Controlador de acceso de reconocimiento facial

Manual de usuario

V1.0.1

Prefacio

General

Este manual presenta la instalación y el funcionamiento básico del controlador de acceso de reconocimiento facial (en adelante denominado "controlador de acceso").

Las instrucciones de seguridad

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

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

Revisión histórica

Versión	Revisión de contenido	Fecha de lanzamiento
V1.0.0	Primer lanzamiento	Agosto 2019

Sobre el manual

- El manual es solo de referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por las operaciones que no cumplan con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y reglamentos de las regiones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio al cliente para obtener el último programa y la documentación complementaria.
- Todavía puede haber una desviación en los datos técnicos, la descripción de las funciones y operaciones, o errores en la impresión. Si hay 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 compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, póngase en contacto con el proveedor o servicio al cliente si se produce algún problema al utilizar el dispositivo.
- Si existe alguna incertidumbre o controversia, consulte nuestra explicación final.

Importantes salvaguardas y advertencias

Este capítulo describe los contenidos que cubren el manejo adecuado del controlador de acceso, la prevención de riesgos y la prevención de daños a la propiedad. Lea este contenido detenidamente antes de usar el controlador de acceso, cumpla con ellos cuando lo use y guárdelo para futuras referencias.

Requisito de operación

- No coloque ni instale el controlador de acceso en un lugar expuesto a la luz solar o cerca de la 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 potencia.
- No desmonte el controlador de acceso.
- Transporte, use y almacene el controlador de acceso bajo las condiciones de humedad y temperatura permitidas.

Seguridad ELECTRICA

- El uso incorrecto de la batería puede provocar incendios, explosiones o inflamaciones.
- Al reemplazar la batería, asegúrese de usar el mismo modelo.
- Utilice los cables de alimentación recomendados en la región y cumpla con la especificación de potencia nominal.
- Use el adaptador de corriente provisto con el controlador de acceso; de lo contrario, podría provocar lesiones personales y daños en el dispositivo.
- La fuente de alimentación debe cumplir con el requisito del estándar de seguridad de voltaje extra bajo (SELV) y suministrar energía con voltaje nominal que cumpla con el requisito de fuente de energía limitada de acuerdo con IEC60950-1. Tenga en cuenta que el requisito de la fuente de alimentación está sujeto a la etiqueta del dispositivo.
- Conecte el dispositivo (estructura tipo I) a la toma de corriente con toma de tierra de protección.
- El acoplador del aparato es un dispositivo de desconexión. Cuando use el acoplador, mantenga el ángulo para una fácil operación.

Tabla de contenido

1 Visión general

1.1 Introducción

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

1,2 Caracteristicas

- Admite desbloqueo facial, desbloqueo de tarjeta IC, desbloqueo de huellas digitales y desbloqueo de contraseña; desbloquear por período
- Con caja de detección de rostros; la cara más grande entre las caras que aparecen al mismo tiempo se reconoce primero; el tamaño máximo de la cara se puede configurar en la web
- Lente WDR gran angular de 2MP; con luz de llenado automático / manual
- Distancia de la cámara frontal: 0.3 m – 2.0 m; altura humana: 0.9 m – 2.4 m
- Con el algoritmo de reconocimiento facial, el terminal puede reconocer más de 360 posiciones en el rostro humano.
- Precisión de verificación facial> 99.5%; baja tasa de reconocimiento falso
- Soporte de reconocimiento de perfil; el ángulo del perfil es 0 ° –90 °
- Apoyo a la detección de vida
- Apoye la alarma de coacción y la alarma de manipulación
- Admite usuarios generales, usuarios de coacción, usuarios de patrulla, usuarios de listas negras, usuarios VIP, usuarios invitados y usuarios discapacitados
- Con 4 modos de visualización de estado de desbloqueo y varios modos de aviso de voz

1.3 Dimensión y Componente

El controlador de acceso tiene dos tipos: controladores de acceso de 7 pulgadas y 10 pulgadas. Consulte la Figura 1-1 a la Figura 1-4.

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

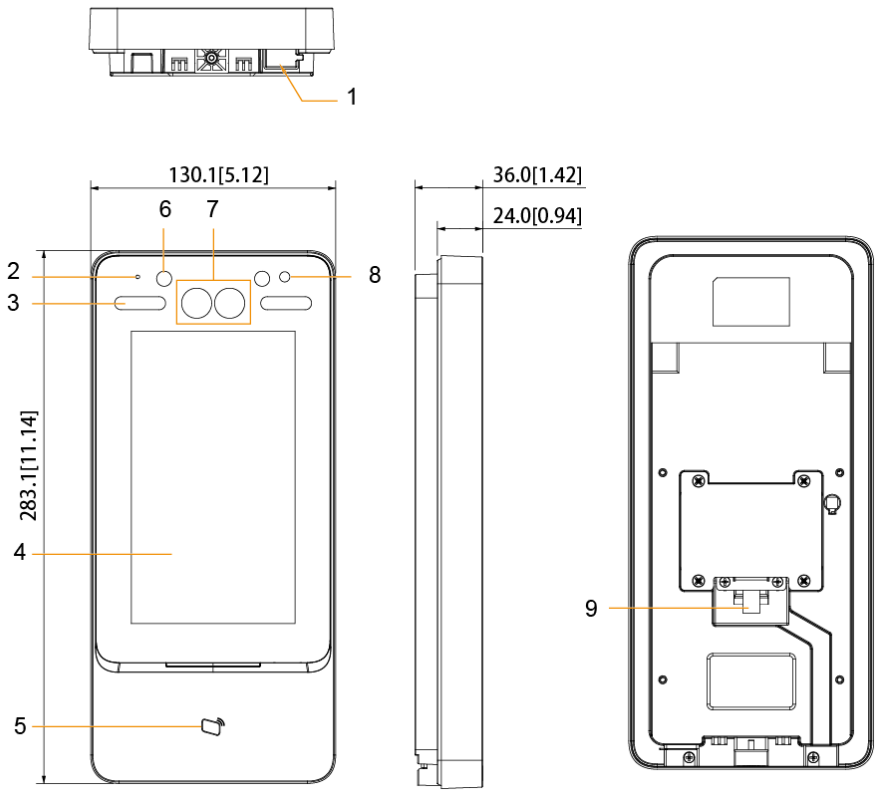


Table 1-1 Com ponent d escription (1)

No. Nombre		No.	Nombre
1	Puerto USB	6 6	Luz IR
2	MIC	7 7	Cámara doble
3	Luz de relleno blanco	8	Fototransistor
4 4	Monitor	9 9	Entrada de cable
5 5	Área de deslizamiento de tarjeta -		-

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

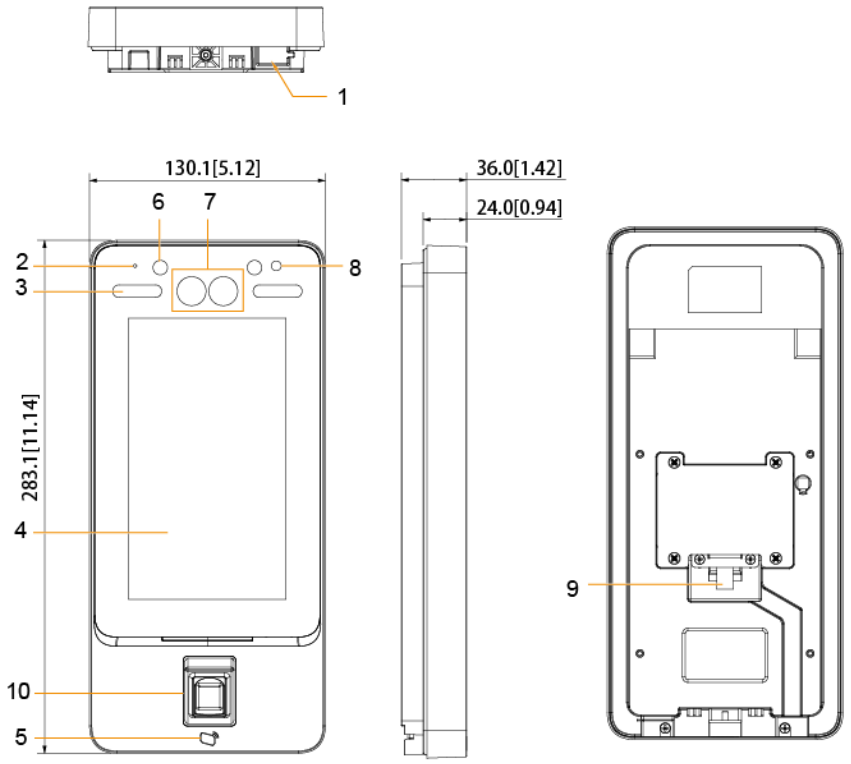


Table 1-2 Com pan de maíz nt descripción (2)

No.	Nombre	No.	Nombre
1	Puerto USB	6 6	Luz IR
2	MIC	7 7	Cámara doble
3	Luz de relleno blanco	8	Fototransistor
4 4	Monitor	9 9	Entrada de cable
5 5	Área de deslizamiento de tarjeta	10	Sensor de huellas digitales

Dimensiones y componentes (3) (mm [pulgadas]) Figura 1-3

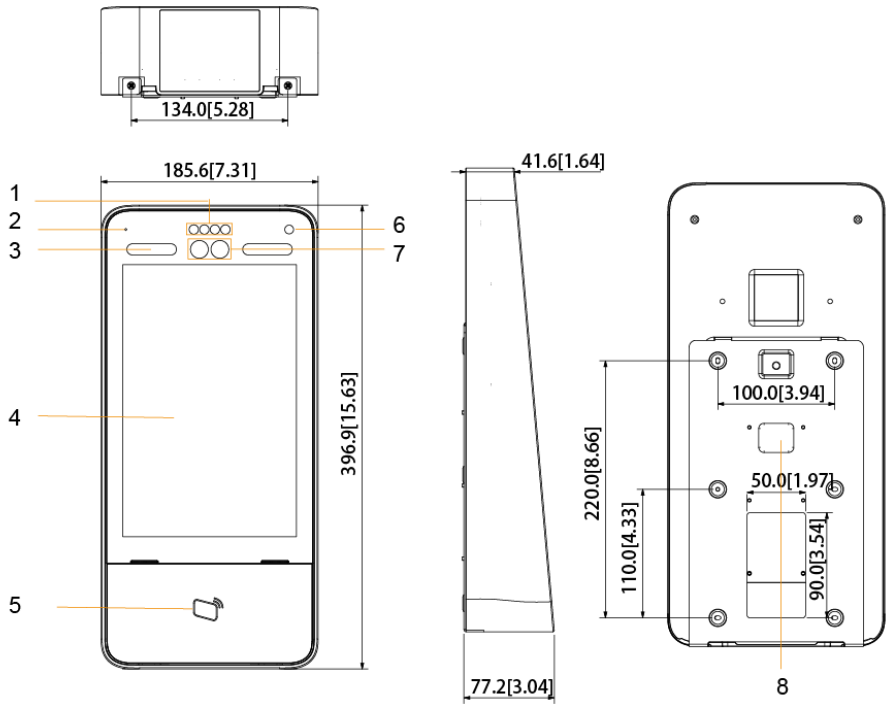


Table 1-3 Com pan de maíz nt descripción (3)

