de red de 100M es 192.168.2.108.

Figure 4-4 Acceso



Step 2 Introduzca el nombre de usuario y la contraseña.

- El nombre de administrador predeterminado es admin y la contraseña es la contraseña de inicio de sesión después de inicializar el acceso controlador . Modifique el administrador regularmente y mantenga correctamente por el bien de la seguridad.
- Si olvida la contraseña de inicio de sesión del administrador, puede hacer clic en**¿Se te olvidó tu contraseña?**para reinicialo. Ver " 4.3 Restablecimiento de la contraseña ."

Step 3 Hacer clic**Acceso**.

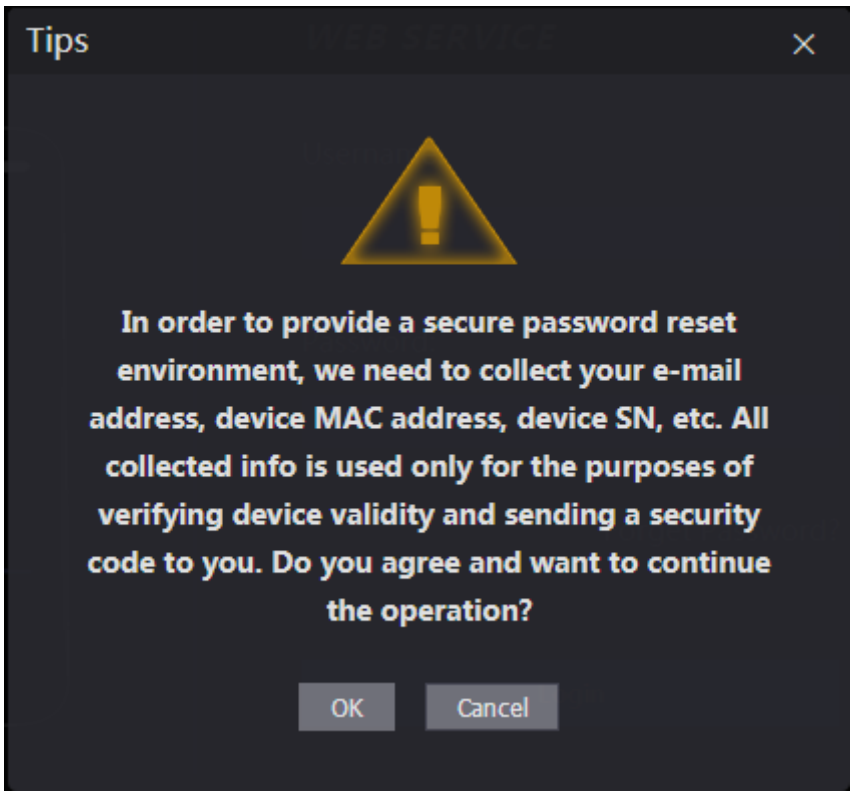
Se ha iniciado sesión en la interfaz web.

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**¿Se te olvidó tu contraseña?**en la interfaz de inicio de sesión. Él**Consejos**se muestra la interfaz.

Figure 4-5 Consejos

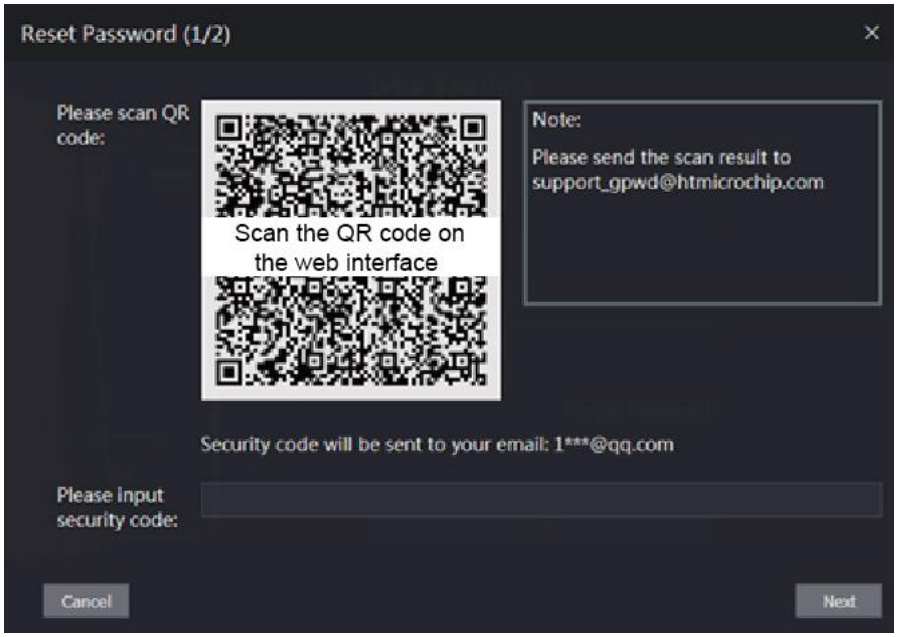


Step 2 Lea los consejos.

Step 3 Hacer clic**DE ACUERDO**.

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

Figure 4-6 Restablecer la contraseña



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

- Como máximo se generarán dos códigos de seguridad escaneando el mismo código QR. Si los códigos de seguridad dejan de ser válidos, para obtener más códigos de seguridad, actualice el código QR.
- Debe enviar el contenido que obtiene después de escanear el código QR al dirección de correo electrónico designada, y luego obtendrá el código de seguridad.
- Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, será convertirse en inválido.
- Si se ingresan códigos de seguridad incorrectos cinco veces consecutivas, el administrador se congelará durante cinco minutos.

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

Step 6 **próximo**.

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

Step 7 Restablece y confirma la nueva contraseña.

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

Step 8 Hacer clic**DE ACUERDO**, y el restablecimiento se completa.

4.4 Enlace de alarma

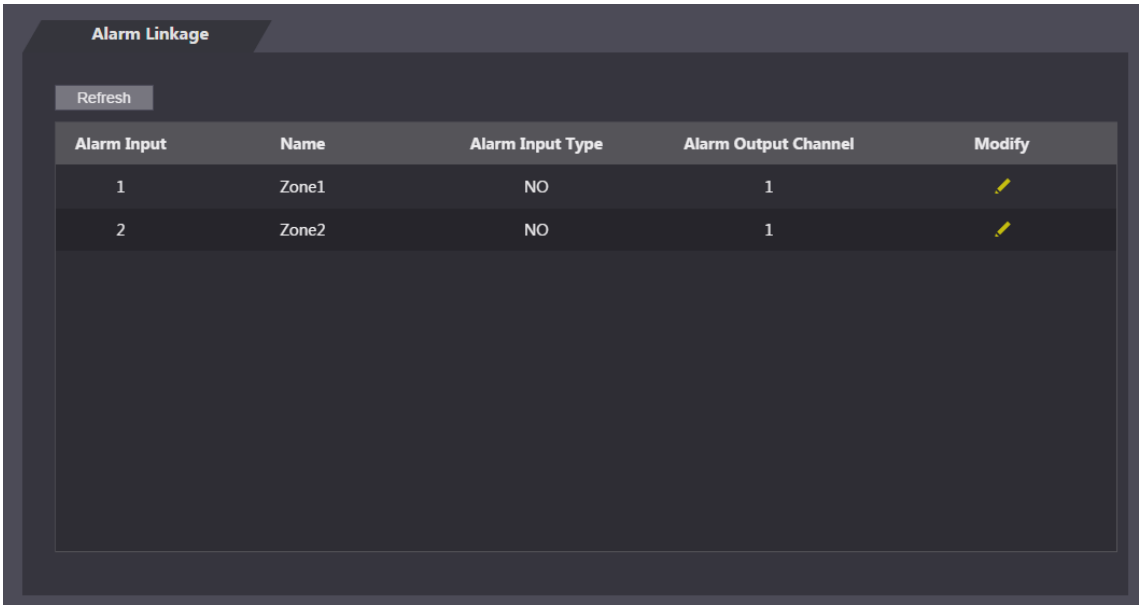
4.4.1 Configuración de enlace de alarma

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

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

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

Figure 4-7 Enlace de alarma



Step 2 Hacer clic  , y luego puede modificar los parámetros de enlace de alarma.

Figure 4-8 Modificación del parámetro de enlace de alarma

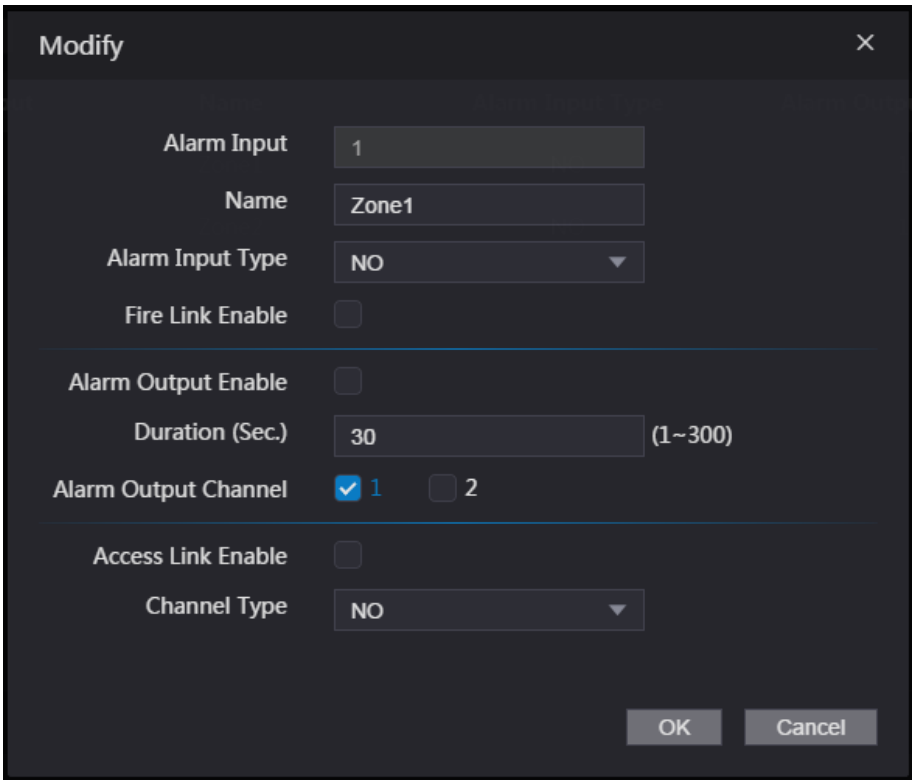


Tabla 4-1 Descripción del parámetro de enlace de alarma

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

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

La configuración en la web se sincronizará con la configuración en el cliente si el el controlador de acceso se agrega a un cliente.

