Controlador de acceso de reconocimiento facial con unidad de control de temperatura

Manual de usuario

V1.0.0

Prefacio

General

Este manual presenta la instalación y las operaciones detalladas del controlador de acceso de reconocimiento facial con unidad de control de temperatura (en lo sucesivo, "controlador de acceso").

Este manual se aplica a los controladores de acceso modelo G y modelo J. Las figuras de los controladores de acceso modelo G se muestran en el manual, por ejemplo.

Las instrucciones de seguridad

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

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

Revisión histórica

Versión	Contenido de la revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento.	Mayo de 2021

Acerca del manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No nos hacemos responsables de ninguna pérdida ocasionada por las operaciones que no cumplan con el manual.
- El manual se actualizaría de acuerdo con las últimas leyes y regulaciones de las regiones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si existe inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el manual. Por favor

póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.

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

Advertencias y medidas de seguridad importantes

Este capítulo describe el contenido que cubre el manejo adecuado del controlador de acceso, la prevención de peligros y la prevención de daños a la propiedad. Lea atentamente estos contenidos antes de utilizar el controlador de acceso, cúmplalos al utilizarlos y guárdelos en un lugar seguro 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 el 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 en 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.
- Cuando se usa en exteriores con alta temperatura, no toque directamente la superficie del controlador de acceso, como la pantalla, la carcasa trasera de metal y el sensor de huellas dactilares.

Seguridad ELECTRICA

- El uso inadecuado de la batería puede provocar un incendio, una explosión o una inflamación.
- Cuando reemplace la batería, asegúrese de que se use el mismo modelo.
- Utilice los cables de alimentación recomendados en la región y cumpla con la especificación de potencia nominal.
- Utilice el adaptador de corriente provisto con el controlador de acceso; de lo contrario, podría provocar lesiones personales y daños en el controlador de acceso.
- Utilice una fuente de alimentación que cumpla con ES1 pero que no supere los límites de PS2 definidos en IEC 62368-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas del controlador de acceso.
- Conecte el controlador de acceso (estructura tipo I) a la toma de corriente con toma de tierra de protección. El
- acoplador del aparato es un dispositivo de desconexión. Cuando utilice el acoplador, mantenga el ángulo para facilitar la operación.

Tabla de contenido

Prefacio..... I

Salvaguardias y advertencias importantes .....

III 1 Resumen 1

1.1 Introducción 1

1.2 Características 1

1.3 Aplicación 1

2 Operaciones del sistema 3

2.1 Procedimiento de configuración básica 3

2.2 Iconos comunes 3

2.3 Inicialización 4

2.4 Interfaz de espera 4

2.5 Menú principal 6

2.6 Métodos de desbloqueo 7

2.6.1 Tarjetas 7

2.6.2 Rostro 7

2.6.3 Huellas digitales 7

2.6.4 Contraseña de usuario 8

2.6.5 Contraseña de administrador 8

2.7 Gestión de usuarios 8

2.7.1 Agregar nuevos usuarios 8

2.7.2 Visualización de la información del usuario 10

2.8 Gestión de acceso 10

2.8.1 Gestión de períodos ..... .11

2.8.2 Desbloquear 12

2.8.3 Configuración de alarma ..... .14

2.8.4 Estado de la puerta 15

2.8.5 Tiempo de retención de bloqueo 15

2.9 Asistencia 15

2.10 Comunicación de red ..... dieciséis

2.10.1 Configuración de IP .....dieciséis

2.10.2 Registro activo 17

2.10.3 Wi-Fi 18

2.10.4 Configuración del puerto serie 18

2.10.5 Configuración Wiegand 19

2.11 Sistema 20

2.11.1 Hora 20

2.11.2 Parámetro de cara 20

2.11.3 Modo de imagen 23

2.11.4 Volumen 23

2.11.5 Idioma 23

2.11.6 Luz infrarroja 23

2.11.7 Configuración de pantalla 23

2.11.8 Restaurar la configuración de fábrica 24

2.11.9 Reiniciar 24

2.12 USB 24
2.12.1 Exportación USB 25
2.12.2 Importación USB 25
2.12.3 Actualización USB 26
2.13 Características 26
2.13.1 Configuración de privacidad 28
2.13.2 Comentarios sobre los resultados 29
2.14 Registro 31
2.15 Información del sistema 32
3 Operaciones web 33
3.1 Inicialización 33
3.2 Iniciar sesión 34
3.3 Restablecimiento de la contraseña 35
3.4 Parámetro de puerta 37
3.5 Enlace de alarma 39
3.5.1 Configuración del enlace de alarma 39
3.5.2 Registro de alarmas 40
3.6 Configuración de Talkback 41
3.6.1 Servidor SIP 41
3.6.2 Configuración local 43
3.6.3 Gestión de números VTO 45
3.6.4 Gestión de números VTH 46
3.6.5 Gestión de VTS 48
3.6.6 Estado en línea 49
3.6.7 Registros de llamadas 50
3.7 Sección de tiempo 51
3.7.1 Configuración de la sección de tiempo 51
3.7.2 Configuración de grupo de vacaciones 51
3.7.3 Configuración de grupo de vacaciones 52
3.8 Capacidad de datos 53
3.9 Configuración de video 53
3.9.1 Velocidad de datos 53
3.9.2 Imagen 54
3.9.3 Exposición 56
3.9.4 Detección de movimiento 57
3.9.5 Ajuste de volumen 59
3.9.6 Modo de imagen 59
3.9.7 Codificación local 60
3.10 Detección de rostro 60
3.11 Configuración de red 63
3.11.1 TCP / IP 63
3.11.2 Puerto ..... sesenta y cinco
3.11.3 Registro 66
3.11.4 P2P 66
3.12 Gestión de la seguridad 67
3.12.1 Autoridad de propiedad intelectual 67
3.12.2 Sistemas 68

3.13 Gestión de usuarios 69
3.13.1 Agregar usuarios 70
3.13.2 Modificación de la información del usuario 70
3.13.3 Usuario ONVIF 70
3.14 Mantenimiento 71
3.15 Gestión de la configuración 71
3.15.1 Exportación del archivo de configuración 71
3.15.2 Importación del archivo de configuración 72
3.15.3 Por defecto 72
3.16 Actualización 72
3.17 Información de la versión 73
3.18 Usuario en línea 73
3.19 Registro del sistema 73
3.19.1 Registros del sistema 73
3.19.2 Registro de administración 74
3.19.3 Desbloquear registros 74
3.20 Calibración de fusión 75
3.21 Avanzado 75
3.22 Salir 76
4 Configuración de CA SmartPSS 77
4.1 Iniciar sesión 77
4.2 Agregar dispositivos 77
4.2.1 Búsqueda automática 77
4.2.2 Adición manual 78
4.3 Gestión de usuarios 79
4.3.1 Configuración del tipo de tarjeta 79
4.3.2 Agregar usuario 80
4.3.3 Emisión de tarjetas en lotes 86
4.3.4 Exportación de información de usuario 87
4.4 Configuración de permisos 87
4.4.1 Agregar grupo de permisos 87
4.4.2 Configuración de permisos 89
4.5 Gestión de acceso 90
4.5.1 Apertura y cierre de puertas de forma remota 90
4.5.2 Configuración de Siempre Abierto y Siempre Cerrado 91
4.5.3 Restablecimiento del estado de la puerta 91
4.6 Gestión de asistencia 92
4.6.1 Búsqueda de informes 92
4.6.2 Otras configuraciones 93
5 Preguntas frecuentes 94
Apéndice 1 Notas de comparación / grabación facial 95
Apéndice 2 Recomendaciones de ciberseguridad 98

1.1 Introducción

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

1.2 Características

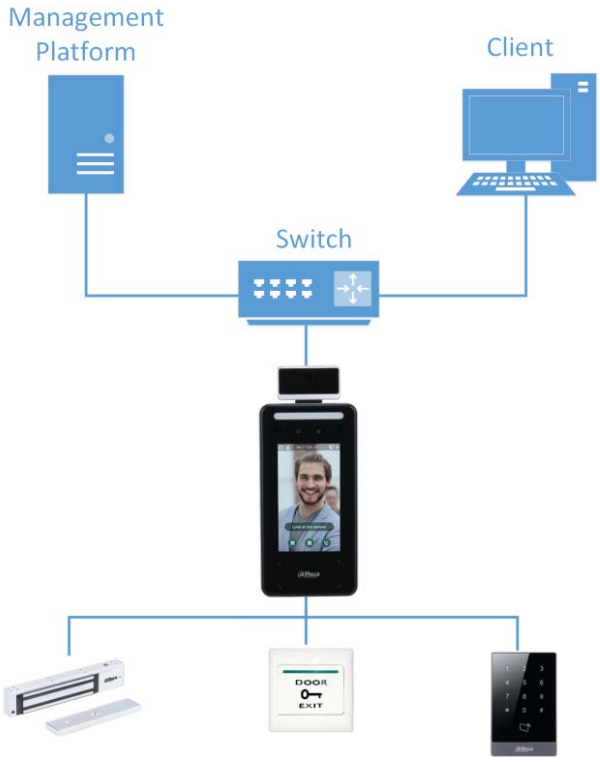
- Pantalla LCD, la resolución del controlador de acceso de 4,3 pulgadas es de 480 × 272.
- Admite desbloqueo facial, desbloqueo de tarjeta IC, desbloqueo de huellas dactilares y desbloqueo de contraseña; desbloquear por período.
- Con un cuadro de detección de rostros, se reconoce primero el rostro más grande entre los rostros que aparecen al mismo tiempo; el tamaño máximo de la cara se puede configurar en la interfaz web. Lente WDR gran angular de 2MP;
- con iluminador automático / manual.
- La distancia de reconocimiento facial es de 0,3 m – 1,5 m.
- 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 falso reconocimiento. Admite
- el reconocimiento de perfiles; el ángulo del perfil es de 0 ° a 90 °. Admite la
- detección de vitalidad.
- Admite alarma de coacción, alarma de manipulación, alarma de intrusión, alarma de tiempo de espera de contacto de puerta, alarma de tarjeta ilegal que excede el umbral, alarma de contraseña ilegal que excede el umbral y alarma externa. Admite usuarios generales,
- usuarios de patrulla, usuarios de listas de bloqueo, usuarios VIP, usuarios invitados, otros usuarios y usuarios personalizados.

- Varios modos de visualización del estado de desbloqueo para proteger la privacidad del
- usuario. Admite el control de la temperatura corporal.

1.3 Aplicación

El controlador de acceso es aplicable a parques, edificios de oficinas, escuelas, fábricas, áreas residenciales y otros lugares. La identidad se verifica mediante reconocimiento facial para lograr el paso sinpercepción.

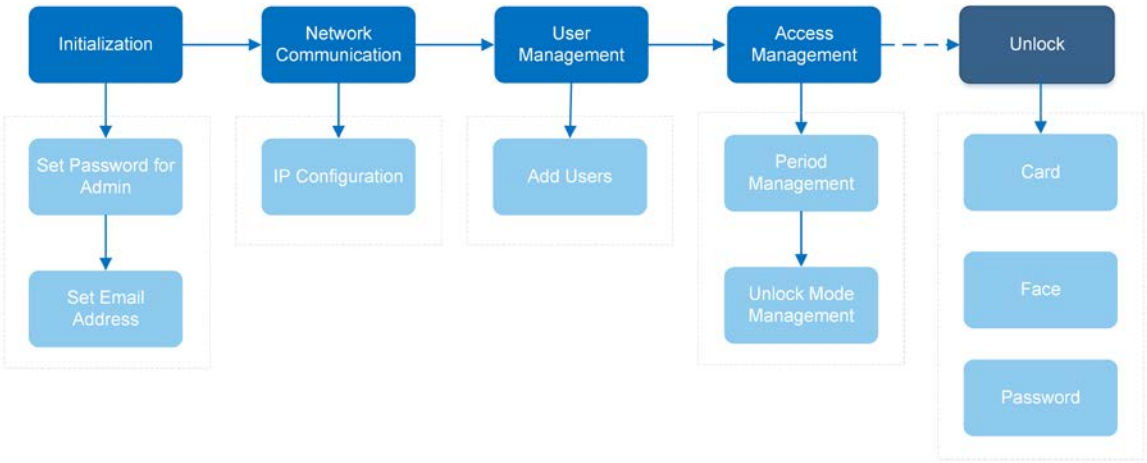
Figura 1-1 Redes



2 Operaciones del sistema

2.1 Procedimiento de configuración básica

Figura 2-1 Procedimiento de configuración básica



2.2 Iconos comunes

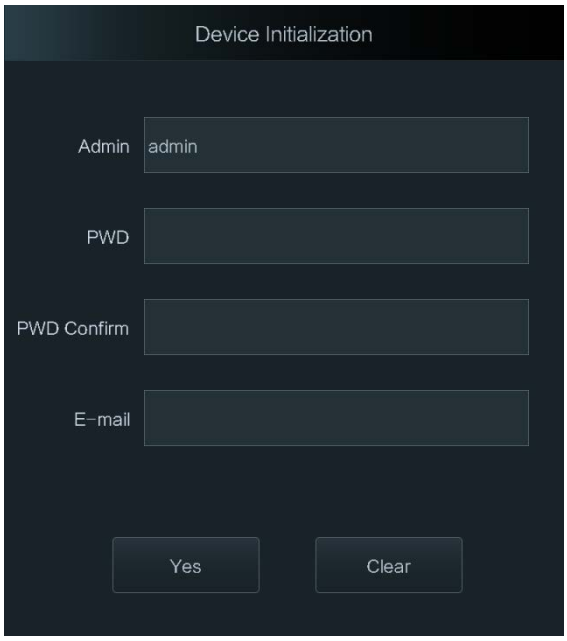
Tabla 2-1 Descripción de los iconos

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

2.3 Inicialización

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

Figura 2-2 Inicialización



- El administrador y la contraseña configurados en esta interfaz se utilizan para iniciar sesión en la plataforma de administración web.
- La contraseña de administrador se puede restablecer a través de la dirección de correo electrónico que ingresó si el administrador la olvida.
- 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 '";: &).

2.4 Interfaz de espera

Puede desbloquear la puerta a través de rostros, huellas dactilares, contraseñas y tarjetas.

- Los métodos de desbloqueo pueden variar según los modelos.
- Si no hay operaciones en 30 segundos, el controlador de acceso pasará al modo de espera.
- Las interfaces de espera que se muestran en esta sección son solo de referencia y pueden diferir de las reales.

Figura 2-3 Interfaz de espera del modelo J

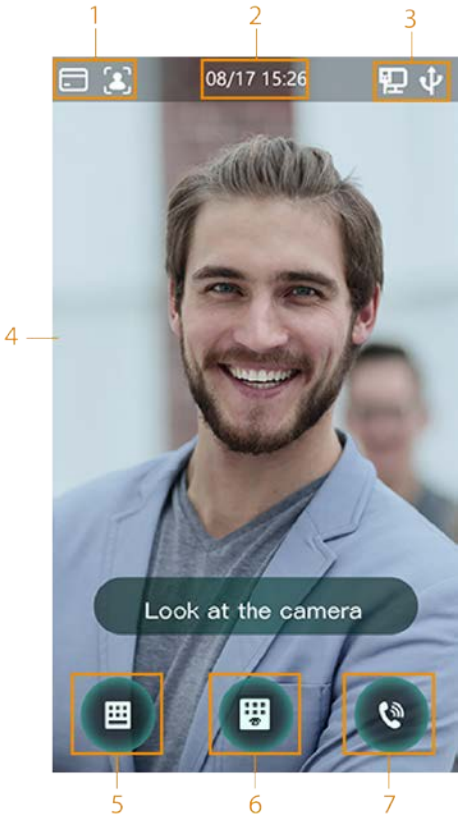


Figura 2-4 Interfaz de espera del modelo G

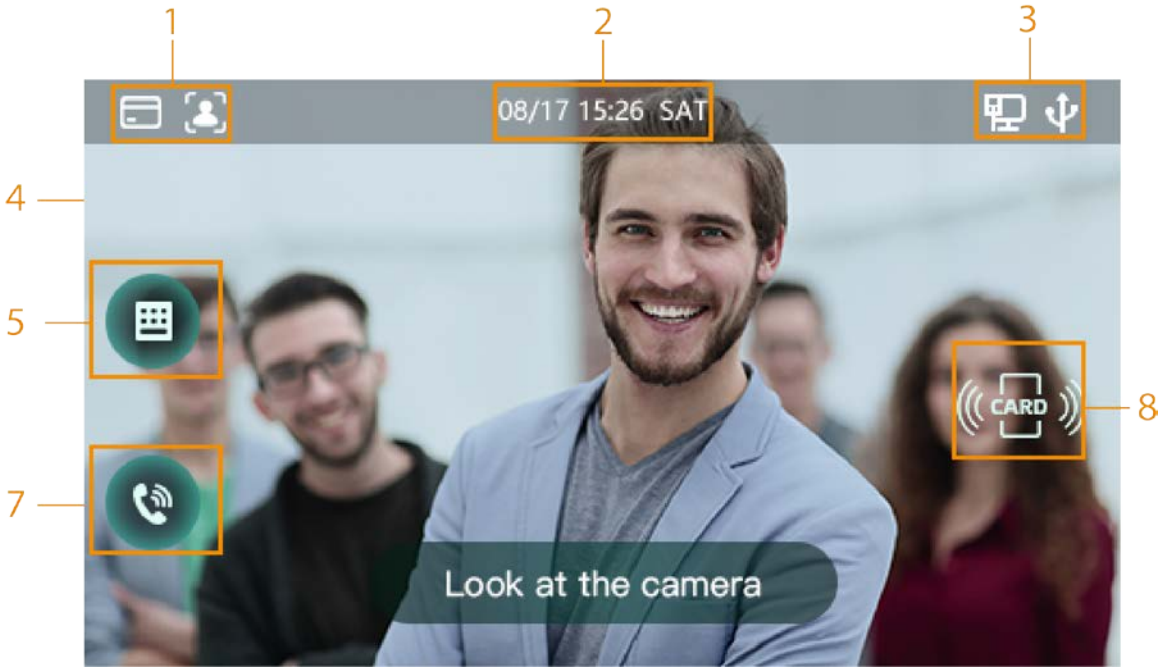


Tabla 2-2 Descripción de la página de inicio

No.	Descripción
1	Métodos de desbloqueo: tarjeta, rostro, huella digital y contraseña. Cuando la tarjeta, el rostro, la huella digital y la contraseña están configurados como modo de desbloqueo, el icono de contraseña no se mostrará en la esquina superior izquierda del controlador de acceso.
2	Fecha y hora. Muestra la fecha y hora actual.

No.	Descripción
3	Muestra el estado de la red y el estado del USB.
4	Área de reconocimiento facial.
5	Icono de desbloqueo de contraseña.
6	Icono de desbloqueo de contraseña de administrador.
7	Toque para llamar a otros dispositivos.
8	Área de deslizamiento de tarjetas.

2.5 Menú principal

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

Paso1 En la interfaz de espera, mantenga pulsado 3 s para ir al **Inicio de sesión de administrador** interfaz.

Paso2 Seleccione un método de entrada al menú principal.

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

Figura 2-5 Inicio de sesión de administrador

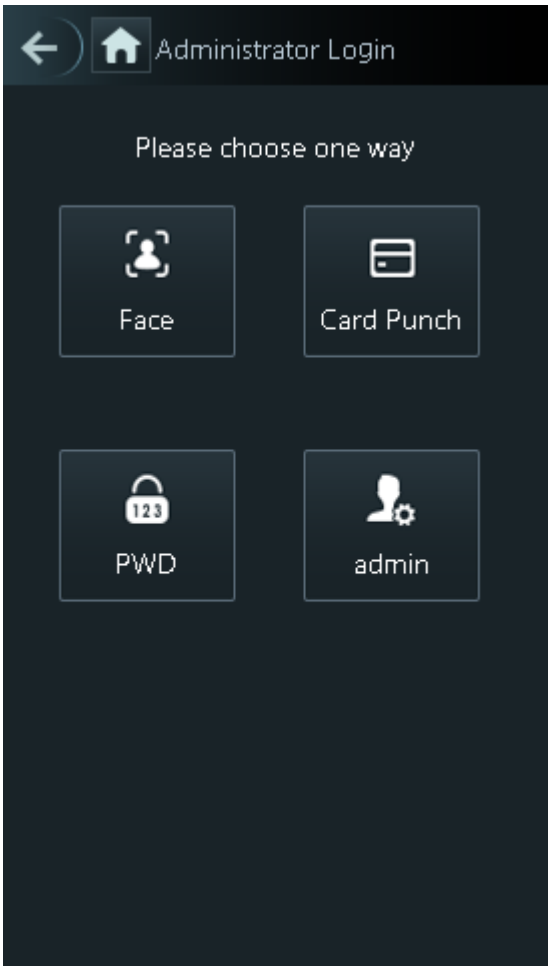


Figura 2-6 Menú principal

2.6 Métodos de desbloqueo

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

2.6.1 Tarjetas

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

2.6.2 Cara

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

2.6.3 Huellas digitales

Coloque su huella digital en el sensor de huellas digitales para desbloquear la puerta.

Solo algunos modelos admiten esta función.

2.6.4 Contraseña de usuario

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

Paso1 toque  en la página de inicio.

Paso2 Toque **Desbloqueo de PWD**.

Paso3 Ingrese el ID de usuario y la contraseña, y luego toque .

La puerta está desbloqueada.

2.6.5 Contraseña de administrador

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

No se puede utilizar la contraseña de administrador cuando se selecciona NC en "2.8.1.5 Periodo NC".

Paso1 toque  en la página de inicio.

Paso2 Toque **Admin PWD**.

Paso3 Ingrese la contraseña de administrador y luego toque .

La puerta está desbloqueada.

2.7 Gestión de usuarios

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

2.7.1 Agregar nuevos usuarios

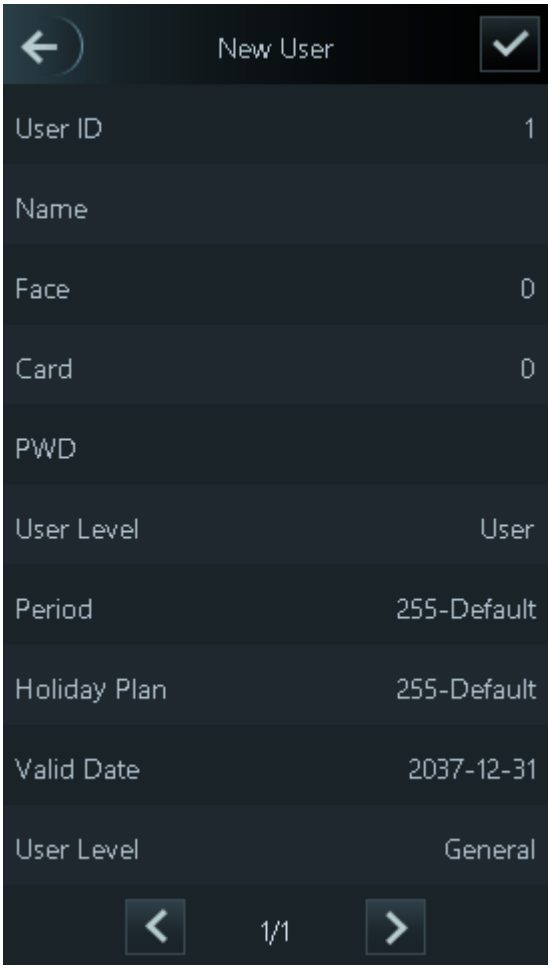
Puede agregar nuevos usuarios ingresando ID de usuario, nombres, imágenes de caras, tarjetas, contraseñas, seleccionando niveles de usuario y más.

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

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Seleccione **Usuario> Nuevo usuario**.

Figura 2-7 Información de nuevo usuario



Paso3 Configure los parámetros en la interfaz.

Tabla 2-3 Descripción del nuevo parámetro de usuario

Parámetro	Descripción
ID de usuario	Ingrese los ID de usuario. Las identificaciones pueden ser números, letras y sus combinaciones, y la longitud máxima de la identificación es de 32 caracteres. Cada identificación es única.
Nombre	Ingrese nombres con un máximo de 32 caracteres (incluidos números, símbolos y letras).
Cara	Asegúrese de que su rostro esté centrado en el marco de captura de la imagen y el controlador de acceso tomará una foto del rostro 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.
PWD	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 controlador de acceso a un lector de tarjetas periférico. Hay botones en el lector de tarjetas.

Parámetro	Descripción
Nivel de usuario	Puede seleccionar un nivel de usuario para nuevos usuarios. Hay dos opciones: - Usuario: los usuarios solo tienen permiso de desbloqueo de 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 autenticación de identidad de administrador.
Período	Puede establecer un período en el que el usuario puede desbloquear la puerta. "Consulte 3.7 Sección de tiempo" para obtener más detalles.
Plan de vacaciones	Puede establecer un plan de vacaciones en el que el usuario puede abrir la puerta. "Consulte 3.7 Sección de tiempo" para obtener más detalles.
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 de bloqueo: los usuarios de la lista de bloqueo no tienen permiso de desbloqueo. Cuando intenten desbloquear la puerta, el controlador de acceso le indicará que se trata de un usuario de lista de - bloqueo. Invitado: Los invitados pueden abrir la puerta en determinadas ocasiones. Una vez que superan los tiempos máximos, no pueden volver a desbloquear la puerta. - Patrulla: los usuarios en 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. - Otro: cuando personas especiales desbloquean la puerta, habrá un retraso de 5 segundos antes de que se cierre la puerta. - Usuario personalizado 1: reservado para personalización. Los usuarios pueden desbloquear la puerta normalmente. - Usuario personalizado 2: reservado para personalización. Los usuarios pueden desbloquear la puerta normalmente.
Tiempo de uso	Cuando el nivel de usuario es Invitado, puede establecer el número máximo de veces que el usuario puede desbloquear la puerta.

Paso4 Toque  para guardar la configuración.

2.7.2 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.

2.8 Gestión de acceso

Puede realizar la gestión de acceso en el período, el modo de desbloqueo, la alarma, el estado de la puerta y el tiempo de retención de la cerradura. Grifo**Acceso** para ir a la interfaz de administración de acceso.

2.8.1 Gestión de períodos

Puede establecer períodos, períodos de vacaciones, períodos del plan de vacaciones, períodos de puerta normalmente cerrada, períodos de puerta normalmente cerrada y períodos de verificación remota.

2.8.1.1 Configuración de período

Para los controladores de acceso modelo G, puede configurar períodos localmente; para los controladores de acceso modelo J, puede configurar períodos a través de la interfaz web.

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.

2.8.1.2 Grupo de vacaciones

Para los controladores de acceso modelo G, puede configurar grupos de vacaciones localmente; para los controladores de acceso modelo J, puede configurar grupos de vacaciones a través de la interfaz web.

Puede establecer vacaciones en grupo y luego puede establecer planes para grupos de vacaciones. Puede configurar 128 grupos cuyo rango de números es 0-127. Puede agregar 16 días festivos a un grupo. Configure la hora de inicio y la hora de finalización de un grupo de vacaciones, y luego los usuarios solo podrán desbloquear la puerta en los períodos que establezca.

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

2.8.1.3 Plan de vacaciones

Para los controladores de acceso modelo G, puede configurar planes de vacaciones localmente; para los controladores de acceso modelo J, puede configurar planes de vacaciones a través de la interfaz web.

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

2.8.1.4 Periodo NO

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

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

2.8.1.5 Periodo NC

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

2.8.1.6 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.

Necesitas habilitar **Período de verificación remota**.

-  significa habilitado.
-  significa no habilitado.

2.8.2 Desbloquear

Hay dos modos de desbloqueo: modo de desbloqueo y modo de control de temperatura. Los modos de desbloqueo que se describen en esta sección son solo de referencia y pueden variar según el modelo.

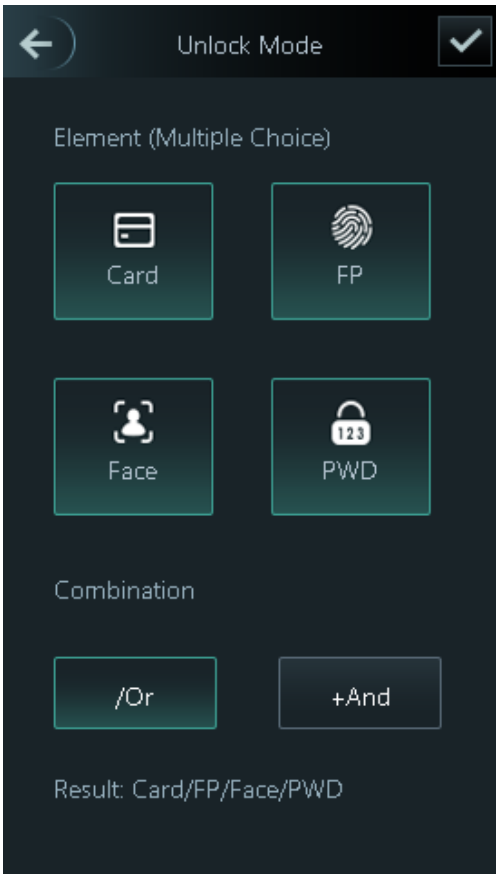
2.8.2.1 Modo de desbloqueo

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

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Seleccione **Acceso> Modo de desbloqueo> Modo de desbloqueo**.

Figura 2-8 Elemento (opción múltiple)



Paso3 Seleccione uno o más métodos de desbloqueo.

- Los métodos de desbloqueo que se muestran en la figura anterior son solo de referencia y pueden variar según los modelos.
- Toque de nuevo un método de desbloqueo seleccionado para anular su selección.

Paso4 Seleccione un modo de combinación.

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

Paso5 Toque para guardar la configuración.

Paso6 Habilitar **Modo de desbloqueo**.

- significa habilitado.
- significa no habilitado.

2.8.2.2 Modo de monitoreo de temperatura

El controlador de acceso desbloqueará la puerta cuando su temperatura sea normal.

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Seleccione **Acceso> Modo de desbloqueo**y luego habilite **Solo modo de monitoreo de temperatura**.

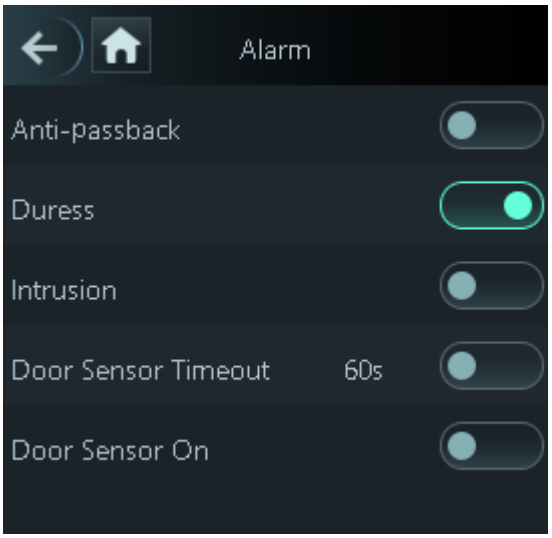
2.8.3 Configuración de alarma

Los administradores pueden gestionar el permiso de desbloqueo de los visitantes mediante la configuración de alarmas.

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Seleccione **Acceso> Alarma**.

Figura 2-9 Alarma



-  significa habilitado.
-  significa discapacitado.

Tabla 2-4 Parámetros en la interfaz de alarma

Parámetro	Descripción
Anti-passback	Una vez habilitado el anti-passback, los usuarios deben verificar las identidades tanto para la entrada como para la salida; de lo contrario, se activará una alarma. - Si una persona entra con la identidad verificada y sale sin la identidad verificada, se activará una alarma cuando la persona intente ingresar nuevamente y la persona ya no tendrá permiso para abrir la puerta. - Si una persona entra sin verificar la identidad, se activará una alarma cuando la persona intente salir con la identidad verificada, y la persona ya no tendrá permiso para abrir la puerta.
Coacción	Se activará una alarma cuando se utilice una tarjeta de coacción o una contraseña de coacción para desbloquear la puerta.
Intrusión	Se activará una alarma de intrusión si se desbloquea una puerta sin que se libere 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 excede 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 encendido	Solo cuando el **Sensor de puerta encendido** está habilitado puede activarse la alarma de intrusión y la alarma de tiempo de espera del sensor de puerta.

2.8.4 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.
- Normal: si **Normal** está seleccionado, la puerta se desbloqueará y bloqueará según su configuración.

2.8.5 Bloqueo de tiempo de retención

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

2.9 Asistencia

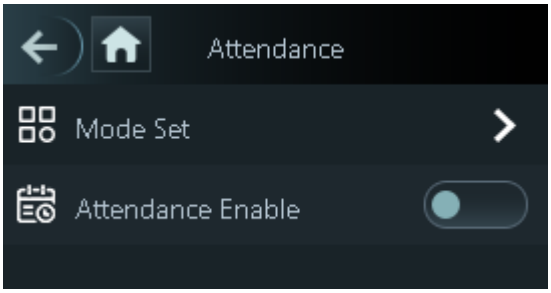
Puede habilitar la asistencia y configurar el modo de asistencia según sea necesario.

Esta función debe funcionar con una plataforma. Para obtener más información, consulte el manual del usuario correspondiente.

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Toque **Asistencia**y luego toque  para permitir la asistencia.