No.	Nombre	No.	Nombre
1	Luz IR	6 6	Fototransistor
2	MIC	7 7	Cámara doble
3	Luz de relleno blanco	8	Entrada de cable
4 4	Monitor	9 9	-
5 5	Área de deslizamiento de tarjeta 10		-

Dimensiones y componentes (4) (mm [pulgadas]) Figura 1-4

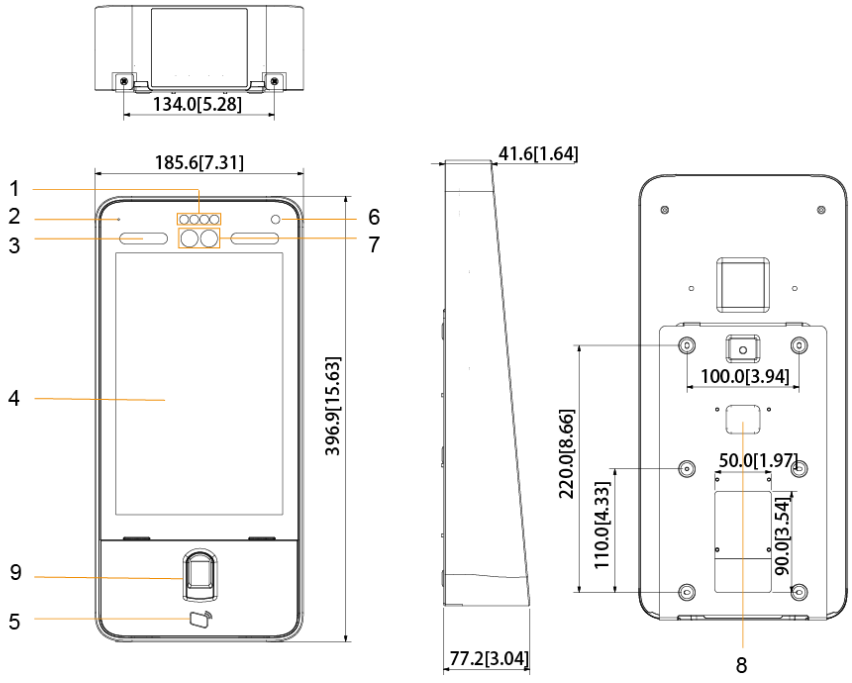


Tabla 1-4 Com pan de maíz nt descripción (4)

No.	Nombre	No.	Nombre
1	Luz IR	6 6	Fototransistor
2	MIC	7 7	Cámara doble
3	Luz de relleno blanco	8	Entrada de cable
4 4	Monitor	9 9	Sensor de huellas dactilares
5 5	Área de deslizamiento de tarjeta 10		-

2 Instalación

2.1 Conexiones de cable

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

Tabla 2-1 Descripción del puerto

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

Puerto	Color del cable Nombre del cable		Descripción
CON2	blanco y rojo	ALARM1_NO	La alarma 1 normalmente abre el puerto de salida.
	Blanco y naranja	ALARM1_COM	Alarma 1 puerto de salida común.
	blanco y azul	ALARM2_NO	La alarma 2 normalmente abre el puerto de salida.
	Blanco y gris	ALARM2_COM	Alarma 2 puerto de salida común.
	Blanco y verde	GND	Conectado al puerto GND común.
	Blanco marrón	ALARMA1	Alarma 1 puerto de entrada.
	Blanco y amarillo	GND	Conectado al puerto GND común.
	Blanco y morado	ALARMA2	Puerto de entrada de alarma 2.
CON3	Negro Y Rojo	RX	Puerto de recepción RS-232.
	Negro y naranja	TX	Puerto de envío RS-232.
	Negro y azul	GND	Conectado al puerto GND común.
	Negro y gris	SR1	Utilizado para la detección de contacto de puerta.
	Negro y verde	PUSH1	Botón de apertura de puerta de puerta No.1
	Negro y marrón	DOOR1_COM	Puerto común de control de bloqueo.
	Negro y amarillo	PUERTA1_NO	El control de bloqueo normalmente abre el puerto.
	Negro y morado	DOOR1_NC	Control de bloqueo puerto normalmente cerrado.

2.2 Instalación

Los métodos de instalación de todos los controladores son los mismos. Asegúrese de que la distancia entre la lente y el suelo sea de 1,4 metros. Ver Figura 2-1.

Figura 2-1 Altura de instalación

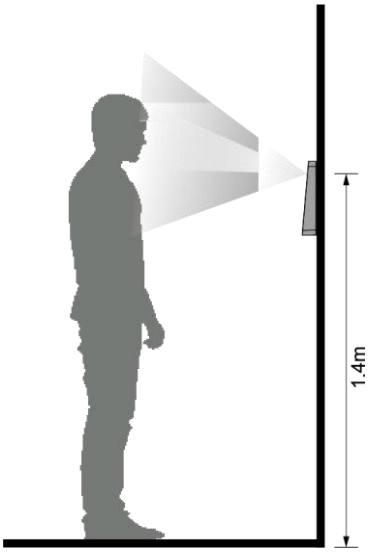
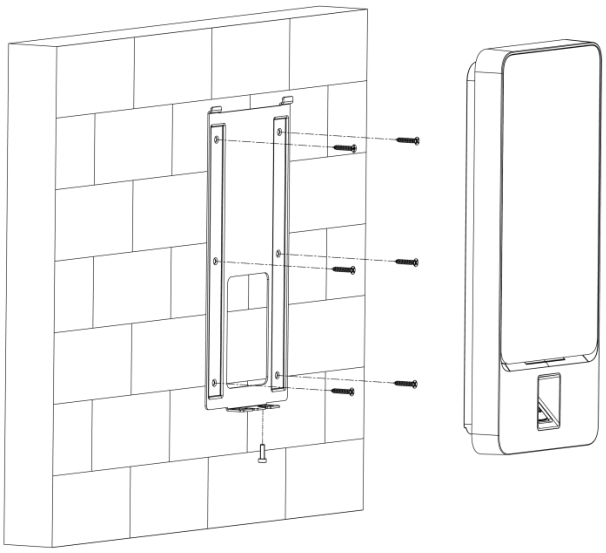


Figura 2-2 Diagrama de instalación



Procedimiento de instalación

Paso 1 Taladre siete agujeros (seis agujeros de instalación de soporte y una entrada de cable) en la pared según los agujeros en el soporte.

Paso 2 Fije el soporte en la pared instalando los tornillos de expansión en los seis soportes agujeros de instalación

Paso 3 Conecte los cables para el controlador de acceso.

Consulte "2.1 Conexiones de cable".

Paso 4 Cuelgue el controlador de acceso en el gancho del soporte.

Paso 5 Apriete los tornillos en la parte inferior del controlador de acceso.

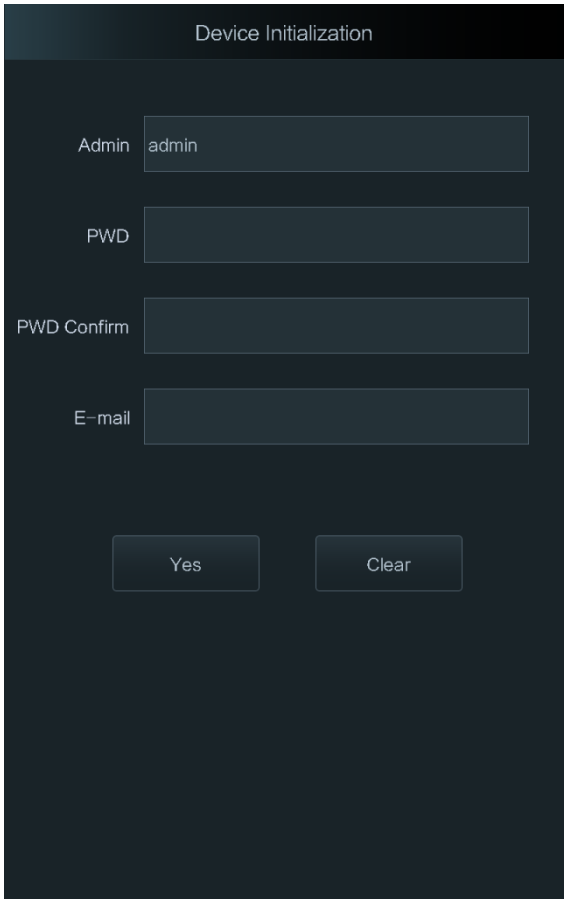
Paso 6 La instalación está completa.

3 Operación del sistema

3.1 Inicialización

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

Figura 3-1 Inicialización



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

3.2 Interfaz de espera

Puede desbloquear la puerta a través de caras, contraseñas, tarjetas y huellas digitales. Ver tabla 3-1.

Si no hay operaciones en 30 segundos, el controlador de acceso pasará al modo de espera.

Figura 3-2 Página de inicio

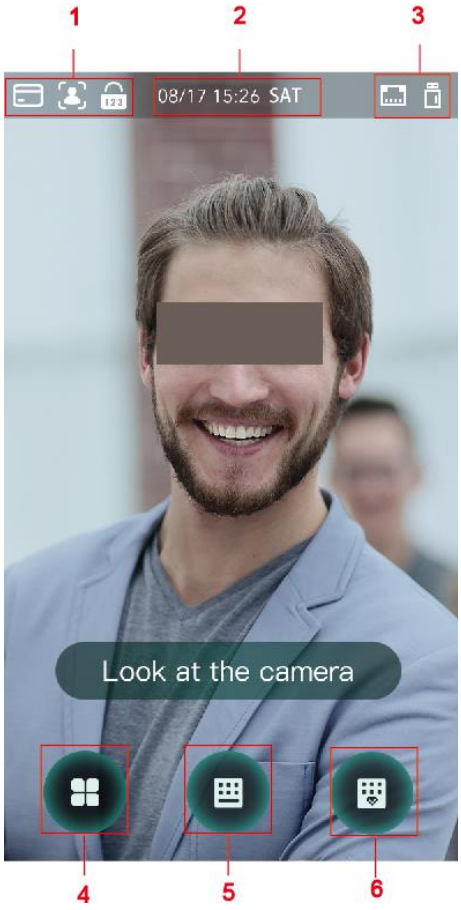


Tabla 3-1 Descripción de la página de inicio

No.	Descripción
1	Métodos de desbloqueo: tarjeta, cara, huella digital y contraseña. Cuando la tarjeta, la cara, la huella dactilar y la contraseña están configuradas como modo de desbloqueo, el icono de contraseña no se mostrará en la esquina superior izquierda del controlador de acceso. 2
	Fecha y hora: aquí se muestra la fecha y hora actuales. 3
	El estado de la red y el estado del USB se muestran aquí.
4 4	Icono del menú principal. Solo el administrador puede ingresar al menú principal. 5 5
	Icono de desbloqueo de contraseña. 6 6
	Icono de desbloqueo de contraseña de administrador.