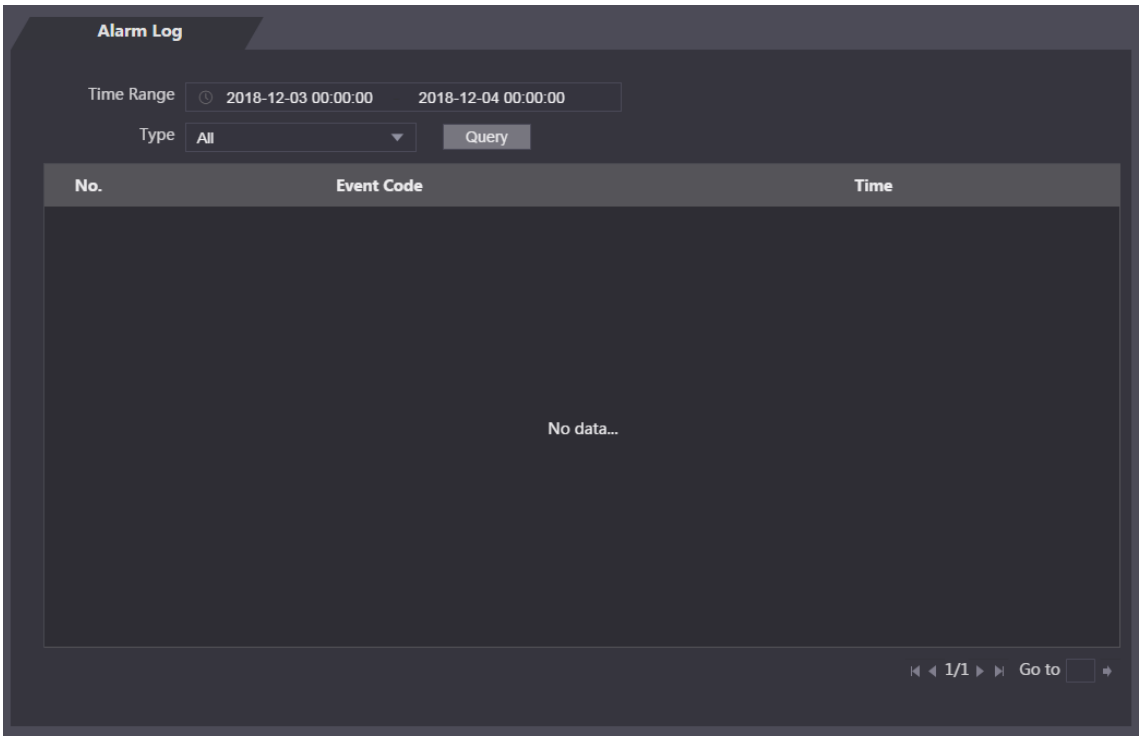
4.4.2 Registro de alarmas

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

Step 1 Seleccione Vinculación de alarmas > Registro de alarmas.

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

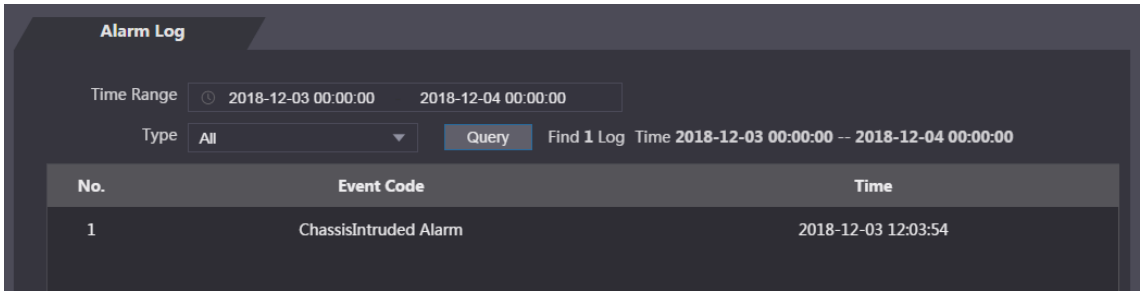
Figure 4-9 Registro de alarmas



Step 2 Seleccione un intervalo de tiempo y un tipo de alarma y, a continuación, haga clic en**Consulta**.

Se muestran los resultados de la consulta.

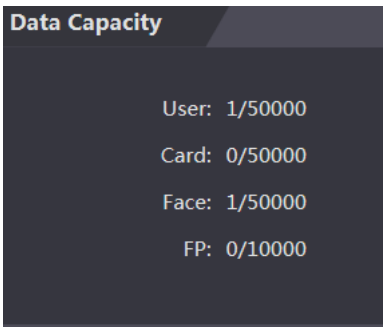
Figure 4-10 Resultados de la consulta



4.5 Capacidad de datos

Puede ver cuántos usuarios, tarjetas e imágenes de rostros puede contener el controlador de acceso en el **Capacidad de datos**interfaz.

Figure 4-11 Capacidad de datos



4.6 Configuración de vídeo

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

4.6.1 Velocidad de datos

Figure 4-12 Velocidad de datos

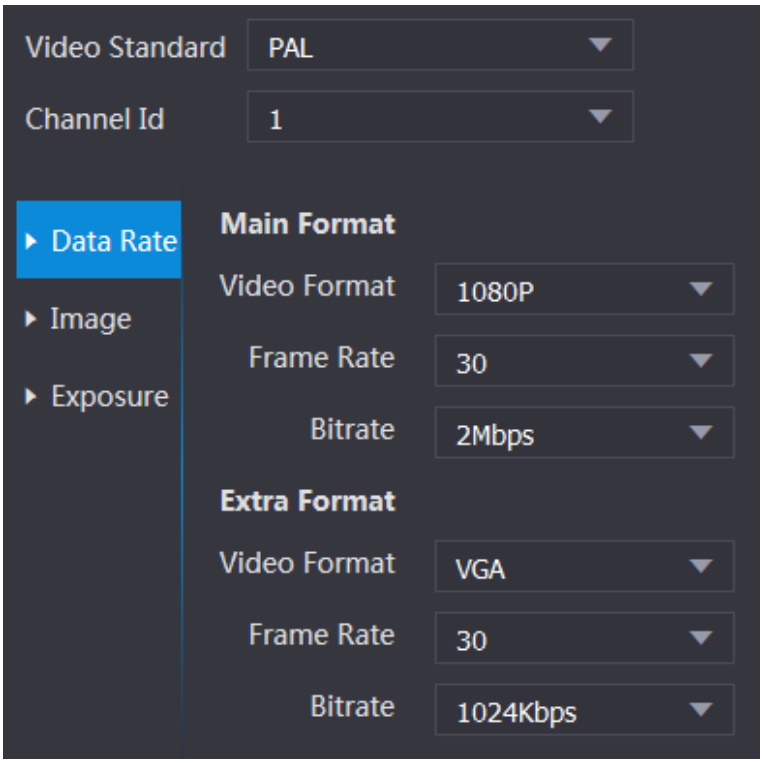


Tabla 4-2 Descripción del parámetro de velocidad de datos

Parámetro	Descripción
Estándar de vídeo	Hay dos opciones: NTSC y PAL. Seleccione un estándar de acuerdo con el estándar de video de su región.
Canal	Hay dos opciones: 1 y 2. 1 es cámara de luz blanca y 2 es cámara de luz IR.

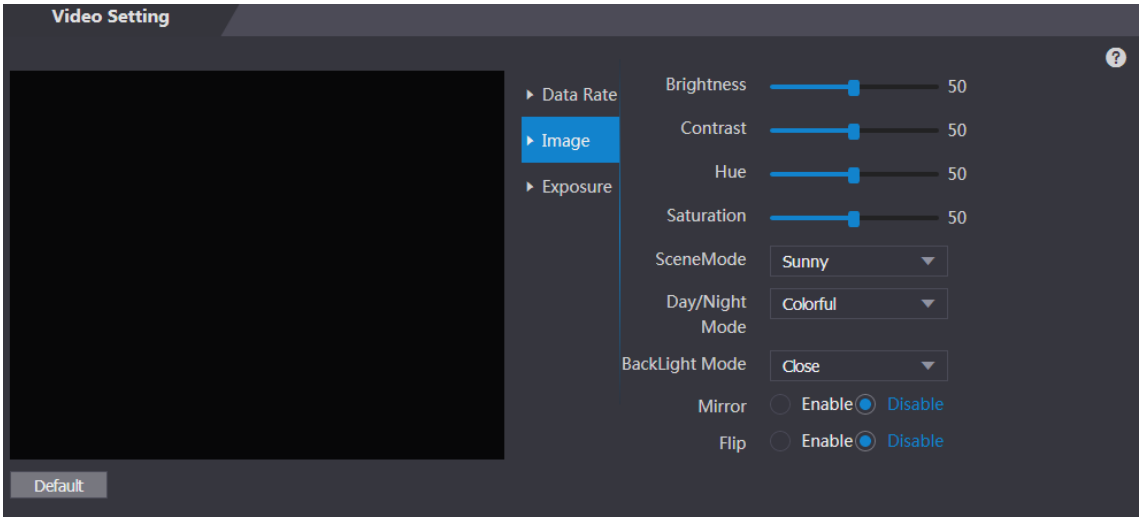
Parámetro		Descripción
Principal Formato	Formato de video	Hay cuatro opciones: D1, VGA, 720p y 1080p. Seleccione una opción de acuerdo con la calidad de video que desee.
	Cuadros por segundo	La velocidad a la que aparecen fotogramas consecutivos en una pantalla. Él el rango de velocidad de fotogramas es de 1 a 30 fps.
	Tasa de bits	El número de bits que se transmiten o procesan por unidad de tiempo. Hay cinco opciones: 2Mbps, 4Mbps, 6Mbps, 8Mbps y 10Mbps.
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. Él el rango de velocidad de fotogramas es de 1 a 30 fps.
	Tasa de bits	El número de bits que se transmiten 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.