Figura 2-10 Asistencia

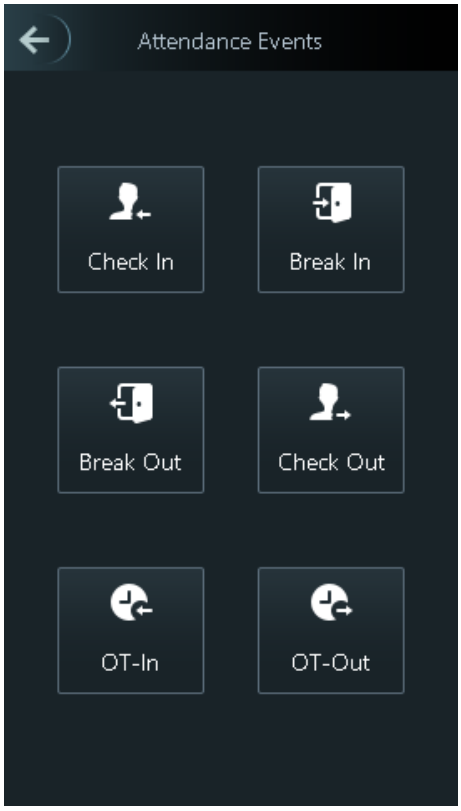


Paso3 Toque **Modo establecido** para establecer un modo de asistencia y el tiempo para diferentes estados de asistencia.

- **Modo automático / manual**: Muestra el estado de asistencia de acuerdo con la hora de entrada o salida. Si la hora de entrada o salida no está definida, puede tocar**Eventos de asistencia** y seleccione un estado de asistencia según sea necesario.
- **Modo automático**: Muestra el estado de asistencia de acuerdo con la hora de entrada o salida.
- **Modo manual**: Debe seleccionar manualmente un estado de asistencia al registrarse o salir.

- **Modo fijo**: El estado de asistencia se fija cuando ingresa o sale en la interfaz de espera.

Figura 2-11 Estado de asistencia



Para los seis estados, puede definirlos según sea necesario, como **Registrarse** para el comienzo de una jornada laboral y **Fugarse** para el inicio de la pausa para el almuerzo.

2.10 Comunicación de red

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

2.10.1 Configuración de IP

Configure una dirección IP para que el controlador de acceso se conecte a la red.

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Seleccione **Conexión> Red> Dirección IP**y luego configure los parámetros de la dirección IP.

Figura 2-12 Configuración de la dirección IP

Tabla 2-5 Parámetros de configuración de IP

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

Asegúrese de que la computadora utilizada para iniciar sesión en la interfaz web esté en la misma LAN que el controlador de acceso.

2.10.2 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 administración y el controlador de acceso se puede inicializar; debe proteger el permiso de administración de la plataforma en caso de pérdida de datos causada por una operación incorrecta.

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Seleccione **Conexión> Red> Registro activo**.

Paso3 Toque para habilitar el registro activo y luego configurar los parámetros.

Tabla 2-6 Registro activo

Nombre	Parámetro
Dirección IP del servidor	Dirección IP de la plataforma de gestión.

Nombre	Parámetro
Puerto	Número de puerto de la plataforma de gestión.
ID del dispositivo	Número de dispositivo subordinado en la plataforma de gestión.

2.10.3 Wi-Fi

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

Paso1 Inicie sesión en **Menú principal** interfaz.

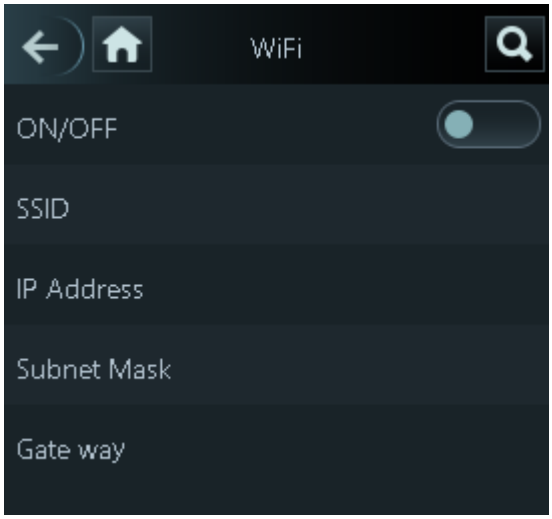
Paso2 Seleccione **Conexión> Red> WiFi**.

Paso3 Toque  para habilitar Wi-Fi.

Paso4 Toque  , seleccione una red y luego ingrese la contraseña.

Puede ver la información de la red en la siguiente interfaz.

Figura 2-13 Wi-Fi



2.10.4 Configuración del puerto serie

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

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Seleccione **Conexión> Puerto serie**.

Figura 2-14 Puerto serie

- Seleccione **Entrada serial** cuando los dispositivos externos que tienen funciones de lectura y escritura de tarjetas están conectados al controlador de acceso. **Entrada serial** 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 serial**, el controlador de acceso enviará información de bloqueo / desbloqueo a otros controladores de acceso. Hay dos tipos de información de bloqueo / desbloqueo: ID de usuario y 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.

2.10.5 Configuración Wiegand

Solo los controladores de acceso modelo J admiten esta función.

Seleccione **Entrada Wiegand** o **Salida Wiegand** respectivamente.

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Seleccione **Conexión> Wiegand**.

Figura 2-15 Wiegand

- Seleccione **Entrada Wiegand** cuando un mecanismo de deslizamiento de tarjeta externo está conectado al controlador de acceso.
- Seleccione **Salida Wiegand** cuando el controlador de acceso funciona como un lector que se puede conectar a otros controladores. Consulte la Tabla 2-7.

Tabla 2-7 Salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	los **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	Configure el valor según sea necesario.
Intervalo de pulso	
Tipo de datos de salida	- **ID de usuario**: Si se selecciona ID de usuario, se generará la ID de usuario. - **Tarjeta No.**: Si se selecciona Número de tarjeta, se emitirá el número de tarjeta.

2.11 Sistema

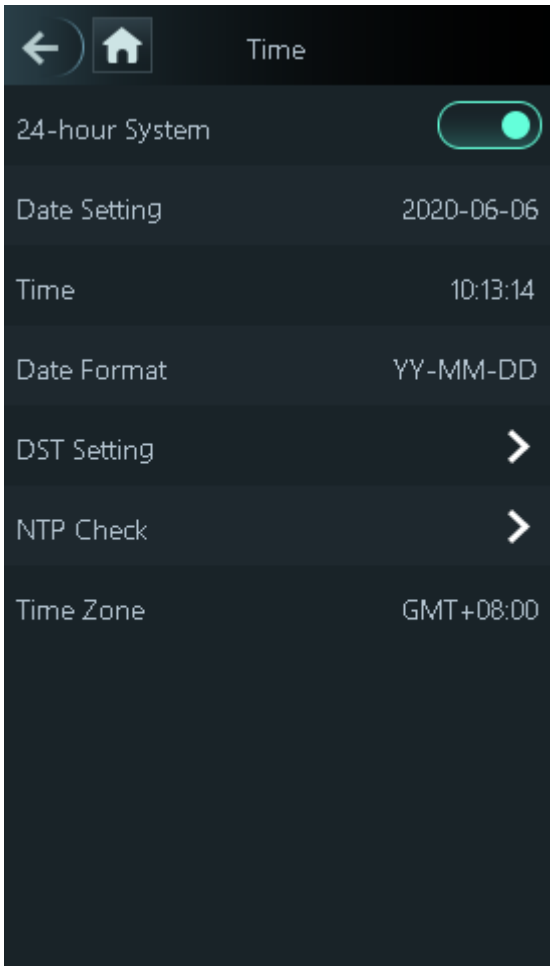
2.11.1 Hora

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

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Seleccione **Sistema> Hora**y luego configure los parámetros de tiempo.

Figura 2-16 Hora



- Cuando seleccionas **Protocolo de tiempo de red** (NTP), primero debe habilitar la función Verificación de NTP. Dirección IP del servidor: ingrese la dirección IP del servidor horario, la hora del controlador de acceso se sincronizará con el servidor horario.
- Puerto: ingrese el número de puerto del servidor horario.
- Intervalo (min): intervalo de verificación NPT. Toque el icono de guardar para guardar.

2.11.2 Parámetro de cara

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Seleccione **Sistema> Parámetro facial**.

Figura 2-17 Parámetro de cara

Paso3 Toque un parámetro y realice la configuración, y luego toque .

Tabla 2-8 Parámetros faciales

Parámetro	Descripción
Umbral facial	Se puede ajustar la precisión del reconocimiento facial. Cuanto mayor sea el valor, mayor será la precisión.
Max. Ángulo de la cara	Configure el ángulo de disparo de los perfiles del panel de control. Cuanto mayor sea el valor, se reconocerá la gama más amplia de perfiles.
Distancia pupilar	La distancia pupilar es el valor de píxel de la imagen entre los centros de las pupilas de cada ojo. Debe establecer un valor apropiado para que el controlador de acceso pueda reconocer caras según sea necesario. El valor cambia según el tamaño de la cara y la distancia entre las caras y la lente. Cuanto más cerca esté la cara de la lente, mayor debe ser el valor. Si un adulto está a 1,5 metros de la lente, el valor de la distancia pupilar puede estar entre 50 y 70. El intervalo de la
Tiempo de espera de reconocimiento	indicación durante el reconocimiento facial válido.
Mensaje de rostro no válido Intervalo (S)	Para un rostro que no tiene permiso de acceso, el controlador indicará que el rostro no es válido. El intervalo de aviso es un intervalo de aviso de rostro no válido.
Umbral anti-falsificación	Esta función evita que las personas se desbloqueen mediante imágenes de rostros o modelos.
Parámetros de temperatura	- **Monitoreo de temperatura**: Habilita o deshabilita esta función. - **Temp Rect**: Establezca si se muestra el cuadro de control de temperatura o no. - **Distancia de monitoreo de temperatura** (cm): 50 por defecto. Debe controlar su temperatura alejándose del controlador de acceso a la distancia que defina. Solo ciertos modelos admiten este parámetro. - **Duración de la corrección de temperatura (ms)**: Al controlar la temperatura,

Parámetro	Descripción
	el controlador de acceso tomará el valor de temperatura después del tiempo definido por este parámetro. Solo ciertos modelos admiten este parámetro. - **Umbral de temperatura alta**: Establece el umbral de temperatura. La temperatura corporal monitoreada se considerará alta si es mayor o igual al valor establecido. Solo ciertos modelos admiten este parámetro. - **Temperatura máxima / mínima**: Establezca el rango de temperatura que necesita. Si la temperatura monitoreada es más baja que el límite inferior, indicará que la temperatura es demasiado baja; si es superior al límite superior, indicará que hay una fuente de calor que interfiere con la función. - **Valor de corrección de temperatura**: Este parámetro es para pruebas. La diferencia del entorno de monitoreo de temperatura puede causar la desviación de temperatura entre la temperatura monitoreada y la temperatura real. Puede seleccionar varias muestras monitoreadas para la prueba y luego corregir la desviación de temperatura con este parámetro de acuerdo con la comparación entre la temperatura monitoreada y la temperatura real. Por ejemplo, si la temperatura monitoreada es 0.5 ° C más baja que la temperatura real, el valor de corrección se establece en 0.5 ° C; si la temperatura monitoreada es 0,5 ° C más alta que la temperatura real, el valor de corrección se establece en -0,5 ° C. - **Modo de monitoreo de temperatura**: Solo ciertos modelos admiten este parámetro. - Automático: utiliza un mapa de calor facial para el reconocimiento facial; si no se encuentran mapas de calor, cambiará automáticamente al modo de calibración. - Termograma: utiliza solo un mapa de calor para el reconocimiento facial y el control de la temperatura. - Calibración: utiliza una imagen de luz blanca de una cara para el reconocimiento facial, y luego extrae y aplica las coordenadas en el mapa de calor de la cara para monitorear la temperatura. - **Unidad de temperatura**: Seleccione ° C o ° F. - **Valor de compensación de Evn**: Este valor se agregará a la temperatura ambiente monitoreada. Solo ciertos modelos admiten este parámetro. - **Estrategia de temperatura**: Solo ciertos modelos admiten este parámetro. - **Máximo**: Toma la temperatura más alta como resultado. - **Promedio**: Tome la temperatura media como resultado.

Parámetro	Descripción
	Solo el controlador de acceso con una unidad de monitoreo de temperatura admite este parámetro.
Parámetros de máscara	- **No detectar**: La máscara no se detecta durante el reconocimiento facial. - **Recordatorio de máscara**: La máscara se detecta durante el reconocimiento facial. Si la persona es detectada sin usar una máscara, el sistema le recordará la máscara y se permitirá el paso. - **Intercepción de máscara**: La máscara se detecta durante el reconocimiento facial. Si se detecta a la persona sin usar una máscara, el sistema le recordará la máscara y no se permitirá el paso. - **Umbral de reconocimiento de máscara**: Cuando se detecta una máscara, este valor se aplicará al reconocimiento facial. Cuanto mayor sea el valor, mayores serán los requisitos de precisión y más difícil de reconocer a una persona que lleva una máscara.

2.11.3 Modo de imagen

Hay tres opciones:

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

2.11.4 Volumen

Grifo  O  para ajustar el volumen.

2.11.5 Idioma

Los siguientes idiomas están disponibles: inglés, italiano, español, japonés, ruso, turco, polaco, coreano, árabe, español (América Latina) y tailandés.

2.11.6 Luz infrarroja

Grifo  O  para ajustar el brillo de la luz infrarroja.

Cuanto mayor sea el valor, más brillante será la luz infrarroja.

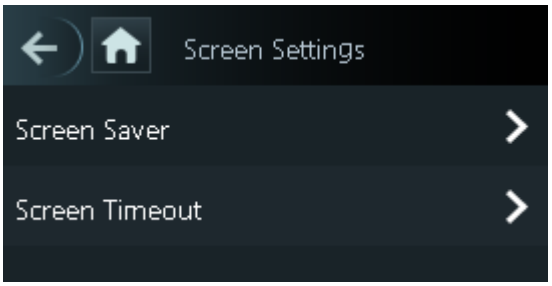
2.11.7 Configuración de pantalla

Puede configurar el tiempo del protector de pantalla y el tiempo de apagado de la pantalla.

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Seleccione **Sistema> Configuración de pantalla**.

Figura 2-18 Configuración de pantalla



2.11.8 Restaurar la configuración de fábrica

⚠

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

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

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

2.11.9 Reiniciar

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Seleccione **Sistema> Reiniciar**y se reiniciará el controlador de acceso.

2.12 USB

⚠

- Asegúrese de que el USB esté insertado en el controlador de acceso antes de exportar la información del usuario y actualizar.
- Durante la exportación o actualización, no extraiga el USB ni opere el controlador de acceso; de lo contrario, la exportación o la actualización fallarán.
- Exporte la información de un controlador de acceso al USB y luego impórtela a otro controlador de acceso. Los diferentes modelos admiten diferentes tipos de información, como rostros y huellas dactilares.
- También se puede utilizar USB para actualizar el programa.

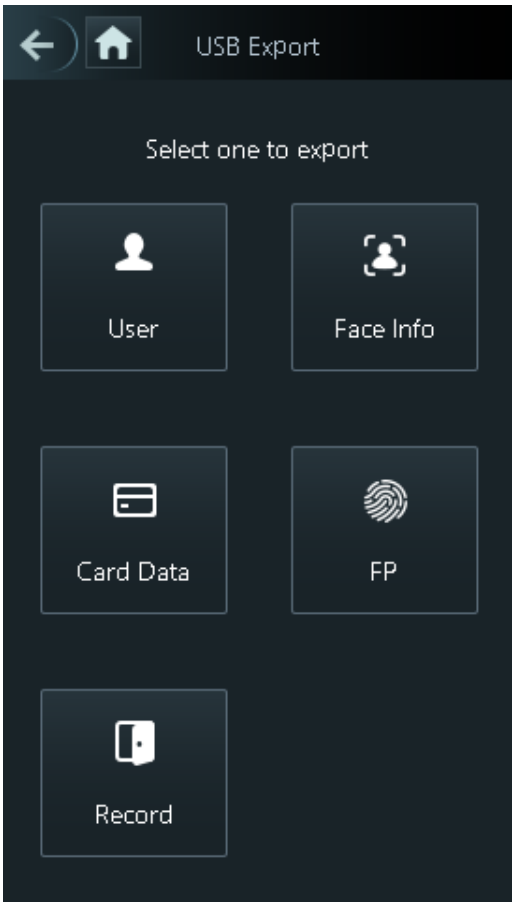
2.12.1 Exportación USB

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.

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Seleccione **USB> Exportación USB**.

Figura 2-19 Exportación USB



Paso3 Seleccione el tipo de datos que desea exportar.

Solo ciertos modelos admiten huellas dactilares.

Paso4 Toque **OK**.

Los datos se guardarán en el USB.

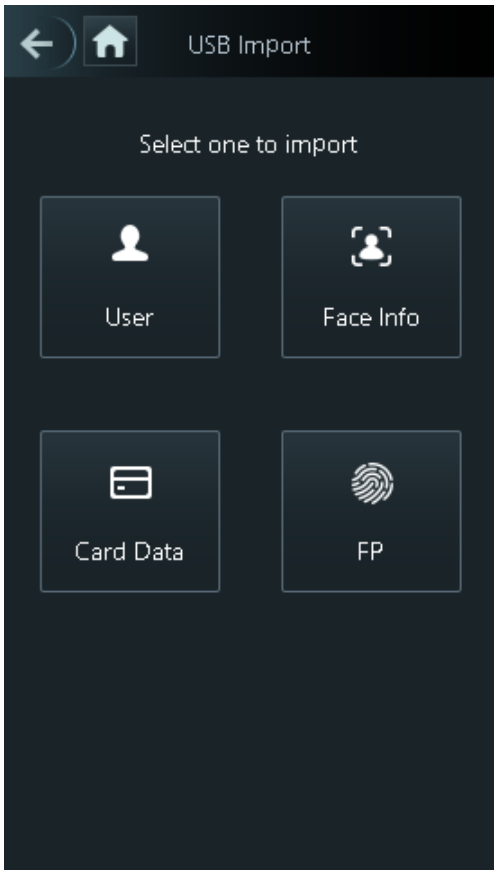
2.12.2 Importación USB

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

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Seleccione **USB> Importación USB**.

Figura 2-20 Importación USB



Paso3 Seleccione el tipo de datos que desea importar.

Paso4 Toque **OK**.

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

2.12.3 Actualización USB

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

Paso1 Cambie el nombre del archivo de actualización a "update.bin" y guarde el archivo "update.bin" en el directorio raíz.

directorio de la unidad flash USB.

Paso2 Inicie sesión en **Menú principal** interfaz.

Paso3 Seleccione **USB> Actualización USB**.

Paso4 Toque **OK**.

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

2.13 Funciones

Puede realizar configuraciones sobre privacidad, número de tarjeta inverso, módulo de seguridad, tipo de sensor de puerta y retroalimentación de resultados.

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Toque **Características**.

Figura 2-21 Características

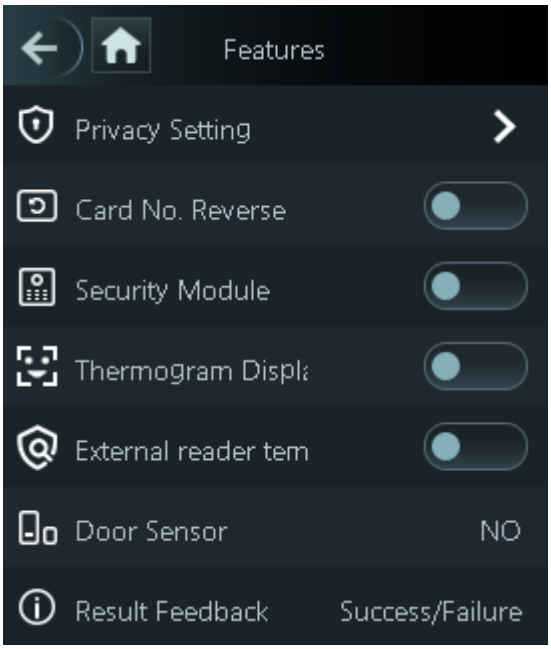


Tabla 2-9 Descripción de funciones

Parámetro	Descripción
Configuración de privacidad	Consulte "2.13.1 Configuración de privacidad" para obtener más detalles.
Número de tarjeta reverso	Si el lector de tarjetas de terceros debe conectarse al controlador de acceso a través del puerto de salida wiegand, debe habilitar la función de inversión del número de tarjeta; de lo contrario, la comunicación entre el controlador de acceso y el lector de tarjetas de terceros podría fallar debido a una discrepancia de protocolo.
Módulo de seguridad	- Si el módulo de seguridad está habilitado, debe comprar el módulo de seguridad de control de acceso por separado. El módulo de seguridad necesita una fuente de alimentación independiente para proporcionar energía. - Una vez que el módulo de seguridad está habilitado, el botón de salida, el control de bloqueo y el enlace de extinción de incendios no serán válidos.
Pantalla de termograma	Muestre un mapa de calor en la esquina superior izquierda. Solo algunos modelos admiten esta función.
Temperatura del lector externo Vigilancia	Enciéndalo y el lector de tarjetas también controlará la temperatura de una persona.
Sensor de puerta	**NO** para normalmente abierto o **CAROLINA DEL NORTE** para normalmente cerrado.
Comentarios de resultados	Seleccione un modo de retroalimentación de resultados durante el desbloqueo. Consulte "2.13.2 Comentarios de resultados".

2.13.1 Configuración de privacidad

Figura 2-22 Configuración de privacidad

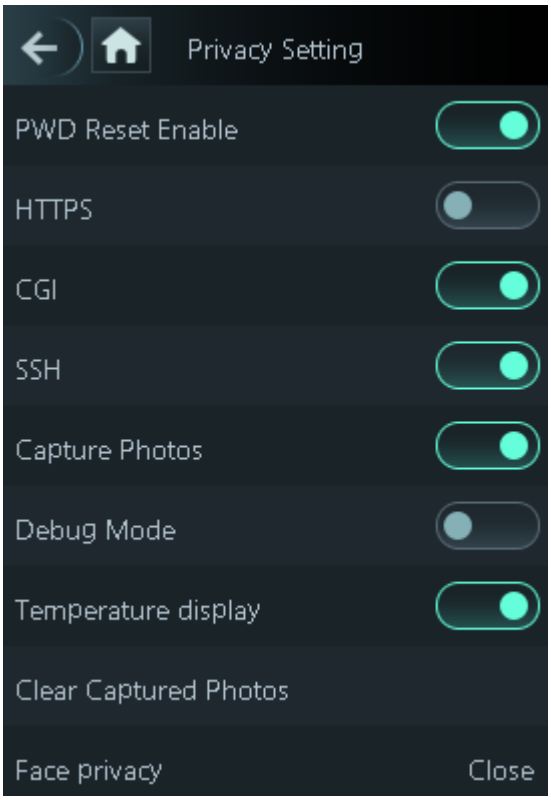


Tabla 2-10 Configuración de privacidad

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

Parámetro	Descripción
Modo de depuración	Habilite este modo para mostrar la temperatura del cuerpo negro en la interfaz de espera. Puede corregir la temperatura del cuerpo negro en consecuencia. - Solo algunos modelos admiten esta función. - Cuando este modo está habilitado, la puerta no se puede abrir por ningún método.
Temperatura Monitor	Si está habilitado, la temperatura se mostrará en los resultados de desbloqueo.
Borrar capturado Fotos	Elimina todas las fotos capturadas.
Privacidad facial	Si está habilitado, la interfaz de espera se cubrirá en mosaico.

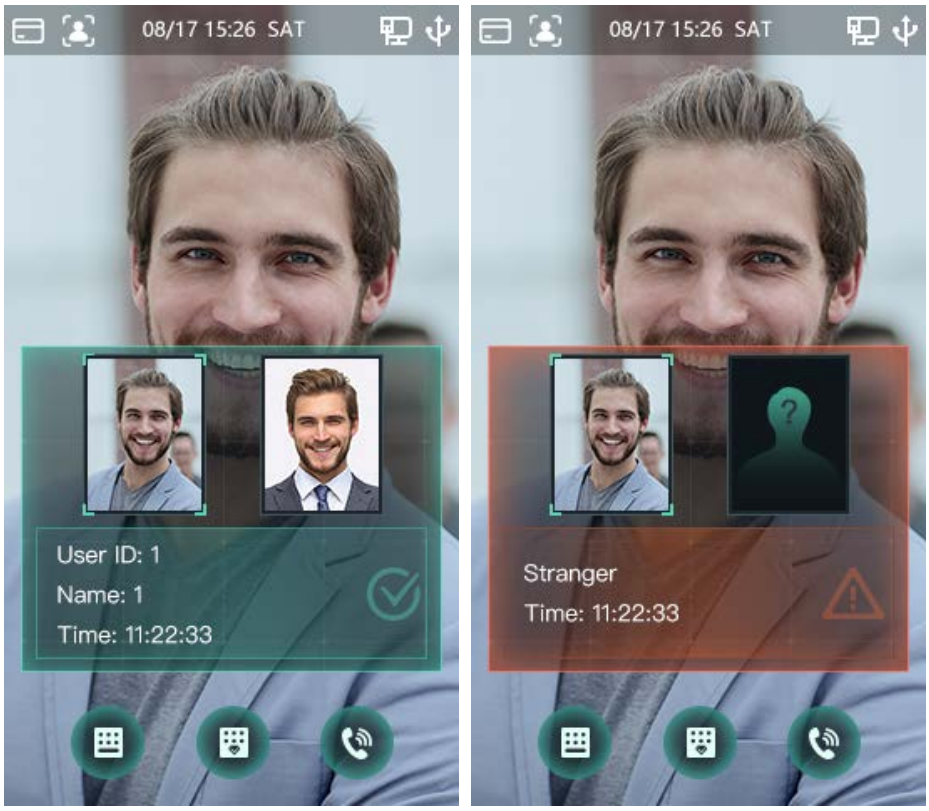
2.13.2 Comentarios sobre los resultados

Hay 4 modos de retroalimentación de resultados: éxito / fracaso, solo nombre, foto y nombre y fotos y nombre. Puede seleccionar un modo de retroalimentación de resultados según sea necesario.

Modo Fotos y nombre

La imagen de la cara capturada, la imagen guardada en la base de datos de caras, el ID de usuario, el nombre de usuario y la hora se muestran durante el desbloqueo.

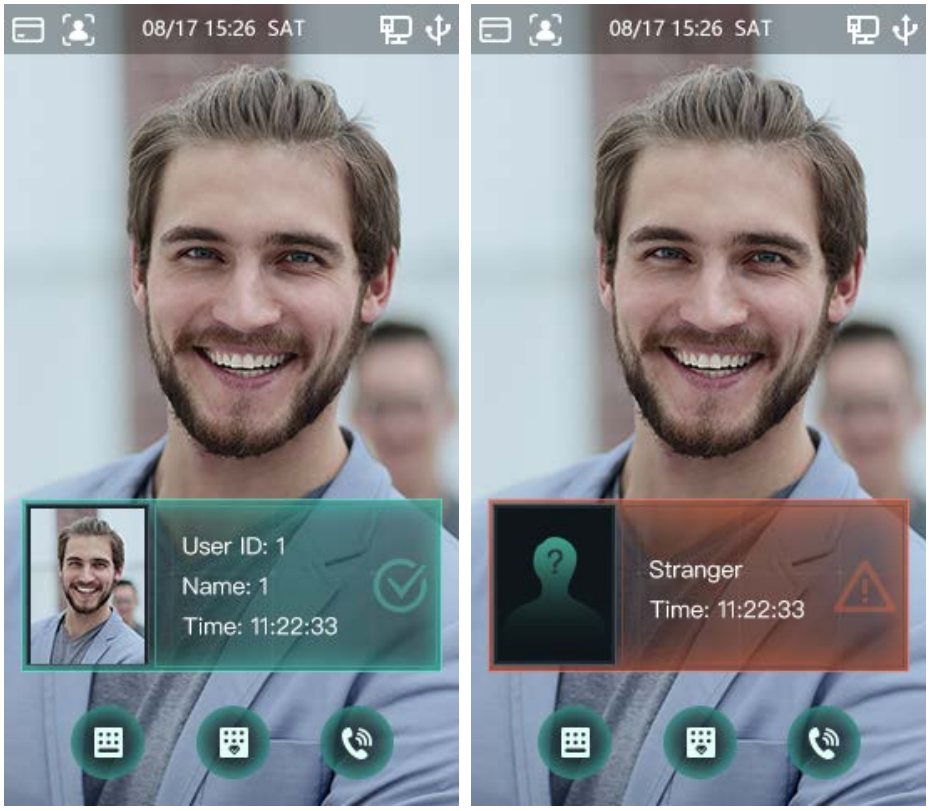
Figura 2-23 Modo de fotos y nombre (1)



Modo de foto y nombre

La imagen guardada en la base de datos de rostros, la identificación de usuario, el nombre de usuario y la hora se muestran durante el desbloqueo.

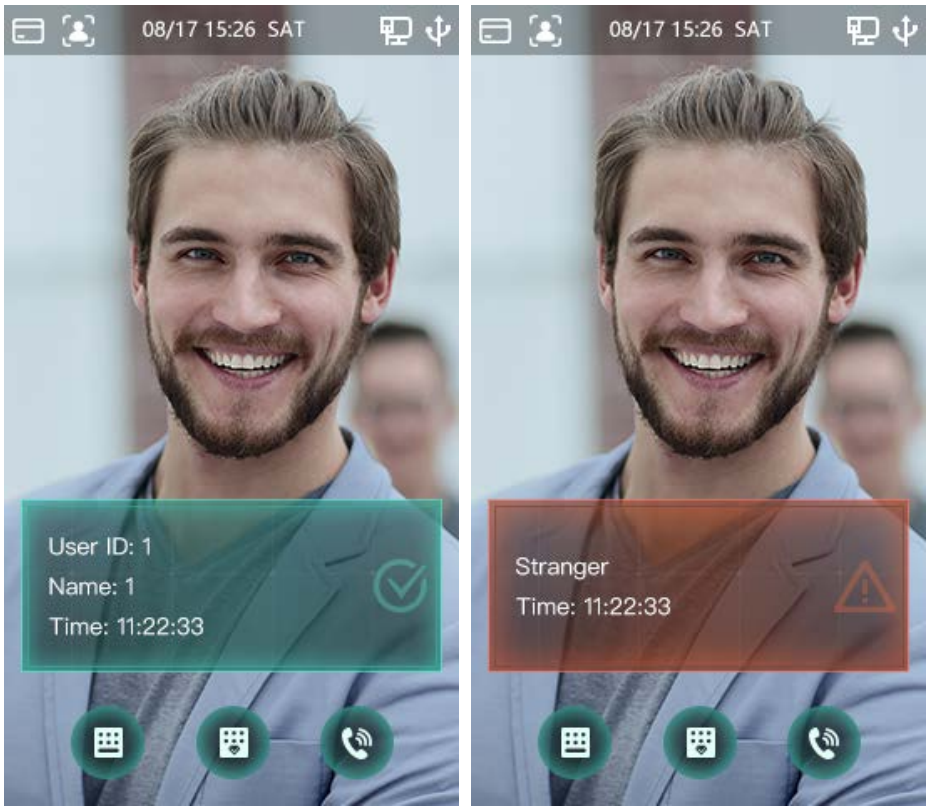
Figura 2-24 Modo de foto y nombre (2)



Solo modo de nombre

Durante el desbloqueo, solo se muestran el ID de usuario, el nombre de usuario y la hora.

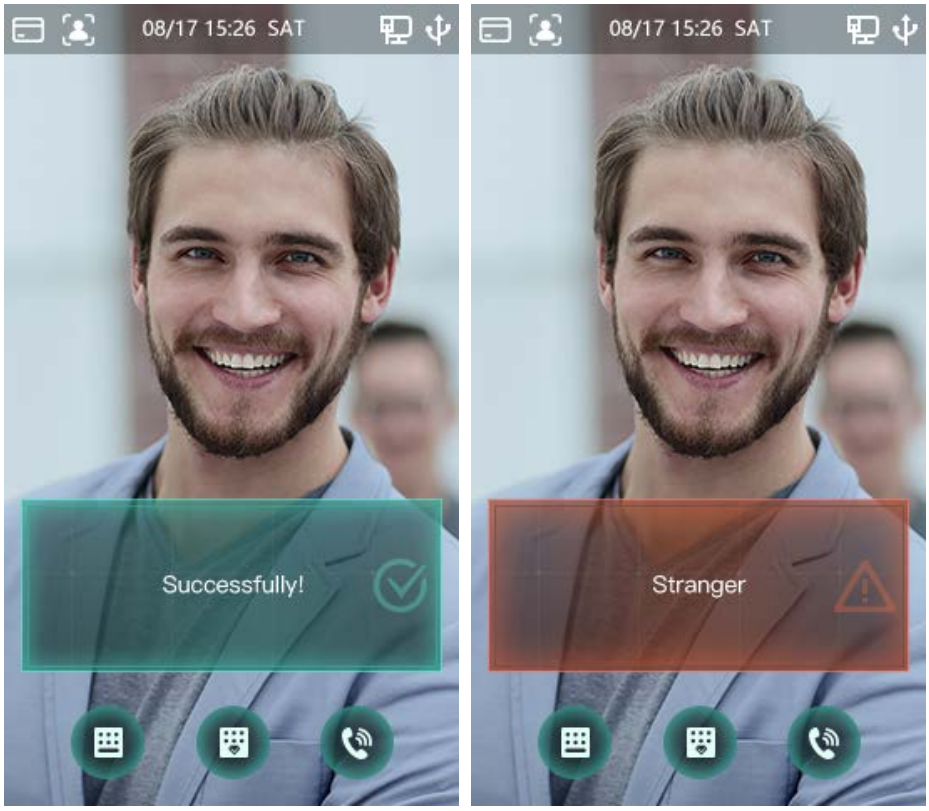
Figura 2-25 Modo de solo nombre



Modo de éxito / fracaso

Solo muestra el éxito o el fracaso durante el desbloqueo.