3,3 Métodos de desbloqueo

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

3.3.1 Tarjetas

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

3.3.2 Cara

Asegúrese de que su rostro esté centrado en el marco de reconocimiento de rostros, y luego puede desbloquear la puerta.

3.3.3 Huellas digitales

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

3.3.4 Contraseñas de usuario

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

Paso 1 Grifo  en la página de inicio.

Paso 2 Ingrese la ID de usuario y luego toque  .

Paso 3 Ingrese la contraseña de usuario y luego toque  .

La puerta está desbloqueada.

3.3.5 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 niveles de usuario, modos de desbloqueo, períodos, planes de vacaciones y anti-passback.

La contraseña de administrador no se puede usar cuando se selecciona NC en "3.6.1.5 Periodo NC".

Paso 1 Grifo  en la página de inicio.

Paso 2 Grifo **Por favor, introduzca el administrador PWD.**

Paso 3 Ingrese la contraseña de administrador y luego toque  .

La puerta está desbloqueada.

3.4 Menú principal

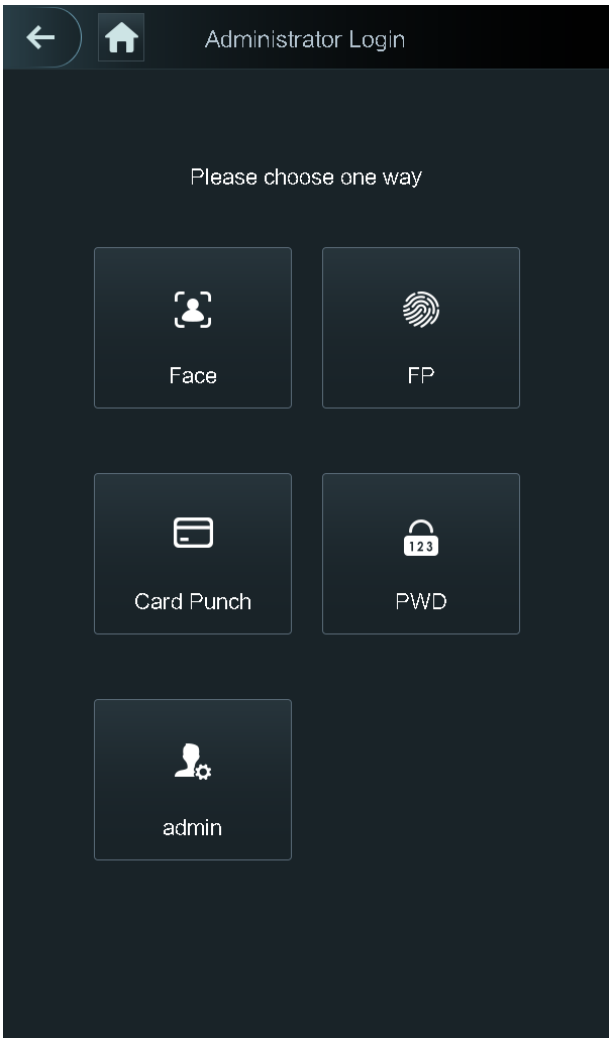
Los administradores pueden agregar usuarios de diferentes niveles, establecer parámetros relacionados con el acceso, hacer la configuración de la red, ver registros de acceso e información del sistema, y más en el menú principal.

Paso 1 Grifo  en la interfaz de espera.

los **Inicio de sesión de administrador** Se muestra la interfaz.

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

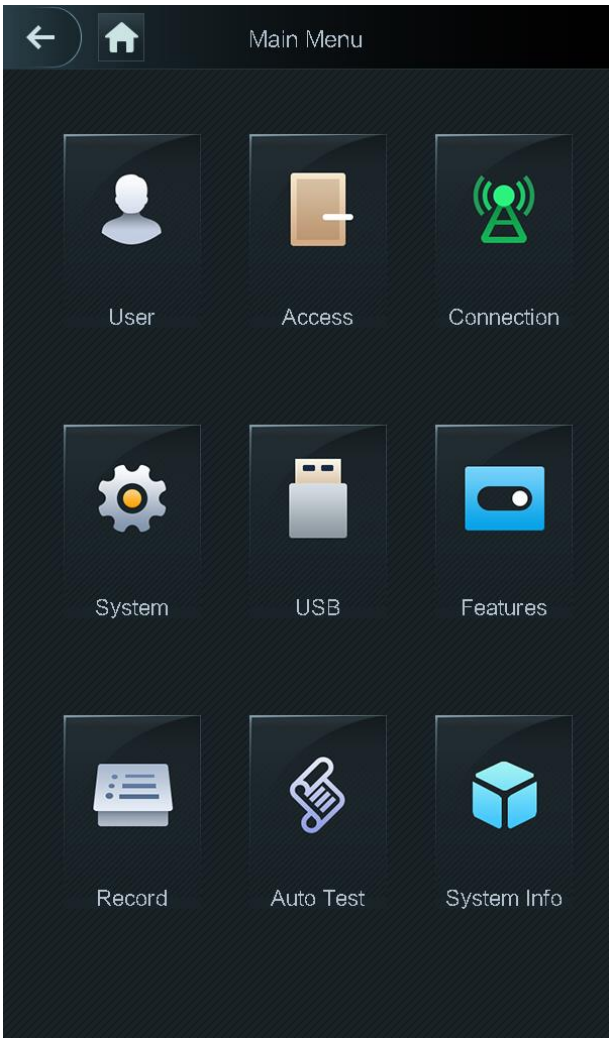
Figura 3-3nicio de sesión del administrador



Paso 2 Seleccione un método de ingreso al menú principal.

Se muestra la interfaz del menú principal.

Figura 3-4 Menú principal



3.5 Gestión de usuarios

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

3.5.1 Agregar nuevos usuarios

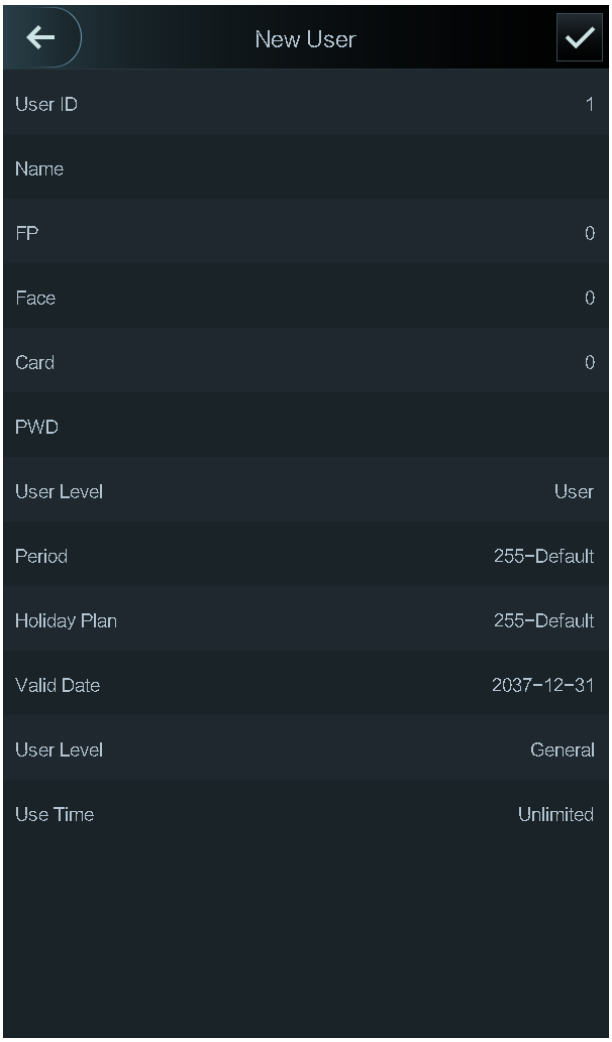
Puede agregar nuevos usuarios ingresando ID de usuario, nombres, importando huellas digitales, imágenes faciales, tarjetas, contraseñas, seleccionando niveles de usuario y más.

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

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

los **Información de nuevo usuario** Se muestra la interfaz. Ver Figura 3-5.

usuario Figura 3-5 Información del nuevo



Paso 2 Configurar parámetros en la interfaz. Ver tabla 3-2.

Tabla 3-2 Descripción del nuevo parámetro de usuario

Parámetro	Descripción
ID de usuario	Puede ingresar ID de usuario. Los ID pueden ser números, cartas y sus combinaciones, y la longitud máxima de la ID es de 32 caracteres.
Nombre	Puede ingresar nombres con un máximo de 32 caracteres (incluidos números, símbolos y letras).
FP	Como máximo, se pueden registrar tres huellas digitales de un usuario, y una huella digital debe verificarse tres veces. Puede habilitar la función Duress FP debajo de cada huella digital, y solo una de las tres huellas digitales puede ser la huella digital de coacción. Las alarmas se activarán si se usa una huella dactilar forzada para desbloquear la puerta. No se recomienda que seleccione la primera huella digital como huella digital de coacción.
Cara	Asegúrese de que su cara esté centrada en el marco de captura de imágenes y que el controlador de acceso tomará una foto de la cara del nuevo usuario automáticamente. Para más detalles, vea el *Guía de inicio rápido*.

Parámetro	Descripción
Tarjeta	Puede registrar cinco tarjetas 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. Puedes 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 la tarjeta.
PWD	La contraseña de desbloqueo de la puerta. La longitud máxima de los dígitos de ID es 8.
Nivel de usuario	Puede seleccionar un nivel de usuario para nuevos usuarios. Hay dos opciones: • Usuario: los usuarios solo tienen autorización para desbloquear la puerta. • Administrador: los administradores no solo pueden desbloquear la puerta sino que también tienen autoridad 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 pueda desbloquear la puerta.
Plan de vacaciones	Puede establecer un plan de vacaciones en el que el usuario pueda desbloquear la puerta.
Fecha válida	Puede establecer un período durante el cual la información de desbloqueo del usuario es válida.
Nivel de usuario	Hay seis niveles: • General: los usuarios generales pueden desbloquear la puerta normalmente. • Lista negra: cuando los usuarios de la lista negra desbloquean la puerta, el personal de servicio obtener un aviso • Invitado: Los invitados pueden desbloquear la puerta en ciertos momentos. Una vez que exceden los tiempos máximos, no pueden volver a abrir la puerta. Patrulla: los usuarios de parole pueden • hacer un seguimiento de su asistencia, pero no tienen desbloquear autoridad. • VIP: cuando VIP abre la puerta, el personal de servicio recibirá un aviso. • Deshabilitar: cuando los deshabilitados desbloquean la puerta, habrá un retraso de 5 segundos antes de que se cierre la puerta.
Use Time	Cuando el nivel de usuario es Guest, puede establecer el número máximo de veces que El usuario puede desbloquear la puerta.