4.6.2 Imagen

Hay dos canales, y necesita configurar parámetros para cada canal.

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

Figure 4-13 Imagen



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

Tabla 4-3 Descripción del parámetro de imagen

Parámetro	Descripción
Brillo	Cuanto mayor sea el valor, más brillantes serán las imágenes.
Contraste	El contraste es la diferencia de luminancia o color que hace que un objeto sea distinguible. Cuanto mayor sea el valor de contraste, mayor será el brillo y el contraste de color.
Matiz	Cuanto mayor sea el valor, más profundo será el color.
Saturación	Cuanto mayor sea el valor, más brillantes serán los colores.

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

4.6.3 Exposición

Tabla 4-4 Descripción de los parámetros de exposición

Parámetro	Descripción
Contra parpadeo	● 50 Hz: cuando la frecuencia de servicio de la corriente alterna es de 50 Hz, la exposición se ajusta automáticamente para asegurarse de que no haya rayas en las imágenes. ● 60 Hz: cuando la frecuencia de servicio de la corriente alterna es de 60 Hz, la exposición se ajusta automáticamente para asegurarse de que no haya rayas en las imágenes. ● Exterior: Cuando**Exterior**está seleccionado, se puede cambiar el modo de exposición.
Modo de exposición	 - cuando seleccionas**Exterior**en la lista desplegable Antiparpadeo, puede seleccionar**Prioridad de obturador**como el modo de exposición. - Los modos de exposición de diferentes dispositivos pueden variar, y el real

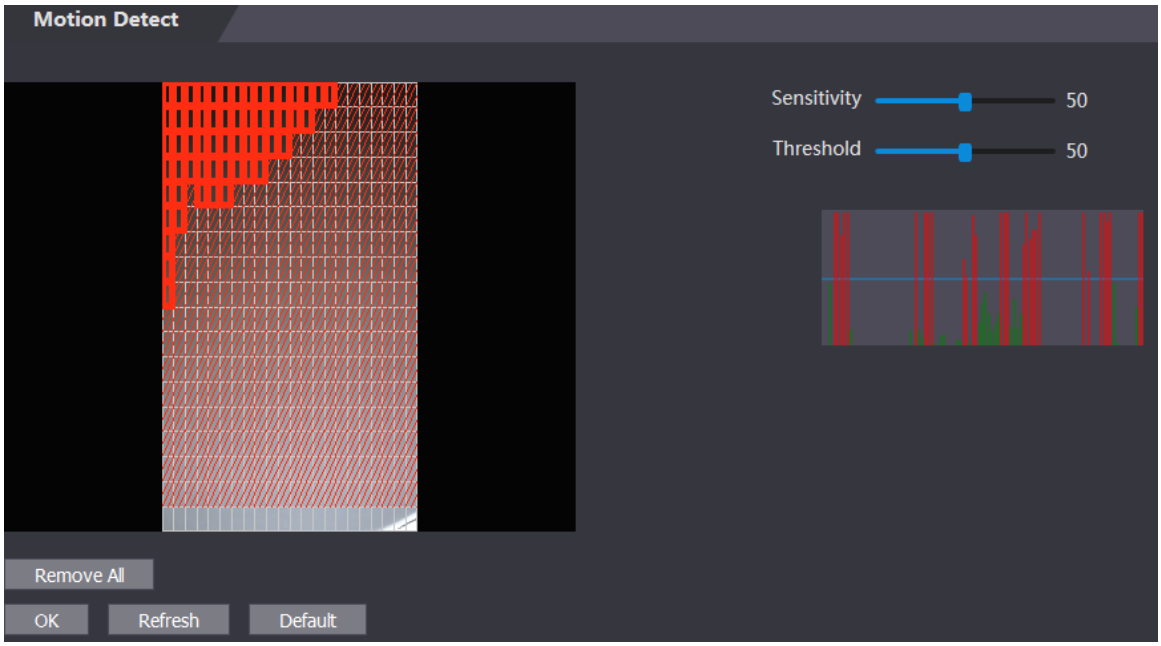
Parámetro	Descripción
	prevalecerá el producto. Puede seleccionar entre: ● Automático: el controlador de acceso ajustará automáticamente el brillo de las imágenes. ● Prioridad de obturador: el controlador de acceso ajustará el brillo de la imagen según el rango de valores de exposición del obturador. Si el brillo de la imagen no es suficiente y el valor del obturador ha alcanzado el límite superior o inferior, el controlador de acceso 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 selecciona**Gama personalizada**, puede personalizar el rango de valores del obturador.
Rango de valor de ganancia	Cuando se establece el rango de valores de ganancia, se mejorará la calidad del video.
Exposición Compensación	Puede aumentar el brillo del video ajustando el valor de compensación de exposición.
NR 3D	Cuando se habilita la Reducción de ruido 3D (RD), se puede reducir el ruido de video y se producirán videos de alta definición.
Grado	Puede ajustar el valor de 3D NR cuando 3D NR está activado. Cuanto mayor sea el valor, menor será el ruido.

4.6.4 Detección de movimiento

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

Step 1 Seleccione Configuración de video > Configuración de video > Detección de movimiento. Él**Detección de movimiento**se muestra la interfaz.

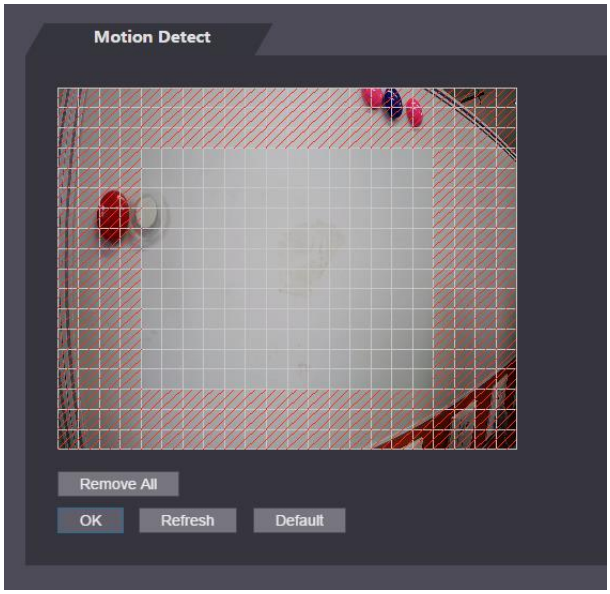
Figure 4-14 Detección de movimiento



Step 2 Mantenga presionado el botón izquierdo del mouse y luego arrastre el mouse en el área roja. Él **Detección de movimiento**se muestra el área.

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

Figure 4-15 Área de detección de movimiento



Step 3 Establezca la sensibilidad y el umbral.

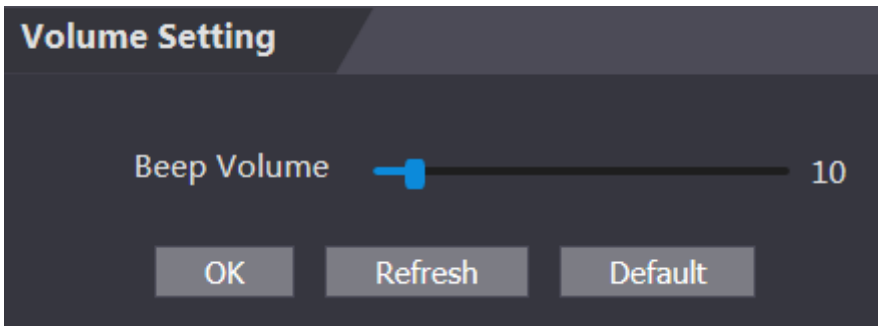
- La sensibilidad representa la capacidad de cada rejilla para detectar movimiento. Cuanto más grande sea es el valor, mayor es la sensibilidad.
- El umbral es la condición de detección de movimiento. Cuando el número de cuadrícula alcanza el umbral, se activará la detección de movimiento. Cuanto menor sea el valor, más es probable que se active la detección de movimiento.
- Cuando el número de cuadrícula es menor que el umbral, aparecerá una línea verde; cuando la rejilla el número es mayor que el umbral, aparecerá una línea roja. Consulte la Figura 4-14.

Step 4 Hacer clic**DE ACUERDO**para terminar el ajuste.

4.6.5 Configuración de volumen

Puede ajustar el volumen del altavoz del controlador de acceso.