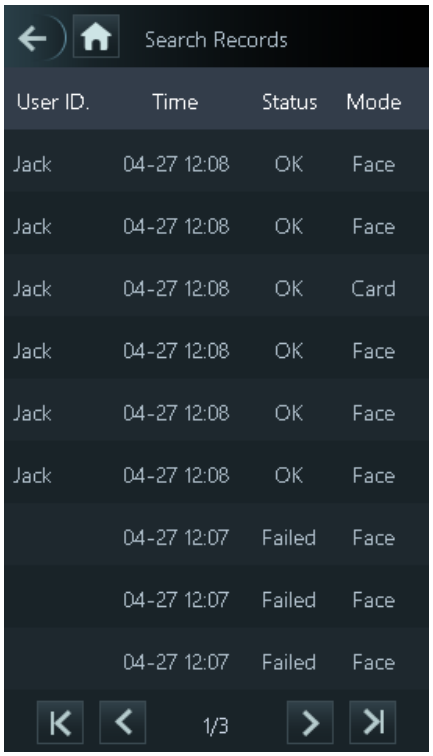
Figura 2-26 Modo de éxito / fracaso



2.14 Registro

Puede consultar todos los registros de desbloqueo.

Figura 2-27 Buscar registros perforados



2.15 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.

Paso1 Inicie sesión en **Menú principal** interfaz.

Paso2 Toque **Información del sistema**.

Figura 2-28 Información del sistema

3 Operaciones web

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

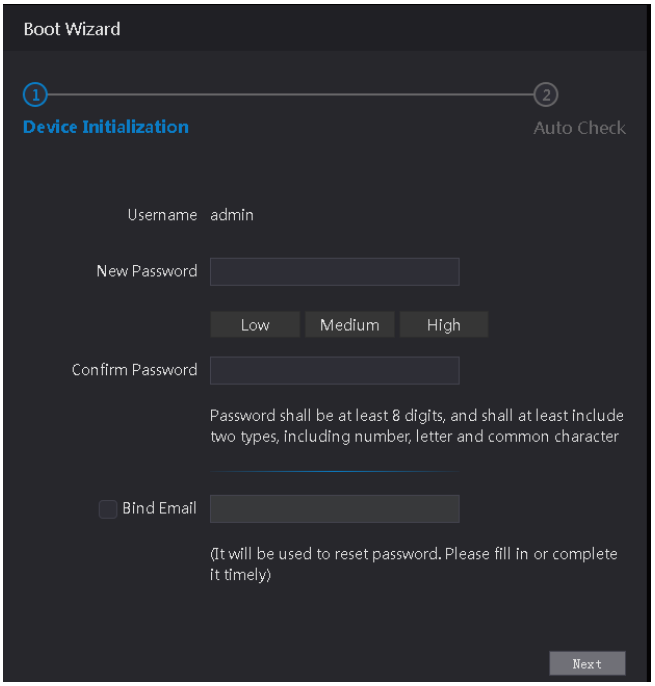
3.1 Inicialización

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

Paso1 Abra el navegador web IE e introduzca la dirección IP (la dirección predeterminada es 192.168.1.108) del controlador de acceso en la barra de direcciones y, a continuación, 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 controlador de acceso.

Figura 3-1 Inicialización

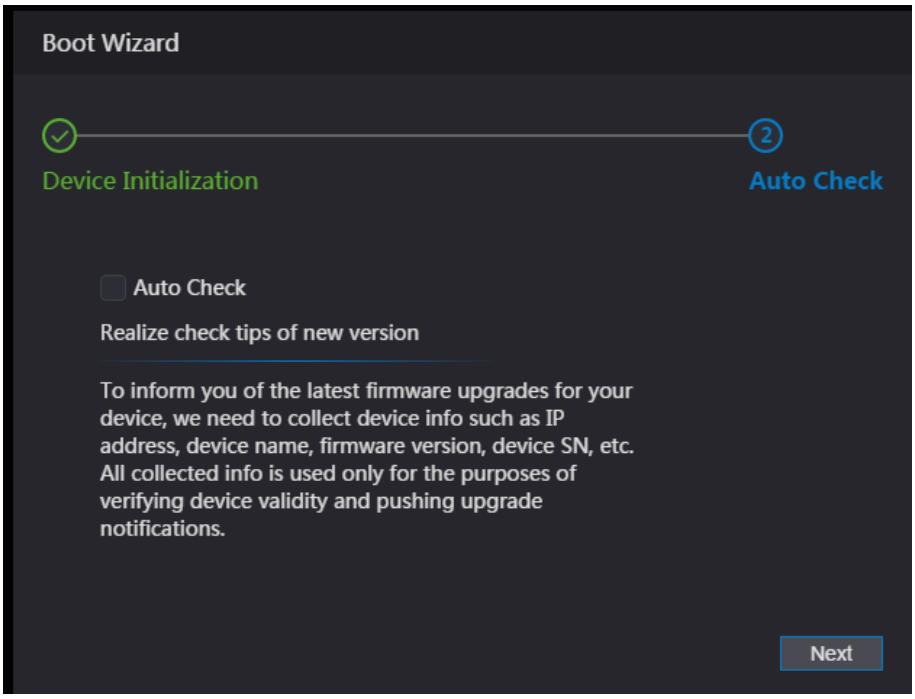


Paso2 Ingrese la nueva contraseña, confirme la contraseña, ingrese una dirección de correo electrónico y luego haga clic en **próximo**.

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

Paso3 Haga clic en **próximo**.

Figura 3-2 Comprobación automática

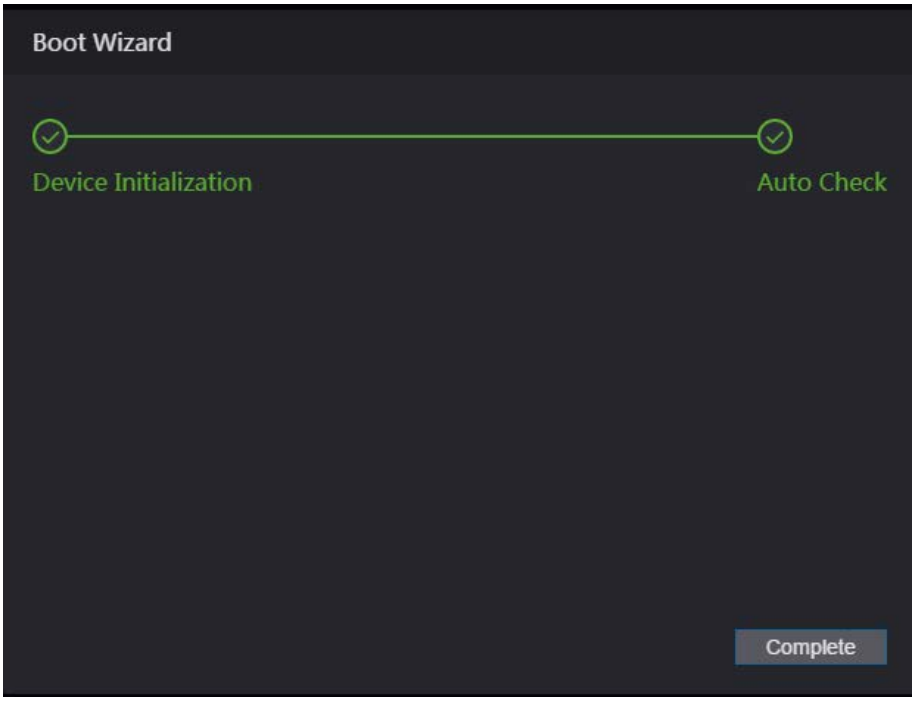


Paso4 Puede decidir si desea seleccionar **Verificación automática** o no.

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

Paso5 Haga clic en **próximo**.

Figura 3-3 Configuración finalizada



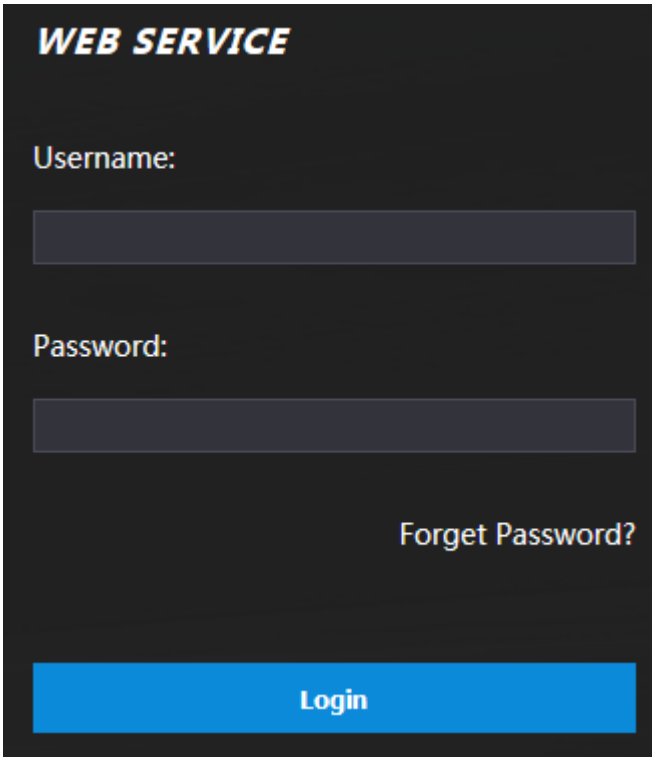
Paso6 Haga clic en **Completo**y se completa la inicialización.

3.2 Iniciar sesión

Paso1 Abra el navegador web IE, introduzca la dirección IP del controlador de acceso en la barra de direcciones y prensa **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 controlador de acceso.
- La dirección IP predeterminada es 192.168.1.108.

Figura 3-4 Inicio de sesión



Paso2 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 controlador de acceso. Cambie la contraseña de administrador con regularidad y consérvela correctamente.
- Si olvida la contraseña de inicio de sesión de administrador, puede hacer clic en **¿Contraseña olvidada?** para restablecerlo. Consulte "3.3 Restablecimiento de la contraseña".

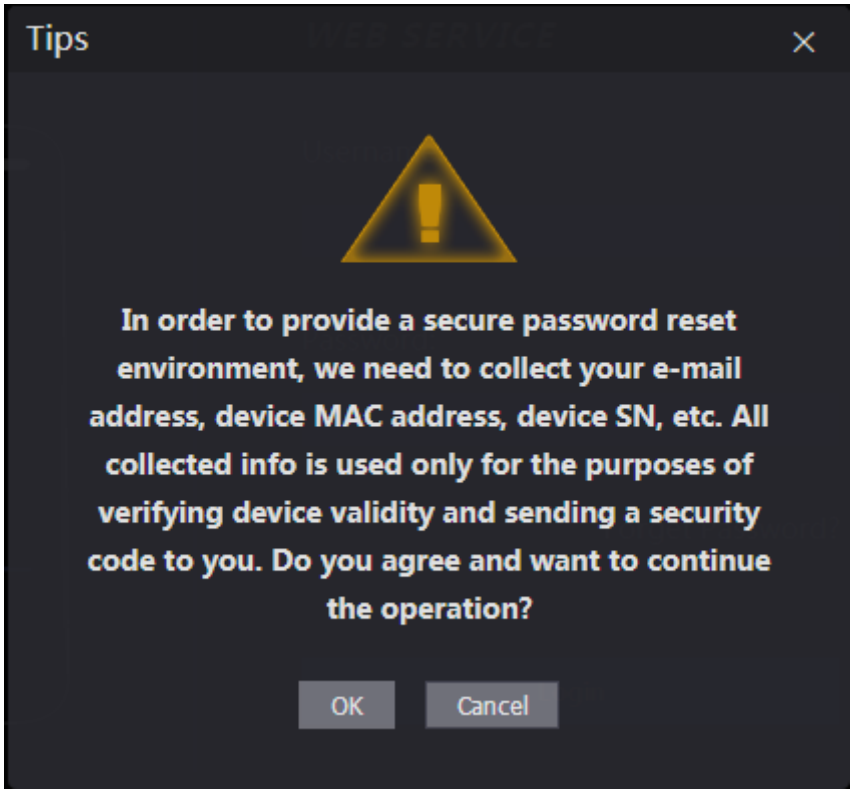
Paso3 Haga clic en **Acceso**.

3.3 Restablecimiento de la contraseña

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

Paso1 clic **¿Se te olvidó tu contraseña?** en la interfaz de inicio de sesión.

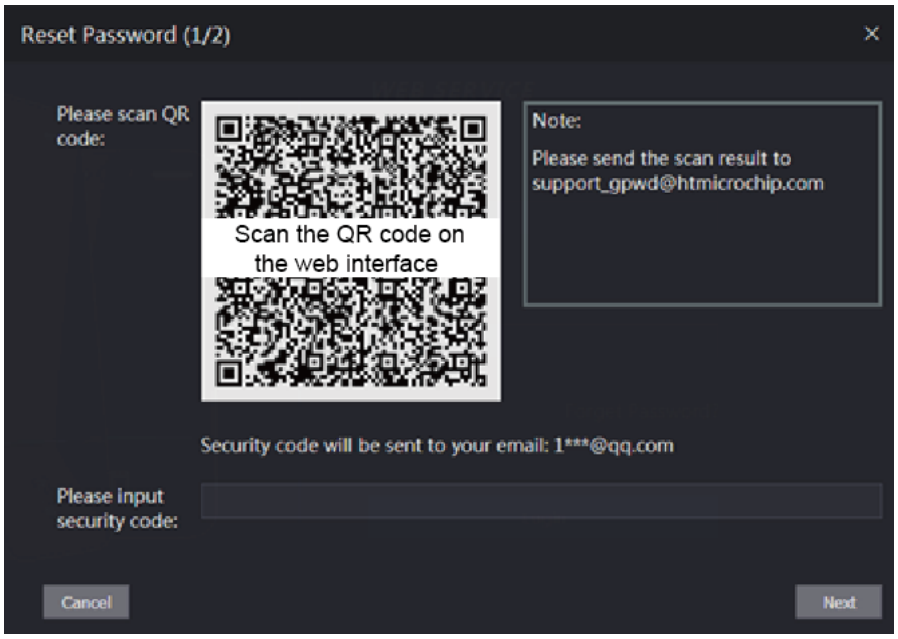
Figura 3-5 Consejos



Paso2 Lea los consejos.

Paso3 Haga clic en **OK**.

Figura 3-6 Restablecer contraseña



Paso4 Escanee el código QR en la interfaz y obtendrá el código de seguridad.

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

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

Paso5 Ingrese el código de seguridad que ha recibido.

Paso6 Haga clic en **próximo**.

Paso7 Restablezca y confirme la nueva contraseña.

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

Paso8 Haga clic en **OK**y se completa el reinicio.

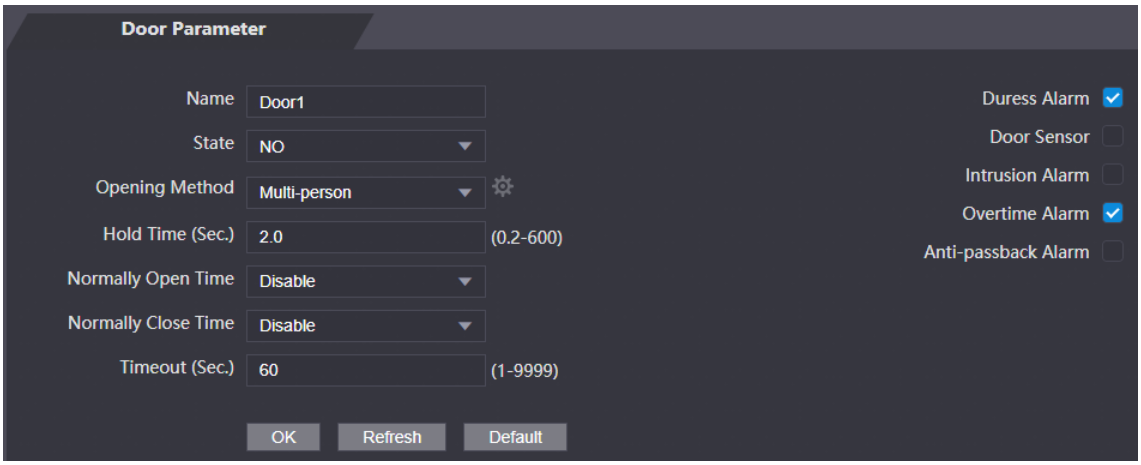
3.4 Parámetro de puerta

Configure los parámetros de control de acceso.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Parámetro de puerta**.

Figura 3-7 Parámetros de la puerta

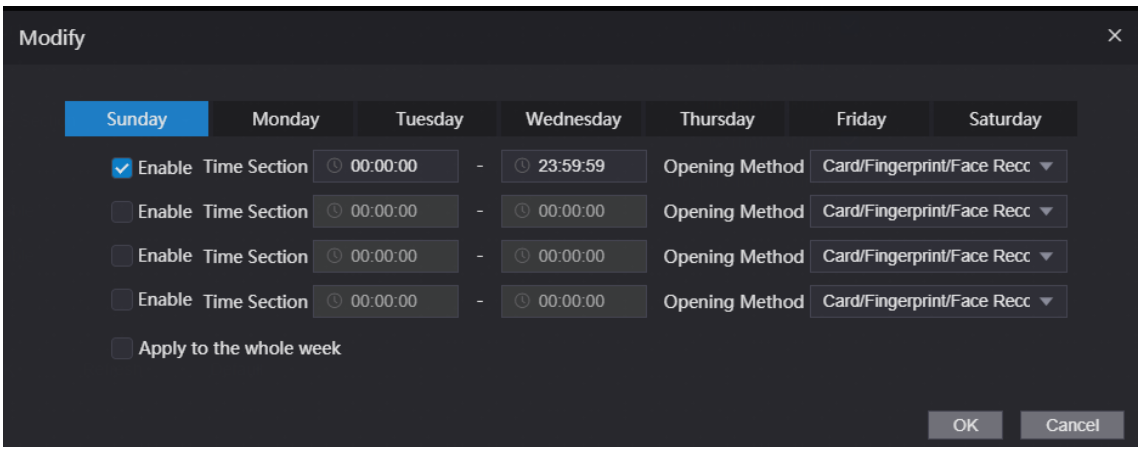


Paso3 Configurar **Método de apertura**.

- Sección de tiempo

  1) Haga clic en.

Figura 3-8 Parámetro de sección de tiempo



2) Configure la hora y el método de apertura para una sección de tiempo. Puede configurar hasta cuatro secciones de tiempo para cada día.

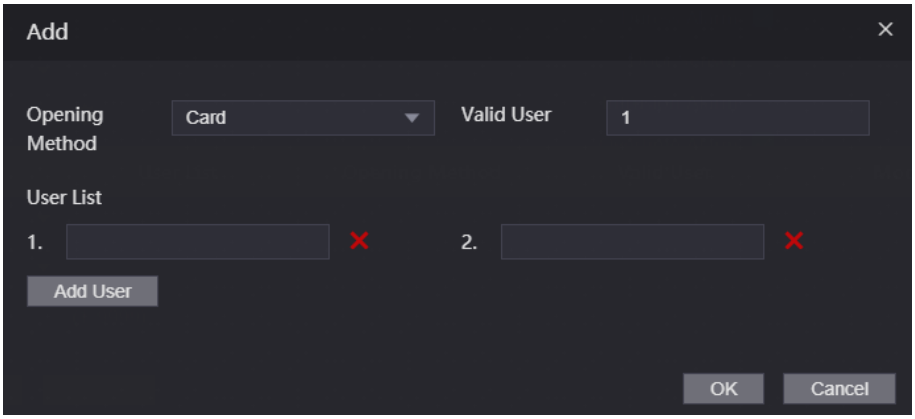
3) (Opcional) Seleccione **Aplicar a toda la semana** para copiar la configuración a otros días.

4) Haga clic en **OK**

- Multi personas

1) Haga clic en y luego haga clic en **Agregar**.

Figura 3-9 Parámetro para varias personas



2) Seleccione un método de apertura e ingrese un número de usuario válido.

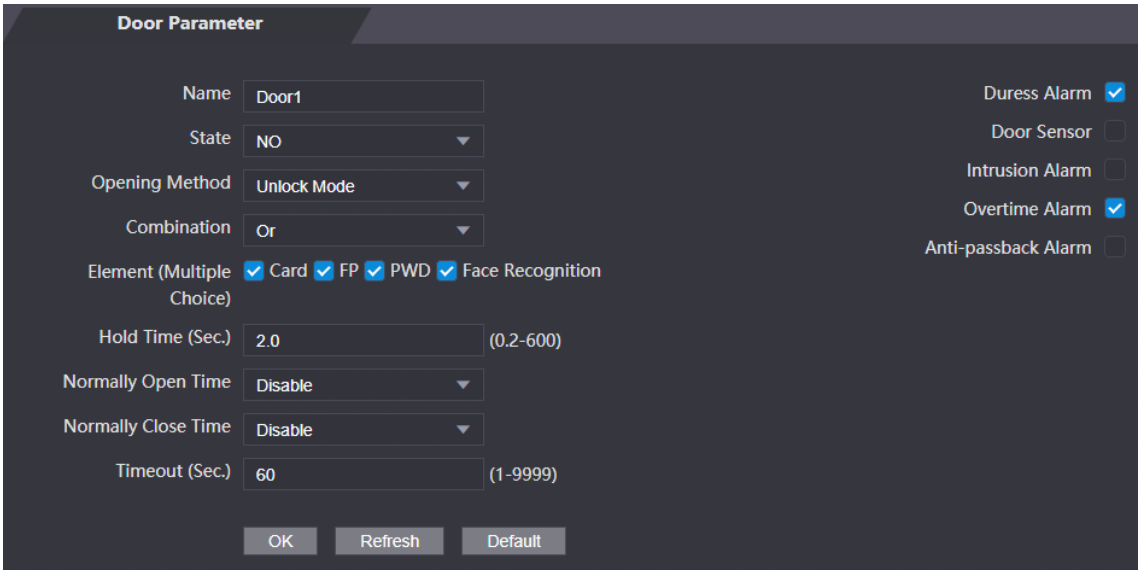
3) En el **Lista de usuarios** sección, ingrese el ID de los usuarios según sea necesario. Para la identificación de usuario, consulte "2.7 Gestión de usuarios".

- No se pueden agregar usuarios VIP, de patrulla y de lista de bloqueo.
- Todos los usuarios de diferentes grupos deben verificar sus identidades en el orden de grupo para desbloquear la puerta.

- Modo de desbloqueo

1) Seleccione los métodos de desbloqueo en **Elemento (opción múltiple)**.

Figura 3-10 Parámetros del modo de desbloqueo



2) Seleccionar **O** o **Y**. **O** significa que debe utilizar todos los métodos definidos para abrir la puerta; **Y** significa que puede abrir la puerta con cualquiera de los métodos definidos.

3) Seleccione los métodos de desbloqueo para **Elemento (opción múltiple)**.

Paso4 Configure otros parámetros.

Tabla 3-1 Descripción de los parámetros

Parámetro	Descripción
Nombre	Ingrese un nombre para la puerta que controla este controlador de acceso.
Estado	Seleccione **CAROLINA DEL NORTE** para normalmente cerrado, o **NO** para normalmente abierto. Si se selecciona cualquiera, el método de apertura definido no será efectivo.
Método de apertura	Vea el paso 3 anterior.
Tiempo de espera (seg.)	Desbloquea la duración. Si expira, la puerta se bloqueará.
Normalmente abierto Tiempo	La puerta estará siempre abierta o cerrada.
Normalmente cerca Tiempo	
Tiempo de espera (seg.)	Se activará una alarma de tiempo de espera si la puerta permanece desbloqueada durante más tiempo que este valor.
Alarma de coacción	Consulte la Tabla 2-4.
Sensor de puerta	
Alarma de intrusión	
Alarma de horas extras	
Anti-passback Alarma	

Paso5 Haga clic en **OK**.

3.5 Enlace de alarma

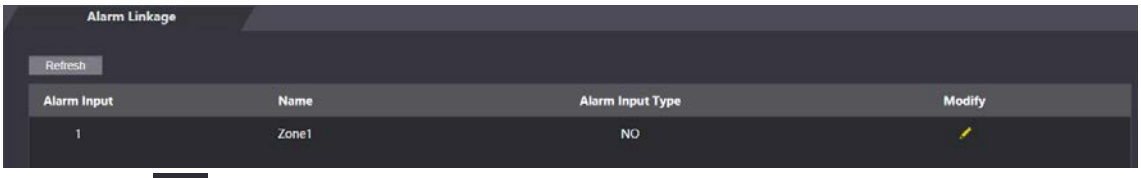
3.5.1 Configuración del enlace de alarma

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

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Enlace de alarma> Enlace de alarma**.

Figura 3-11 Enlace de alarma



Paso3 Haga clic en  para modificar los parámetros de vinculación de alarmas.

Figura 3-12 Cambiar los parámetros de vinculación de alarmas

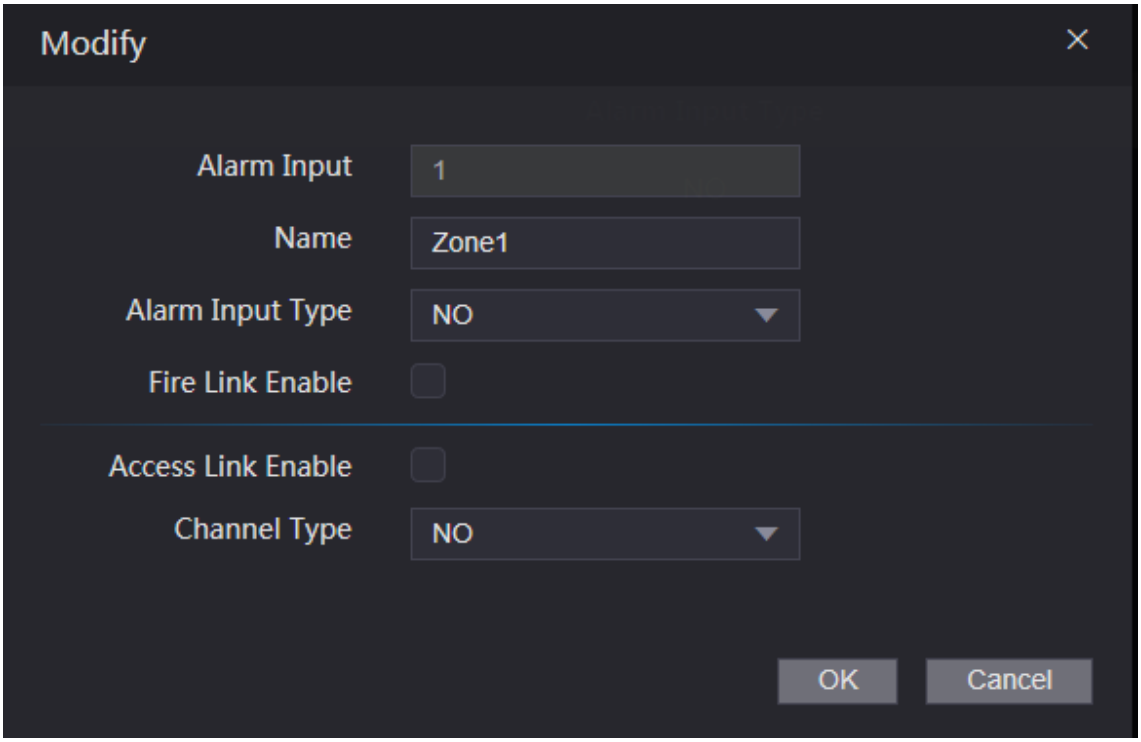


Tabla 3-2 Descripción del parámetro de vinculación de alarmas

Parámetro	Descripción
Entrada de alarma	No puede modificar el valor. Manténgalo predeterminado.
Nombre	Ingrese un nombre de zona.
Tipo de entrada de alarma	Si el tipo de entrada de alarma del dispositivo de alarma que compró es **NO**, entonces debes seleccionar **NO**; de lo contrario, debe seleccionar**CAROLINA DEL NORTE**.
Activar 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 entrada de alarma y el enlace de acceso son NO de forma predeterminada si el enlace de incendio está habilitado.
Activar enlace de acceso	Si está habilitado, 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.

Paso4 Haga clic en **OK**y luego se completa la configuración.

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

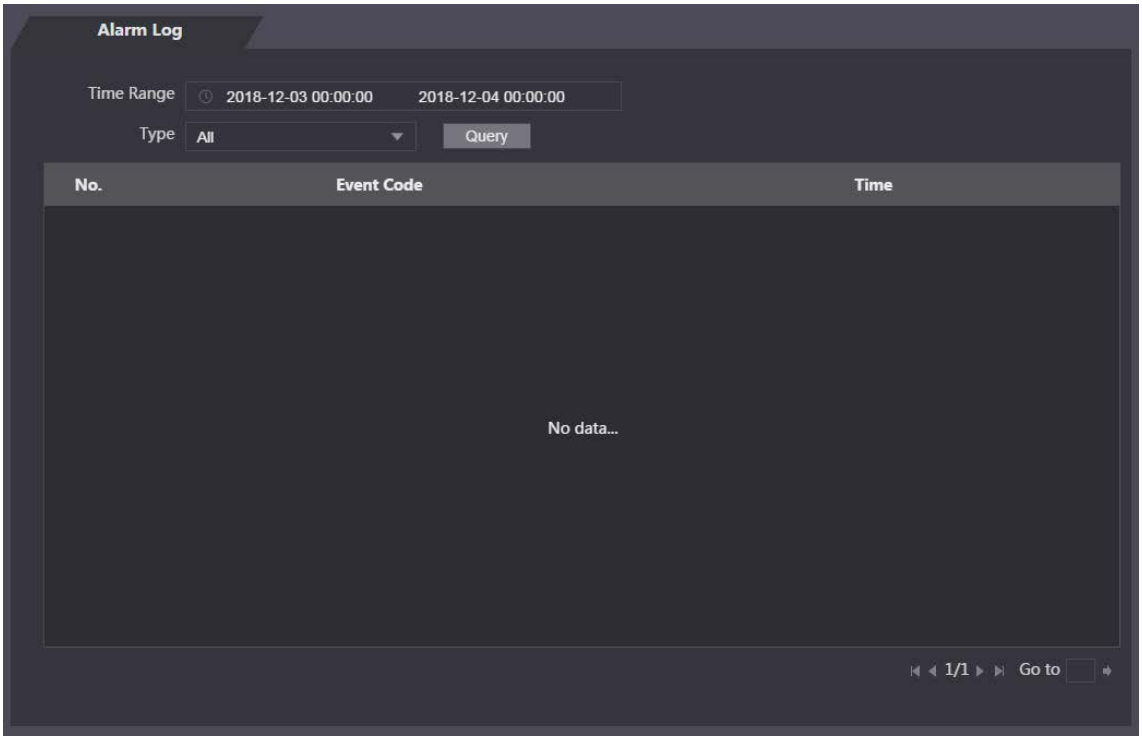
3.5.2 Registro de alarmas

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

Paso1 Inicie sesión en la interfaz web.

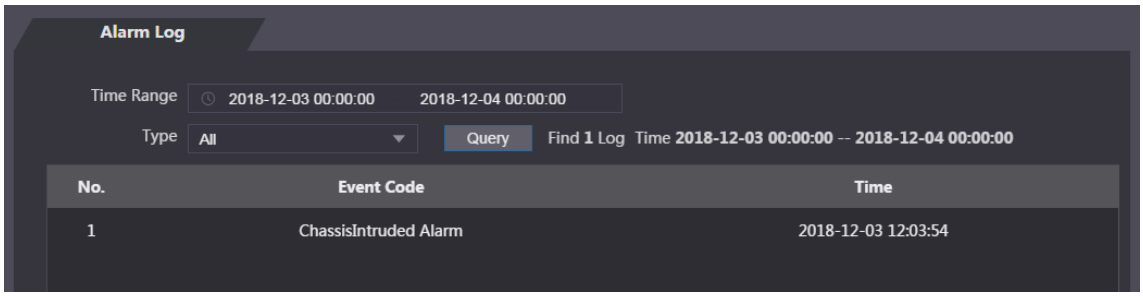
Paso2 Seleccione **Enlace de alarmas> Registro de alarmas**.

Figura 3-13 Registro de alarmas



Paso3 Seleccione un rango de tiempo y un tipo de alarma y luego haga clic en **Consulta**. Se muestran los resultados de la consulta.