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

3.5.2 Visualización de información del usuario

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

3.6 Gestión de Acceso

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

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

3.6.1 Gestión del período

Puede establecer períodos, períodos de vacaciones, períodos del plan de vacaciones, períodos de puertas normalmente encendidos, períodos de puertas normalmente cerradas y períodos de verificación remota.

3.6.1.1 Configuración del período

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

3.6.1.2 Grupo de vacaciones

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

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

3.6.1.3 Plan de vacaciones

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

3.6.1.4 Sin período

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.

3.6.1.5 Periodo NC

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

3.6.1.6 Período de verificación remota

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

Debe habilitar el Período de verificación remota.

-  significa habilitado.
-  significa no habilitado.

3.6.2 Desbloqueo

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

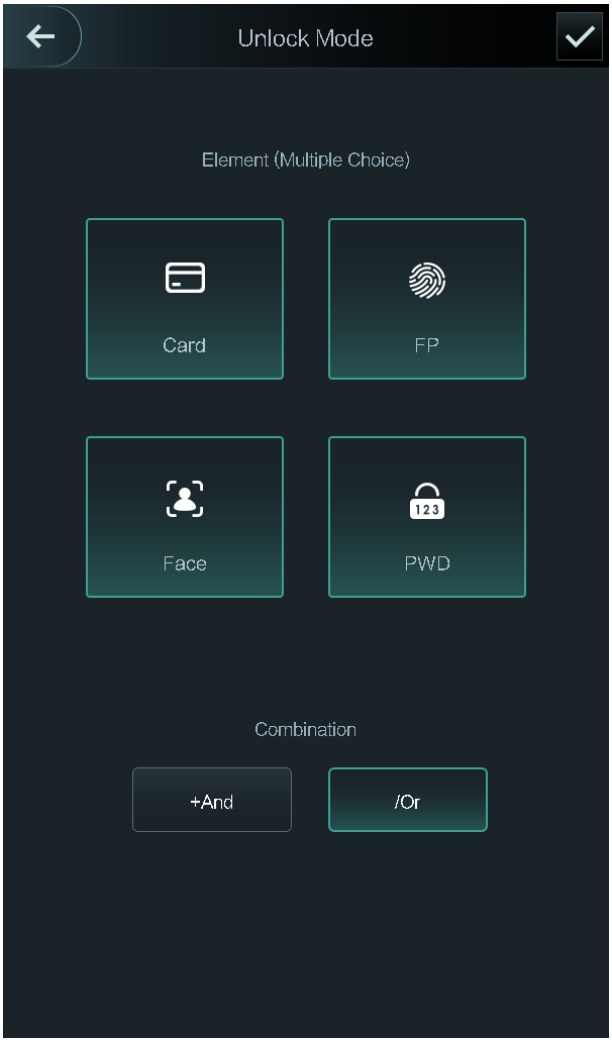
3.6.2.1 Modo de desbloqueo

Cuando el **Modo de desbloqueo** está activado, los usuarios pueden desbloquear mediante tarjetas, huellas digitales, caras, contraseñas o cualquiera de los métodos de desbloqueo.

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

los **Elemento (opción múltiple)** Se muestra la interfaz. Ver Figura 3-6.

3-6 Elemento (opción múltiple) Figura



Paso 2 Seleccione los modos de desbloqueo.

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

Paso 3 de combinación.

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

Paso 4 Grifo  para guardar la configuración.

Paso 5 Y luego el **Modo de desbloqueo** Se muestra la interfaz. Habilite el modo de desbloqueo.

-  significa habilitado.
-  significa no habilitado.

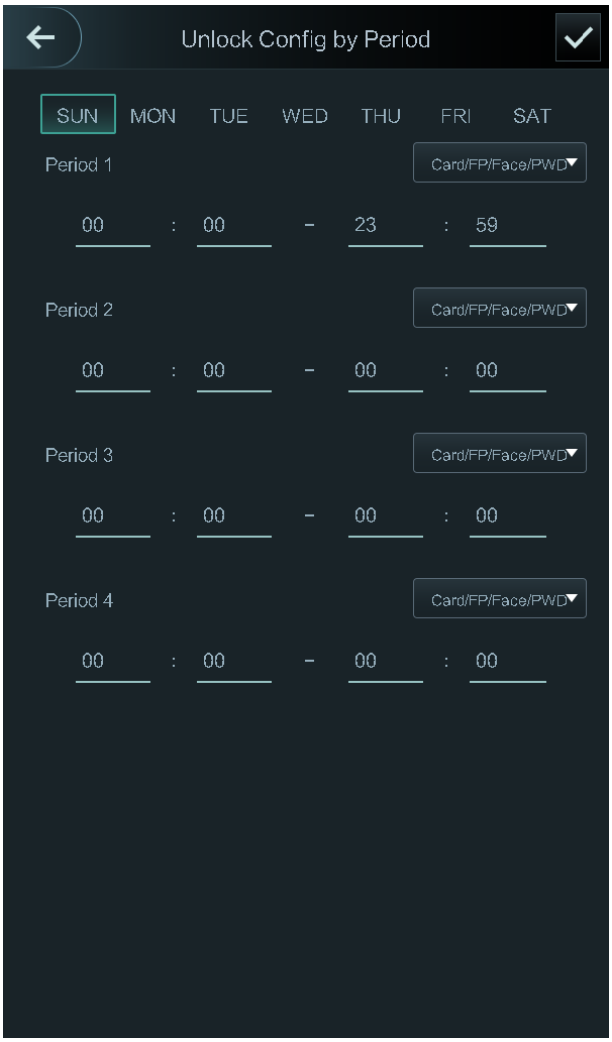
3.6.2.2 Desbloqueo por período

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

Paso 1 Seleccione Evaluar> Modo de desbloqueo> Desbloquear por período.

los **Desbloquear configuración por período** Se muestra la interfaz. Ver Figura 3-7.

Figura 3-7 Desbloqueo por período



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

Paso 3 Grifo  para guardar la configuración.

los **Modo de desbloqueo** Se muestra la interfaz. Habilite la

Paso 4 función Desbloquear por período.

-  significa habilitado.
-  significa no habilitado.

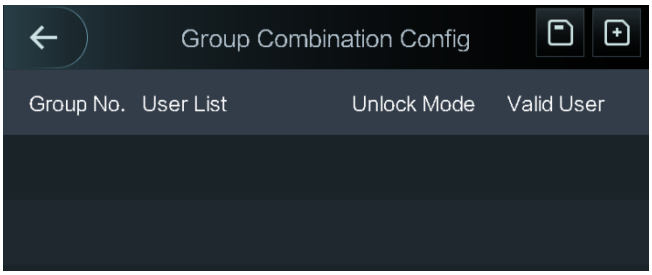
3.6.2.3 Combinación de grupo

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

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

los **Configuración de combinación de grupo** Se muestra la interfaz. Ver Figura 3-8.

Figura 3-8 Combinación de grupo



Paso 2 Grifo  para crear un grupo

los **Añadir grupo** Se muestra la interfaz. Ver Figura 3-9.

Figura 3-9 Agregar un grupo

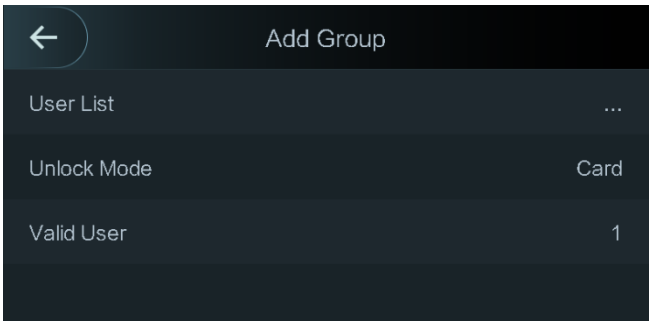


Tabla 3-3 Parámetros de grupo

Parámetro	Descripción
Lista de usuarios	Agregue usuarios al grupo recién creado. 1. Toque **Lista de usuarios.** los **Lista de usuarios** Se muestra la interfaz. 2. Toque  , y luego ingrese una identificación de usuario. 3. Toque  para guardar la configuración.
Modo de desbloqueo	Hay cuatro opciones: **Tarjeta, FP, PWD** y **Cara.**
Usuario válido	Los usuarios válidos son los que tienen autorización de desbloqueo. Las puertas se pueden desbloquear solo cuando el número de usuarios para desbloquear las puertas es igual al número de usuario válido. • Los usuarios válidos no pueden exceder el número total de usuarios en un grupo. • Si los usuarios válidos son iguales al número total de usuarios en un grupo, las puertas solo pueden ser desbloqueado por todos los usuarios del grupo. • Si los usuarios válidos son menores que el número total de usuarios en un grupo, puertas puede ser desbloqueado por cualquier usuario cuyo número sea igual al número de usuario válido.

Paso 3 Grifo  para volver a la interfaz anterior.

Paso 4 Grifo  para guardar la configuración.

Paso 5 Habilitar el **Combinación grupal.**

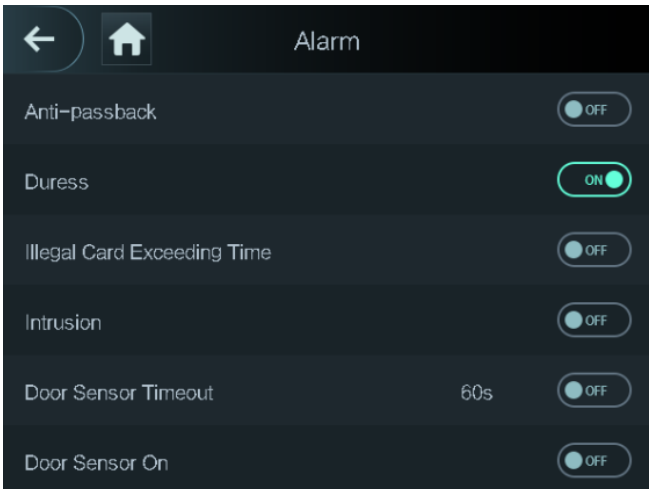
-  significa habilitado.
-  significa no habilitado.