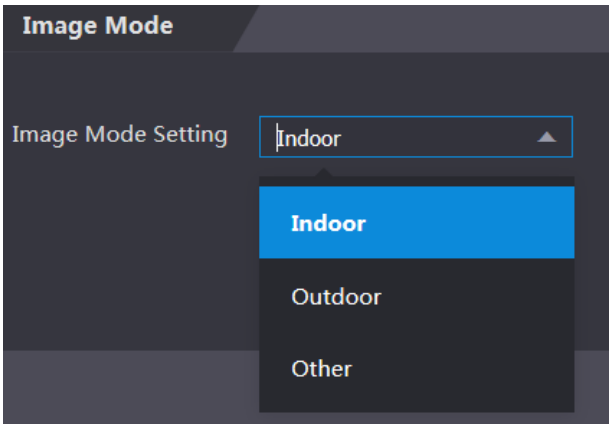
Figure 4-16 Ajuste de volumen



4.6.6 Modo de imagen

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

Figure 4-17 Modo de imagen

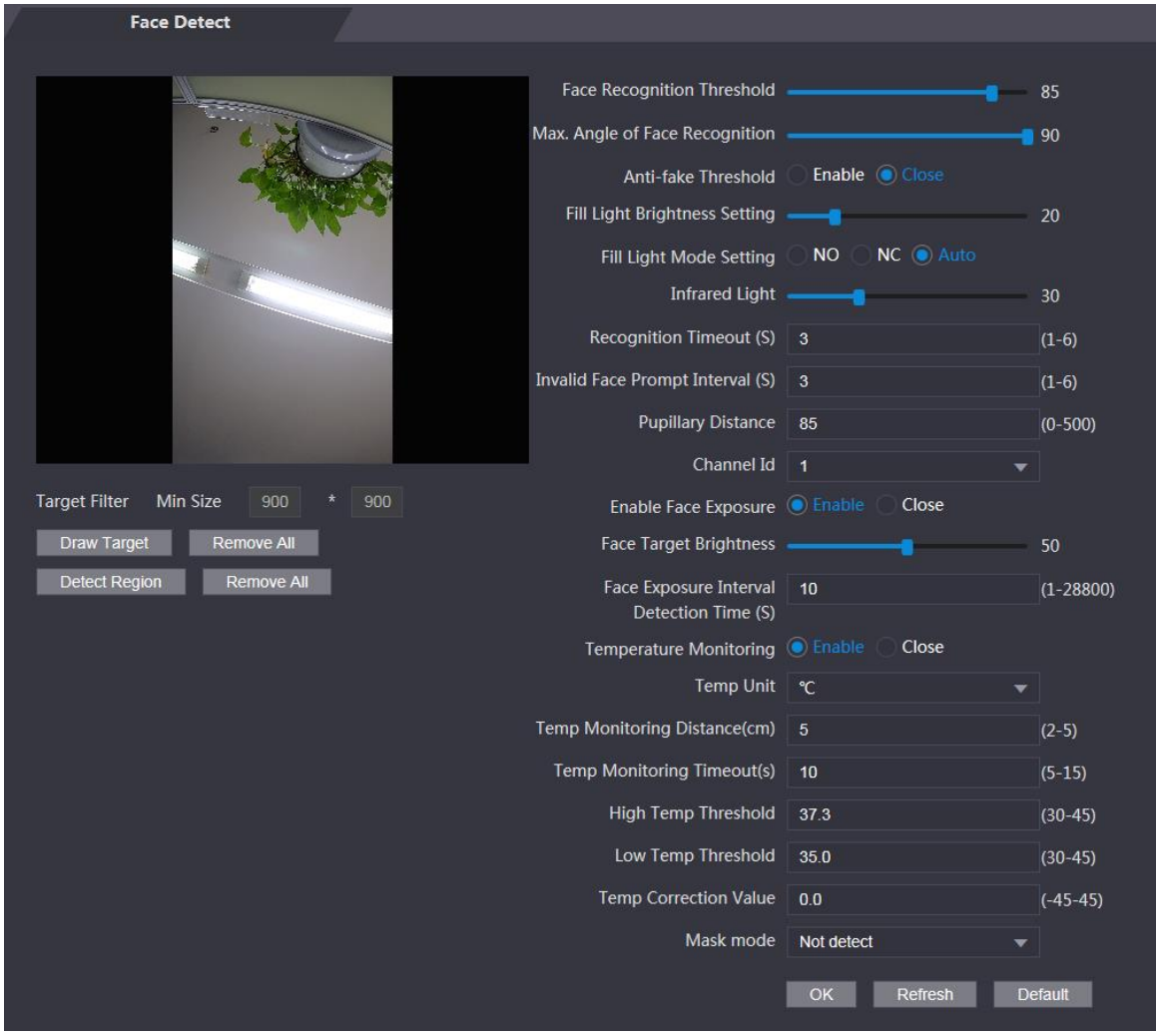


4.7 Detección de rostro

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

Step 1 Seleccione**Detección de rostro**.

Figure 4-18 Detección de rostros



Step 2 Configurar parámetros.

Tabla 4-5 Descripción del parámetro de detección de rostros

Parámetro	Descripción
Rostro Reconocimiento Límite	Cuanto mayor sea el valor, mayor será la precisión.
máx. Ángulo de reconocimiento facial	Cuanto mayor sea el ángulo, se reconocerá una gama más amplia de perfiles.
Umbral anti-falsificación	Esta función evita que las personas se desbloqueen mediante imágenes de rostros humanos o modelos de rostros. Hay dos opciones:**Permitir**y**Cerrar**.
Brillo de luz de relleno Entorno	Puede configurar el brillo de la luz de relleno.
Llenar Luz Modo Entorno	Hay tres modos de luz de relleno. ● NO: La luz de llenado normalmente está encendida. NC: ● La luz de llenado normalmente está cerrada. ● Automático: la luz de relleno se encenderá automáticamente cuando se active un evento de detección de movimiento. Cuando**Auto**está seleccionado, la luz de relleno no estará encendida incluso si el valor de la luz infrarroja es superior a 19.

Parámetro	Descripción
Luz infrarroja	Ajuste el brillo IR arrastrando la barra de desplazamiento.
Reconocimiento Se acabó el tiempo	Cuando una persona que no tiene el permiso de acceso se para frente al controlador de acceso y obtiene el reconocimiento facial, el controlador indicará que el reconocimiento facial falló. El intervalo de solicitud se denomina tiempo de espera de reconocimiento.
Indicación de cara no válida Intervalo	Cuando una cara sin permiso de acceso se para frente al controlador de acceso, el controlador indicará que la cara no es válida. El intervalo de solicitud es un intervalo de solicitud de cara no válido.
Distancia pupilar	La distancia pupilar es el valor de píxel de la imagen entre los centros de las pupilas de cada ojo. Debe establecer un valor apropiado para que el controlador de acceso pueda reconocer las caras según sea necesario. El valor cambia según el tamaño de la cara y la distancia entre las caras y la lente. Cuanto más cerca esté la cara de la lente, mayor debe ser el valor. Si un adulto está a 1,5 metros de la lente, el valor de la distancia pupilar puede estar entre 50 y 70.
Permitir Rostro Exposición	Después de habilitar la exposición del rostro, el rostro humano será más claro cuando el controlador de acceso se instale en el exterior.
Canal ID	Hay dos opciones: 1 y 2. 1 es cámara de luz blanca y 2 es cámara de luz IR.
Dibujar objetivo	Hacer clic**Dibujar objetivo**, y luego puede dibujar el marco mínimo de detección de rostros. Hacer clic**Eliminar todo**y puede eliminar todos los marcos que dibujó.
Detectar región	Hacer clic**Detectar región**, mueva el mouse y podrá ajustar la región de detección de rostros. Hacer clic**Eliminar todo**y puede eliminar todas las regiones de detección.
Rostro Objetivo Brillo	El valor predeterminado es 50. Ajuste el brillo según sea necesario.
Rostro Exposición Intervalo	Después de que se detecte una cara, el controlador de acceso emitirá luz para iluminar la cara y el controlador de acceso no volverá a emitir luz hasta que haya transcurrido el intervalo establecido.
Temperatura Vigilancia	Establezca si habilitar el control de la temperatura corporal. ● Unidad de temperatura: Seleccione una unidad de temperatura. ● Distancia de control de temperatura (cm): el valor predeterminado es de 5 cm. Establezca otros valores para permitir el control de la temperatura dentro de una distancia definida que oscila entre 2 cm y 5 cm. ● Umbral de temperatura alta: establezca el umbral de temperatura alta. La temperatura corporal monitoreada se considerará alta si es mayor o igual que el valor establecido. ● Umbral de temperatura baja: establece el umbral de temperatura baja. La temperatura corporal monitoreada no será monitoreada si es menor que el valor establecido. ● Valor de corrección de temperatura: este parámetro es para realizar 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 varios

Parámetro	Descripción
	muestras monitoreadas para la prueba, y luego corrija la desviación de temperatura por 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 inferior a 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. ● Tiempo de espera de monitoreo de temperatura: establezca la duración del monitoreo de temperatura. Si el tiempo de monitoreo es más largo que este valor, la pantalla le pedirá que inicie el siguiente monitoreo de temperatura. Solo el controlador de acceso con una unidad de monitoreo de temperatura admite este parámetro.
Modo máscara	● Sin detección: la máscara no se detecta durante el reconocimiento facial. ● Recordatorio de máscara: la máscara se detecta durante el reconocimiento facial. Si se detecta a la persona sin usar una máscara, el sistema le indicará un recordatorio de máscara y se le permitirá el paso. ● Intercepción de máscara: la máscara se detecta durante el reconocimiento facial. Si la persona es detectada sin usar una máscara, el sistema le indicará un recordatorio de la máscara y no se le permitirá el paso.

Step 3 Hacer clic**DE ACUERDO**para terminar el ajuste.

4.8 Configuración de red

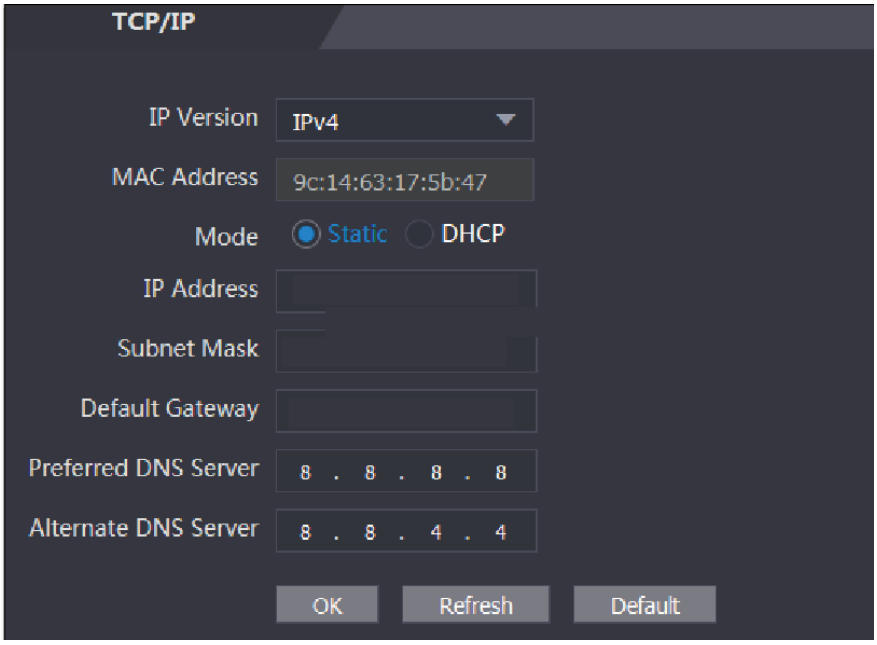
4.8.1 TCP/IP

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

Asegúrese de que el controlador de acceso esté conectado a la red correctamente.

Step 1 Seleccione Configuración de red > TCP/IP.

Figure 4-19 TCP/IP



Step 2 Configurar parámetros.