Figura 3-14 Resultados de la consulta



3.6 Configuración de Talkback

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

3.6.1 Servidor SIP

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

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

3.6.1.1 Controlador de acceso como servidor SIP

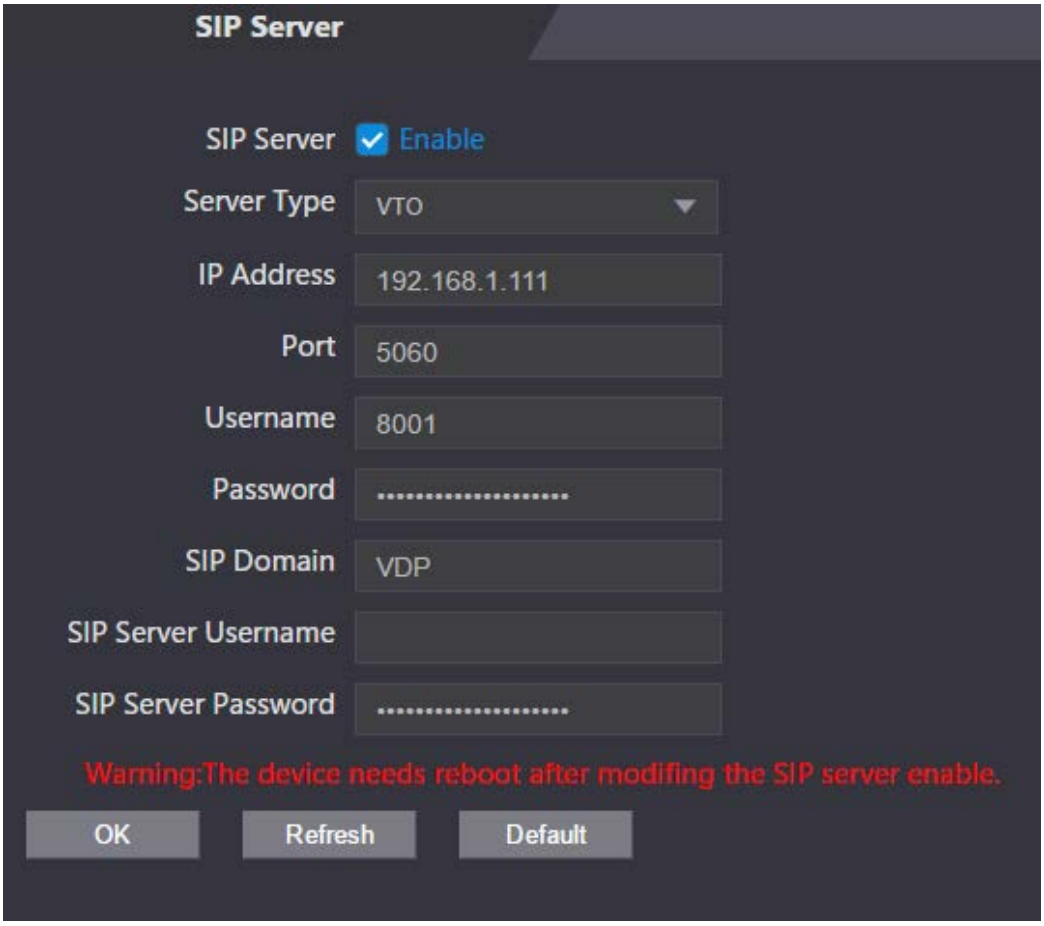
Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de Talkback> Servidor SIP**.

Paso3 Habilitar **Servidor SIP**y luego haga clic en **OK**. El

controlador de acceso se reiniciará.

Figura 3-15 Servidor SIP (1)



3.6.1.2 Otro dispositivo como servidor SIP

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de Talkback> Servidor SIP**.

Paso3 Desactivar **Servicio SIP**, y luego establezca **Tipo de servidor** para **VTO**.

Paso4 Configure los parámetros

Figura 3-16 Servidor SIP (2)

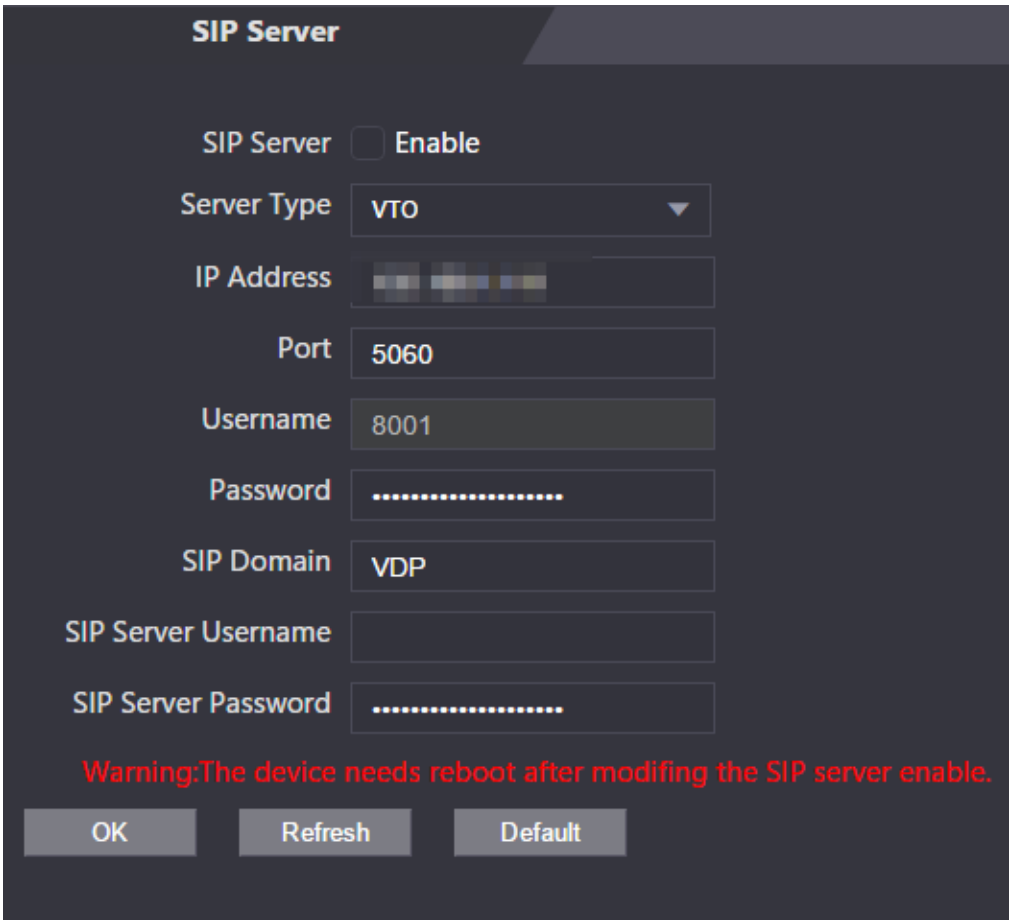


Tabla 3-3 Descripción de los parámetros del servidor SIP (1)

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

Paso5 Haga clic en **OK**.

3.6.2 Configuración local

Configure el tipo y número de dispositivo.

3.6.2.1 Controlador de acceso como servidor SIP

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de Talkback> Local**.

Paso3 Configure los parámetros.

Figura 3-17 Local (1)

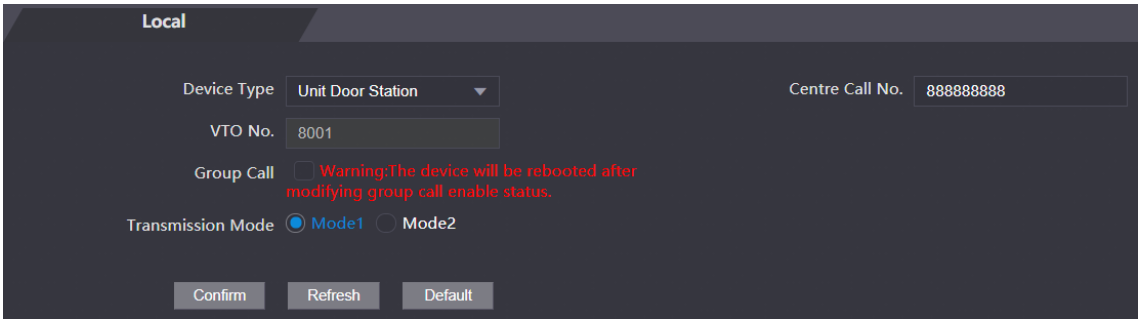


Tabla 3-4 Descripción de los parámetros

Parámetro	Descripción
Tipo de dispositivo	El controlador de acceso solo puede funcionar como una unidad VTO.
Número de llamada del centro	Ingrese un número para el centro de gestión. Puede contener hasta nueve dígitos. No se puede
VTO No.	configurar cuando el controlador de acceso funciona como servidor SIP. Cuando está habilitado, todos
Llamada grupal	los VTH secundarios también recibirán la llamada cuando el controlador de acceso esté llamando a un VTH principal. Esta función solo está disponible cuando el controlador de acceso funciona como servidor SIP.
Transmisión Modo	- Mode1: Llamada en tiempo real, pero el video y el sonido pueden estar retrasados con una red deficiente. - Mode2: No es una llamada en tiempo real, pero garantiza un video y sonido fluidos.

Paso4 Haga clic en **Confirmar**.

3.6.2.2 Otro dispositivo como servidor SIP

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de Talkback> Local**.

Paso3 Configure los parámetros.

Figura 3-18 Local (2)

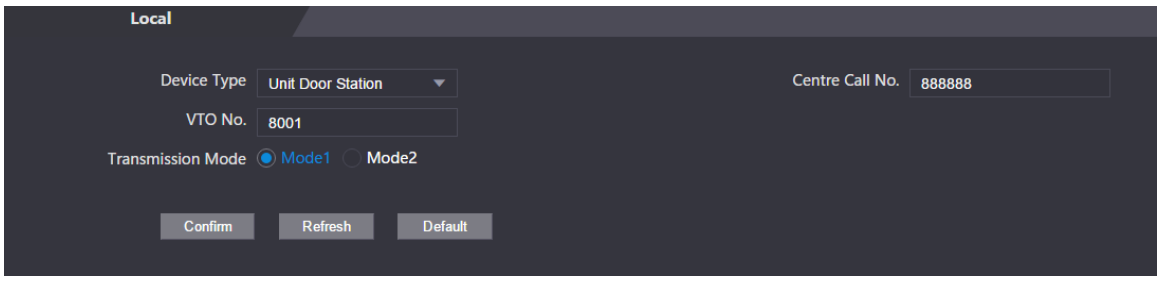


Tabla 3-5 Descripción de los parámetros

Parámetro	Descripción
Tipo de dispositivo	El controlador de acceso puede funcionar como una estación de puerta de la unidad o una
Número de llamada del centro	estación de cerca. Ingrese un número para el centro de gestión. Puede contener hasta nueve dígitos.
VTO No.	Establezca un número. - Debe tener cuatro dígitos. Los dos primeros deben ser 80 y el último

Parámetro	Descripción
	dos comienza con 01, como 8001. - Si hay varios VTO, sus números de VTO no pueden ser los mismos.
Modo de transmisión	- **Mode1**: Llamada en tiempo real, pero el vídeo y el sonido pueden retrasarse con una red deficiente. - **Mode2**: No es una llamada en tiempo real, pero garantiza un video y un sonido fluidos.

3.6.3 Gestión de números VTO

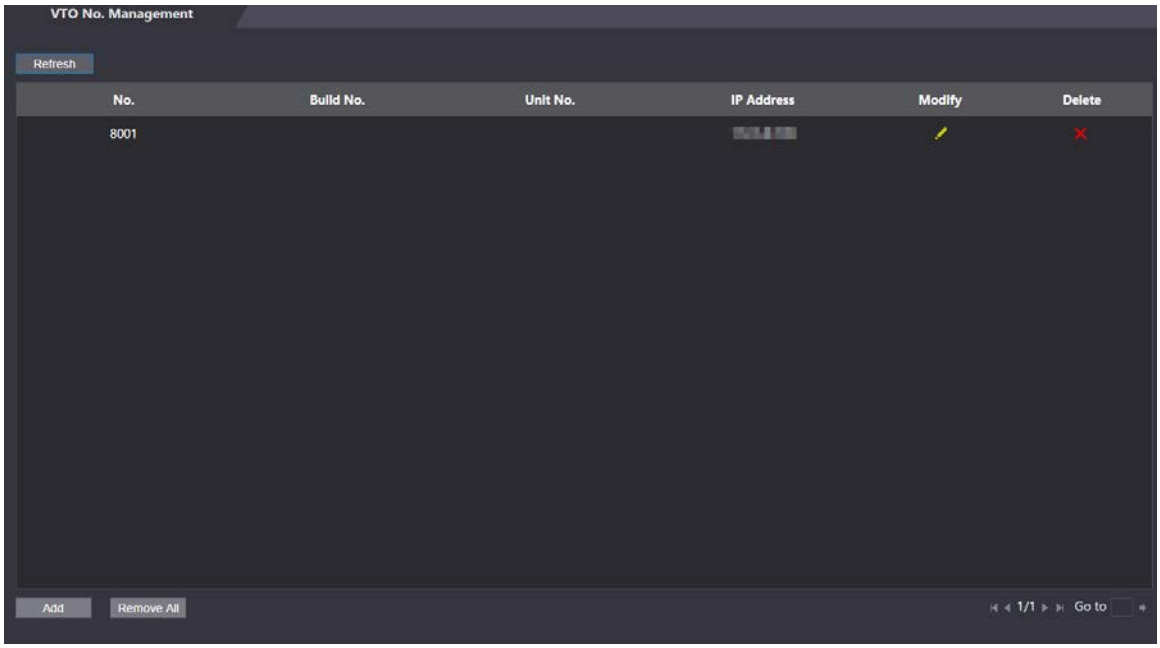
Cuando el controlador de acceso funciona como servidor SIP, agregue otros VTO para llamarlos.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de Talkback> Gestión de números de VTO**.

Paso3 Haga clic en **Agregar**.

Figura 3-19 Gestión del número de VTO



Paso4 Configure los parámetros.

Figura 3-20 Agregar una estación de puerta

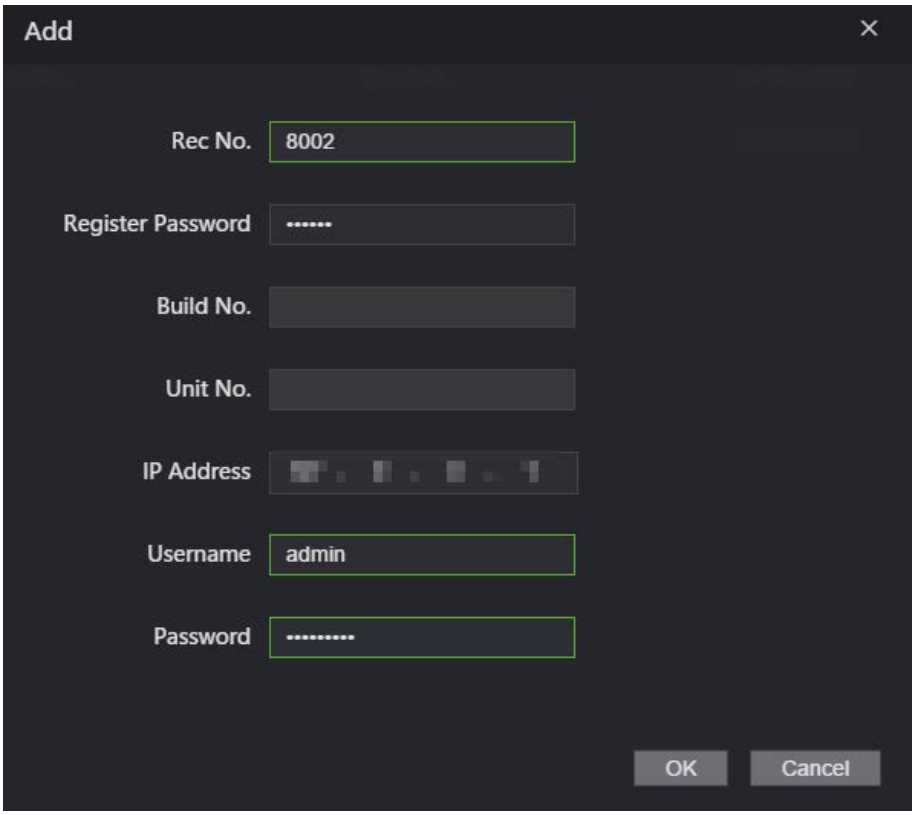


Tabla 3-6 Descripción de los parámetros

Parámetro	Descripción
Rec No.	Ingrese un número para el VTO que desea agregar.
Registrar contraseña	Manténgalo predeterminado.
Construir No.	No se puede configurar.
Numero de unidad.	
Dirección IP	Dirección IP del VTO que desea agregar.
Nombre de usuario	Nombre de usuario de inicio de sesión de la interfaz web y contraseña del VTO que desea agregar.
Contraseña	

Paso5 Haga clic en **OK**.

3.6.4 Gestión de números VTH

Cuando el controlador de acceso funciona como servidor SIP, agregue VTH para llamarlos.

Cuando hay VTH principales y secundarios, primero debe habilitar la función de llamada de grupo antes de agregarlos. Consulte "3.6.2.1 Controlador de acceso como servidor SIP".

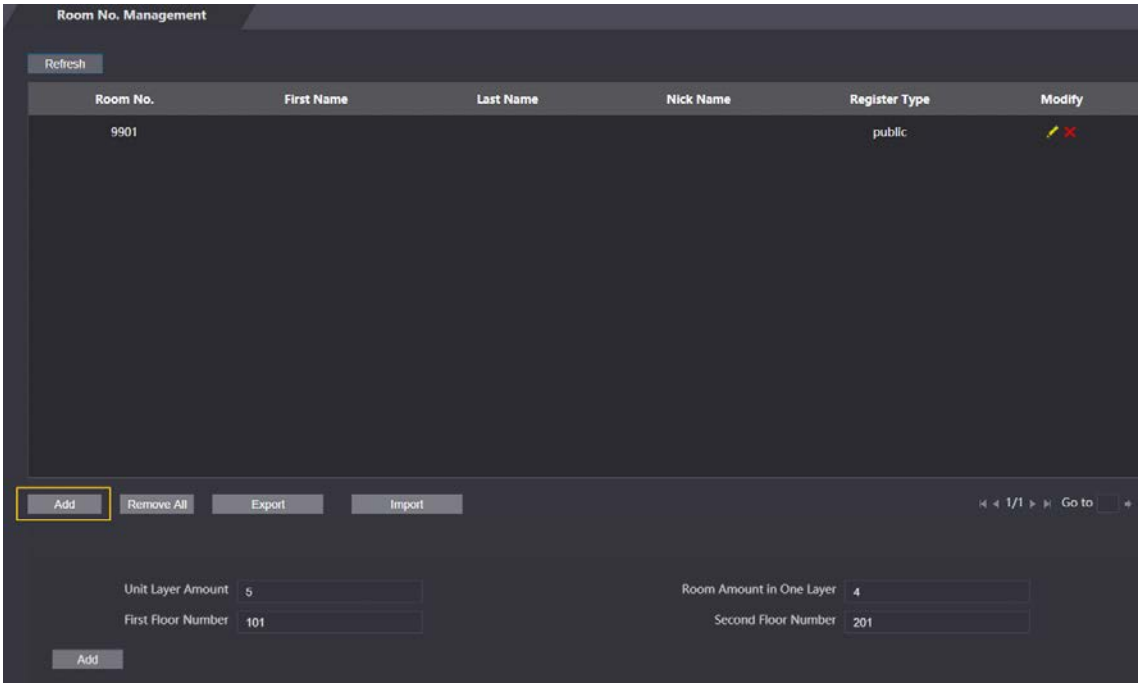
3.6.4.1 Agregar VTHs uno por uno

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de Talkback> Gestión de número de habitación**.

Paso3 Haga clic en **Agregar**.

Figura 3-21 Gestión de número de habitación



Paso4 Ingrese la información.

Figura 3-22 Agregue un VTH

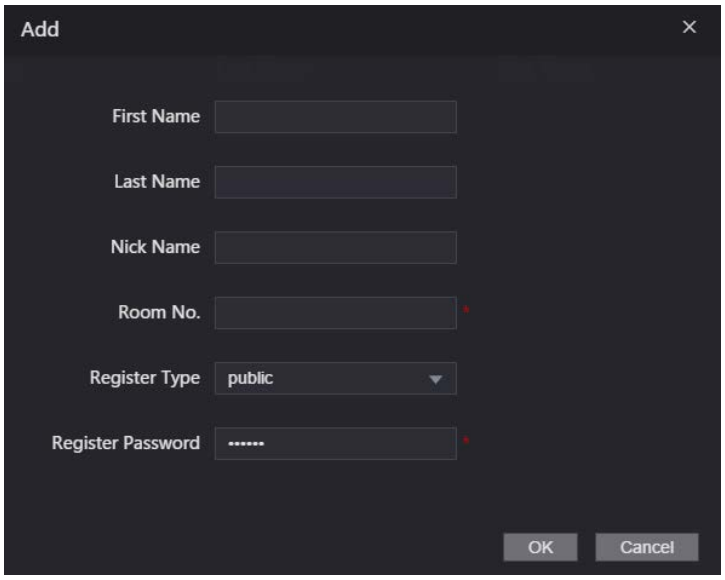


Tabla 3-7 Descripción de los parámetros

Parámetro	Descripción
Primer nombre	Diferenciarse de otros rVTHs.
Apellido	
Apodo	
Habitación no.	Número de habitación del VTH. - Puede contener hasta cinco dígitos y debe ser el mismo que el configurado en el monitor interior. - Cuando hay VTH principales y secundarios, el número de habitación del VTH principal debe terminar con "-0", y el de los VTH secundarios con "-1", "-2", "-3" ... Por ejemplo, el VTH principal es 101-0, los sub VTH son 101-1, 101-2 y 101-3.

Parámetro	Descripción
Tipo de registro	Manténgalo predeterminado.
Registrarse	
Contraseña	

Paso5 Haga clic en **OK**.

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

3.6.4.2 Agregar VTH en lotes

Puede agregar hasta 1024 VTH.

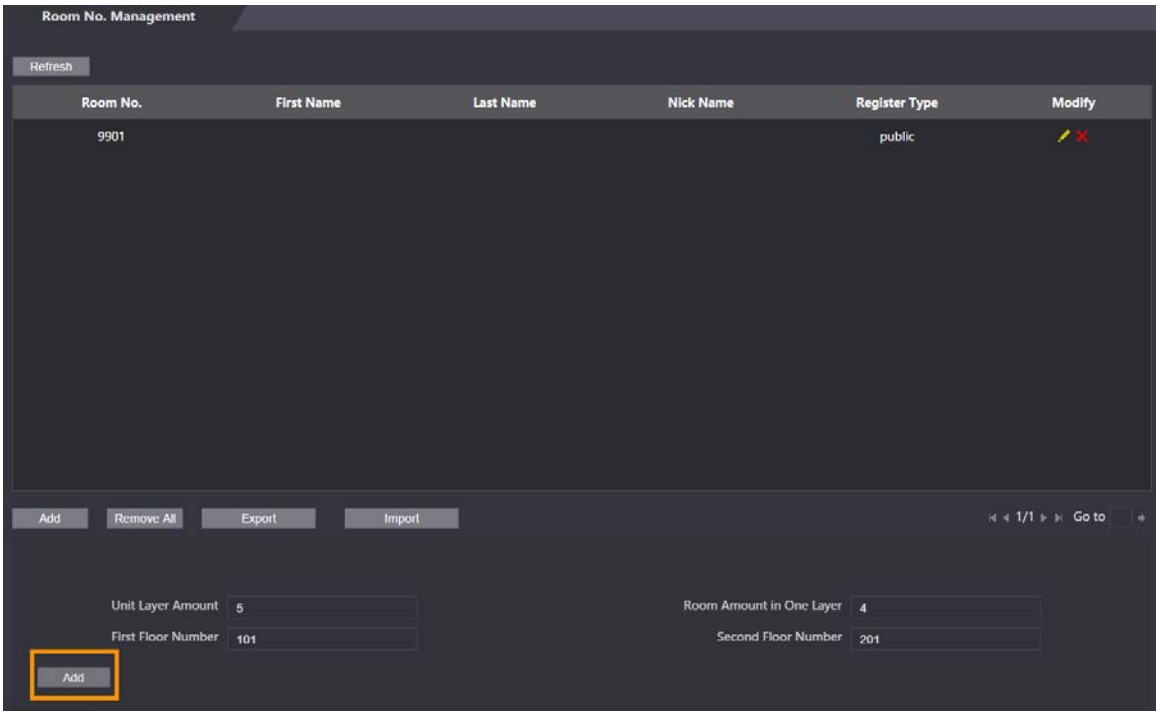
Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de Talkback> Gestión de número de habitación**.

Paso3 Configurar **Cantidad de capa unitaria**, **Cantidad de habitación en una capa**, **Número del primer piso** y **Número del segundo piso**.

Paso4 Haga clic en **Agregar**.

Figura 3-23 Agregar monitores de interior en lotes



3.6.5 Gestión de VTS

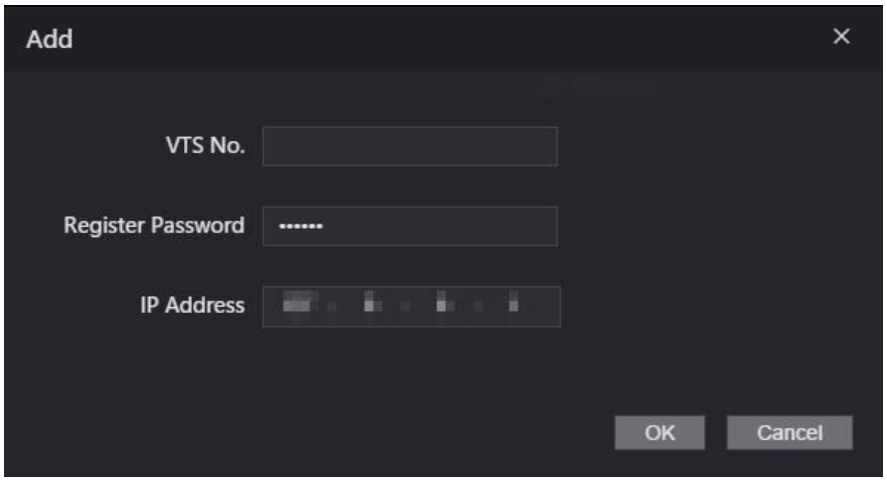
Cuando el controlador de acceso funciona como servidor SIP, agregue estaciones maestras (VTS) para llamarlos.

Paso1 Inicie sesión en la web.

Paso2 Seleccione **Configuración de Talkback> Administración de VTS**.

Paso3 Haga clic en **Agregar**.

Figura 3-24 Agregar dispositivos de administración



Paso4 Ingrese la información.

- **VTS No.**: Puede contener hasta nueve dígitos.
- **Registrar contraseña**: Manténgalo predeterminado.
- **Dirección IP**: Dirección IP del VTS.

Paso5 Haga clic en **OK**.

Operaciones relacionadas

- : Modifica la información de un VTS.
- : Elimina un VTS.

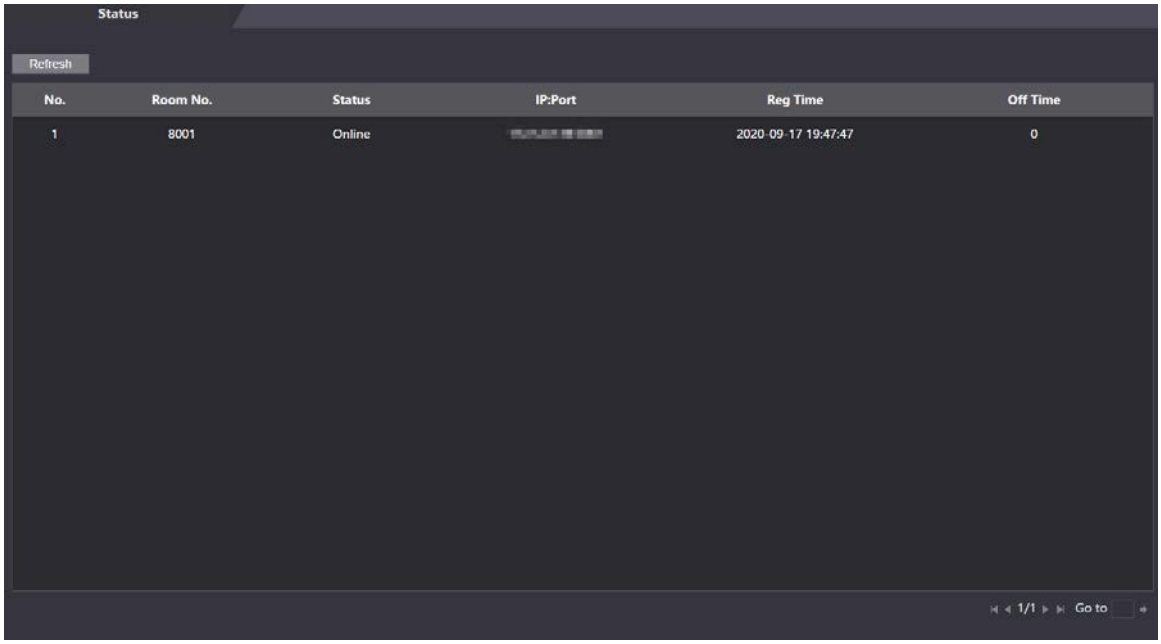
3.6.6 Estado en línea

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

Paso1 Inicie sesión en la web.

Paso2 Seleccione **Configuración de Talkback> Estado**.

Figura 3-25 Estado



3.6.7 Registros de llamadas

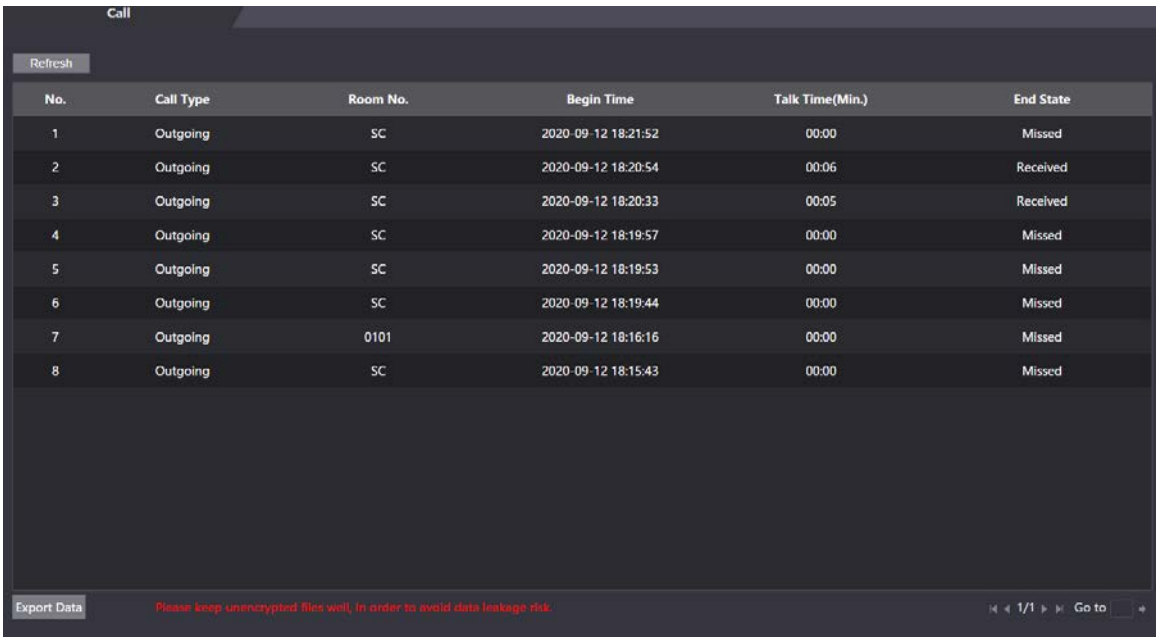
Puede consultar hasta 1024 registros de llamadas.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de Talkback> Llamada**.

Paso3 (Opcional) Haga clic en **Exportar datos** para exportar todos los registros.

Figura 3-26 Registros de llamadas



3.7 Sección de tiempo

Configure secciones de tiempo y planes de vacaciones, y luego puede definir cuándo un usuario tiene los permisos para desbloquear puertas.