3.6.3 Configuración de alarma

Los administradores pueden administrar la autorización de desbloqueo de los visitantes a través de la configuración de la alarma.

Seleccione **Acceso> Alarma.** Se muestra la interfaz de alarma. Ver Figura 3-10.

Figura 3-10 Alarma



-  significa habilitado.
-  significa no habilitado.

Tabla 3-4 Parámetros en la interfaz de alarma

Parámetro	Descripción
Anti-passback	• Si una persona abre la puerta con la identidad verificada por el acceso controlador, pero cuando la persona sale sin que el controlador de acceso verifique la identidad, se activará una alarma y la persona ya no tendrá autoridad para desbloquear la puerta. Si una persona ingresa a un edificio o una habitación sin deslizar la tarjeta, • y la persona deslizó la tarjeta para salir, entonces la persona ya no tendrá autoridad para abrir la puerta.
Coacción	Se activará una alarma cuando se use una tarjeta de coacción, una contraseña de coacción o una huella dactilar de coacción para desbloquear la puerta.
Tarjeta ilegal que excede el tiempo	Después de usar una tarjeta no autorizada para desbloquear la puerta más de 5 veces en 50 segundos, se activará una alarma.
Intrusión	Se activará una alarma de intrusión si se desbloquea una puerta sin liberar el contacto de la puerta.
Tiempo de espera del sensor de puerta	Se activará una alarma de tiempo de espera si el tiempo que un usuario tarda 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 si se activa la alarma de intrusión y la alarma de tiempo de espera del sensor de puerta.

3.6.4 Estado de la puerta

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

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

3.6.5 Tiempo de retención de bloqueo

Tiempo de retención de bloqueo es la duración en que se desbloquea la cerradura. Si el bloqueo se ha desbloqueado durante un período que excede la duración, el bloqueo se bloqueará automáticamente.

3.7 Red de comunicacion

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

3.7.1 Dirección IP

3.7.1.1 Configuración de IP

Configure una dirección IP para el controlador de acceso para que esté conectado a la red. Ver Figura 3-11 y Tabla 3-5.

Figura 3-11 Configuración de la dirección IP

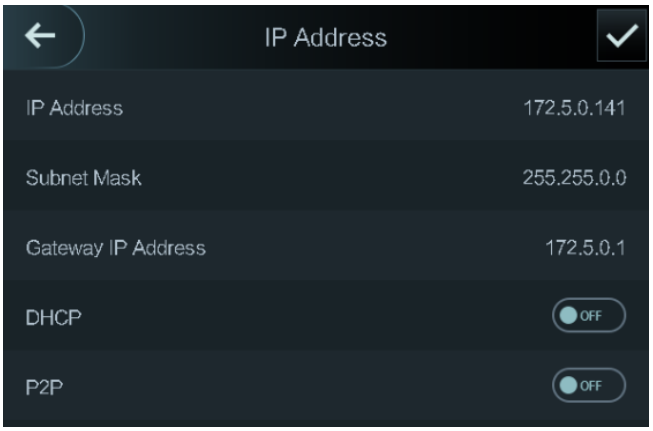


Tabla 3-5 Parámetros de configuración de IP

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

3.7.1.2 Registro activo

Al registrarse activamente, 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 a la autoridad de administración de la plataforma en caso de pérdida de datos causada por un mal funcionamiento.

Para el parámetro de registro activo, consulte la Tabla 3-6.

Tabla 3-6 Registro activo

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

3.7.1.3 Wi-Fi

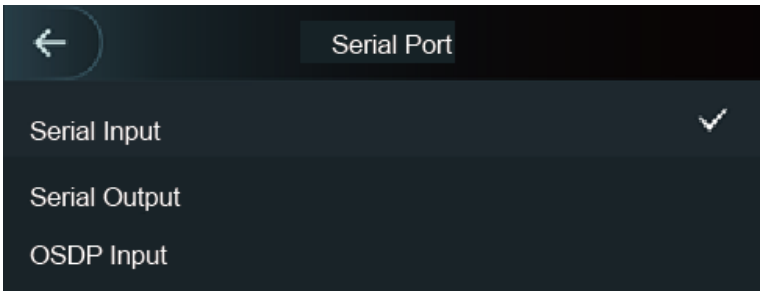
Puede conectar el controlador de acceso a la red a través de Wi-Fi si el controlador de acceso tiene la función Wi-Fi.

3.7.2 Configuración del puerto serie

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

Seleccione **Conexión> Puerto serie,** y luego el **Puerto serial** Se muestra la interfaz. Ver Figura 3-12.

Figura 3-12 Puerto serial



- Seleccione **Entrada en serie** cuando los dispositivos externos con funciones de lectura y escritura de tarjetas están conectados al controlador de acceso. **Entrada en serie** se selecciona para permitir que la información de la tarjeta de acceso se envíe al controlador de acceso y a la plataforma de administración.
- Para controladores de acceso con reconocimiento facial, reconocimiento de huellas digitales, lectura de tarjeta y funciones de escritura, si selecciona **Salida en serie,** El controlador de acceso enviará información de bloqueo / desbloqueo al controlador de acceso. Hay dos tipos de información de bloqueo / desbloqueo:
  - ID de usuario
  - Tarjeta no.
- Seleccione **Entrada OSDP** cuando el lector de tarjetas del protocolo OSDP está conectado al controlador de acceso. El controlador de acceso puede enviar información de la tarjeta a la plataforma de administración.

Este controlador de acceso no se puede conectar a otros dispositivos como lector de tarjetas.

3.7.3 Configuración de Wiegand

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

Seleccione **Conexión> Weigand,** y luego el **Weigand** Se muestra la interfaz. Ver Figura 3-13.

Figura 3-13 Weigand

- Seleccione **Entrada Weigand** cuando un mecanismo de deslizamiento de tarjeta externo está conectado al controlador de acceso.

- Seleccione **Salida Weigand** cuando el controlador de acceso funciona como un lector que se puede conectar al controlador. Ver Tabla 3-7.

Tabla 3-7 Salida de Weigand

Parámetro	Descripción
Tipo de salida Weigand	El tipo de salida Weigand determina el número de tarjeta o el dígito del número que puede ser reconocido por el controlador de acceso. • Weigand26, tres bytes, seis dígitos. • Weigand34, cuatro bytes, ocho dígitos. • Weigand66, ocho bytes, dieciséis dígitos.
Ancho de pulso	Puede establecer el ancho de pulso y el intervalo de pulso.
Intervalo de pulso	
Tipo de datos de salida	Puede seleccionar los tipos de datos de salida. • ID de usuario: si se selecciona ID de usuario, se generará la ID de usuario. • Número de tarjeta: si se selecciona el número de tarjeta, el número de tarjeta será salida.

Este controlador de acceso no se puede conectar a otros dispositivos como lector de tarjetas.

3.8 Sistema

3.8.1 Tiempo

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

- Cuando selecciona Network Time Protocol (NTP), primero debe habilitar la función NTP Check. 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.

3.8.2 Parámetro de cara

Figura 3-14 Parámetro de la cara

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

Tabla 3-8 Parámetro de cara

Nombre	Descripción
Umbral de reconocimiento facial	La precisión del reconocimiento facial se puede ajustar. Cuanto mayor sea el valor, mayor será la precisión.
Max. Ángulo de reconocimiento facial	Puede configurar el ángulo de disparo de los perfiles del panel de control. Cuanto mayor sea el valor, se reconocerá el rango más amplio de los perfiles.
Distancia pupilar	La distancia pupilar es el valor de píxel de la imagen entre los centros de las pupilas en 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 será el valor. Si un adulto está a 1.5 metros de la lente, el valor de la distancia pupilar puede estar entre 50 y 70.
Tiempo de espera de reconocimiento	Cuando una persona que no tiene la autoridad de acceso se para frente al controlador de acceso y se le reconoce el rostro, el controlador le indicará que el reconocimiento de rostro falló. El intervalo de solicitud se denomina tiempo de espera de reconocimiento.
Intervalo de reconocimiento	Cuando una persona que tiene la autoridad de acceso se para frente al controlador de acceso y se le reconoce el rostro, el controlador le indicará que el reconocimiento de rostro se haya realizado correctamente. El intervalo de solicitud es el intervalo de reconocimiento.
Umbral antifalsificación	Esta función evita que las personas desbloqueen imágenes de rostros humanos o modelos de rostros. Cuanto mayor sea el valor, más difíciles serán las imágenes faciales para desbloquear la puerta. El rango de valores recomendado es superior a 80.

3.8.3 Configuración del modo de luz de relleno

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

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

3.8.4 Configuración del brillo de la luz de relleno

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

3.8.5 Ajuste de volumen

Grifo  o  para ajustar el volumen.

3.8.6 Ajuste del brillo de la luz IR

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

3.8.7 Parámetro FP

Establezca el nivel de precisión de la huella digital. Cuanto mayor sea el nivel, menor será la tasa de reconocimiento falso.

3.8.8 Restaurar a la configuración de fábrica

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

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

- 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 retenidas.

3.8.9 Reiniciar

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

3.9 USB

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

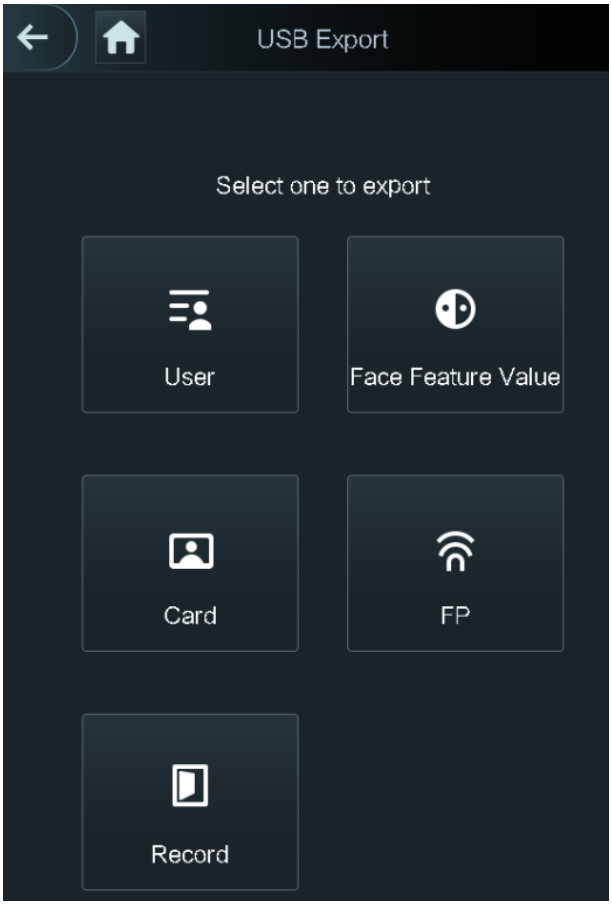
3.9.1 Exportación USB

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.