Tabla 4-6 TCP/IP

Parámetro	Descripción
Versión IP	Hay una opción: IPv4.
Dirección MAC	Se muestra la dirección MAC del controlador de acceso.
Modo	• Estático Establezca la dirección IP, la máscara de subred y la dirección de la puerta de enlace manualmente. • DHCP - Después de habilitar DHCP, la dirección IP, la máscara de subred y la dirección de la puerta de enlace no se pueden configurar. - Si DHCP es efectivo, la dirección IP, la máscara de subred y la dirección de la puerta de enlace se mostrarán automáticamente; si DHCP no es efectivo, la dirección IP, la máscara de subred y la dirección de la puerta de enlace serán cero. - Si desea ver la IP predeterminada cuando DHCP está activo, debe desactivar 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 Máscara de subred Puerta de enlace predeterminada	Ingrese la dirección IP y luego configure la máscara de subred y la dirección de la puerta de enlace. La dirección IP y la dirección de la puerta de enlace deben estar en el mismo segmento de red.
Privilegiado DNS Servidor	Configure la dirección IP del servidor DNS preferido.
Alterno DNS Servidor	Establezca la dirección IP del servidor DNS alternativo.

Step 3 Hacer clic**DE ACUERDO**para completar el ajuste.

4.8.2 Puerto

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

Step 1 Seleccione Configuración de red > Puerto. Él**Puerto**se muestra la interfaz.

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

Excepto la conexión máxima, debe reiniciar el controlador de acceso para hacer el configuración efectiva después de modificar los valores.

Tabla 4-7 Descripción del puerto

Parámetro	Descripción
máx. Conexión	Puede establecer las conexiones máximas de clientes a las que se puede conectar el controlador de acceso. Los clientes de plataformas 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 al iniciar sesión a través de los navegadores.
Puerto HTTPS	El valor predeterminado es 443.
Puerto RTSP	El valor predeterminado es 554.

Step 3 Hacer clic**DE ACUERDO**para completar el ajuste.

4.8.3 Registro

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

Step 1 Seleccione Configuración de red > Registro automático.

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

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

Tabla 4-8 Descripción del registro automático

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

Step 3 Hacer clic**DE ACUERDO**para completar el ajuste.

4.8.4 P2P

La computación o redes punto a punto es una arquitectura de aplicación distribuida que divide tareas o cargas de trabajo entre pares. Los usuarios pueden descargar la aplicación móvil escaneando el código QR y luego registrar una cuenta para poder administrar más de un controlador de acceso.

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 controlador de acceso a una red externa; de lo contrario el no se puede utilizar el controlador de acceso.

Figure 4-20 P2P

Step 1 Seleccione Configuración de red > P2P. Él**P2P**se muestra la interfaz. Seleccione**Permitir**para

Step 2 habilitar la función P2P. Hacer clic**DE ACUERDO**

Step 3 para completar el ajuste.

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

4.9 Configuración de la fecha

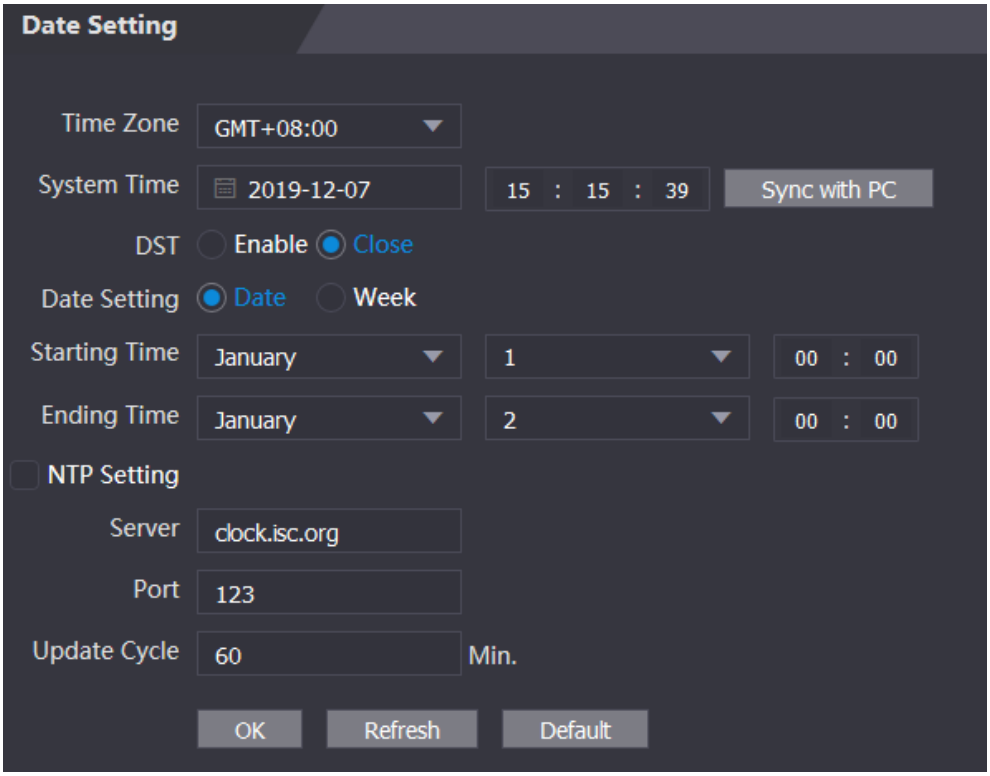
Debe configurar la zona horaria, la hora, el horario de verano y el NTP para el controlador de acceso.

Solo los controladores de acceso de ciertos modelos admiten esta función.

Step 1 Seleccione Configuración de fecha.

Él**Configuración de la fecha**se muestra la interfaz.

Figure 4-21 Configuración de la fecha



Step 2 Establecer parámetros.

Tabla 4-9 Ajuste de fecha

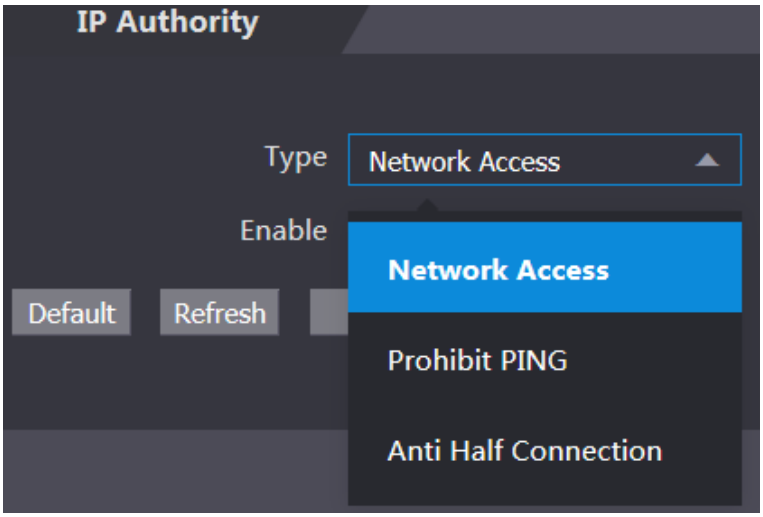
Parámetro	Descripción
Zona horaria	Seleccione la zona horaria según sea necesario.
Hora del sistema	Puede establecer la hora del sistema manualmente o puede hacer clic en**Sincronizar con PC**, para sincronizar la hora del controlador de acceso con la hora de la computadora.
horario de verano	1. Habilite el horario de verano. 2. Selecciona**Fecha**o**Semana**en**Configuración de la fecha**. 3. Establecer**Tiempo de empezar**y**Hora de finalización**.
Configuración NTP	1. Habilitar**Configuración NTP**. 2. Configurar parámetros. - Servidor: Introduzca el nombre de dominio del servidor NTP. La hora del controlador de acceso se sincronizará con el servidor NTP. - Puerto: Introduzca el número de puerto del servidor NTP. - Ciclo de actualización: establezca un ciclo de actualización y, a continuación, la hora del controlador de acceso se actualizará en consecuencia. 3. Haga clic en**DE ACUERDO**.

4.10 Administración de Seguridad

4.10.1 Autoridad de PI

Seleccione un modo de seguridad cibernética según sea necesario.

Figure 4-22 autoridad de PI



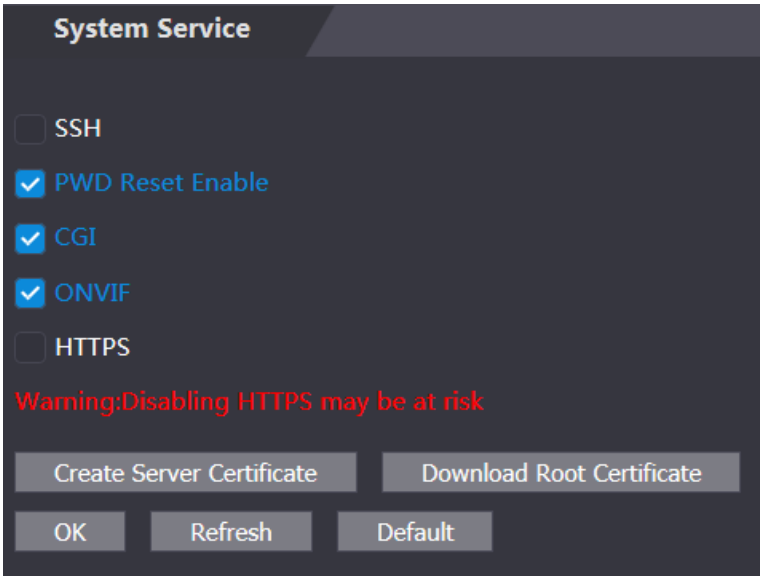
4.10.2 Sistemas

4.10.2.1 Servicio del sistema

Hay cuatro opciones: SSH, PWD Reset Enable, CGI y HTTPS. Consulte "3.12 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 controlador de acceso se sincronizará.

Figure 4-23 servicio del sistema



4.10.2.2 Crear certificado de servidor

Hacer clic**Crear certificado de servidor**, ingrese la información necesaria, haga clic en**Guardar**y luego el controlador de acceso 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 en el**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.