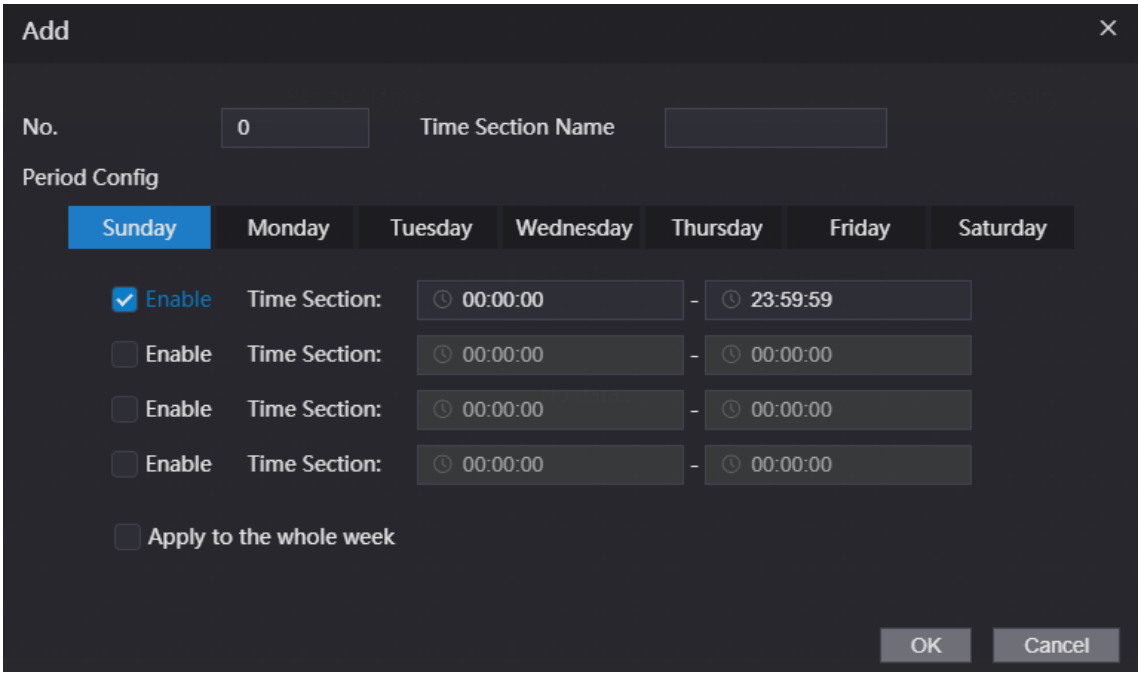
3.7.1 Configuración de la sección de tiempo

Establecer cuándo un usuario puede desbloquear puertas todos los días.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Sección de tiempo> Sección de tiempo**.

Figura 3-27 Parámetros de la sección de tiempo



Paso3 Ingrese un número y un nombre para la sección de tiempo.

Paso4 Configure períodos para cada día. Puede configurar hasta cuatro períodos.

Paso5 (Opcional) Haga clic en **Aplicar a toda la semana** para copiar la configuración a otros días.

Paso6 Haga clic en **OK**.

3.7.2 Configurar grupo de vacaciones

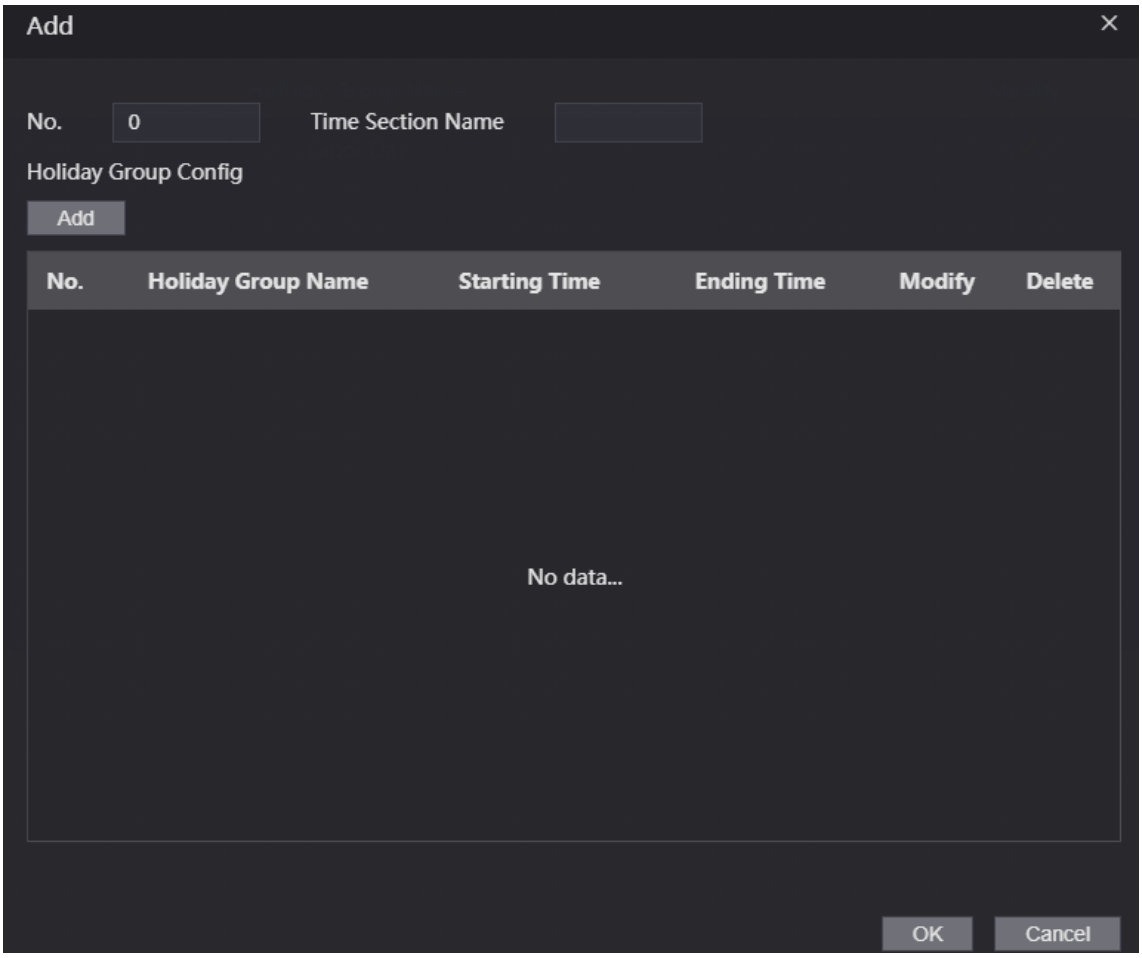
Antes de configurar un plan de vacaciones, debe configurar grupos de vacaciones.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Sección de tiempo> Configuración de grupo de vacaciones**.

Paso3 Haga clic en **Agregar**.

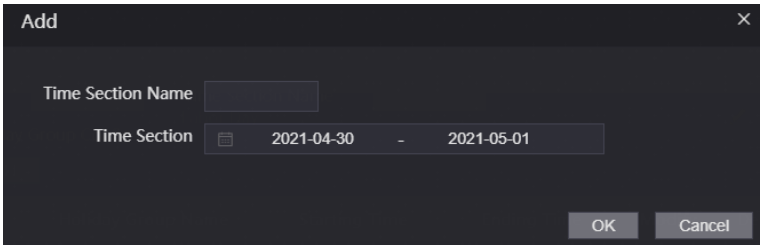
Figura 3-28 Agregar un grupo de vacaciones



Paso4 Introduzca un número y un nombre para el grupo de vacaciones.

Paso5 Haga clic en **Agregar**.

Figura 3-29 Agregar un feriado



Paso6 Ingrese un nombre para las vacaciones, seleccione la fecha de inicio y finalización y luego haga clic en **OK**.

Puede agregar varios días festivos para un grupo de días festivos.

Paso7 Haga clic en **OK**.

3.7.3 Configuración de grupo de vacaciones

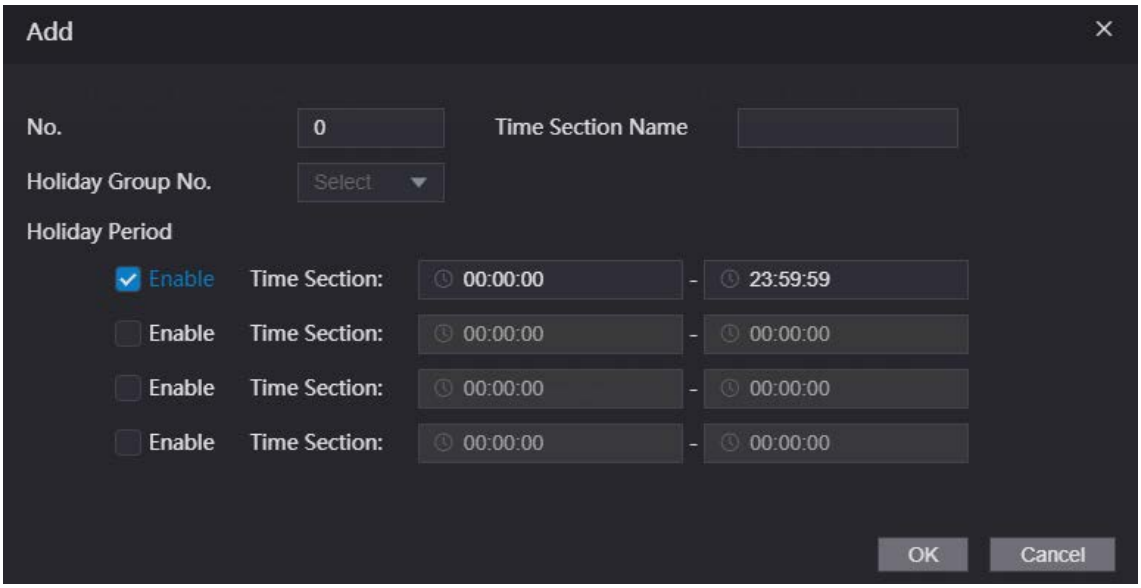
Establece un plan de vacaciones. Al agregar un usuario en el controlador de acceso, puede seleccionar el plan de vacaciones, y luego el usuario solo puede abrir las puertas dentro de los días definidos en el plan de vacaciones.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Sección de tiempo> Configuración del plan de vacaciones**.

Paso3 Haga clic en **Agregar**.

Figura 3-30 Agregar un plan de vacaciones



Paso4 Introduzca un número y un nombre para el plan de vacaciones.

Paso5 Seleccione el número de un grupo de vacaciones que configuró.

Seleccione **255** si no desea seleccionar un grupo de vacaciones.

Paso6 Configure períodos para todos los días del grupo de vacaciones que seleccionó. Puede configurar hasta cuatro periodos.

Paso7 Haga clic en **OK**.

3.8 Capacidad de datos

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

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Capacidad de datos** en la barra de navegación.

3.9 Configuración de video

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.

3.9.1 Velocidad de datos

Puede configurar los parámetros de transmisión para el canal 1.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de video> Configuración de video> Velocidad de datos**.

Figura 3-31 Velocidad de datos

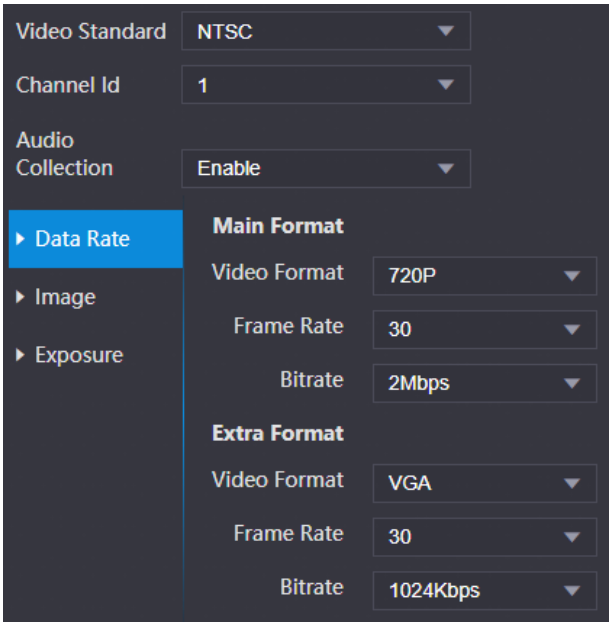


Tabla 3-8 Descripción de los parámetros del flujo

Parámetro		Descripción
Estándar de video		Seleccione **NTSC** o **CAMARADA** de acuerdo con el estándar de video de su región.
Canal		Hay dos opciones: 1 y 2. 1 es una cámara de luz blanca y 2 es una cámara de luz IR.
Colección de audio		Si está habilitado, otros dispositivos también recibirán la transmisión de audio cuando extraigan la transmisión de video del controlador de acceso.
Principal Formato	Formato de video	Seleccione **D1**, **VGA**, **720p** o **1080p** opción de acuerdo con la calidad de video que desee.
	Cuadros por segundo	La velocidad a la que aparecen fotogramas consecutivos en una pantalla. El rango de velocidad de fotogramas es de 1 a 30 fps.
	Tasa de bits	El número de bits que se transportan o procesan por unidad de tiempo. Hay cinco opciones: 2 Mbps, 4 Mbps, 6 Mbps, 8 Mbps y 10
Extra Formato	Formato de video	Mbps. Hay tres opciones: D1, VGA y QVGA.
	Cuadros por segundo	La velocidad a la que aparecen fotogramas consecutivos en una pantalla. El rango de velocidad de fotogramas es de 1 a 30 fps.
	Tasa de bits	El número de bits que se transportan o procesan por unidad de tiempo. Hay opciones: 512 Kbps, 640 Kbps, 768 Kbps, 896 Kbps, 1024 Kbps, 1,25 Mbps, 1,5 Mbps, 1,75 Mbps y 2 Mbps.

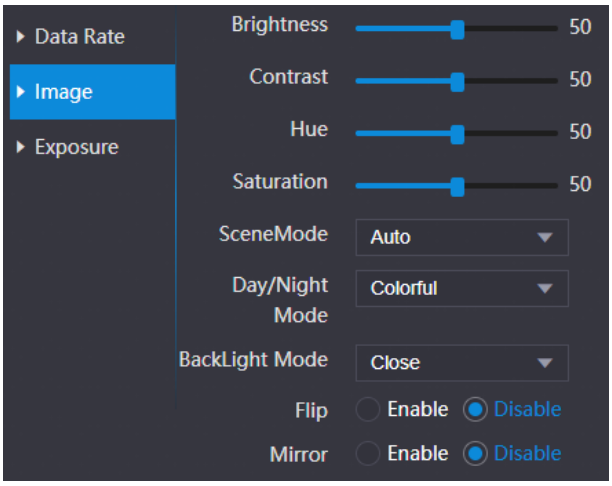
3.9.2 Imagen

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

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de video> Configuración de video> Imagen**.

Figura 3-32 Imagen



Paso3 Seleccione **Amplia dinámica** en el **Modo de luz de fondo**.

Tabla 3-9 Descripción de los parámetros de la imagen

Parámetro	Descripción
Brillo	Cuanto mayor sea el valor, más brillantes serán las imágenes.
Contraste	El contraste es la diferencia de luminancia o color que hace que un objeto sea distinguible. Cuanto mayor sea el valor de contraste, mayor será el brillo y el contraste de color.
Matiz	Cuanto mayor sea el valor, más profundo será el color.
Saturación	Cuanto mayor sea el valor, más brillantes serán los colores. El valor no cambia el brillo de la imagen.
Modo escena	- Cerrar: Sin modos. - Automático: el sistema ajusta automáticamente los modos de escena. - Soleado: en este modo, se reducirá el tono de la imagen. Noche: en - este modo, aumentará el tono de la imagen. **Soleado** está seleccionado de forma predeterminada.
Modo día / noche	El modo día / noche decide el estado de funcionamiento de la luz de relleno. - Automático: el sistema ajusta automáticamente los modos día / noche. Colorido: - en este modo, las imágenes se muestran con colores. - Blanco y negro: en este modo, las imágenes se muestran en blanco y negro.

Parámetro	Descripción
Modo de luz de fondo	- Cerrar: Sin compensación de contraluz. - BLC: la compensación de luz de fondo corrige las regiones con niveles de luz extremadamente altos o bajos para mantener un nivel de luz normal y utilizable para el objeto enfocado. - WDR: en el modo de rango dinámico amplio, el sistema atenúa las áreas brillantes y compensa las áreas oscuras para asegurar la definición de los objetos en las áreas brillantes y oscuras. Cuando hay rostros humanos en la luz de fondo, debe habilitar WDR. - Inhibición: la compensación de altas luces es necesaria para compensar la sobreexposición de altas luces o fuentes de luz fuertes como focos, faros, luces de porche, etc. para crear una imagen que sea utilizable y no superada por una luz brillante.
Espejo	Cuando la función está habilitada, las imágenes se mostrarán con los lados izquierdo y derecho invertidos.
Voltear	Cuando esta función está habilitada, las imágenes se pueden voltear.

3.9.3 Exposición

Puede configurar los parámetros de exposición.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de video> Configuración de video> Exposición**.

Figura 3-33 Exposición

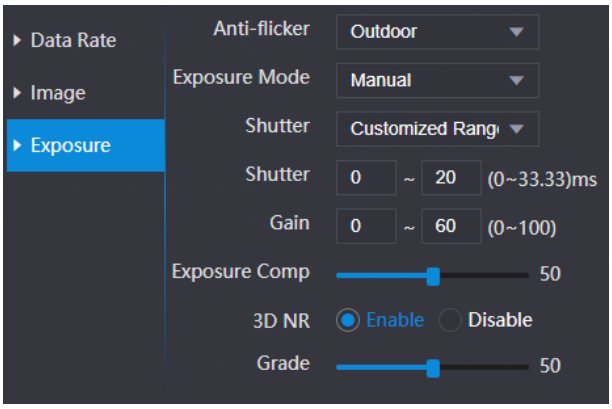


Tabla 3-10 Descripción de los parámetros de exposición

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

Parámetro	Descripción
Exposición Modo	- **Auto**: El controlador de acceso ajustará automáticamente el brillo de las imágenes. - **Prioridad de obturador**: El controlador de acceso ajustará el brillo de la imagen de acuerdo con el rango de valores de exposición del obturador. Si el brillo de la imagen no es suficiente y el valor del obturador ha alcanzado el límite superior o inferior, el 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. - Cuando seleccionas **Exterior** en la lista desplegable Antiparpadeo, puede seleccionar **Prioridad de obturador** como el modo de exposición. - Los modos de exposición que se enumeran a continuación son solo de referencia y pueden variar según los modelos.
Obturador	Si seleccionas **Gama personalizada**, puede personalizar el rango de velocidad del obturador.
	Cuanto menor sea la velocidad del obturador, menor será el tiempo de exposición y más oscuras serán las imágenes.
Ganar	Cuando se establece el rango del valor de ganancia, se mejorará la calidad del video.
Exposición Compensación	Puede aumentar el brillo del video ajustando el valor de compensación de exposición.
3D NR	Cuando la reducción de ruido 3D (RD) está habilitada, se puede reducir el ruido del video y se producirán videos de alta definición.
Calificación	Puede ajustar el valor de 3D NR cuando 3D NR está habilitado. Cuanto mayor sea el valor, menos ruido habrá.

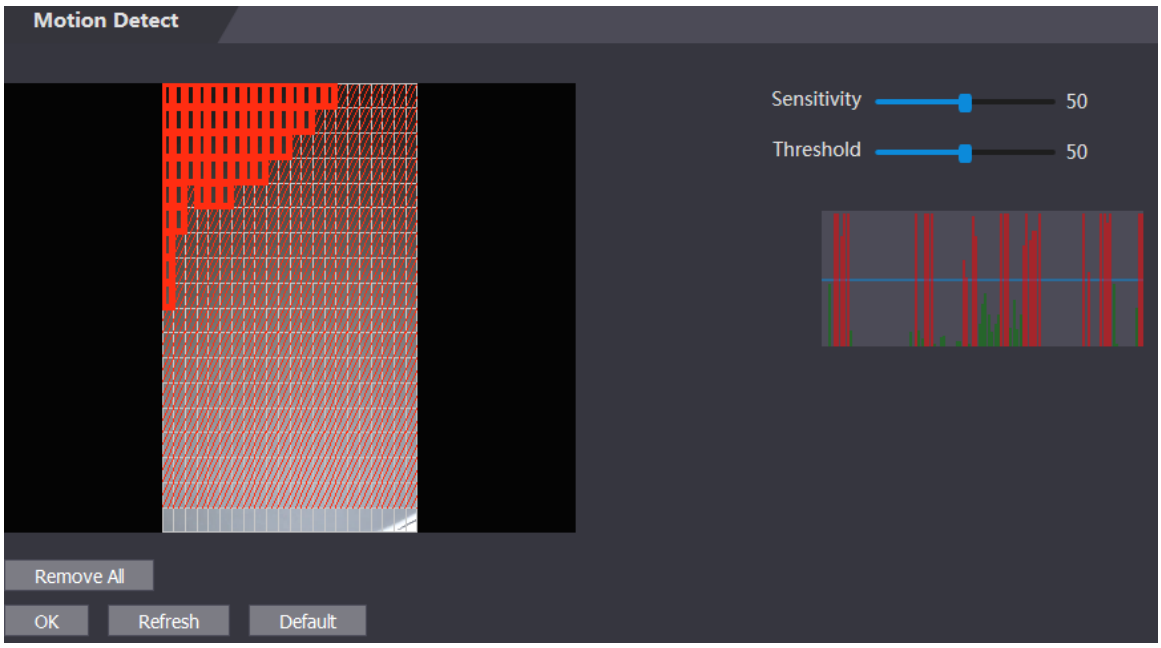
3.9.4 Detección de movimiento

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

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de video> Detección de movimiento**.

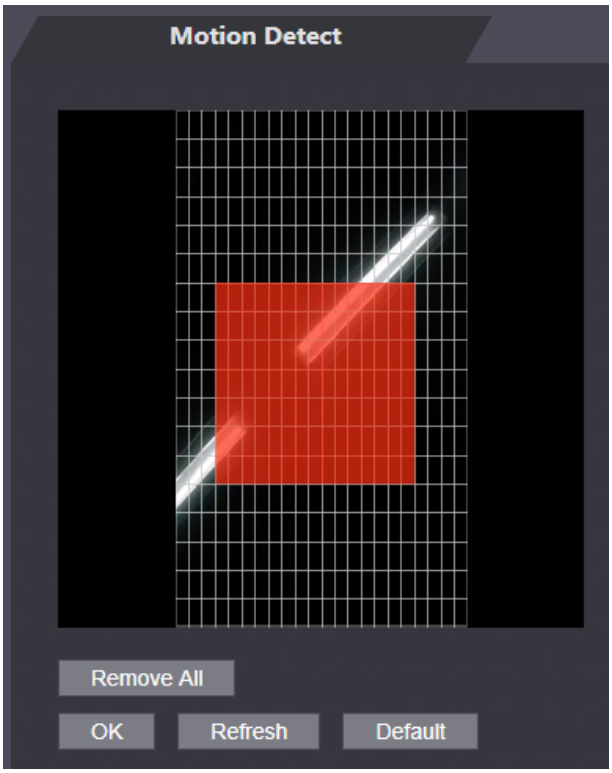
Figura 3-34 Detección de movimiento



Paso3 Mantenga presionado el botón izquierdo del mouse y luego arrastre el mouse en el área roja.

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

Figura 3-35 Área de detección de movimiento



Paso4 Configure la sensibilidad y el umbral.

- La sensibilidad representa la capacidad de cada cuadrícula para detectar el movimiento. Cuanto mayor sea el valor, mayor será la sensibilidad.
- El umbral es la condición de detección de movimiento. Cuando el número de cuadrícula alcanza el umbral, se activará la detección de movimiento. Cuanto menor sea el valor, es más probable que se active la detección de movimiento.
- Cuando el número de cuadrícula es menor que el umbral, aparecerá una línea verde; cuando el número de cuadrícula es mayor que el umbral, aparecerá una línea roja. Vea la Figura 3-34.

Paso5 Haga clic en **OK** para terminar el ajuste.

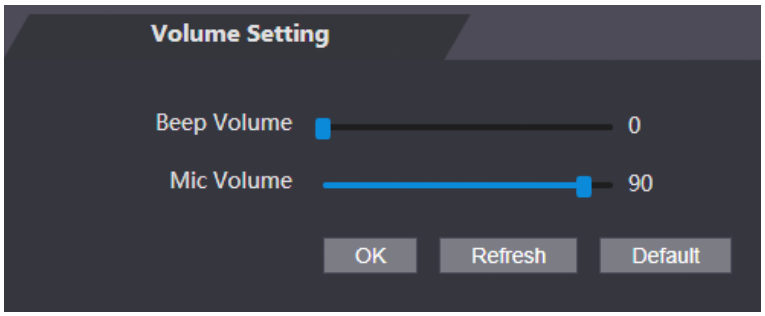
3.9.5 Configuración de volumen

Ajuste el volumen del altavoz o el aviso sonoro.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de video> Configuración de volumen**.

Figura 3-36 Configuración de volumen



3.9.6 Modo de imagen

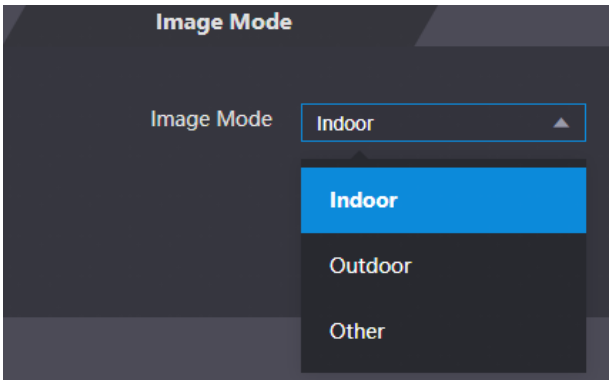
Seleccione interior, exterior u otro según el lugar donde esté instalado el controlador de acceso.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de video> Modo de imagen**.

- **Interior**: El controlador de acceso está instalado en el interior.
- **Exterior**: El controlador de acceso está instalado al aire libre.
- **Otro**: El controlador de acceso se instala en lugares con luz de fondo, como pasillos.

Figura 3-37 Modo de imagen



3.9.7 Codificación local

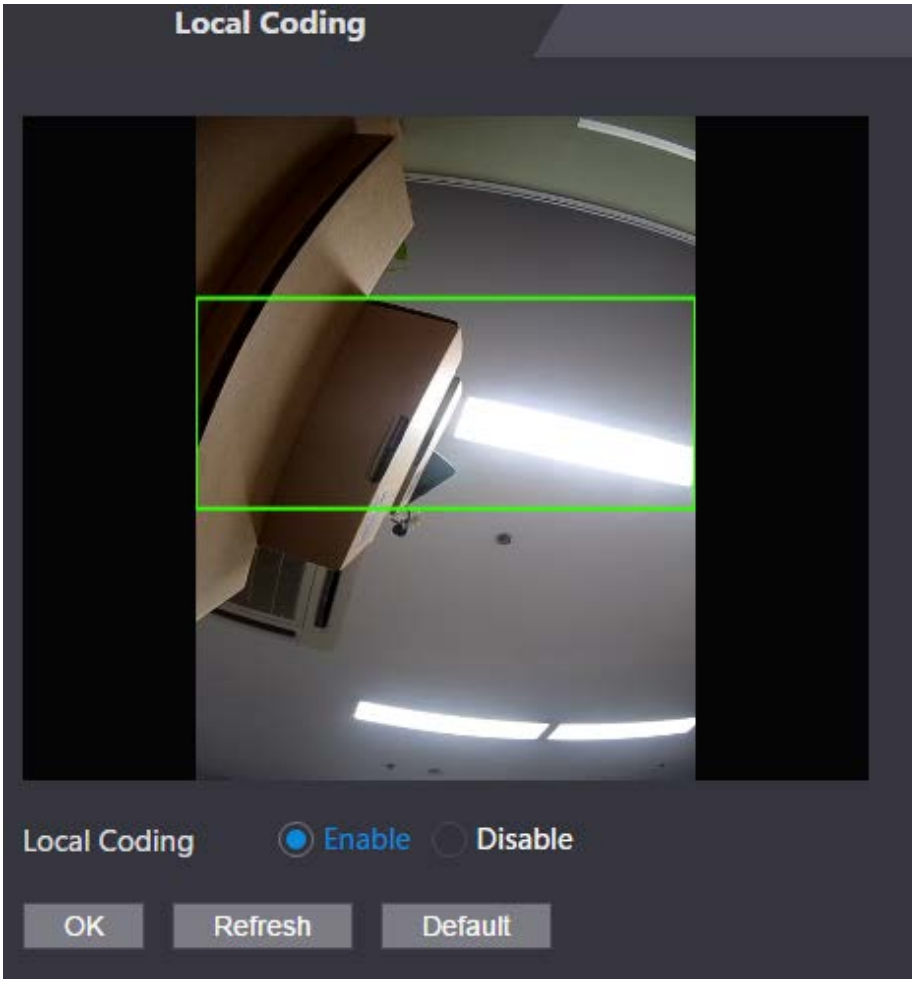
Configure el área que se mostrará en los monitores interiores.

Paso1 Inicie sesión en la web.

Paso2 Seleccione **Configuración de video> Codificación local**.

Paso3 Habilite la función.

Figura 3-38 Codificación local



Paso4 Haga clic en **OK**.

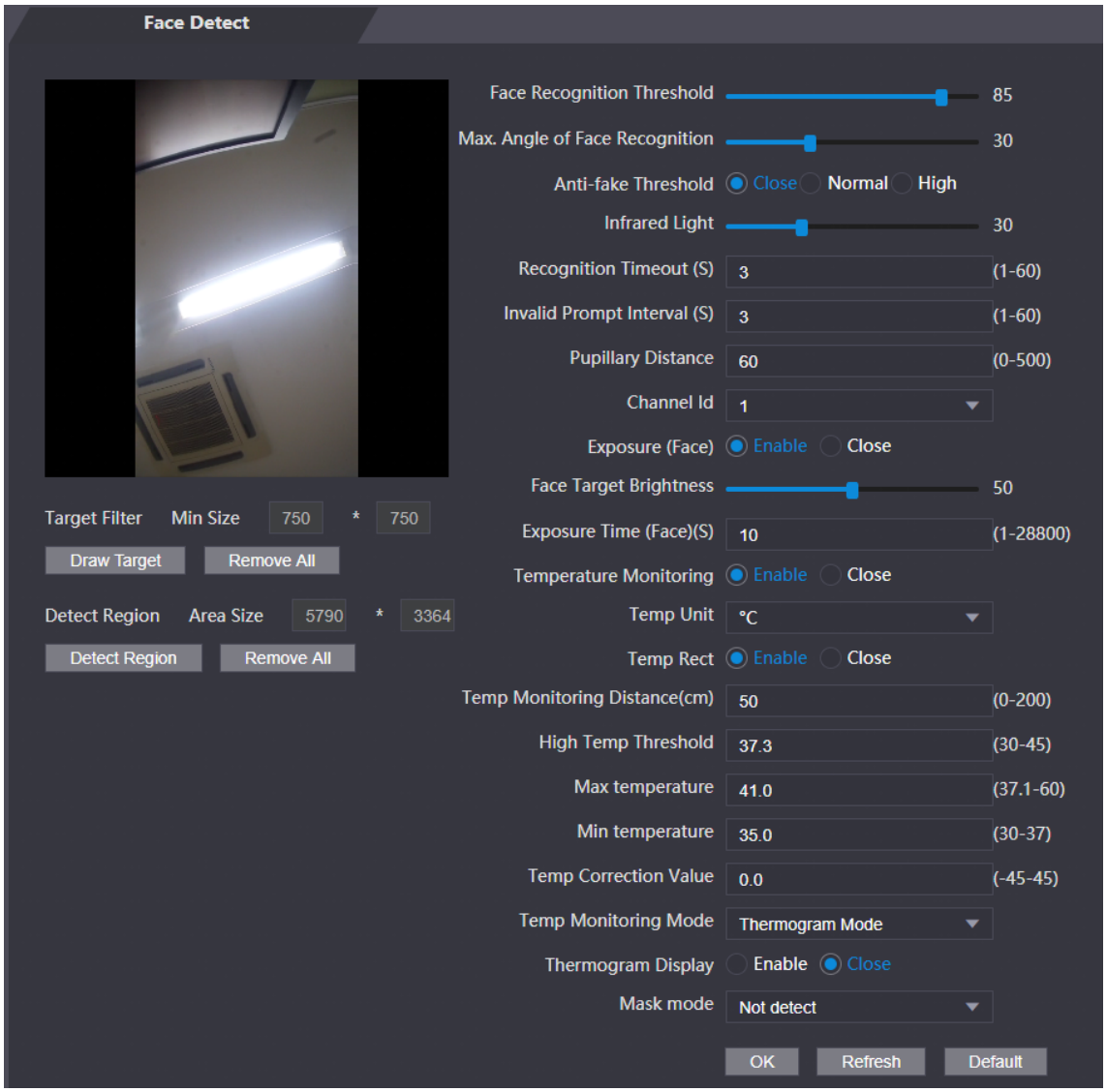
3.10 Detección de rostro

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

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Detección de rostro**.

Figura 3-39 Detección facial



Paso3 Configure los parámetros.

Tabla 3-11 Descripción del parámetro de detección facial

Parámetro	Descripción
Reconocimiento facial Umbral	Cuanto mayor sea el valor, mayor será la precisión.
Max. Ángulo de reconocimiento facial	Cuanto mayor sea el ángulo, se reconocerá la gama más amplia de perfiles.
Umbral anti-falsificación	Esta función evita que las personas se desbloqueen mediante imágenes de rostros o modelos. Ajuste
Luz infrarroja	el brillo de infrarrojos arrastrando la barra de desplazamiento.
Tiempo de espera de reconocimiento	El intervalo del mensaje durante el reconocimiento facial válido. El
Intervalo de solicitud no válido	intervalo de la indicación durante el reconocimiento facial 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 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.