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

los **Exportación USB** Se muestra la interfaz. Ver Figura 3-15.

Figura 3-15 Exportación USB



Paso 2 Seleccione el tipo de datos que desea exportar.

Se muestra el mensaje Confirmar para exportar. Grifo **OKAY.**

Paso 3

Los datos exportados se guardarán en el USB.

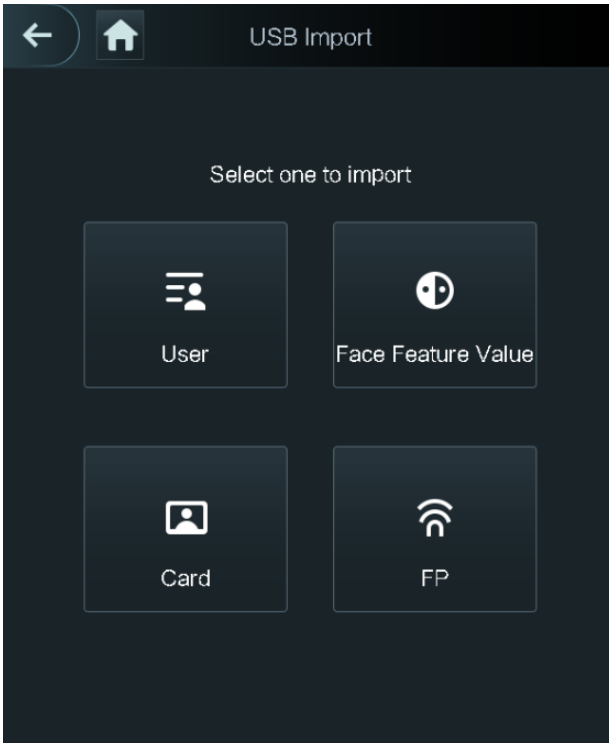
3.9.2 Importar USB

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

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

los **Importar USB** Se muestra la interfaz. Ver Figura 3-16.

Figura 3-16 Importar USB



Paso 2 Seleccione el tipo de datos que desea importar.

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

Paso 3

Los datos en el USB se importarán al controlador de acceso.

3.9.3 Actualización USB

Se puede usar USB para actualizar el sistema.

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

Paso 2 **Actualización USB.**

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

Paso 3

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

3.9.4 Características

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

Para obtener detalles de las funciones mencionadas, consulte la Figura 3-17 y la Tabla 3-9.

Figura 3-17 Caracteristicas

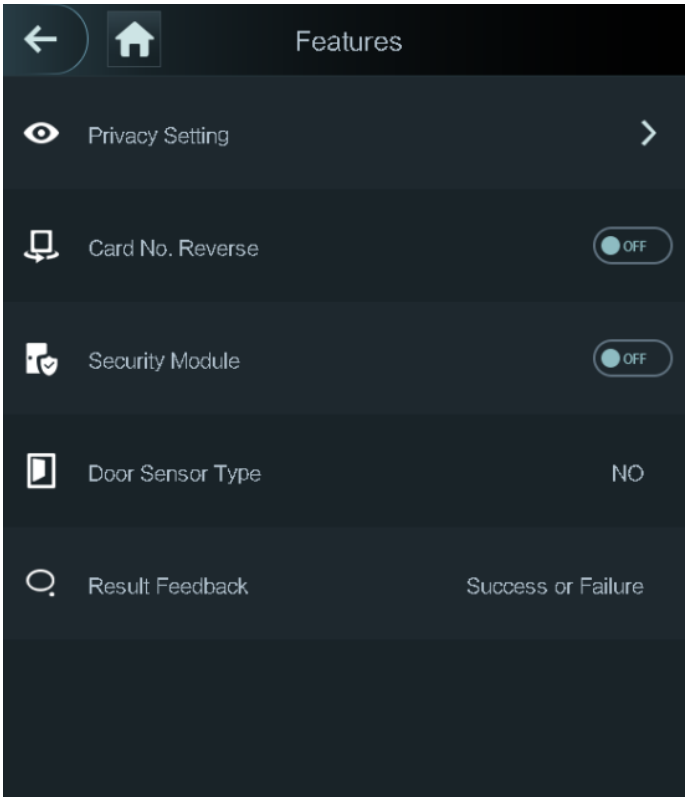


Tabla 3-9 Descripción de la característica

Parámetro	Descripción
Configuración de privacidad	Consulte "3.9.5 Configuración de privacidad" para más detalles.
N ° de tarjeta inversa	Si el lector de tarjetas de terceros necesita estar conectado al controlador de acceso a través del puerto de salida wiegand, debe habilitar la función Invertir número de tarjeta; de lo contrario, la comunicación entre el controlador de acceso y el lector de tarjetas de terceros puede fallar debido a la discrepancia de protocolo.
Módulo de seguridad	• Si el módulo de seguridad está habilitado, debe comprar el acceso Módulo de control de seguridad por separado. El módulo de seguridad necesita una fuente de alimentación separada para proporcionar energía. • Una vez que el módulo de seguridad está habilitado, el botón de salida, el control de bloqueo y el enlace contra incendios no será válido.
Tipo de sensor de puerta	Hay dos opciones: **NO** y **CAROLINA DEL NORTE.**
Feedback del resultado	Muestra si el desbloqueo tuvo éxito o falló.

3.9.5 Configuración de privacidad

Figura 3-18 Configuración de privacidad

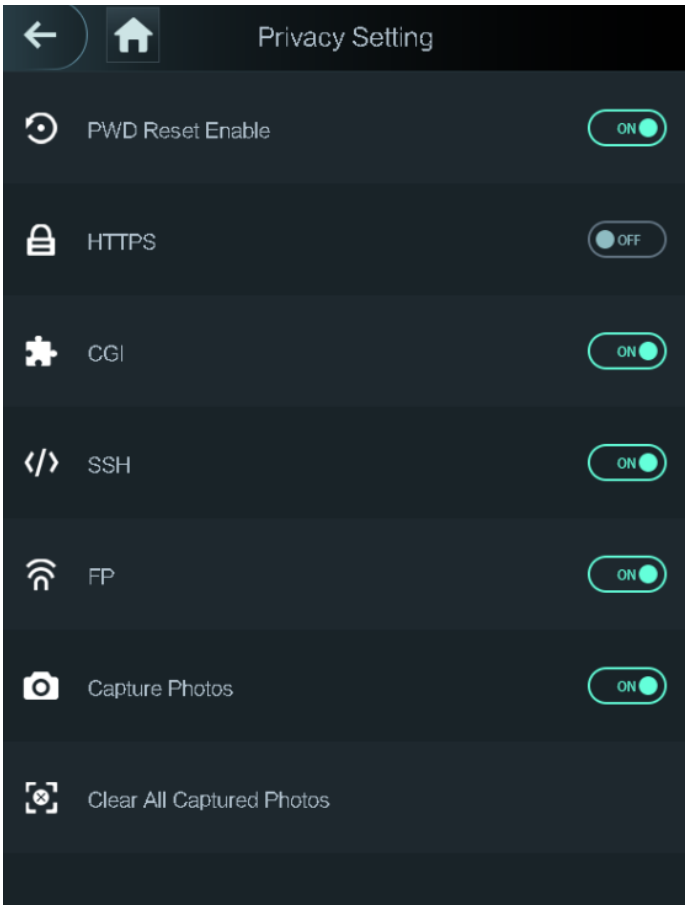


Tabla 3-10 Características

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

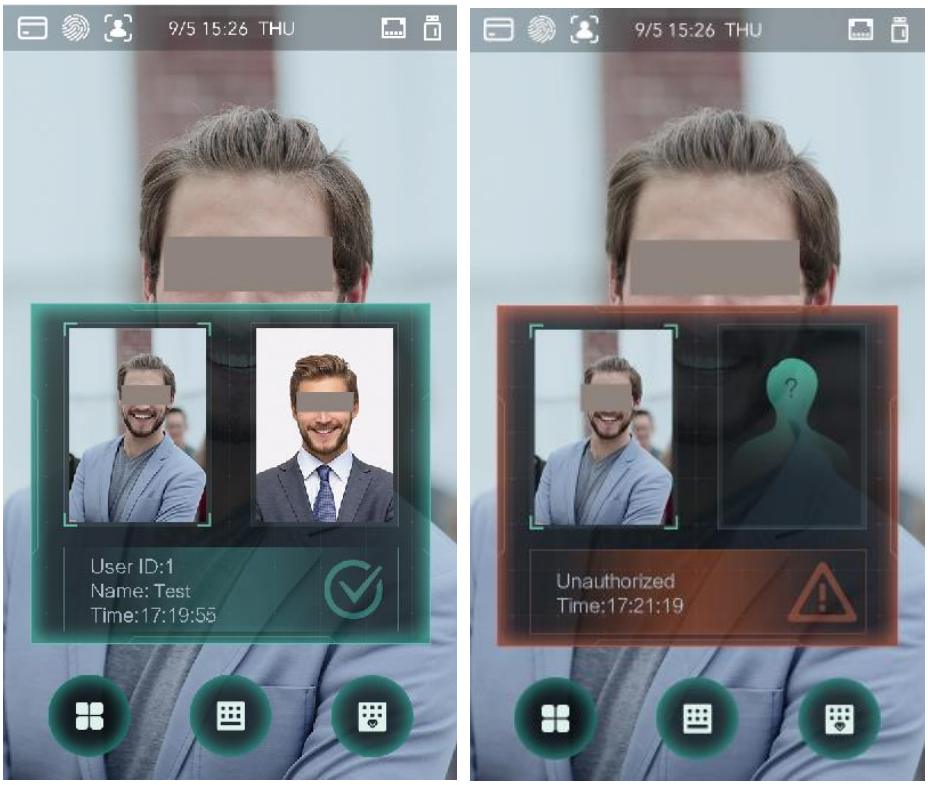
Parámetro	Descripción
FP	Si selecciona APAGADO para Huella digital (FP), la información de la huella digital de los usuarios no se mostrará cuando se graben las huellas digitales o cuando las usen para desbloquear la puerta.
Capturar foto	Si selecciona ACTIVADO, cuando un usuario desbloquea la puerta, la foto del usuario será tomado automáticamente Esta función está activada por defecto.
Borrar todas las fotos capturadas	Toque el icono y puede eliminar todas las fotos capturadas.