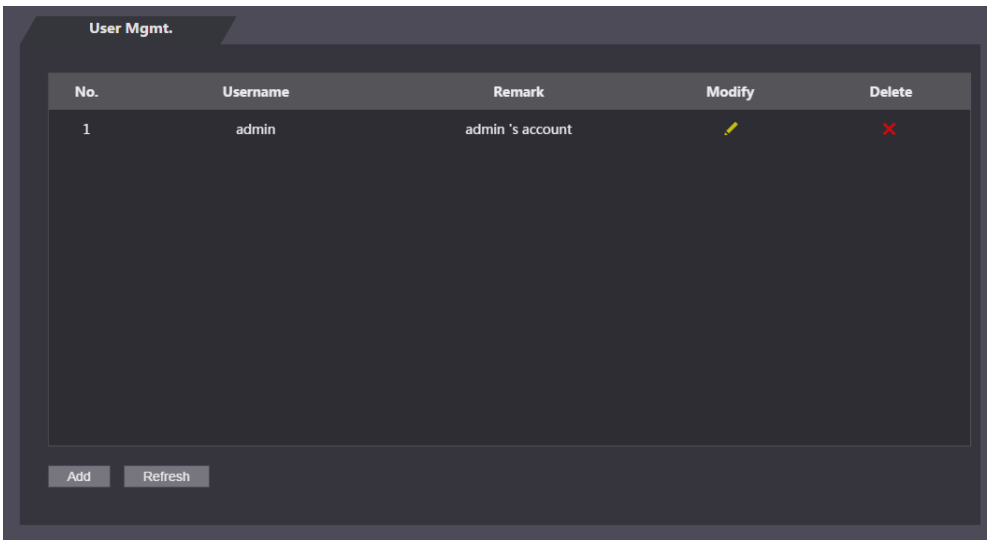
4.11.1 Adición de usuarios

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**DE ACUERDO**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.

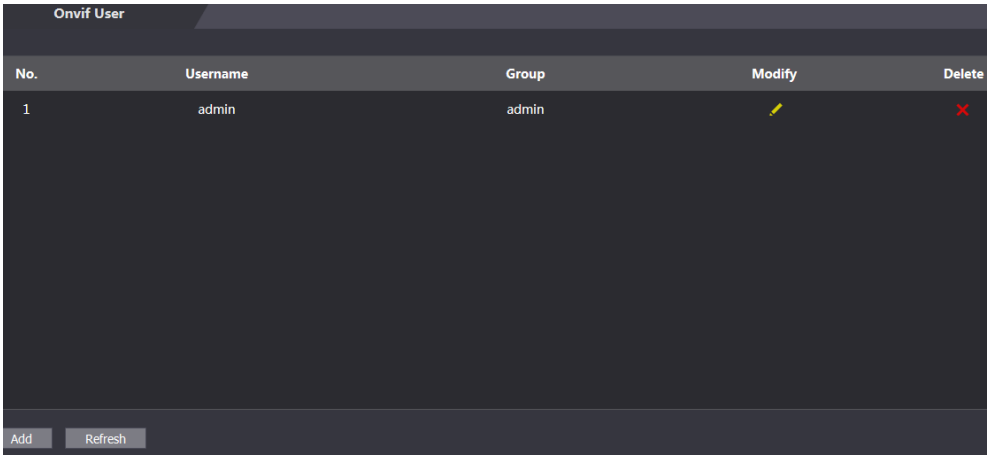
Figure 4-24 Gestión de usuarios



4.11.3 Usuario Onvif

Open Network Video Interface Forum (ONVIF), un foro global y abierto de la industria con el objetivo de facilitar el desarrollo y uso de un estándar abierto global para la interfaz de productos físicos de seguridad basados en IP. Cuando se usa ONVIF, el administrador, el operador y el usuario tienen diferentes permisos del servidor ONVIF. Cree usuarios onvif según sea necesario.

Figure 4-25 Usuario de Onvif

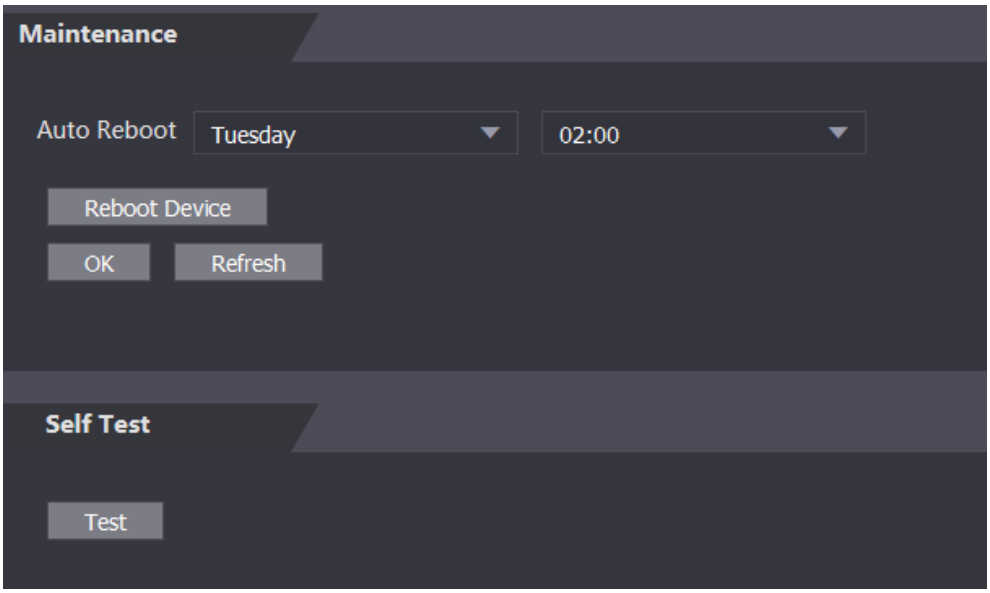


4.12 Mantenimiento

Puede hacer que el controlador de acceso se reinicie en tiempo de inactividad para mejorar la velocidad de ejecución del controlador de acceso. Debe configurar la fecha y la hora de reinicio automático.

La hora de reinicio predeterminada es a las 2 en punto de la mañana del martes. Hacer clic**Reiniciar dispositivo**, el controlador de acceso se reiniciará inmediatamente. Hacer clic**DE ACUERDO**, el controlador de acceso se reiniciará a las 2 de la mañana todos los martes.

Figure 4-26 Mantenimiento



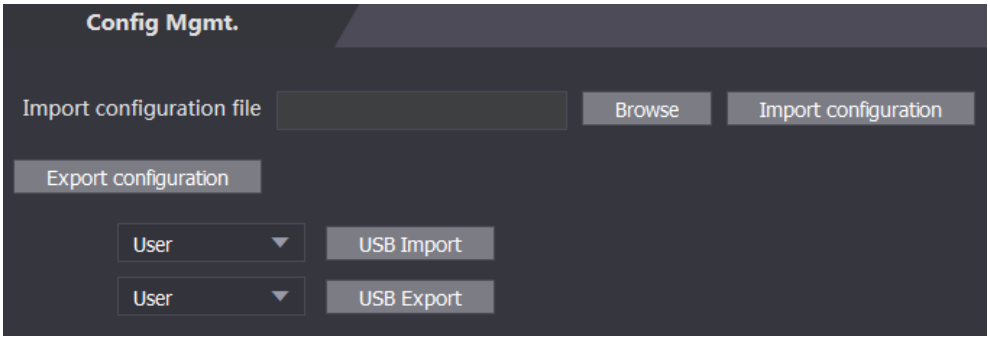
4.13 Gestión de la configuración

Debe realizar la gestión de la configuración, seleccionar la retroalimentación del resultado de desbloqueo, Wiegand y la configuración en serie para el controlador de acceso.

4.13.1 Gestión de configuración.

Cuando más de un controlador de acceso necesita la misma configuración, puede configurar sus parámetros importando o exportando archivos de configuración.

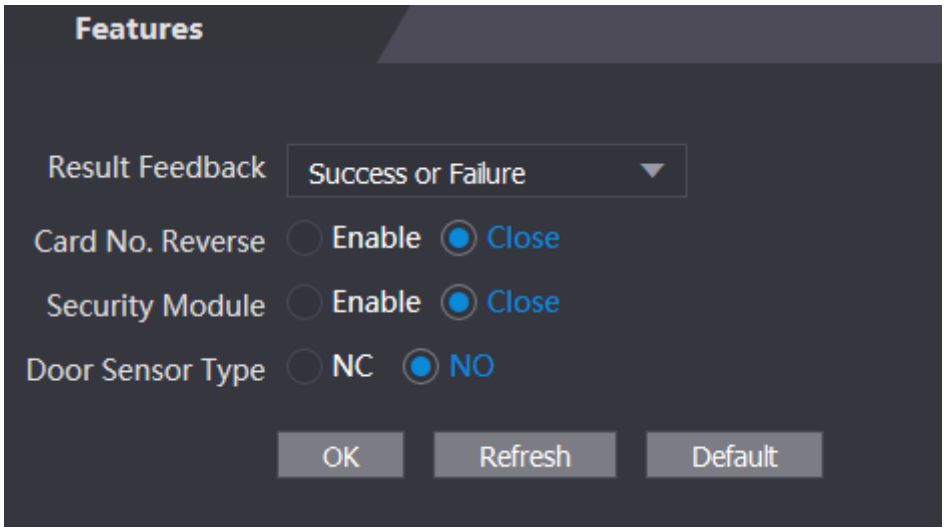
Figure 4-27 Gestión de la configuración



4.13.2 Características

Seleccione el modo de retroalimentación de resultados según sea necesario. Para obtener más información, consulte "3.12.2 Comentarios sobre los resultados".

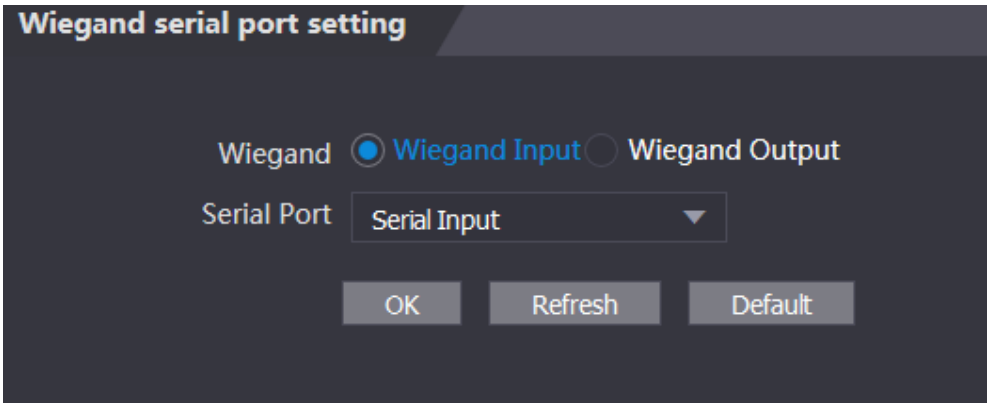
Figure 4-28 Características



4.13.3 Configuración del puerto serie Wiegand

Seleccione la configuración del puerto serie/Wiegand según sea necesario. Para obtener más información, consulte "3.9.2 Configuración del puerto serie" y "3.9.3 Configuración de Wiegand".