Parámetro	Descripción
Canal ID	Hay dos opciones: 1 y 2. 1 es una cámara de luz blanca y 2 es una cámara de luz IR.
Exposición (cara)	Una vez habilitada la exposición facial, el rostro humano se verá más claro cuando el controlador de acceso se instale al aire libre.
Brillo objetivo facial	El valor predeterminado es 50. Ajuste el brillo según sea necesario.
Tiempo de exposición (rostro) (S)	Después de que se detecta un rostro, el controlador de acceso emitirá luz para iluminar el rostro, y el controlador de acceso no emitirá luz nuevamente hasta que haya pasado el intervalo que estableció.
Temperatura Vigilancia	Habilita o deshabilita la función de monitoreo de temperatura.
Unidad de temperatura	Seleccione ° C o ° F.
Temp Rect	Configure si desea mostrar el cuadro de control de temperatura en la interfaz de espera o no.
Corrección de temperatura Duración (ms)	Al monitorear la temperatura, el controlador de acceso tomará el valor de temperatura después del tiempo definido por este parámetro. Solo ciertos modelos admiten este parámetro.
Monitoreo de temperatura Distancia (cm)	50 por defecto. Puede corregir la temperatura monitorizada según sea necesario de acuerdo con la distancia que establezca. Solo ciertos modelos admiten este parámetro.
Umbral de temperatura alta	Establece el umbral de temperatura. La temperatura corporal monitoreada se considerará alta si es mayor o igual al valor establecido. Establezca el rango de temperatura que necesita. Si la temperatura monitoreada es más baja que el límite inferior, indicará que la temperatura es demasiado baja; si es superior al límite superior, indicará que hay una fuente de calor que interfiere con la función.
Temperatura máxima	
Temperatura mínima	
Valor de corrección de temperatura	Este parámetro es para prueba. La diferencia del entorno de monitoreo de temperatura puede causar la desviación de temperatura entre la temperatura monitoreada y la temperatura real. Puede seleccionar varias muestras monitoreadas para la prueba y luego corregir la desviación de temperatura con este parámetro de acuerdo con la comparación entre la temperatura monitoreada y la temperatura real. Por ejemplo, si la temperatura monitoreada es 0.5 ° C más baja que la temperatura real, el valor de corrección se establece en 0.5 ° C; si la temperatura monitoreada es 0.5 ° C más alta que la temperatura real, el valor de corrección se establece en -0.5 ° C.

Parámetro	Descripción
Monitoreo de temperatura Modo	- Automático: utiliza un mapa de calor facial para el reconocimiento facial; si no se encuentran mapas de calor, cambiará automáticamente al modo de calibración. - Termograma: utiliza solo un mapa de calor para el reconocimiento facial y el control de la temperatura. - Calibración: utiliza una imagen de luz blanca de una cara para el reconocimiento facial, y luego extrae y aplica las coordenadas en el mapa de calor de la cara para monitorear la temperatura.  Solo ciertos modelos admiten este parámetro. Muestre un
Pantalla de termograma	mapa de calor en la esquina superior izquierda.  Solo ciertos modelos admiten este parámetro.
Modo de máscara	- **No detectar**: La máscara no se detecta durante el reconocimiento facial. - **Recordatorio de máscara**: La máscara se detecta durante el reconocimiento facial. Si la persona es detectada sin usar una máscara, el sistema le recordará la máscara y se permitirá el paso. - **Intercepción de máscara**: La máscara se detecta durante el reconocimiento facial. Si se detecta a la persona sin usar una máscara, el sistema le recordará la máscara y no se permitirá el paso.
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. Hacer
Detectar región	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.

Paso4 Haga clic en **OK** para terminar el ajuste.

3.11 Configuración de red

3.11.1 TCP / IP

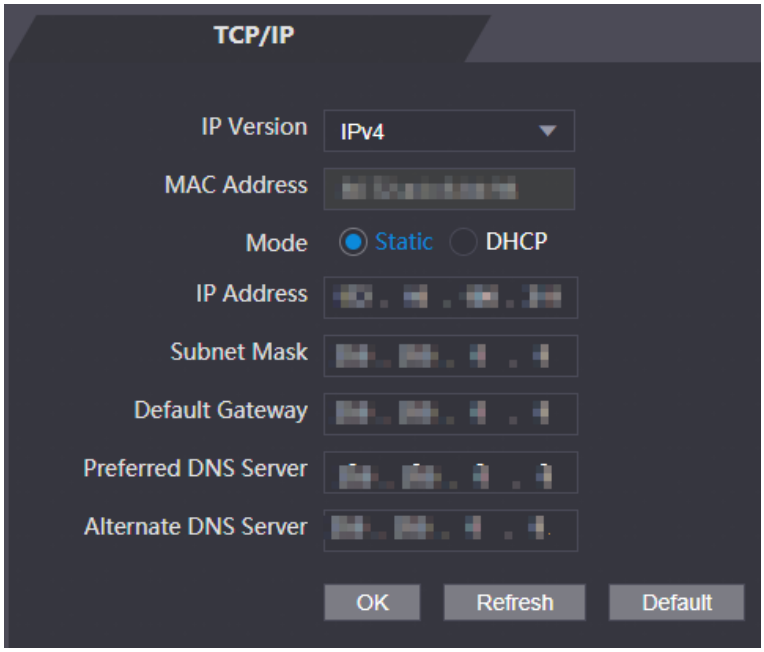
Debe configurar la dirección IP y el servidor DNS para asegurarse de que el controlador de acceso pueda comunicarse con otros dispositivos.

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

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de red> TCP / IP**.

Figura 3-40 TCP / IP



Paso3 Configure los parámetros.

Tabla 3-12 TCP / IP

Parámetro	Descripción
Versión de IP	Hay una opción: IPv4.
Dirección MAC	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 - Una vez que se habilita DHCP, la dirección IP, la máscara de subred y la dirección de la puerta de enlace no se pueden configurar. - Si DHCP es efectivo, la dirección IP, la máscara de subred y la dirección de la puerta de enlace se mostrarán automáticamente; si DHCP no es efectivo, la dirección IP, la máscara de subred y la dirección de la puerta de enlace serán todas cero. - Si desea ver la IP predeterminada cuando DHCP es efectivo, debe deshabilitar DHCP.
Dirección de enlace local	Solo 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 alternativo Servidor	Configure la dirección IP del servidor DNS preferido.

Paso4 Haga clic en **OK** para completar el ajuste.

3.11.2 Puerto

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

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de red> Puerto**.

Paso3 Configure los números de puerto. Consulte la siguiente tabla.

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

Tabla 3-13 Descripción del puerto

Parámetro	Descripción
Conexión máxima	Puede establecer las conexiones máximas de clientes a los que se puede conectar el controlador de acceso. Los clientes de plataforma como SmartPSS AC no se cuentan.
Puerto TCP	El valor predeterminado es 37777.
Puerto HTTP	El valor predeterminado es 80. Si se usa otro valor como número de puerto, debe agregar este valor detrás de la dirección cuando inicie sesión a través de navegadores.
Puerto HTTPS	El valor predeterminado es 443.
Puerto RTSP	El valor predeterminado es 554.

Paso4 Haga clic en **OK** para completar el ajuste.

3.11.3 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.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de red> Registro automático**.

Paso3 Seleccione **Habilitar**e ingrese la IP del host, el puerto y la ID del subdispositivo.

Tabla 3-14 Descripción del registro automático

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

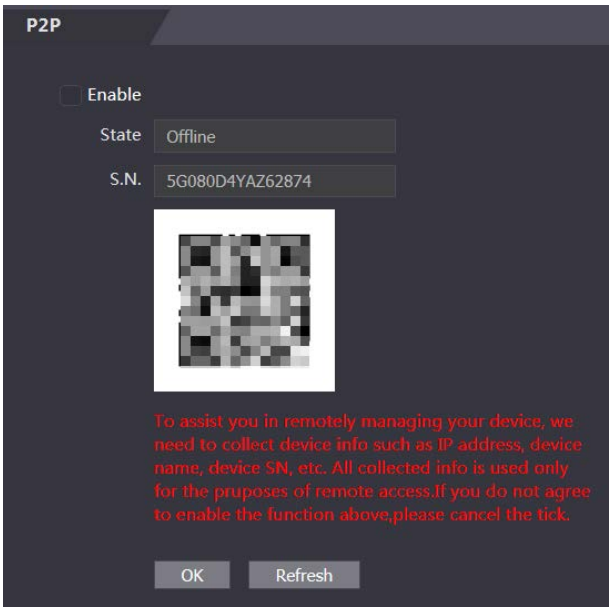
Paso4 Haga clic en **OK** para completar el ajuste.

3.11.4 P2P

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

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

Figura 3-41 P2P



Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Configuración de red> P2P**.

Paso3 Seleccione **Habilitar** para habilitar la función P2P.

Paso4 Haga clic en **OK**.

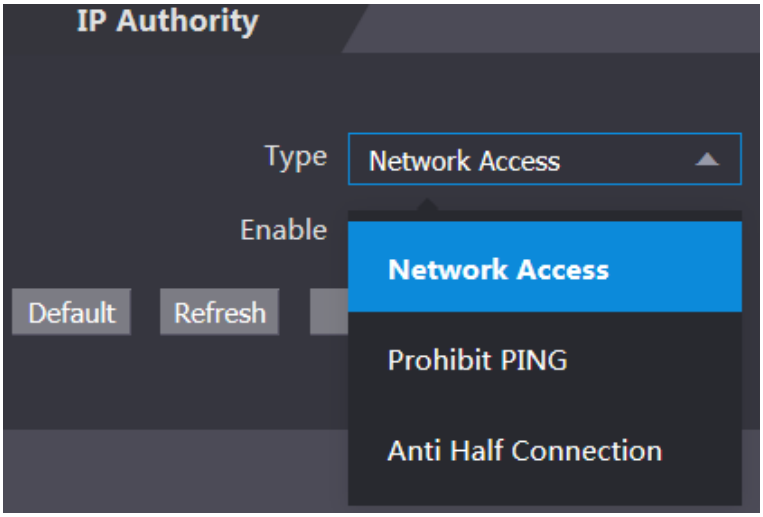
Escanee el código QR en su interfaz web para obtener el número de serie del controlador de acceso.

3.12 Gestión de la seguridad

3.12.1 Autoridad de propiedad intelectual

Seleccione un modo de ciberseguridad según sea necesario.

Figura 3-42 Autoridad de IP



3.12.2 Sistemas

3.12.2.1 Servicio del sistema

Habilite o deshabilite los servicios del sistema según sea necesario.

La configuración del servicio del sistema en la interfaz web se sincroniza con el **Características** interfaz del controlador de acceso.

Figura 3-43 Servicio del sistema

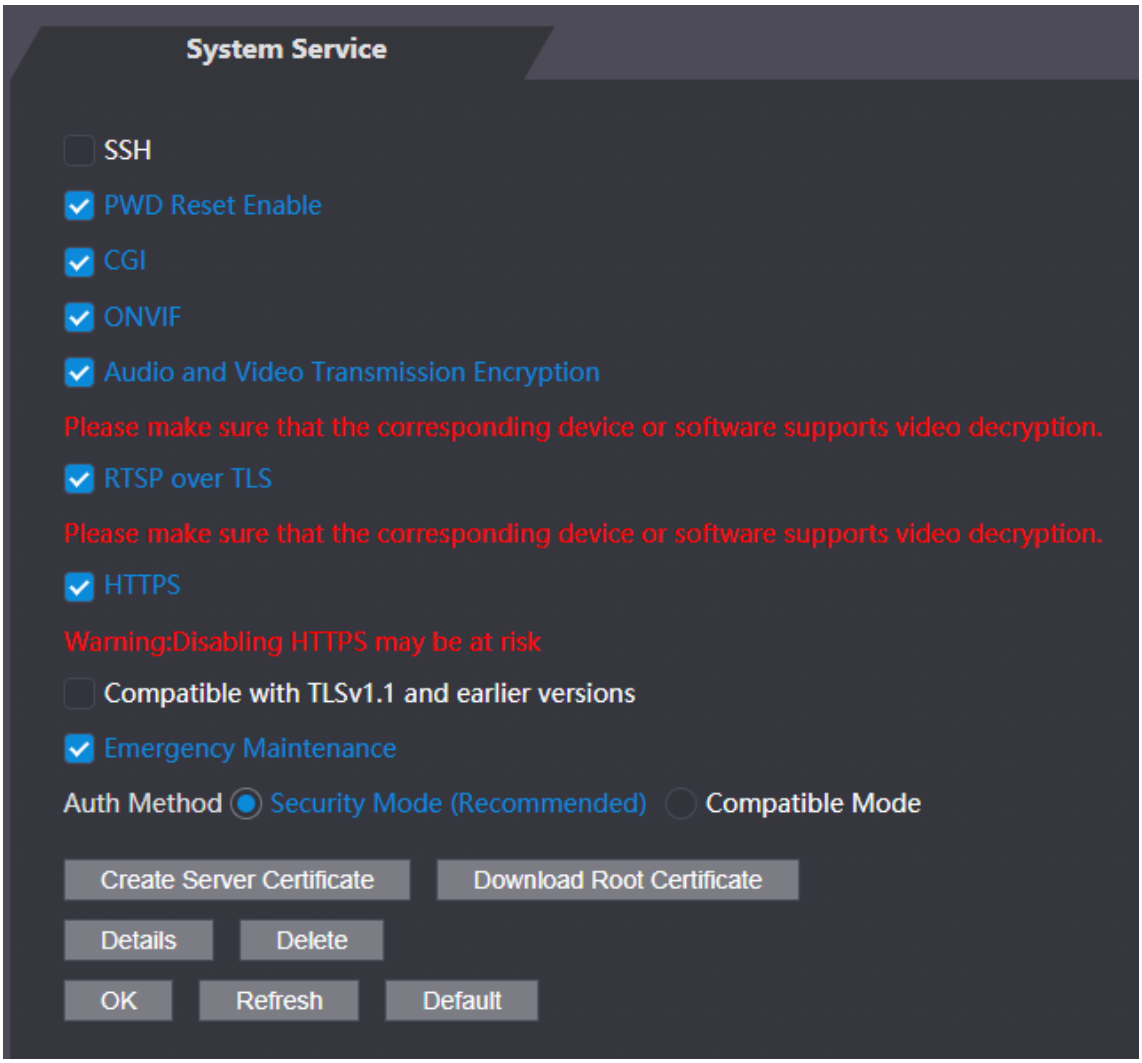


Tabla 3-15 Descripción de los parámetros

Parámetro	Descripción
SSH	Secure Shell (SSH) es un protocolo de red criptográfico para operar servicios de red de forma segura en una red no protegida. Cuando SSH está habilitado, SSH proporciona un servicio criptográfico para la transmisión de datos.
Habilitar restablecimiento de PWD	Si está habilitado, puede restablecer la contraseña. Esta función está habilitada por defecto.

Parámetro	Descripción
CGI	Common Gateway Interface (CGI) ofrece un protocolo estándar para que los servidores web ejecuten programas de manera similar a las aplicaciones de consola que se ejecutan en un servidor que genera páginas web de forma dinámica. Cuando CGI está habilitado, se pueden usar comandos CGI. El CGI está habilitado de forma predeterminada.
ONVIF	Permita que otros dispositivos extraigan la transmisión de video del VTO a través del protocolo ONVIF.
Audio y video Transmisión Cifrado	Cifre todos los datos durante la llamada de voz o video.
RTSP sobre TLS	Salida de flujo de bits cifrado a través de RTSP.
HTTPS	El Protocolo de transferencia de hipertexto seguro (HTTPS) es un protocolo para la comunicación segura a través de una red informática. Cuando HTTPS está habilitado, HTTPS se utilizará para acceder a los comandos CGI; de lo contrario, se utilizará HTTP. Cuando HTTPS está habilitado, el controlador de acceso se reiniciará automáticamente.
Compatible con TLSv1.1 y anteriores versiones	Habilite esta función si su navegador utiliza TLS V1.1 o versiones anteriores.
Emergencia Mantenimiento	Habilítelo para análisis y reparación de fallas. Esta función ocupará los puertos 8088 y 8087.
Método de autenticación	- **modo de seguridad** (recomendado): admite el inicio de sesión con autenticación implícita. - **Modo compatible**: Utilice el método de inicio de sesión anterior.

3.12.2.2 Creación de certificado de servidor

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

3.12.2.3 Descarga del certificado raíz

Paso1 clic **Descargar certificado raíz**.

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

Paso2 Haga doble clic en el **Certificado raíz** que ha descargado para instalar el certificado.

Instale el certificado siguiendo las instrucciones en pantalla.

3.13 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.

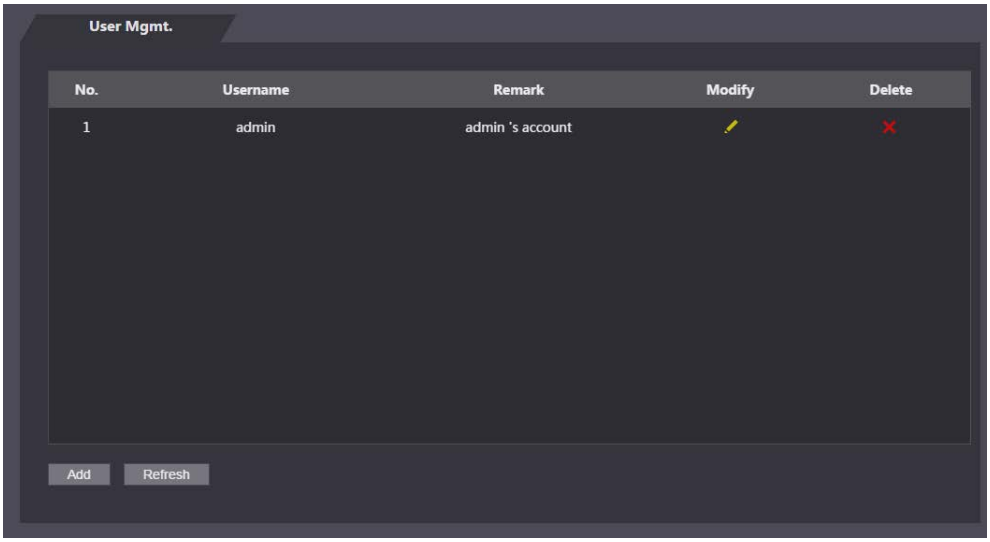
3.13.1 Agregar usuarios

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

3.13.2 Modificación de la información del usuario

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

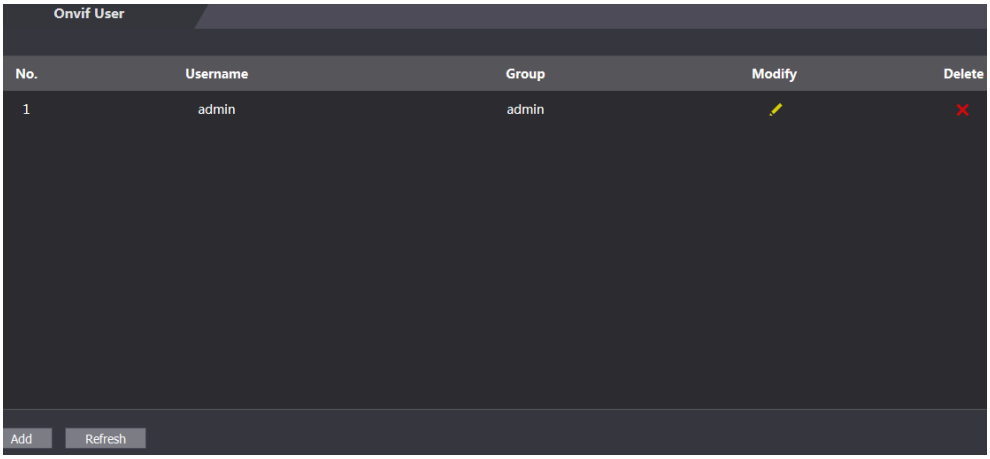
Figura 3-44 Gestión de usuarios



3.13.3 Usuario de ONVIF

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

Figura 3-45 Usuario de Onvif



3.14 Mantenimiento

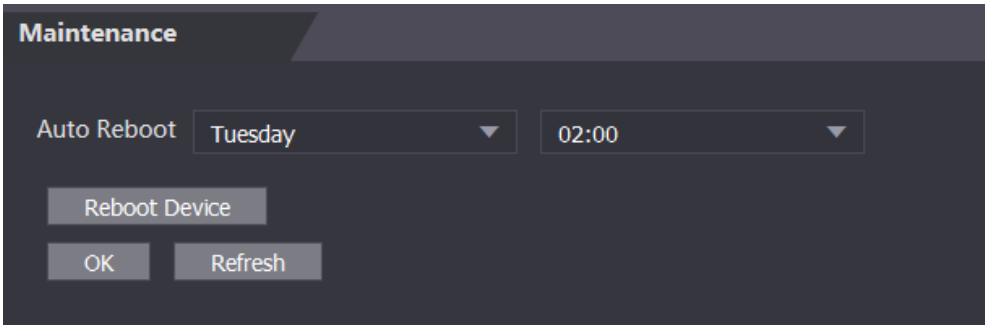
Puede hacer que el controlador de acceso se reinicie en tiempo de inactividad para mejorar la velocidad de funcionamiento del controlador de acceso. Debe configurar la fecha y hora de reinicio automático.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Mantenimiento**.

Paso3 Configure el tiempo de reinicio automático y luego haga clic en **OK**.

Figura 3-46 Mantenimiento



Por ejemplo, el controlador de acceso se reiniciará a las 2 de la mañana todos los martes. Hacer clic **Reiniciar dispositivo**, el controlador de acceso se reiniciará inmediatamente.

3.15 Gestión de la configuración

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

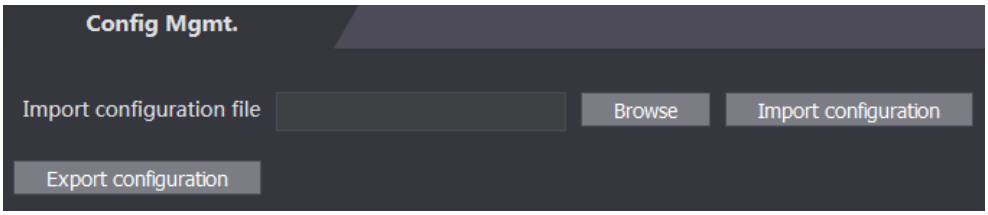
3.15.1 Exportación del archivo de configuración

Puede exportar el archivo de configuración del controlador de acceso para realizar una copia de seguridad.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Config Mgmt.** en la barra de navegación.

Figura 3-47 Gestión de la configuración



Paso3 Haga clic en **Exportar configuración** para guardar el archivo de configuración localmente.

La información de IP del controlador de acceso no se exportará.

3.15.2 Importación del archivo de configuración

Puede importar el archivo de configuración que se exporta desde un controlador de acceso a otro controlador de acceso con el mismo modelo.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Config Mgmt.** en la barra de navegación.

Paso3 En la interfaz de gestión de la configuración, haga clic en **Navegar** para seleccionar el archivo de configuración que desea importar y luego haga clic en **Importar configuración**. El controlador de acceso se reiniciará después de importar el archivo de configuración.

3.15.3 Por defecto

- **Restaurar fábrica:** Restablezca todos los datos y la configuración del controlador de acceso.
- **Restaurar fábrica (guardar usuario y registro)**: Restablece todos los datos y la configuración, excepto la información del usuario y los registros.

3.16 Actualización

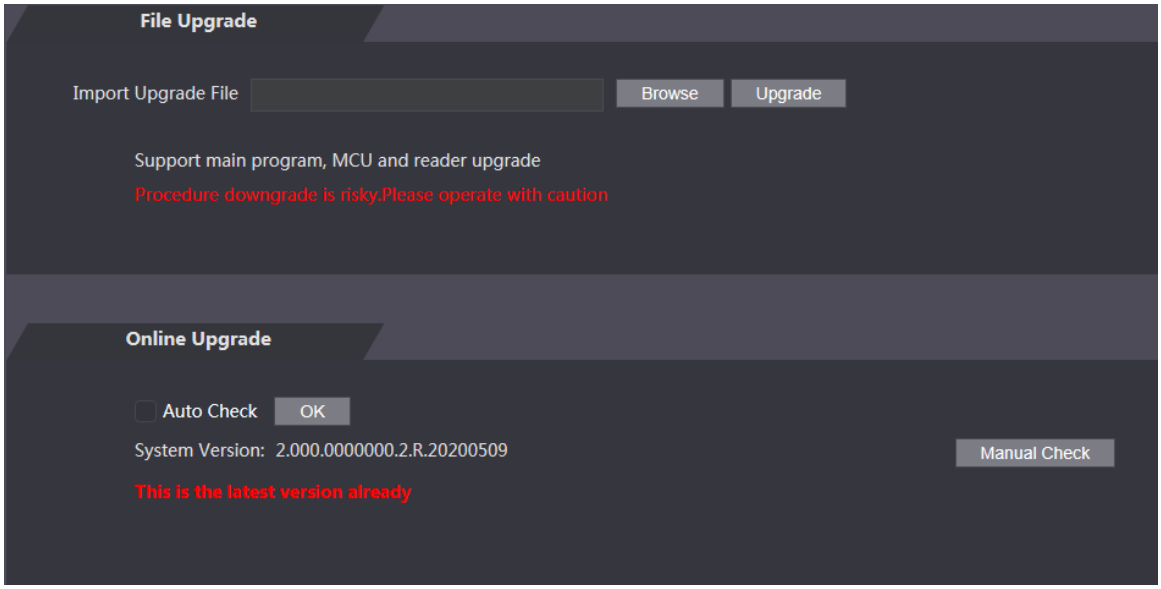
- Exporte el archivo de configuración para realizar una copia de seguridad antes de la actualización y luego impórtelo una vez finalizada la actualización.
- Asegúrese de que se haya obtenido el archivo de actualización. Puede obtenerlo del soporte técnico.
- No desconecte la alimentación ni la red, ni reinicie ni apague el controlador de acceso durante la actualización.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Potenciar** en la barra de navegación.

Paso3 En el **Potenciar** interfaz, haga clic en **Navegar** para seleccionar el archivo de actualización y luego haga clic en **Potenciar**.

Figura 3-48 Actualización



Si la actualización se realiza correctamente, el sistema muestra un mensaje que indica que la actualización se completó. Si la actualización falla, aparecerán los mensajes correspondientes.

- Puedes elegir **Verificación automática** para actualizar el sistema automáticamente. También puede seleccionar **Comprobación manual** para actualizar el sistema manualmente. El controlador de acceso se reiniciará después de la
- actualización. Haces clic**Información de la versión** en el menú de navegación de la izquierda para comprobar la versión
- después de la actualización.

3.17 Información de la versión

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

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Información de la versión** en la barra de navegación.

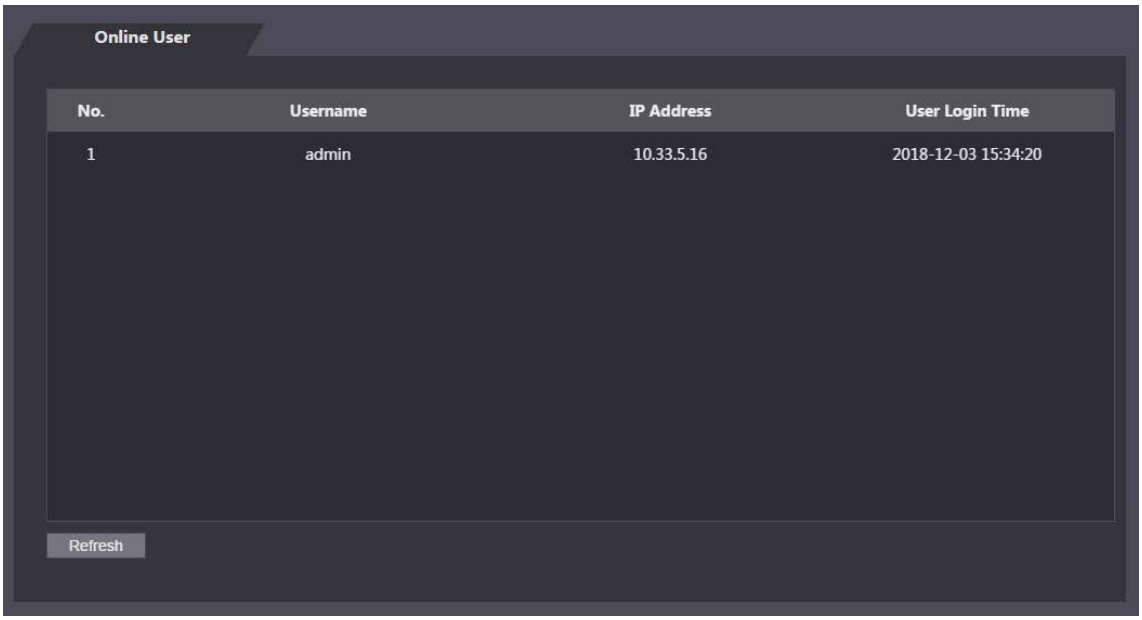
3.18 Usuario en línea

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

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Usuario en línea** en la barra de navegación.

Figura 3-49 Usuario en línea



3.19 Registro del sistema

Vea y haga una copia de seguridad de los registros del sistema, los registros de administración y los registros de desbloqueo.

3.19.1 Registros del sistema

Ver y buscar registros del sistema.

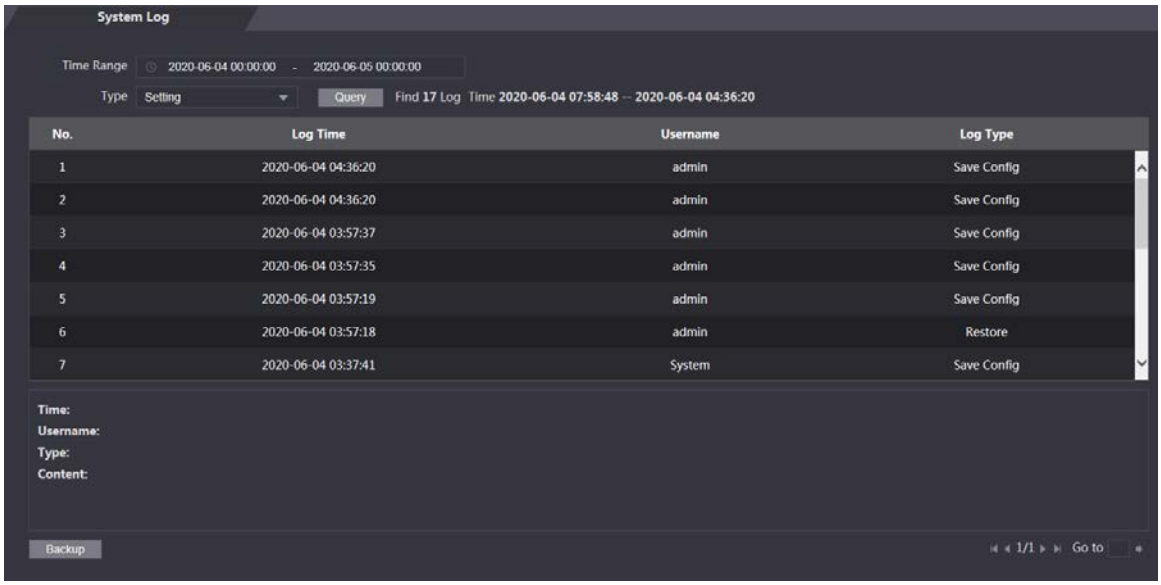
Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Registro del sistema> Registro del sistema**.

Paso3 Seleccione un rango de tiempo y un tipo, y luego haga clic **Consulta**.

Hacer clic **Respaldo** para descargar los resultados.

Figura 3-50 Búsqueda de registros



3.19.2 Registro de administración

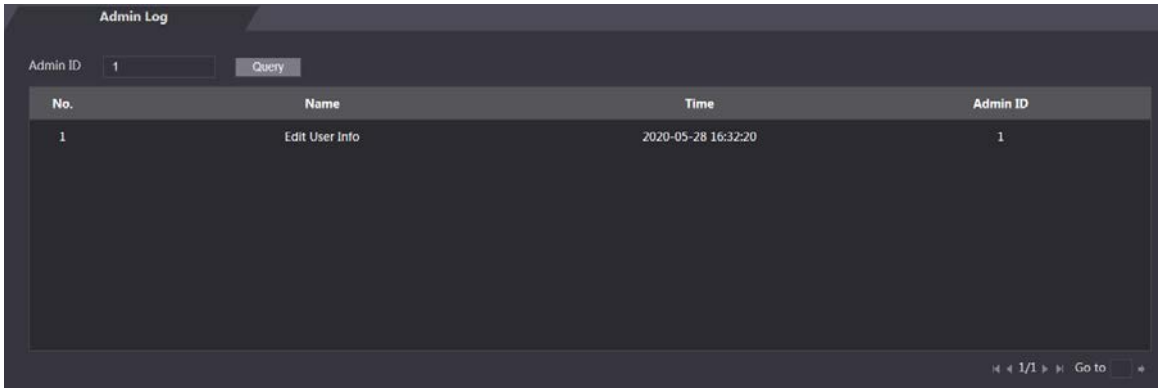
Busque registros de administrador por ID de administrador.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Registro del sistema> Registro de administración**.

Paso3 Ingrese la ID de administrador y luego haga clic en **Consulta**.

Figura 3-51 Registro de administración



3.19.3 Desbloquear registros

Busque registros de desbloqueo y expórtelos.

Paso1 Inicie sesión en la interfaz web.