3.9.6 Comentarios de resultados

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

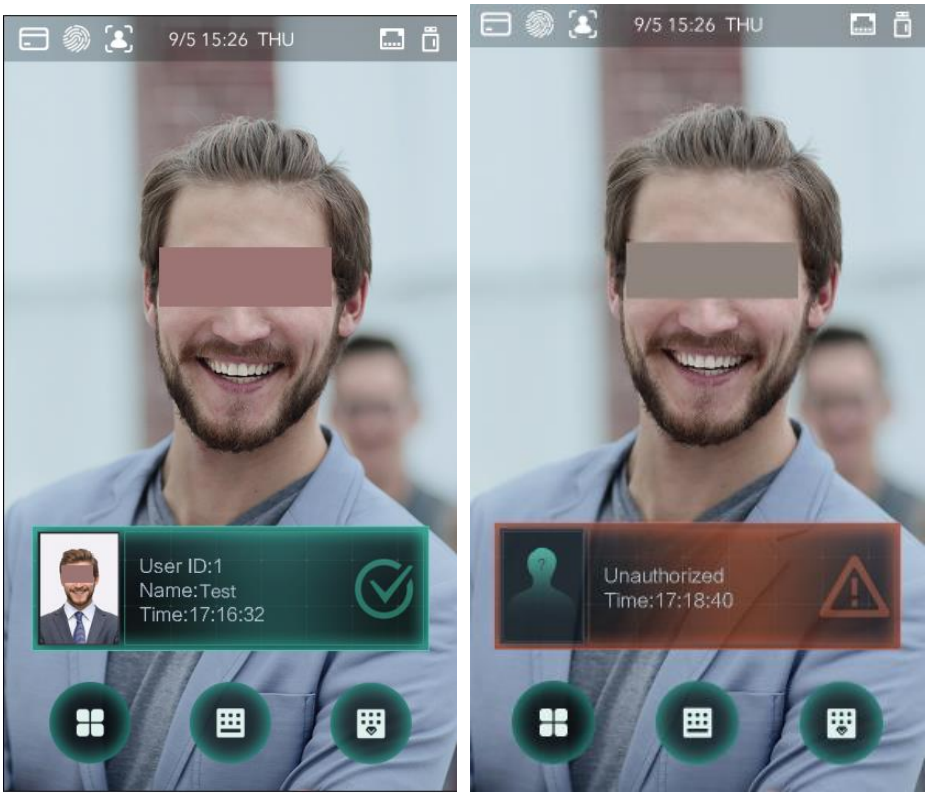
Modo 1

Figura 3-19 Modo 1



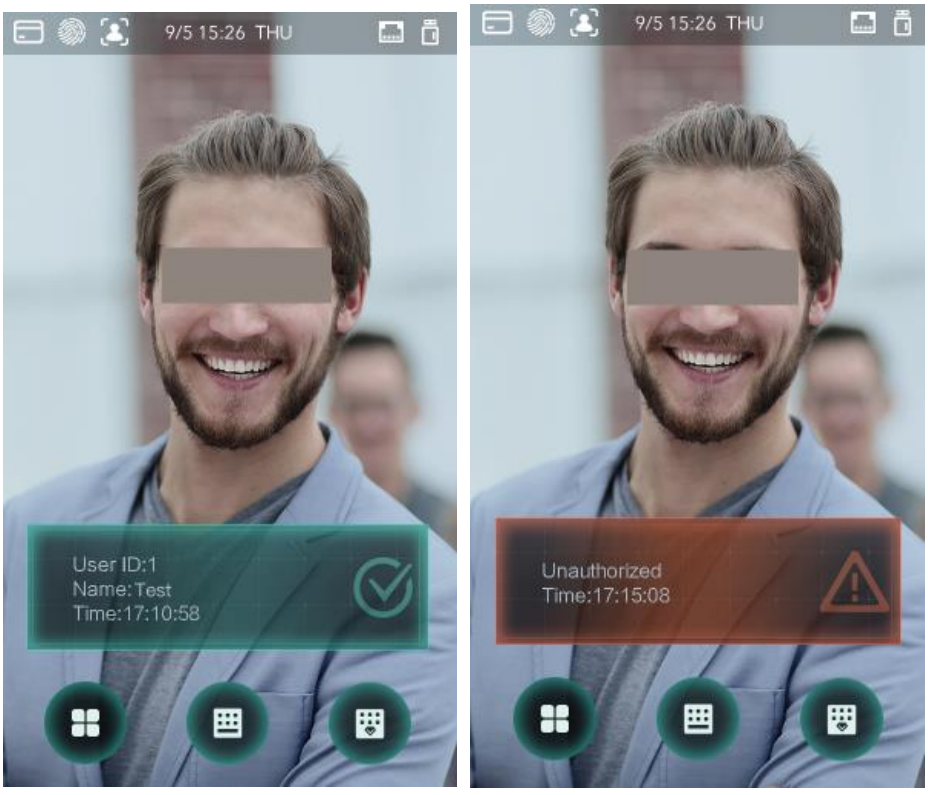
Modo 2

Figura 3-20 Modo 2



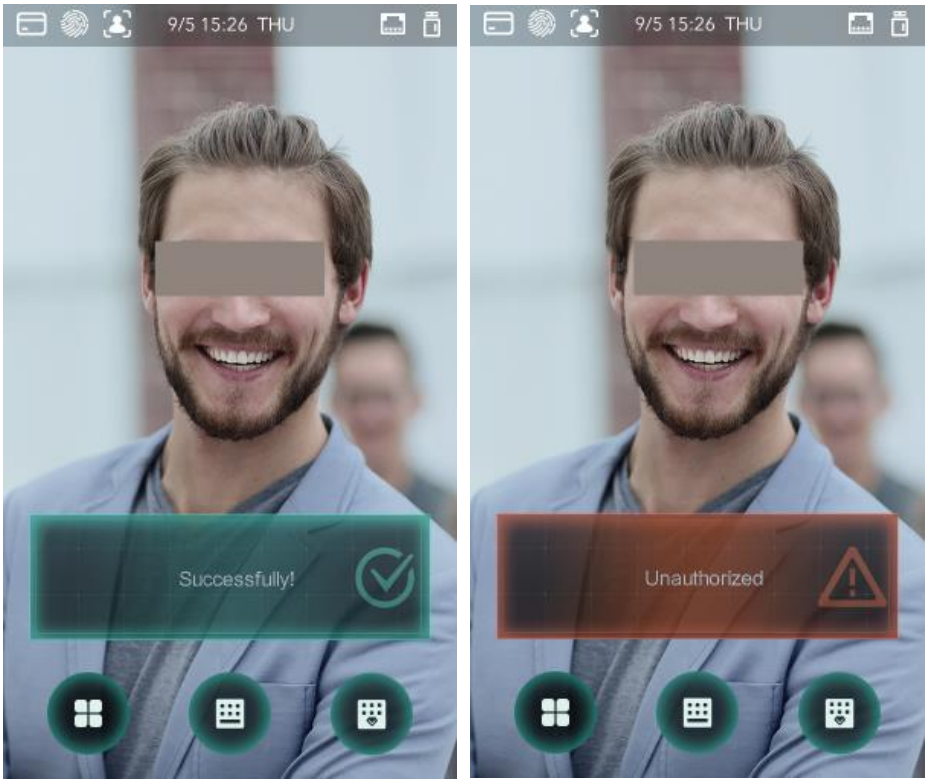
Modo 3

Figura 3-21. Modo 3



Modo 4

Figura 3-22. Modo 4



3.10 Grabar

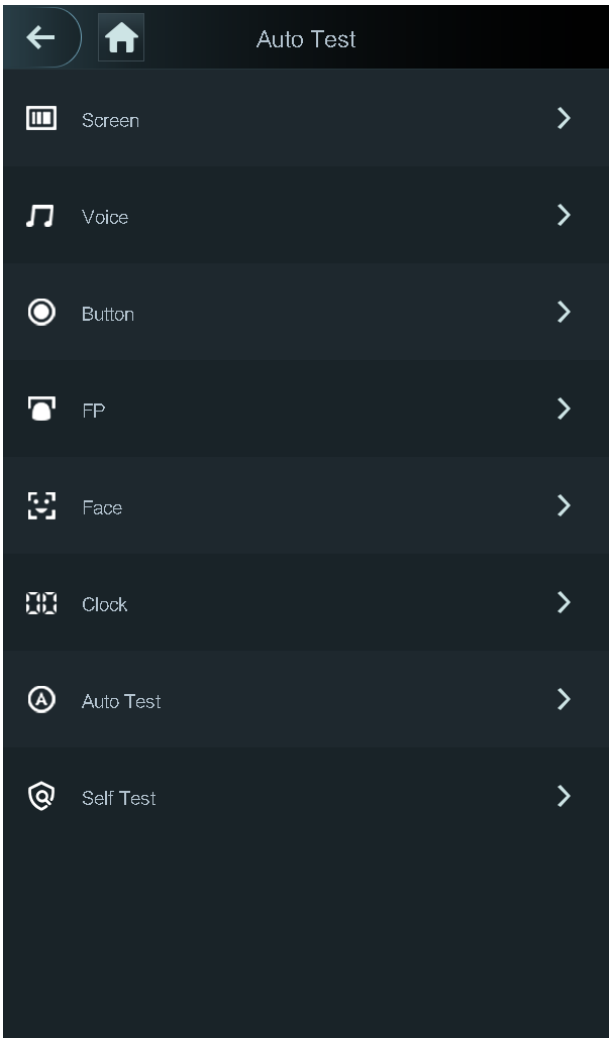
Puede consultar todos los registros de desbloqueo.

Figura 3-23. Buscar registros de perforación

3.11 Auto prueba

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

Figura 3-24 Auto prueba



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

3.12 Información del sistema

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

4 4 Operación web

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

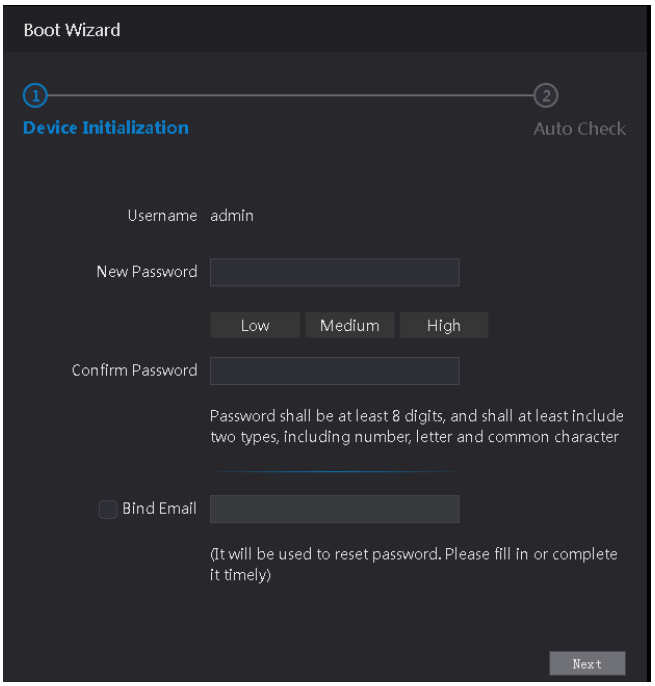
4.1 Inicialización

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

Paso 1 Abra el navegador web IE e ingrese la dirección IP (la dirección predeterminada es 192.168.1.108) del controlador de acceso en la barra de direcciones, y luego presione Entrar. los **Inicialización** Se muestra la interfaz. Ver Figura 4-1.