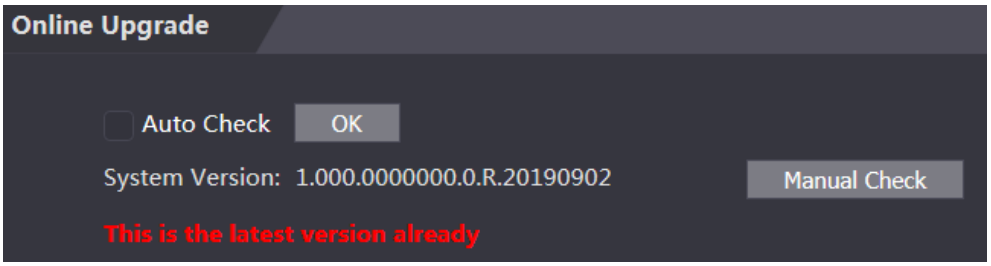
Figure 4-29 Configuración del puerto serie Wiegand



4.14 Mejora

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

Figure 4-30 Mejora



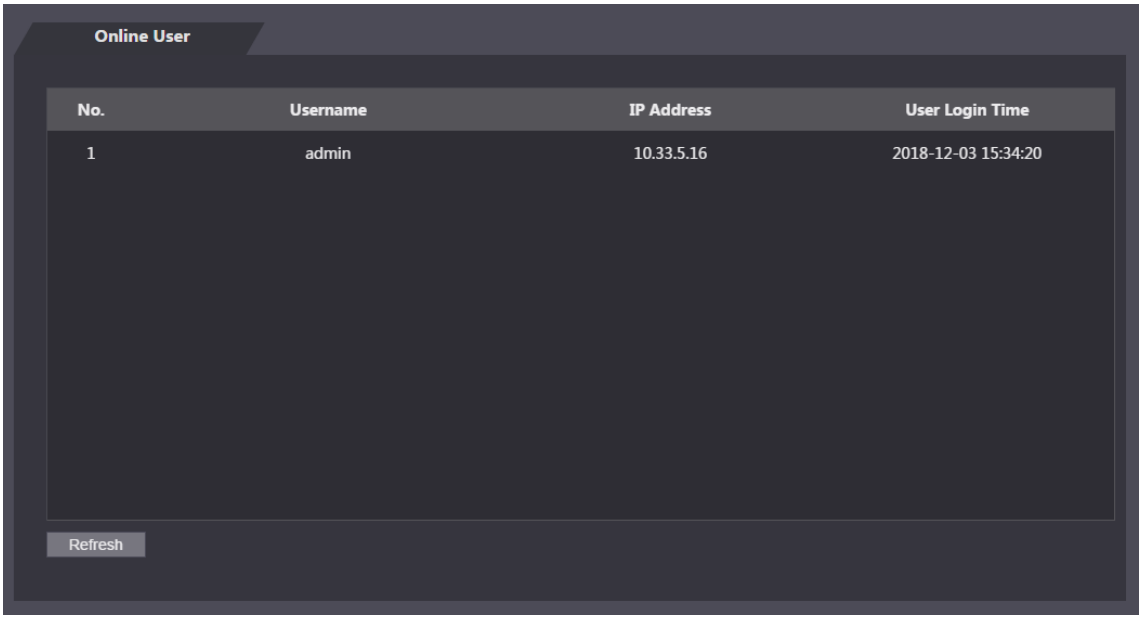
4.15 Información de versión

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.

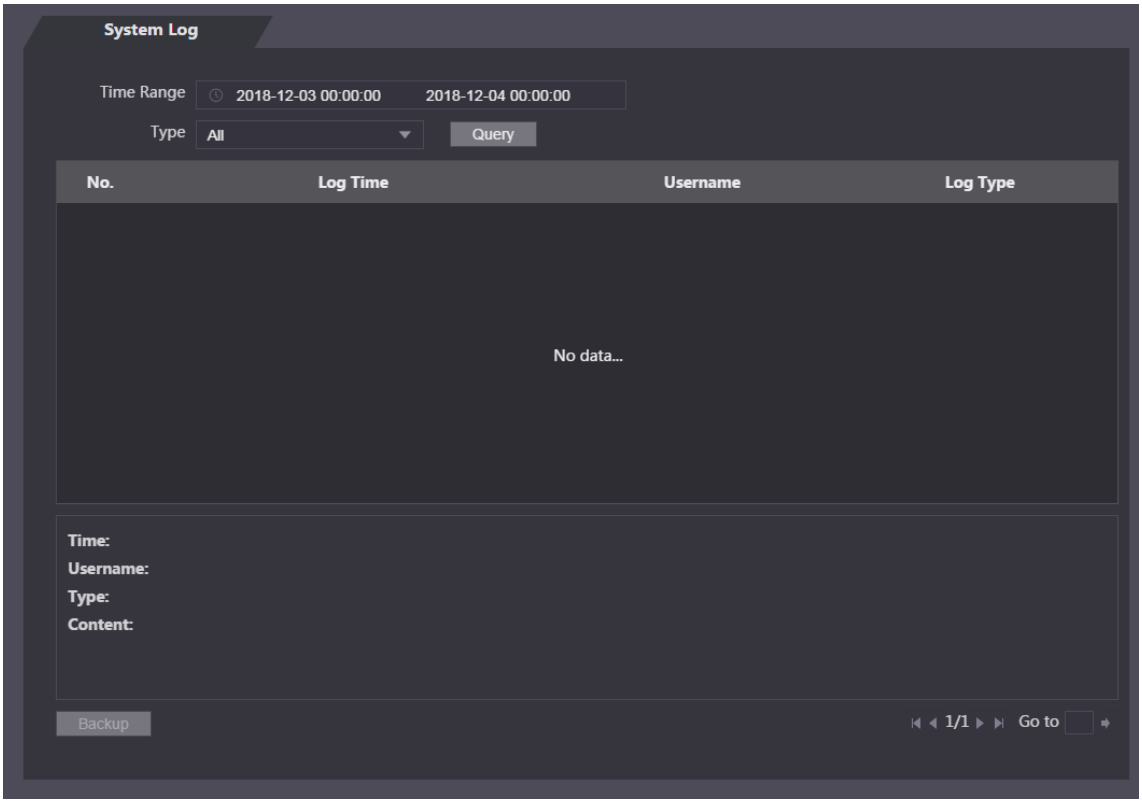
Figure 4-31 Usuario en línea



4.17 Registro del sistema

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

Figure 4-32 Registro del sistema



4.17.1 Consulta de registros

Seleccione un intervalo de tiempo y su tipo, haga clic en**Consulta**, y se mostrarán los registros que cumplen las condiciones.

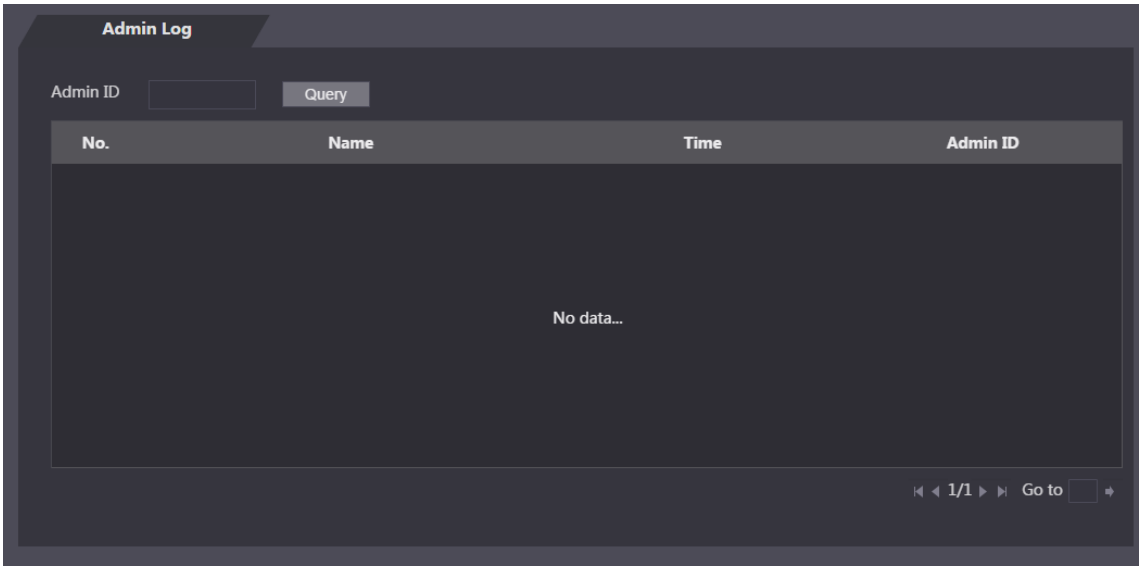
4.17.2 Registros de copia de seguridad

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

4.17.3 Registro de administración

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

Figure 4-33 Registro de administración



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

4.18 Salida

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

5 preguntas frecuentes

1. **El controlador de acceso 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 controlador de acceso.**
   Asegúrese de que Face esté seleccionado en el modo de desbloqueo. Ver "3.8.2 Desbloquear".
   Asegúrese de que Rostro esté seleccionado como modo de desbloqueo en Acceso > Modo de desbloqueo > Combinación de grupo. Ver "3.8.2.3 Combinación de Grupos".
3. **No hay señal de salida cuando el controlador de acceso y el controlador externo están conectados al puerto Wiegand.**
   Compruebe si el cable GND del controlador de acceso y el controlador externo están conectados.
4. **No se pueden realizar 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 controlador de acceso de forma remota.
5. **La información del usuario y las imágenes de la cara no se pueden importar al controlador de acceso.**
   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 10 °C y 40 °C.
- Evite la luz solar directa sobre la unidad de control de temperatura.
- Evite instalar la unidad de monitoreo de temperatura mirando hacia la fuente de luz y el vidrio.
- Mantenga la unidad de monitoreo 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 la temperatura entre la temperatura monitoreada y la temperatura real.
- La sudoración también es una forma en que el cuerpo se enfría automáticamente y disipa el calor, lo que también causará la desviación de la temperatura entre la temperatura monitoreada y la temperatura real.
- Mantenga la unidad de monitoreo de temperatura regularmente (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 cara Grabación/Comparación