Paso2 Seleccione **Registro del sistema> Buscar registros**.

Paso3 Seleccione un rango de tiempo y un tipo, y luego haga clic **Consulta**.

Paso4 Haga clic en **Exportar datos** para descargar los resultados.

3.20 Calibración de fusión

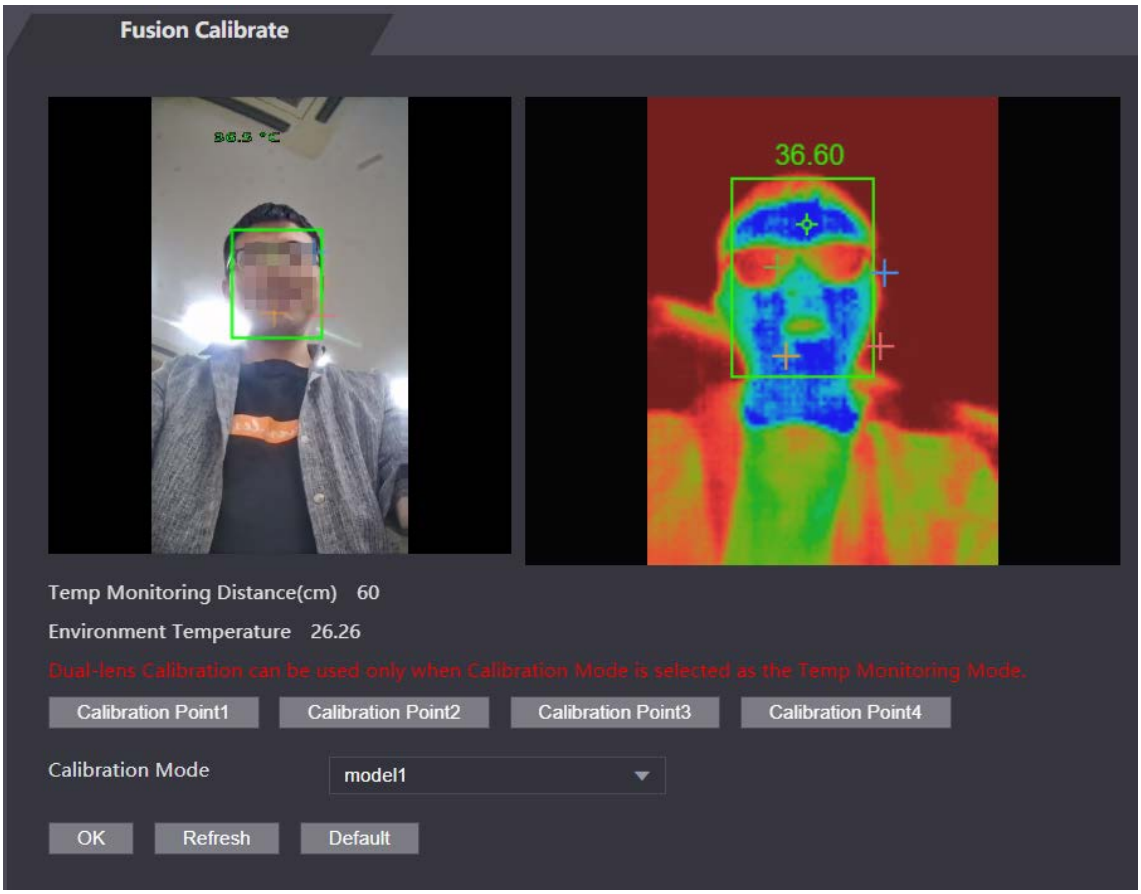
Configure la relación de coordenadas entre la imagen de la cara de luz blanca y el mapa de calor de la cara. Cuando el modo de calibración está habilitado, el controlador de acceso usará la relación de coordenadas para medir la temperatura en el mapa de calor de la cara.

- Solo algunos modelos admiten esta función. Seleccione**Modo de monitoreo de temperatura** para **Modo de calibracion**.
- Consulte "3.10 Detección de rostro" para obtener más detalles.

Paso1 Seleccione **Fusion Calibrate**.

Paso2 Seleccione un modelo de **Modo de calibracion** según el tipo de controlador de acceso.

Figura 3-52 Configurar relación de coordenadas



Paso3 Hacer clic **Punto de calibración 1**.

Paso4 Haga clic en la imagen de la izquierda y luego en la izquierda para establecer una relación entre las dos ubicaciones.

Paso5 Hacer clic**Calibración confirmada**.

Paso6 Repita el paso 2–4 para el punto de calibración 2–4.

Paso7 Hacer clic**OK**.

Paso8 (Opcional) Haga clic en **Defecto** para restablecer toda la configuración a los valores predeterminados.

3.21 Avanzado

Puede ver la temperatura ambiente, la temperatura central y la temperatura de la superficie corporal de un objetivo.

Solo algunos modelos admiten esta función.

3.22 Salir

Hacer clic  en la esquina superior izquierda y luego haga clic en **OK** para cerrar sesión en la interfaz web.

4 Configuración de CA SmartPSS

Puede administrar el controlador de acceso a través del cliente SmartPSS AC. Para configuraciones detalladas, consulte el manual del usuario de SmartPSS AC.

Las interfaces de SmartPSS AC pueden variar según las versiones, y prevalecerá la interfaz real.

4.1 Iniciar sesión

Paso1 Instale el SmartPSS AC.

Paso2 Haga doble clic y luego siga las instrucciones para finalizar la inicialización e iniciar sesión.

4.2 Agregar dispositivos

Debe agregar controladores de acceso al SmartPSS AC. Puede hacer clic**Auto búsqueda** para agregar y hacer clic **Agregar** para agregar dispositivos manualmente.

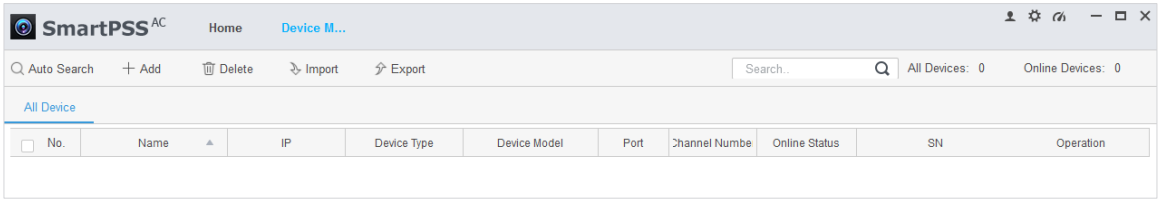
4.2.1 Búsqueda automática

Puede buscar y agregar controladores de acceso en el mismo segmento de red al SmartPSS AC.

Paso1 Inicie sesión en SmartPSS AC.

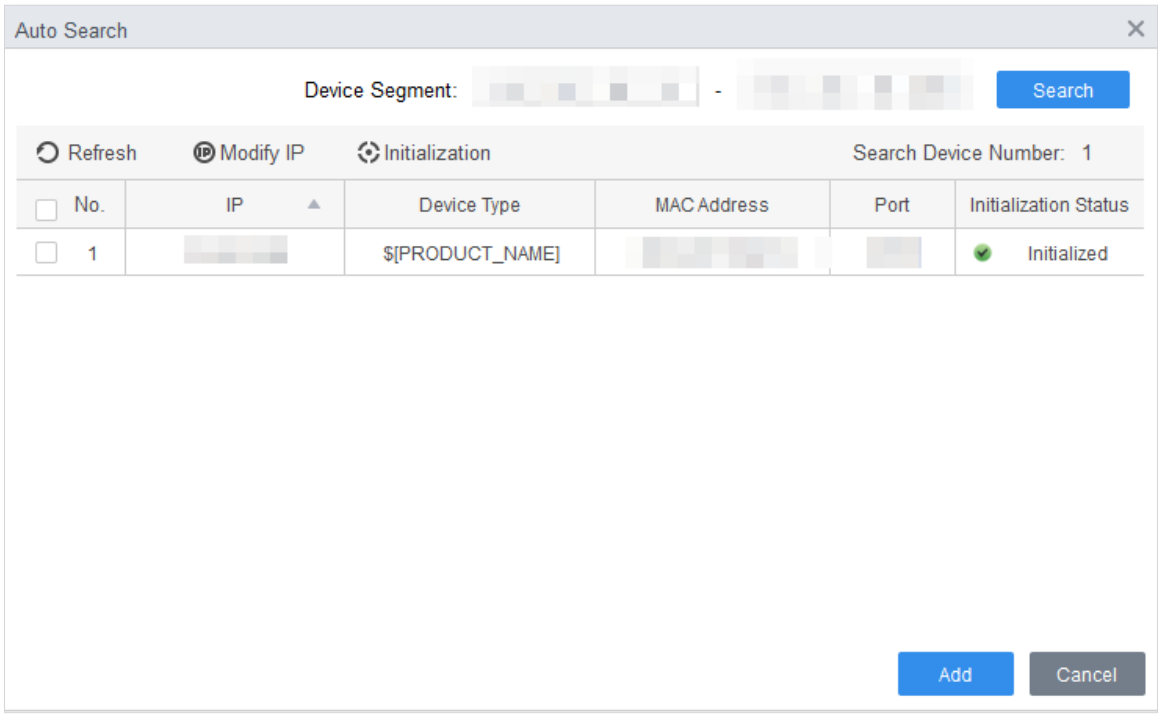
Paso2 Haga clic en **Administrador de dispositivos** en la esquina inferior izquierda.

Figura 4-1 Dispositivos



Paso3 Haga clic en **Auto búsqueda**.

Figura 4-2 Búsqueda automática



Paso4 Ingrese el segmento de red y luego haga clic en **Buscar**. Se mostrará una lista de resultados de búsqueda.

Paso5 Seleccione los controladores de acceso que desea agregar al SmartPSS AC y luego haga clic en **Agregar**. Se mostrará el cuadro de diálogo de información de inicio de sesión.

Paso6 Introduzca el nombre de usuario y la contraseña de inicio de sesión para iniciar sesión.

Puede ver el controlador de acceso agregado en el **Dispositivos** interfaz.

Seleccione un controlador de acceso, haga clic en **Modificar IP**y puede modificar la dirección IP del controlador de acceso. Para obtener detalles sobre la modificación de la dirección IP, consulte el manual del usuario de SmartPSS AC.

4.2.2 Adición manual

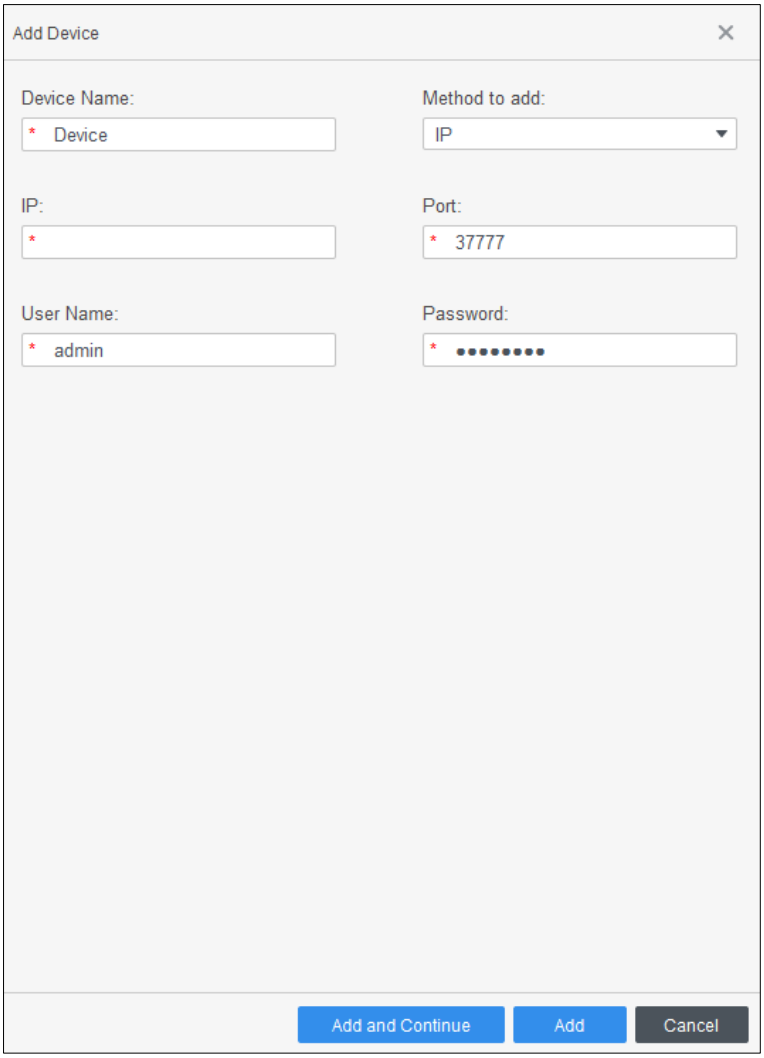
Puede agregar controladores de acceso manualmente. Debe conocer las direcciones IP y los nombres de dominio de los controladores de acceso que desea agregar.

Paso1 Inicie sesión en SmartPSS AC.

Paso2 Haga clic en **Administrador de dispositivos** en la esquina inferior izquierda.

Paso3 Haga clic en **Agregar** sobre el **Dispositivos** interfaz, y el **Agregar manual** Se mostrará la interfaz.

Figura 4-3 Adición manual



Paso4 Ingrese el nombre del dispositivo, seleccione un método para agregar, ingrese la IP, Número de puerto (37777 por defecto), Nombre de usuario y contraseña.

Paso5 Haga clic en **Agregar**, y luego puede ver el controlador de acceso agregado en el **Dispositivos** interfaz.

4.3 Gestión de usuarios

4.3.1 Configuración del tipo de tarjeta

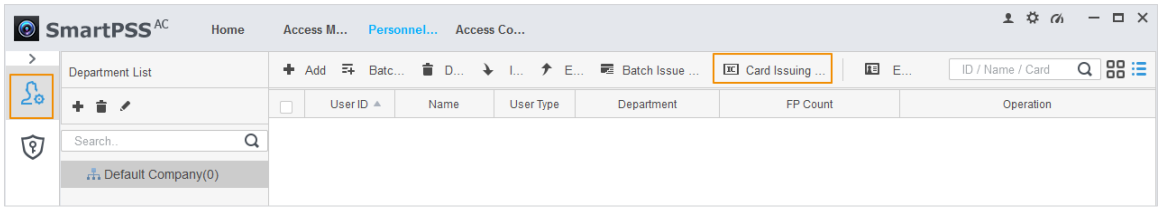
Antes de emitir la tarjeta, configure primero el tipo de tarjeta. Por ejemplo, si la tarjeta emitida es una tarjeta de identificación, seleccione el tipo como tarjeta de identificación.

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

Paso1 Inicie sesión en SmartPSS AC.

Paso2 Haga clic en **Gerente de personal**.

Figura 4-4 Responsable de personal

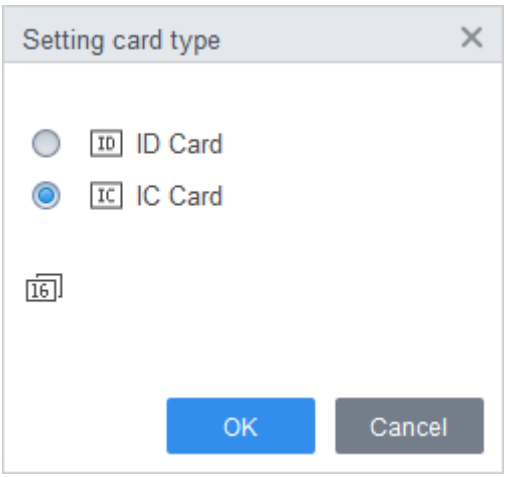


Paso3 En el **Gerente de personal** interfaz, haga clic en  , luego haga clic en  .

Paso4 En el **Configuración del tipo de tarjeta** interfaz, seleccione un tipo de tarjeta.

Paso5 Haga clic en  para seleccionar el método de visualización del número de tarjeta en decimal o en hexadecimal.

Figura 4-5 Configuración del tipo de tarjeta



Paso6 Haga clic en **OK**.

4.3.2 Agregar usuario

Seleccione uno de los métodos para agregar un usuario.

- Agregue al usuario uno por uno manualmente.
- Agregue usuarios por lotes.
- Extrae la información del usuario de otros dispositivos.
- Importar información de usuario del local.

4.3.2.1 Adición manual

Puede agregar usuarios uno por uno manualmente.

Paso1 Inicie sesión en SmartPSS AC.

Paso2 Haga clic en **Administrador de personal> Usuario> Agregar**.

Paso3 Agregue información básica del usuario.

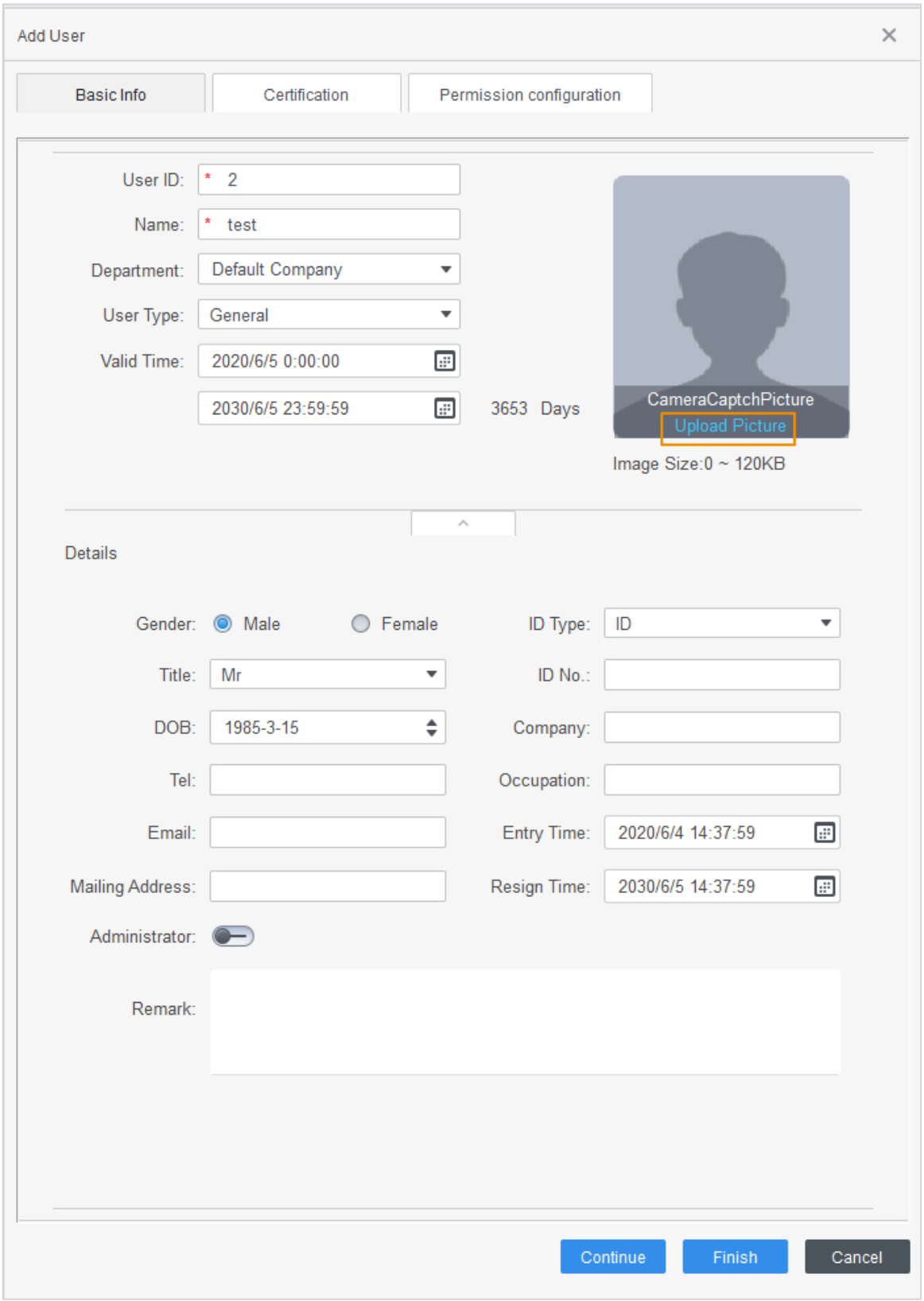
1) Haga clic en el **Información básica** pestaña en el **Agregar usuario** interfaz, y luego agregue información básica del usuario.

2) Haga clic en la imagen y luego haga clic en **Subir foto** para agregar una imagen de cara.

La imagen de la cara cargada se mostrará en el cuadro de captura.

Asegúrese de que los píxeles de la imagen sean superiores a 500 × 500; el tamaño de la imagen es inferior a 120 KB.

Figura 4-6 Agregar información básica



Paso4 Haga clic en el **Pestaña de certificación** para agregar información de certificación del usuario.

- Configurar contraseña.

  Configurar la clave. Para los controladores de acceso de segunda generación, configure la contraseña del personal; para otros dispositivos, configure la contraseña de la tarjeta. La nueva contraseña debe constar de 6 dígitos.

- Configurar tarjeta.

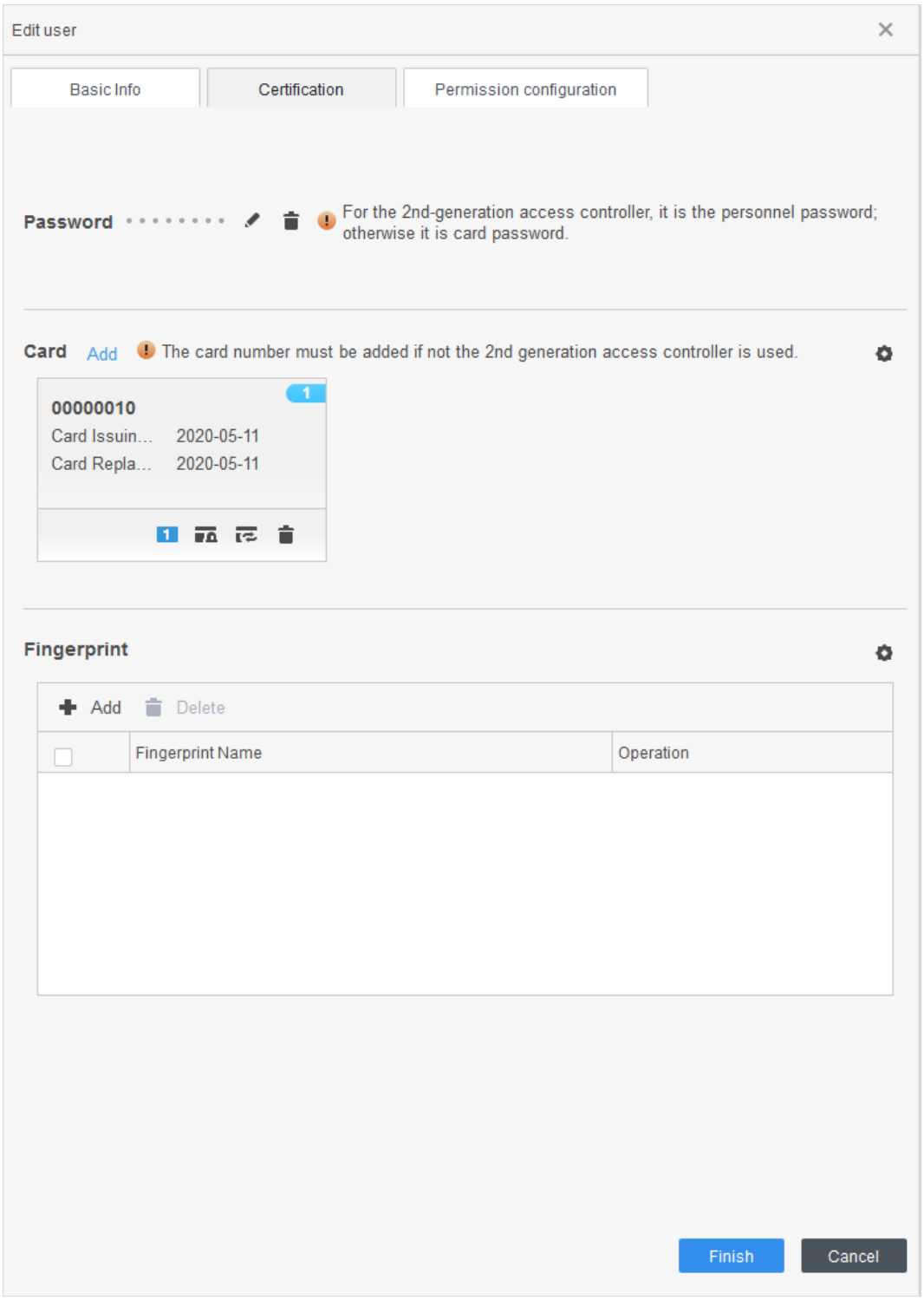
El número de tarjeta se puede leer automáticamente o completar manualmente. Para leer automáticamente, seleccione un lector de tarjetas y luego coloque la tarjeta en el lector de tarjetas. El número de la tarjeta se lee automáticamente después de eso.

1) Hacer clic para seleccionar **Dispositivo** o **Emisor de la tarjeta** como lector de tarjetas.
2) Agregar tarjeta. El número de tarjeta debe agregarse si se utiliza un controlador de acceso que no sea de segunda generación.
3) Después de agregar, puede seleccionar la tarjeta como tarjeta principal o tarjeta de coacción, o reemplazar la tarjeta por una nueva o eliminar la tarjeta.

- Configurar huella digital.

1) Hacer clic para seleccionar **Dispositivo** o **Escáner de huellas dactilares** como recolector de huellas dactilares.
2) Agregar huella digital. Hacer clic**Agregar huella digital** y presione el dedo en el escáner tres veces seguidas.

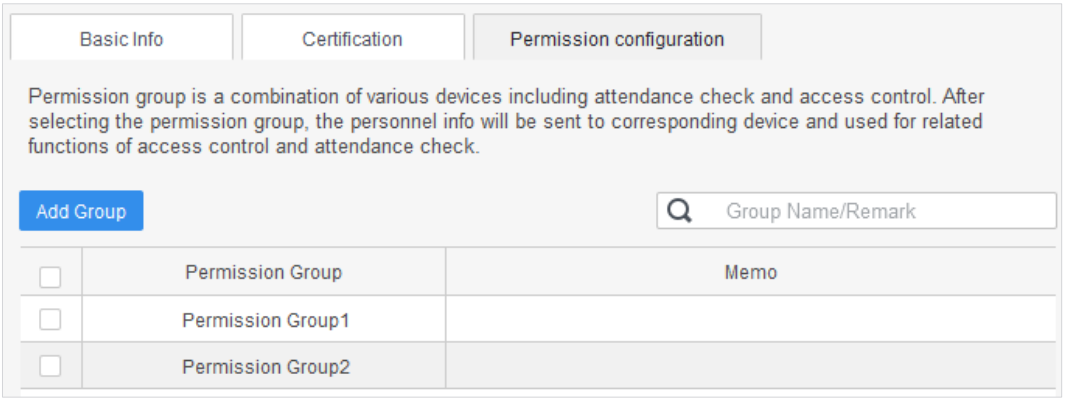
Figura 4-7 Configurar la certificación



Paso5 Configure el permiso para el usuario.

Para obtener más información, consulte "4.4 Configuración de permisos".

Figura 4-8 Configuración de permisos



Paso6 Haga clic en **Terminar**.

4.3.2.2 Agregar lote

Puede agregar usuarios en lotes.

Paso1 Inicie sesión en SmartPSS AC. Hacer clic**Administrador de**

Paso2 **personal> Usuario> Agregar lote**.

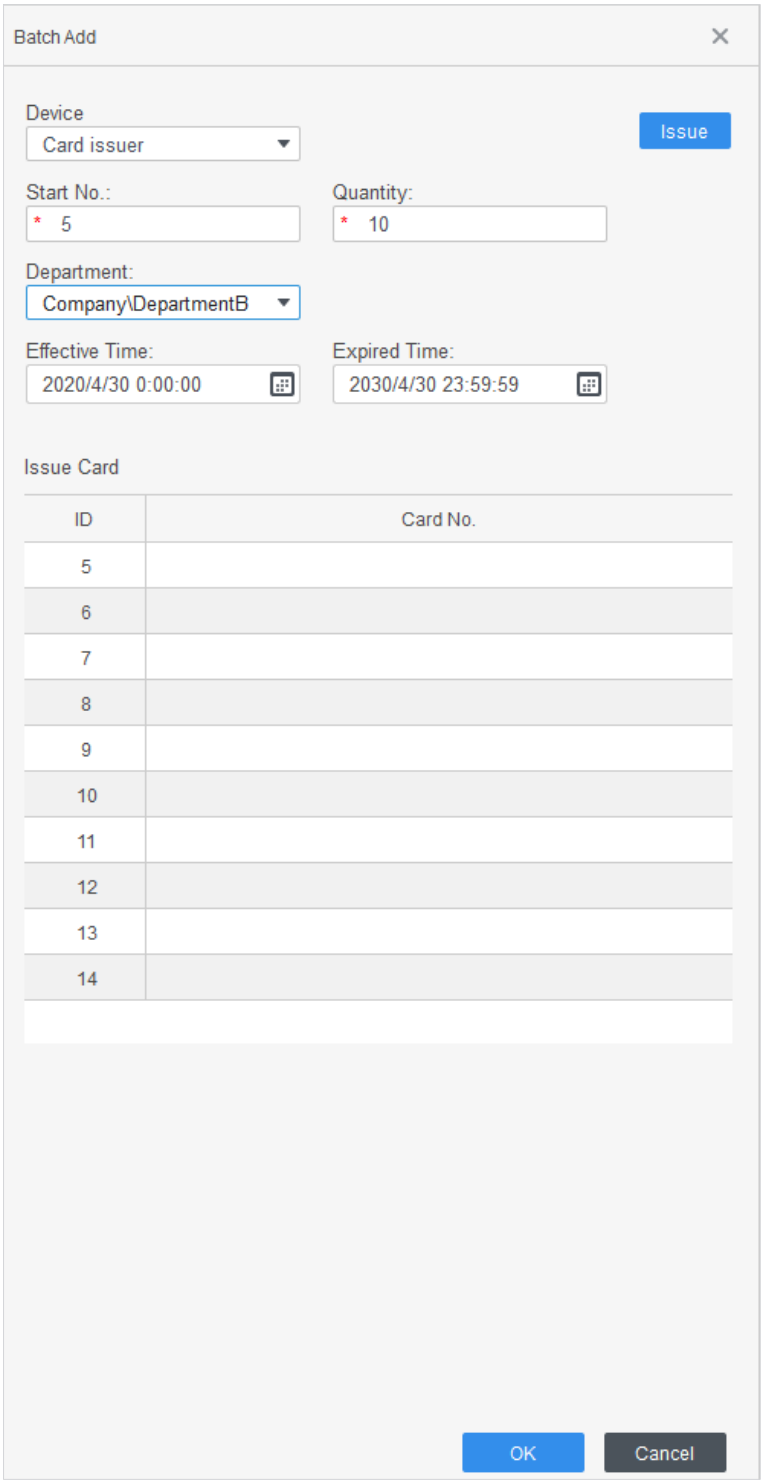
Paso3 Seleccione lector de tarjetas y el departamento de usuario. Establezca el número de inicio, la cantidad de tarjetas, la hora efectiva y la hora de vencimiento de la tarjeta.

Paso4 Hacer clic **Asunto** para empezar a emitir tarjetas**.**

El número de la tarjeta se leerá automáticamente. Hacer clic

Paso5 **Parada** después de emitir la tarjeta y luego haga clic en **OK**.

Figura 4-9 Agregar usuario por lotes



Paso6 En la lista de usuarios, haga clic en  para modificar información o agregar detalles de usuarios.

4.3.2.3 Extracción de usuarios de dispositivos

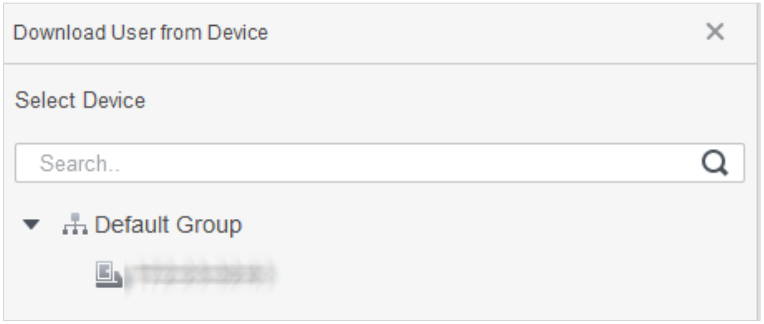
Puede extraer información de usuario de los dispositivos.

Paso1 Inicie sesión en SmartPSS AC.

Paso2 Haga clic en **Administrador de personal> Usuario> Extraer**.

Paso3 Busque y seleccione el dispositivo de destino y luego haga clic en **OK**.

Figura 4-10 Dispositivos con información de usuario



Paso4 Seleccione los usuarios según sea necesario y haga clic **Extraer**.

Paso5 En la lista de usuarios, haga clic en  para modificar información o agregar detalles de usuario.

4.3.2.4 Importar usuario

Puede importar usuarios localmente.

Paso1 Inicie sesión en SmartPSS AC.

Paso2 Haga clic en **Administrador de personal> Usuario> Importar**.

Paso3 Importe la información del usuario según las instrucciones.

4.3.3 Emisión de tarjetas en lotes

Puede emitir tarjetas a los usuarios que se han agregado pero que no tienen tarjeta.

Paso1 Inicie sesión en SmartPSS AC.

Paso2 Seleccione **Responsable de personal> Usuario**.

Paso3 Seleccione los usuarios según sea necesario y luego haga clic en **Tarjeta de emisión por lotes**.

Paso4 Emitir la tarjeta por lotes. El número de tarjeta puede ser leído automáticamente por un lector de tarjetas o ingresado manualmente.

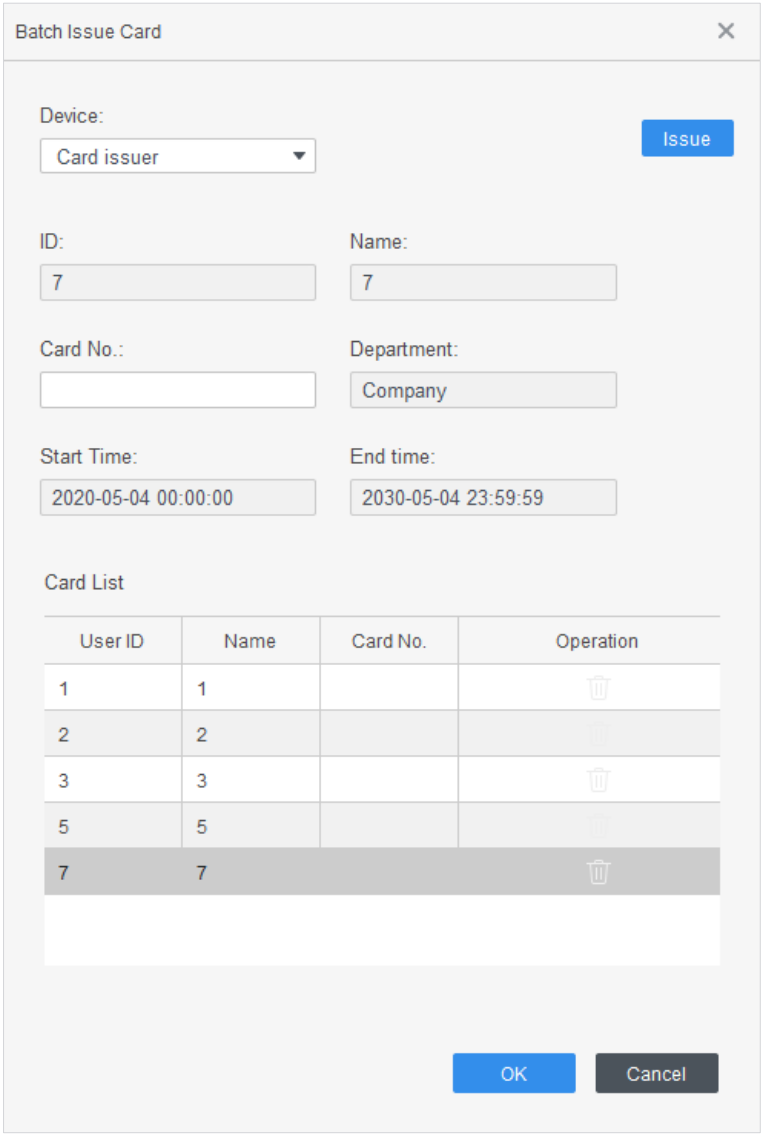
- Lectura automática

1) Seleccione el dispositivo de lectura de tarjetas y luego haga clic en **Asunto**.
2) De acuerdo con la lista de tarjetas, coloque las tarjetas del usuario correspondiente en el lector de tarjetas en secuencia, y luego el sistema leerá automáticamente el número de tarjeta.
3) Modifique la información del usuario, como la hora de inicio y la hora de finalización para la validación de la

- tarjeta. Ingresar manualmente

1) Seleccione el usuario en la lista de tarjetas e ingrese el número de tarjeta correspondiente. Modifique la
2) información del usuario, como la hora de inicio y la hora de finalización para la validación de la tarjeta.

Figura 4-11 Tarjeta de emisión en lotes



Paso5 Haga clic en **OK**.

4.3.4 Exportación de información del usuario

Puede exportar información de usuario.

Paso1 Inicie sesión en SmartPSS AC.

Paso2 Seleccione **Responsable de personal> Usuario**.

Paso3 Seleccione la información de usuario que debe exportarse y luego haga clic en **Exportar** para exportar todo la información del usuario a local.

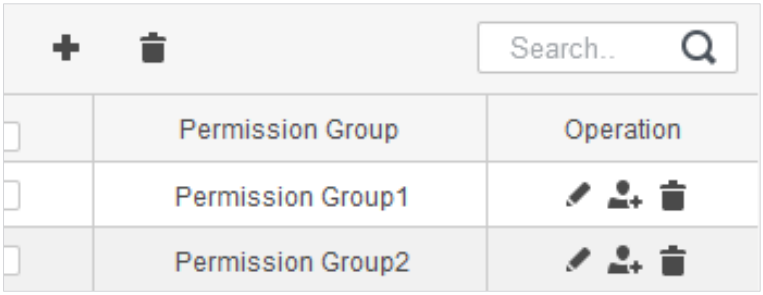
4.4 Configuración de permisos

4.4.1 Agregar grupo de permisos

Paso1 Inicie sesión en SmartPSS AC.

Paso2 Haga clic en **Administrador de personal> Configuración de permisos**.

Figura 4-12 Lista de grupos de permisos



Paso3 Haga clic en  para agregar un grupo de permisos.

Paso4 Configure los parámetros de permisos.

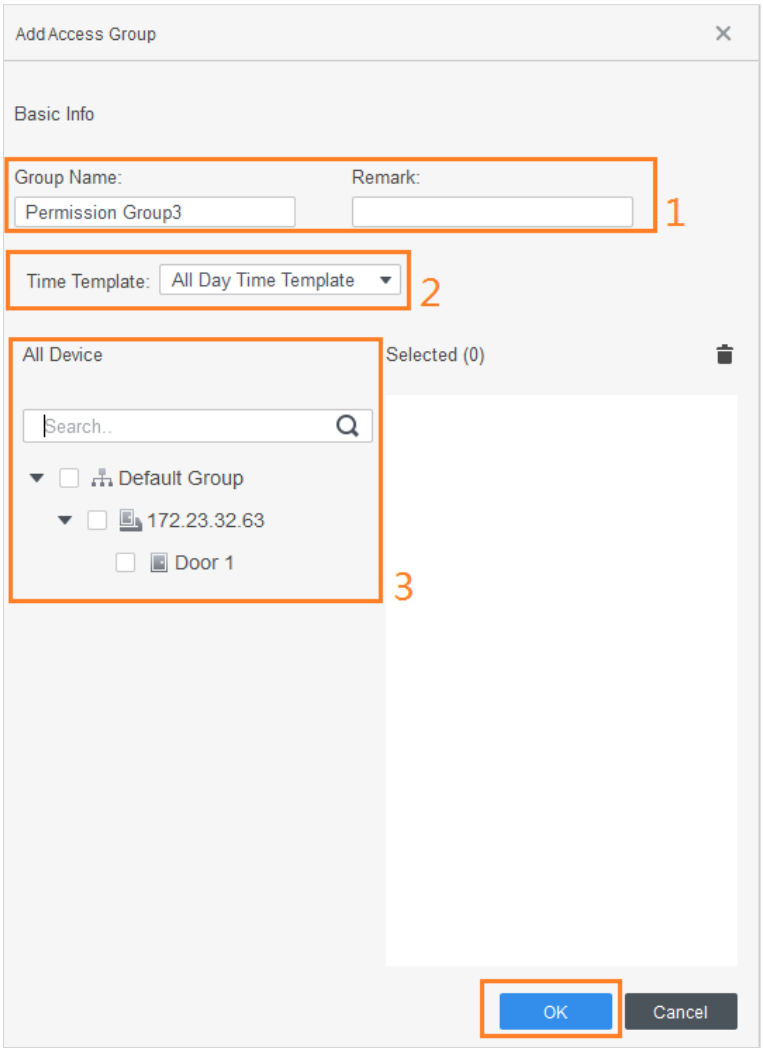
1) Ingrese el nombre del grupo y el comentario.

2) Seleccione la plantilla de tiempo necesaria.

Para obtener detalles sobre la configuración de la plantilla de tiempo, consulte el manual del usuario de SmartPSS AC.

3) Seleccione el dispositivo correspondiente, como la puerta 1.

Figura 4-13 Agregar grupo de permisos



Paso5 Haga clic en **OK**.

Sobre el **Lista de grupos de permisos** interfaz, puede hacer:

- Hacer clic para eliminar el grupo.
- Hacer clic para modificar la información del grupo.
- Haga doble clic en el nombre del grupo de permisos para ver la información del grupo.

4.4.2 Configuración de permisos

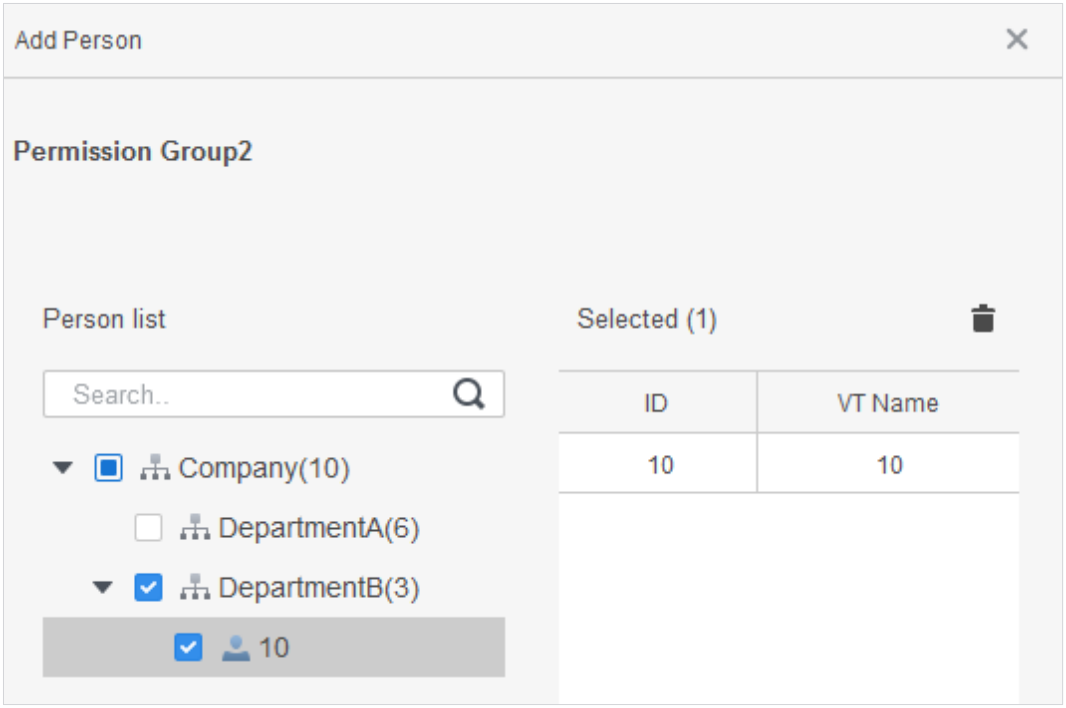
El método para configurar el permiso para el departamento y para los usuarios es similar. Esta sección toma a los usuarios como ejemplo.

Paso1 Inicie sesión en SmartPSS AC.

Paso2 Haga clic en **Administrador de personal> Configuración de permisos**.

Paso3 Seleccione el grupo de permisos de destino y luego haga clic en .

Figura 4-14 Configurar permisos



Paso4 Seleccione el usuario que necesita tener permiso para configurar.

Paso5 Haga clic en **OK**.

4.5 Gestión de acceso

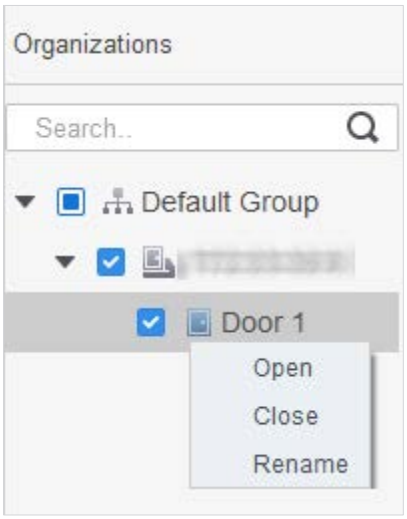
4.5.1 Apertura y cierre de puertas de forma remota

Después de la configuración de acceso, puede controlar la puerta de forma remota a través de SmartPSS AC.

Paso1 clic **Administrador de acceso** en la página de inicio. (O haga clic en**Guía de acceso>**).

Paso2 Controle la puerta de forma remota. Hay dos métodos.

- Método 1: seleccione la puerta, haga clic derecho y seleccione **Abierto**. Figura 4-15 Control remoto (método 1)



- Método 2: haga clic en o para abrir o cerrar la puerta.

Figura 4-16 Control remoto (método 2)

Paso3 Ver el estado de la puerta **Información del evento** lista.

- Filtrado de eventos: seleccione el tipo de evento en el **Información del evento**y la lista de eventos muestra los eventos de los tipos seleccionados. Por ejemplo, seleccione**Alarma**y la lista de eventos solo muestra eventos de alarma.
- Bloqueo de actualización de eventos: haga clic en a la derecha de **Información del evento** para bloquear o desbloquear el evento lista, y luego los eventos en tiempo real no se pueden ver.
- Eliminación de eventos: haga clic en a la derecha de **Información del evento** para borrar todos los eventos de la lista de eventos.

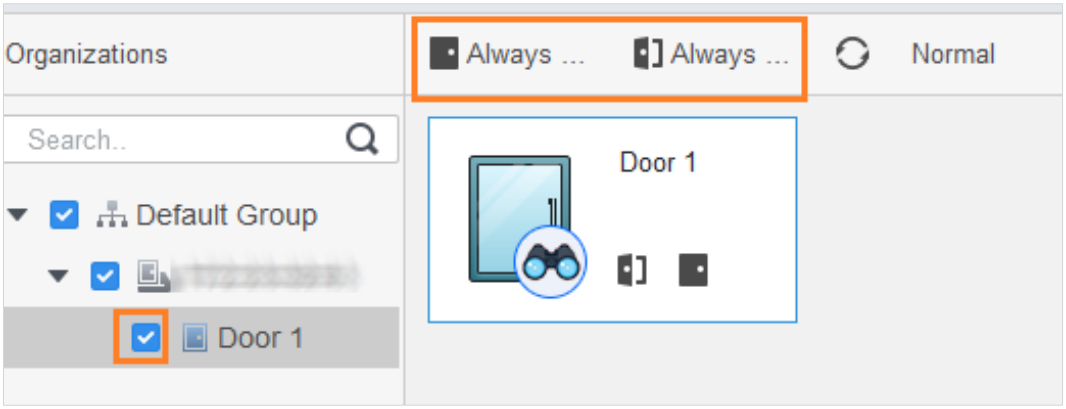
4.5.2 Configuración de siempre abierto y siempre cerrado

Después de configurar siempre abierto o siempre cerrado, la puerta está abierta o cerrada todo el tiempo y no se puede controlar manualmente. Si desea volver a controlar manualmente la puerta, haga clic en**Normal** para restablecer el estado de la puerta.

Paso1 clic **Administrador de acceso** en la página de inicio. (O haga clic en**Guía de acceso>**).

Paso2 Seleccione la puerta necesaria y luego haga clic en **Siempre abierto** o **Siempre cerca**.

Figura 4-17 Establecer siempre abierto o siempre cerrado



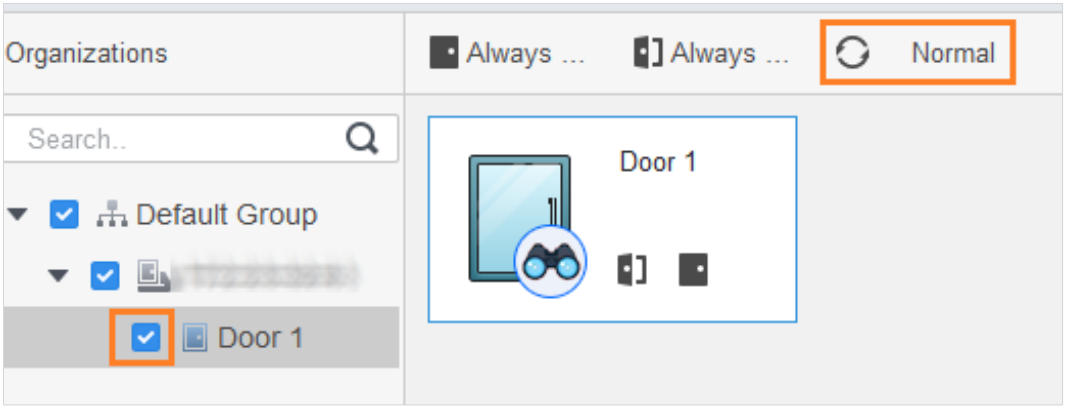
4.5.3 Restablecimiento del estado de la puerta

Hacer clic **Normal** para restablecer el estado de la puerta, si desea volver a controlar manualmente la puerta cuando haya hecho clic **Siempre abierto** o **Siempre cerca**.

Paso1 clic **Administrador de acceso** en la página de inicio. (O haga clic en**Guía de acceso>**).

Paso2 Seleccione la puerta necesaria y luego haga clic en **Normal**. Y luego siga las instrucciones en pantalla para operar.

Figura 4-18 Restablecer el estado de la puerta



4.6 Gestión de asistencia

Puede establecer el tiempo de asistencia, agregar turnos de asistencia, programación de personal, procesar la asistencia, administrar estadísticas de asistencia, buscar informes, agregar días festivos y configurar la asistencia.

4.6.1 Búsqueda de informes

Puede ver la asistencia normal, las anomalías en la asistencia, la asistencia en horas extras y la información del personal aquí. Y las estadísticas se pueden exportar como informes.

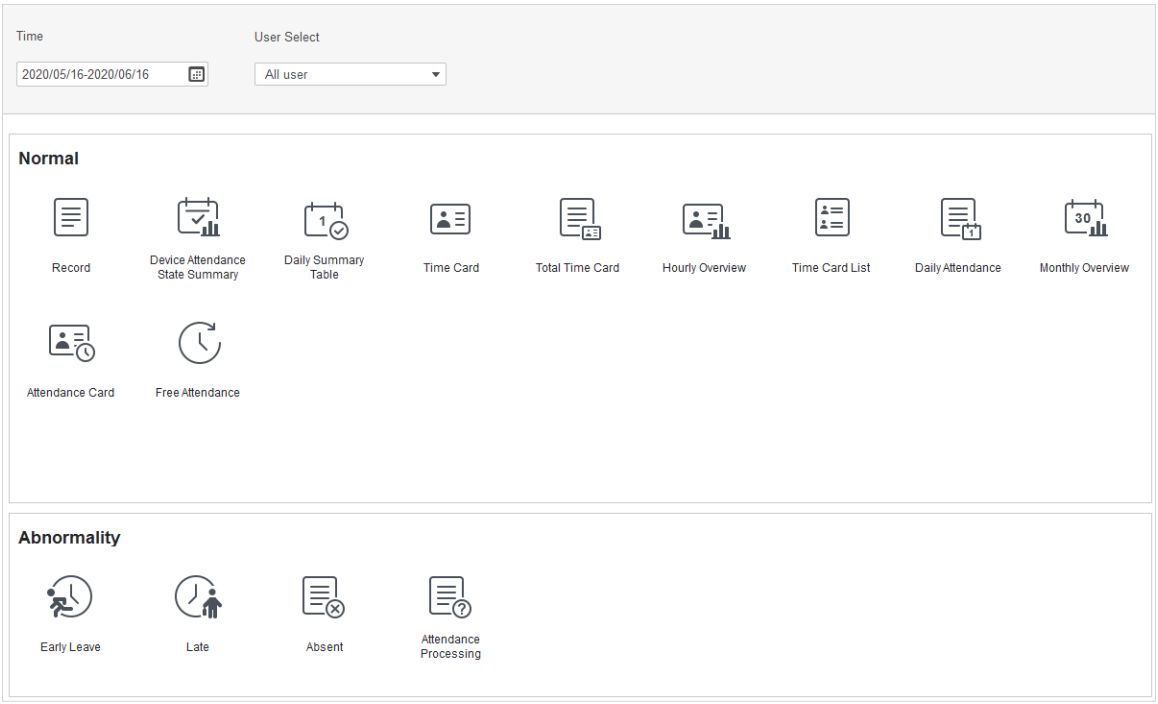
Paso1 Inicie sesión en SmartPSS AC.

Paso2 Haga clic en **Gerente de asistencia**.

Paso3 En la barra de menú de la izquierda, haga clic en .

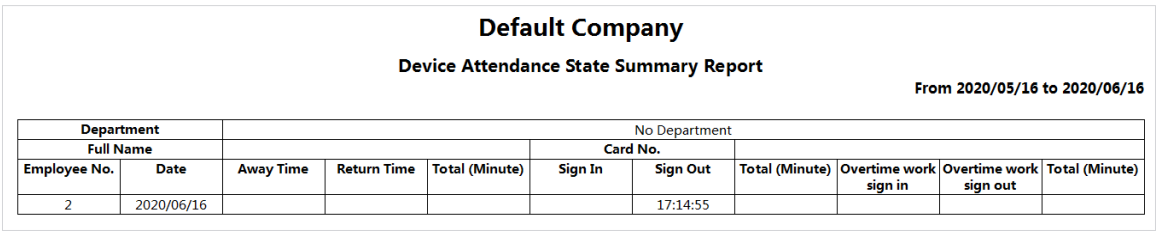
Paso4 Seleccione la hora, el departamento y el tipo de estadística para ver los informes correspondientes.

Figura 4-19 Búsqueda de informes



Una vez que el dispositivo se agrega y se autentica en la plataforma SmartPSS AC, el estado de asistencia correspondiente se informará a la plataforma y la plataforma generará el informe de estado de asistencia correspondiente.

Figura 4-20 Informe de estado de asistencia del dispositivo



Default Company

Device Attendance State Summary Report

From 2020/05/16 to 2020/06/16

Department		No Department								
Full Name					Card No.					
Employee No.	Date	Away Time	Return Time	Total (Minute)	Sign In	Sign Out	Total (Minute)	Overtime work sign in	Overtime work sign out	Total (Minute)
2	2020/06/16					17:14:55				

4.6.2 Otras configuraciones

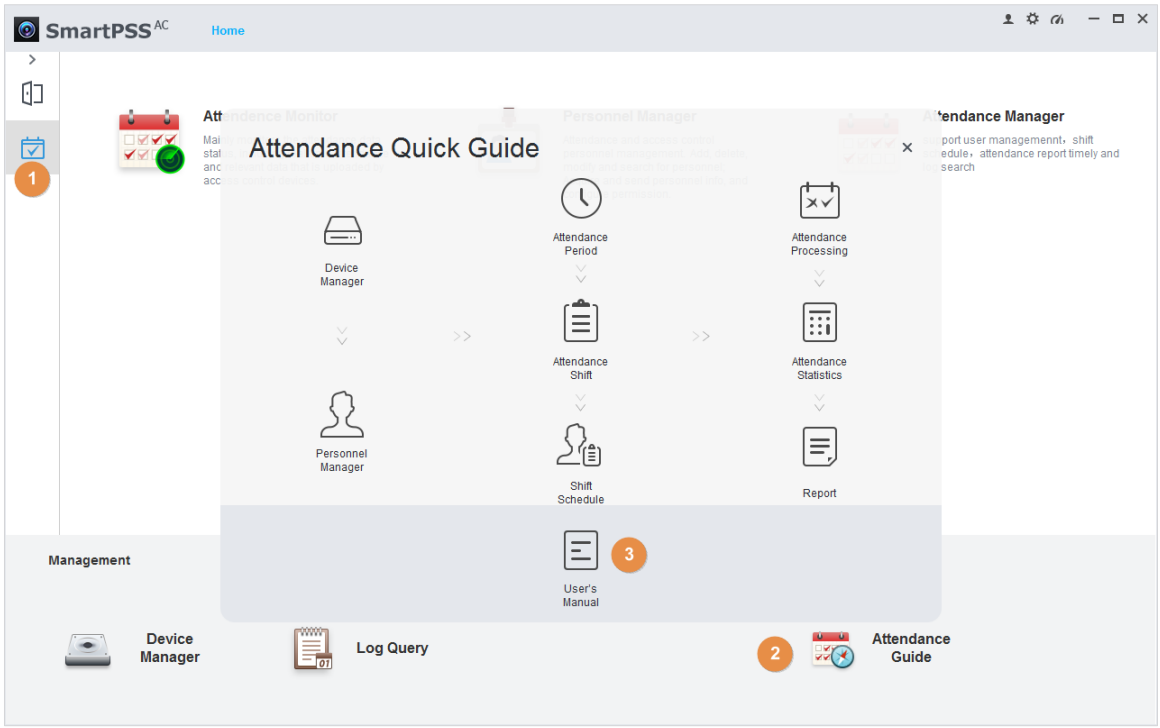
Para otras configuraciones tales como períodos de asistencia, turnos de asistencia, programación de personal, procesamiento de asistencia y estadísticas de asistencia, agregar feriados y configuraciones de asistencia, consulte el manual del usuario de SmartPSS AC.

Paso1 Inicie sesión en SmartPSS AC.

Paso2 Haga clic en  en el menú de la izquierda.

Paso3 Haga clic en **Guía de asistencia** en la esquina inferior derecha.

Figura 4-21 Ver el manual del usuario de SmartPSS AC



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.**

   Asegúrate de eso **Cara** está seleccionado en el modo de desbloqueo. Consulte "2.8.2 Desbloquear".

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 faciales 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.

Apéndice 1 Notas de comparación / grabación facial

Antes del registro

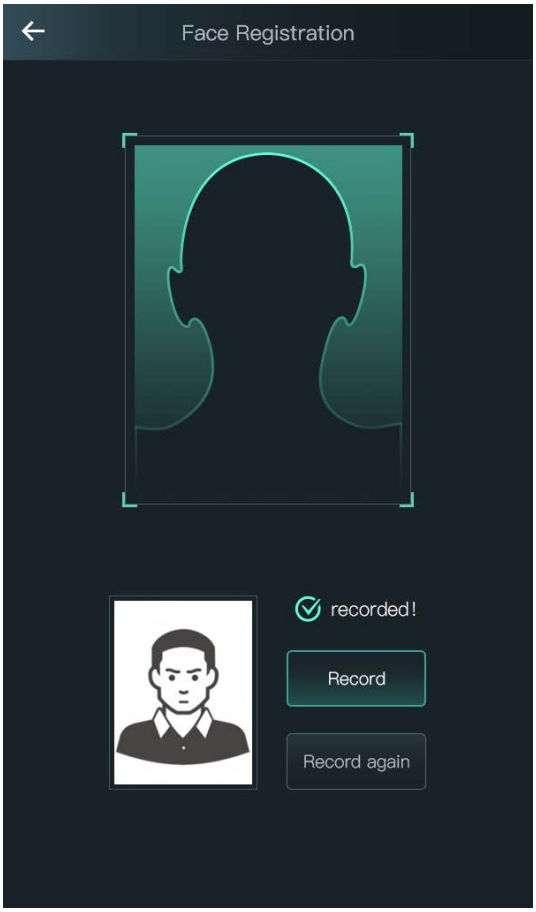
- Los anteojos, los sombreros y la barba pueden influir en el rendimiento del
- reconocimiento facial. No cubra sus cejas cuando use sombreros.
- No cambie mucho el estilo de su barba si va a utilizar el dispositivo; de lo contrario, el reconocimiento facial podría fallar.
- Mantén tu cara limpia.
-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

Durante el registro

Puede registrar rostros a través del controlador de acceso o mediante la plataforma. Para registrarse a través de la plataforma, consulte el manual de usuario de la plataforma.

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

Apéndice Figura 1-1 Registro



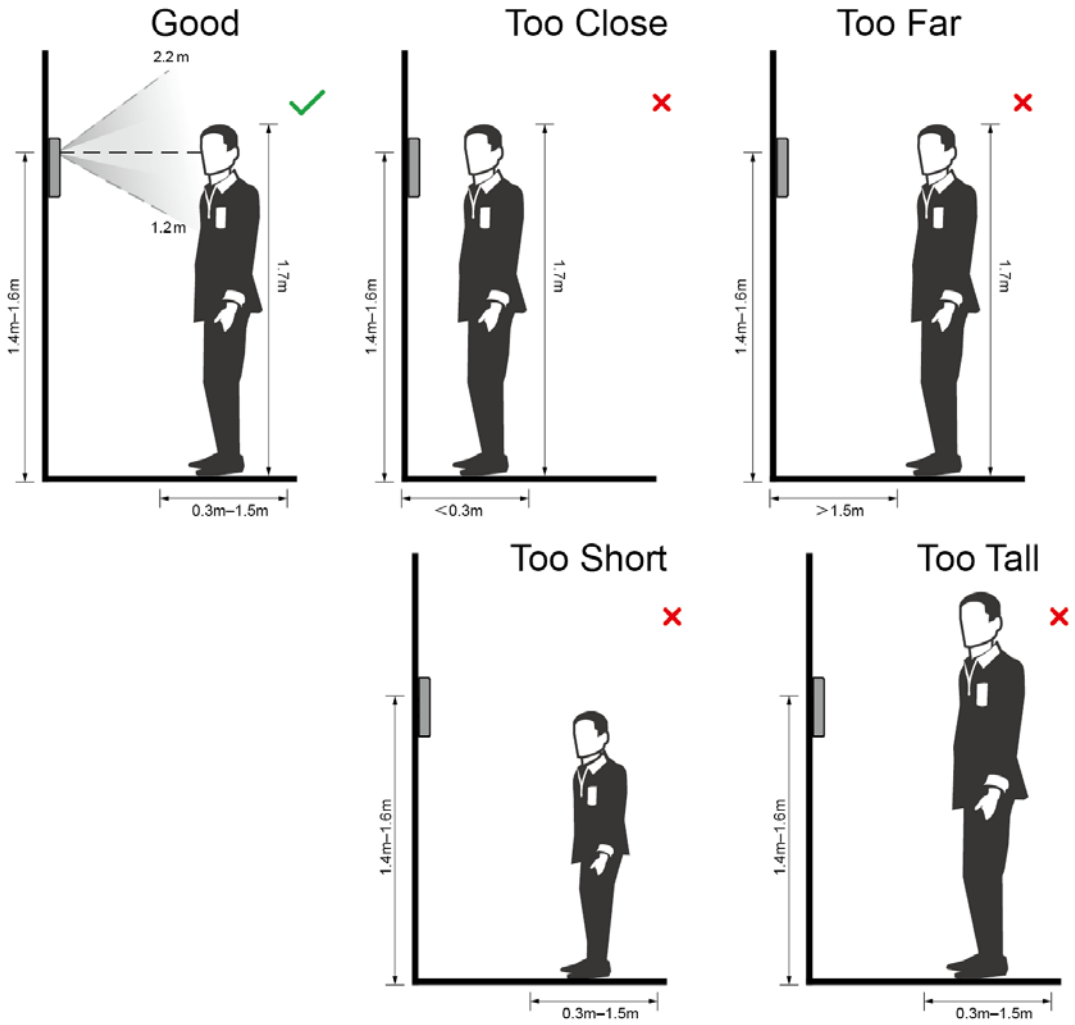
- No sacuda la cabeza o el cuerpo, de lo contrario, el registro podría fallar.

- Evite que aparezcan dos caras en el cuadro de captura al mismo tiempo.

Posición de la cara

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

Apéndice Figura 1-2 Posición adecuada de la cara

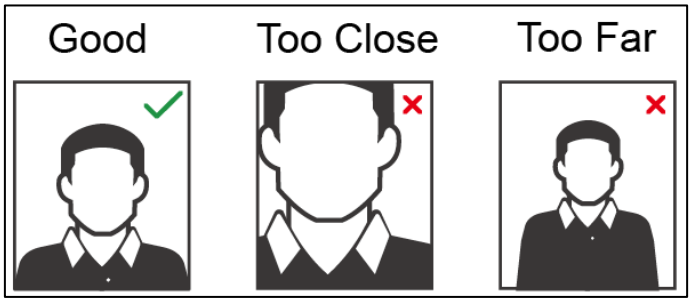


Requisitos de caras

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

Apéndice Figura 1-3 Posición de la cabeza

Apéndice Figura 1-4 Distancia de la cara



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

Apéndice 2 Recomendaciones de ciberseguridad

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

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

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Actualice el firmware y el software cliente a tiempo

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

Es bueno tener "recomendaciones para mejorar la seguridad de la red de su dispositivo:

1. Protección física

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

2. Cambie las contraseñas con regularidad

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

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

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

4. Habilite el bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilite HTTPS

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

7. Enlace de dirección MAC

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

8. Asignar cuentas y privilegios de forma razonable

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

9. Deshabilite los servicios innecesarios y elija modos seguros

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

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

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

10. Transmisión encriptada de audio y video

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

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

11. Auditoría segura

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

12. Registro de red

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

13. Construya un entorno de red seguro

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

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

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