Antes del registro

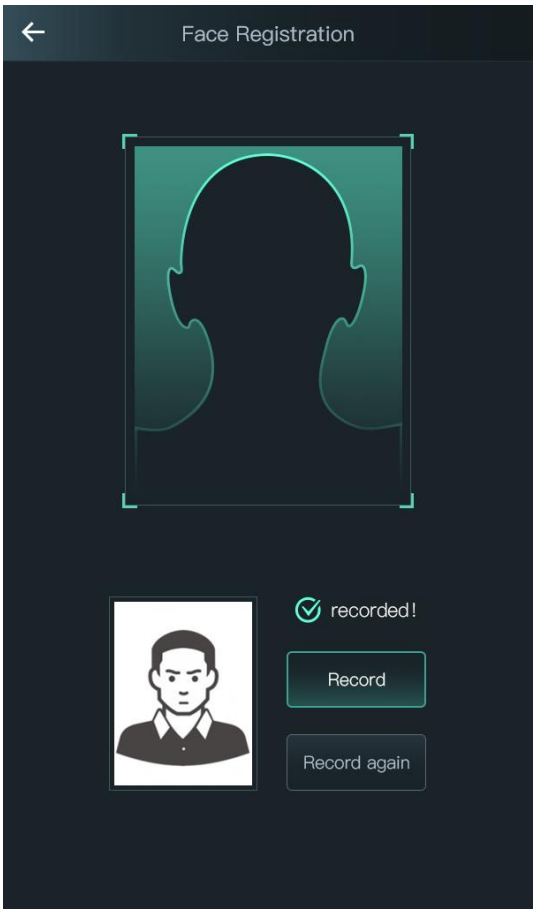
- Las gafas, los sombreros y la barba pueden influir en el rendimiento del
- reconocimiento facial. No cubra sus cejas cuando use sombreros.
- No cambie mucho su estilo de barba si va a usar el dispositivo; de lo contrario, el reconocimiento facial podría fallar.
- Mantén tu cara limpia.
- Mantenga el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

Durante el registro

Puedes registrar rostros a través del controlador de acceso o a través de la plataforma. Para el registro 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. Una imagen de su cara será capturada automáticamente.

Apéndice Figura 2-1 Registro

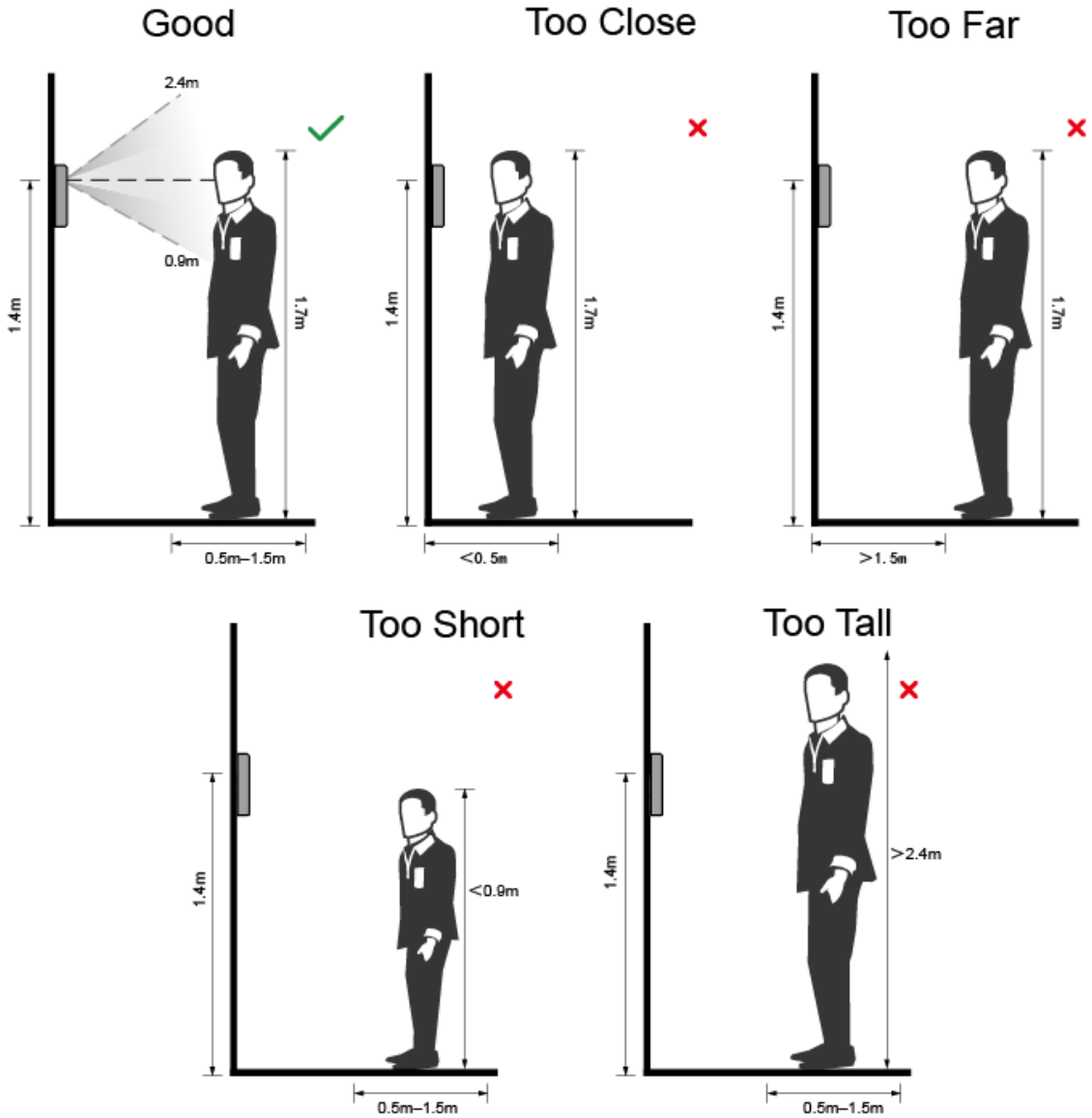


- No sacuda la cabeza o el cuerpo, de lo contrario, el registro podría fallar.
- Evite que aparezcan dos rostros en el cuadro de captura al mismo tiempo.

Posición de la cara

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

Apéndice Figura 2-2 Posición adecuada de la cara

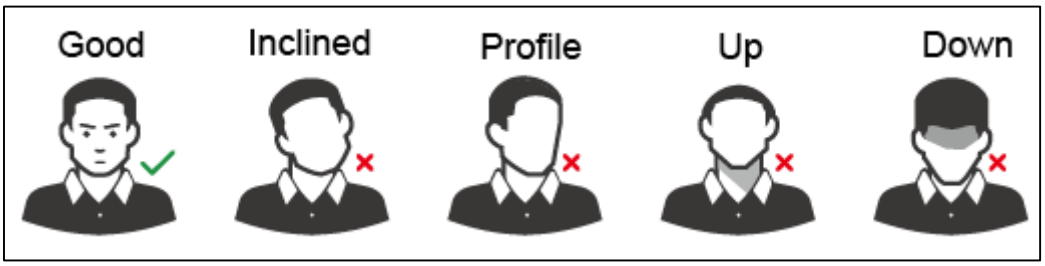


Requisitos de las caras

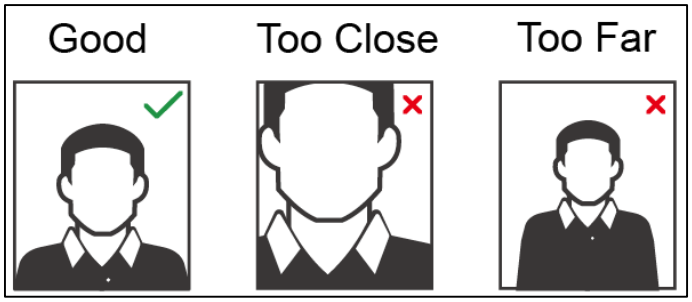
- Asegúrese de que la cara esté limpia y que la frente no esté cubierta por pelo.
- No use anteojos, sombreros, barbas pobladas u otros adornos faciales que influyan en la grabación de imágenes faciales.
- Con los ojos abiertos, sin expresiones faciales, y coloca tu rostro hacia el centro de la cámara.

- 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 imagen la resolución está 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 el ID de la persona son los mismos.
- Asegúrese de que la cara no ocupe 2/3 del área total de la imagen y que la relación de aspecto no no exceda de 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 presentan 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. Use contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Actualice el firmware y el software del cliente a tiempo

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su 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 "verificación automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.

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

Recomendaciones "agradables de 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 y gabinete de computadoras especiales, e implemente un permiso de control de acceso y una administración de claves bien hechos para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de un dispositivo extraíble (como un disco flash USB). , puerto serie), etc.

2. Cambie las contraseñas regularmente

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

3. Establezca y actualice la información de restablecimiento de contraseñas a tiempo

El 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 de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección de contraseña, se sugiere no utilizar aquellas que se pueden adivinar fácilmente.

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilitar HTTPS

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

7. Enlace de dirección MAC

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

8. Asigne cuentas y privilegios de manera razonable

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios razonablemente y asígneles un conjunto mínimo de permisos.

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.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de encriptación WPA2-PSK y configure contraseñas seguras.

10. Transmisión encriptada de audio y video

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

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

11. Auditoría segura

- Verifique a los usuarios en línea: le sugerimos que verifique a los usuarios en línea regularmente para ver si el dispositivo está conectado sin autorización.
- Verifique el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se usaron 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 habilitar la función de registro de red para asegurarse de que los registros críticos se sincronizan con el servidor de registro de red para su seguimiento.

13. Construya un entorno de red seguro

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

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde una red externa.
- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere usar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.

- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts que pueden acceder al dispositivo.