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

Figura 4-1 Inicialización

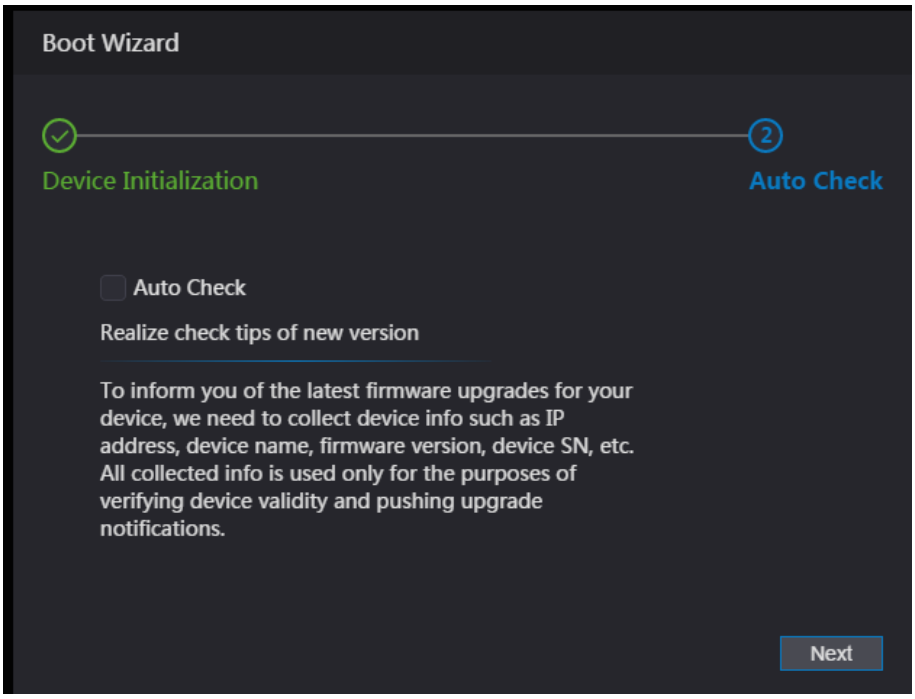


Paso 2 Ingrese la nueva contraseña, confirme la contraseña, ingrese una dirección de correo electrónico y luego toque **Próximo.**

- Por seguridad, mantenga la contraseña correctamente después de la inicialización y cambie la contraseña regularmente.
- La contraseña debe constar de 8 a 32 caracteres no 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 de acuerdo con el mensaje de seguridad de contraseña.
- Cuando necesite restablecer la contraseña de administrador escaneando el código QR, necesitará una dirección de correo electrónico para recibir el código de seguridad. Hacer clic **Próximo.**

Paso 3 los **Verificación automática** Se muestra la interfaz. Ver Figura 4-2.

automáticaFigura 4-2



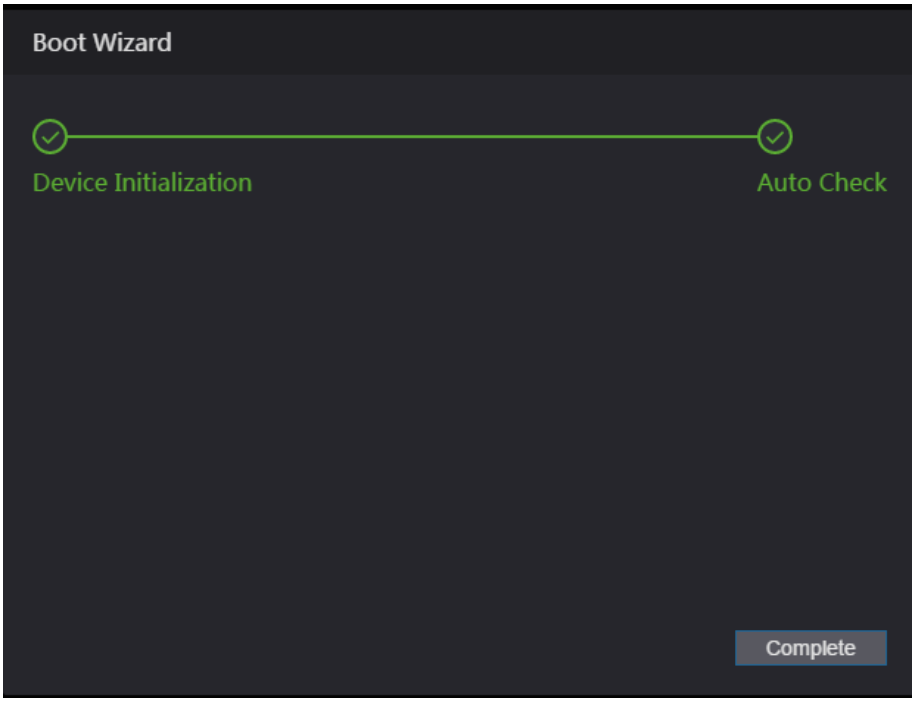
Paso 4 Puedes decidir si seleccionas **Verificación automática** o no.

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

Paso 5

La configuración ha finalizado. Ver Figura 4-3.

Figura 4-3 Configuración terminada



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

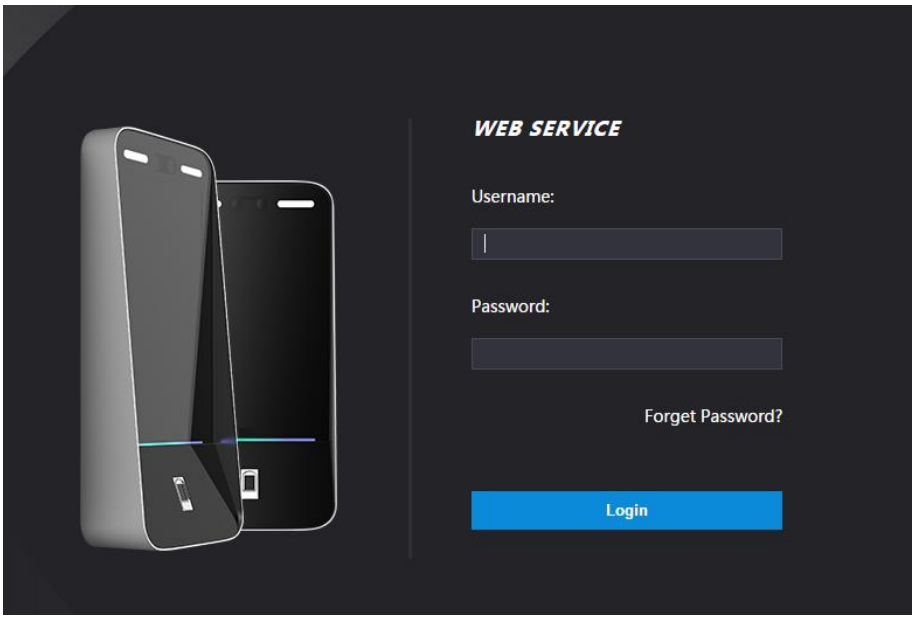
Se muestra la interfaz de inicio de sesión web.

4.2 4.2 Iniciar sesión

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

y presione **Entrar.**

sesión Figura 4-4



Paso 2 Ingrese el nombre de usuario y la contraseña.

- El nombre predeterminado del administrador es admin, y la contraseña es la contraseña de inicio de sesión después de inicializar el controlador de acceso. Modifique el administrador regularmente y guárdelo de manera adecuada por razones de seguridad.
- Si olvida la contraseña de inicio de sesión del administrador, puede hacer clic en **¿Se te olvidó tu contraseña?** para reiniciarlo. Consulte "4.3 Restablecer la contraseña". Hacer clic **Iniciar sesión.**

Paso 3

La interfaz web ha iniciado sesión.

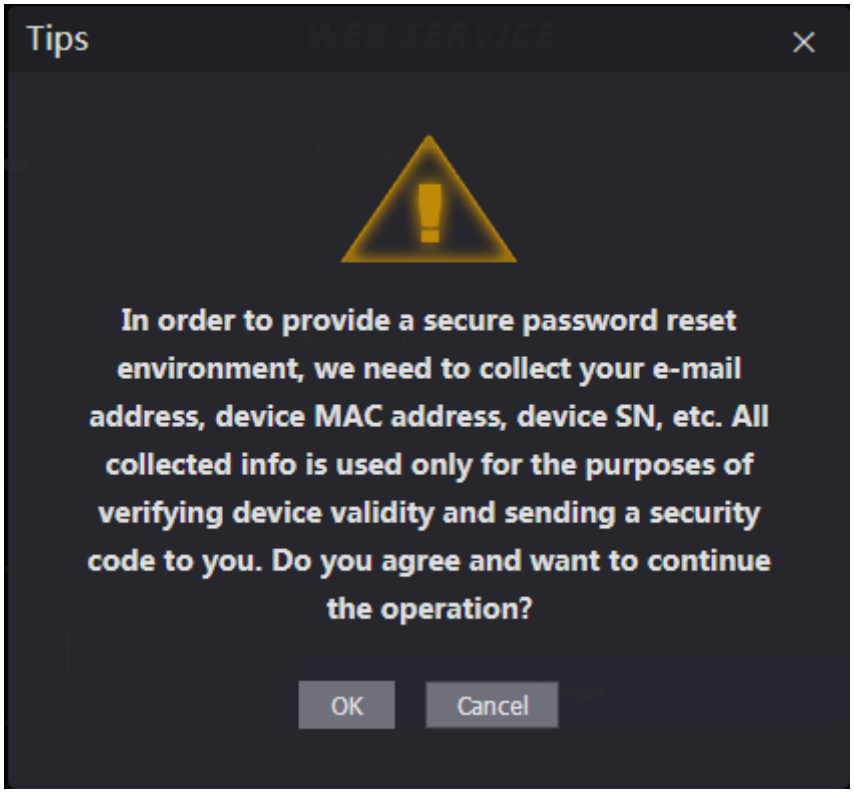
4.3 Restablecer la contraseña

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

Paso 1 Hacer clic **¿Se te olvidó tu contraseña?** en la interfaz de inicio de sesión.

los **Consejos** Se muestra la interfaz.

Figura 4-5 Consejos

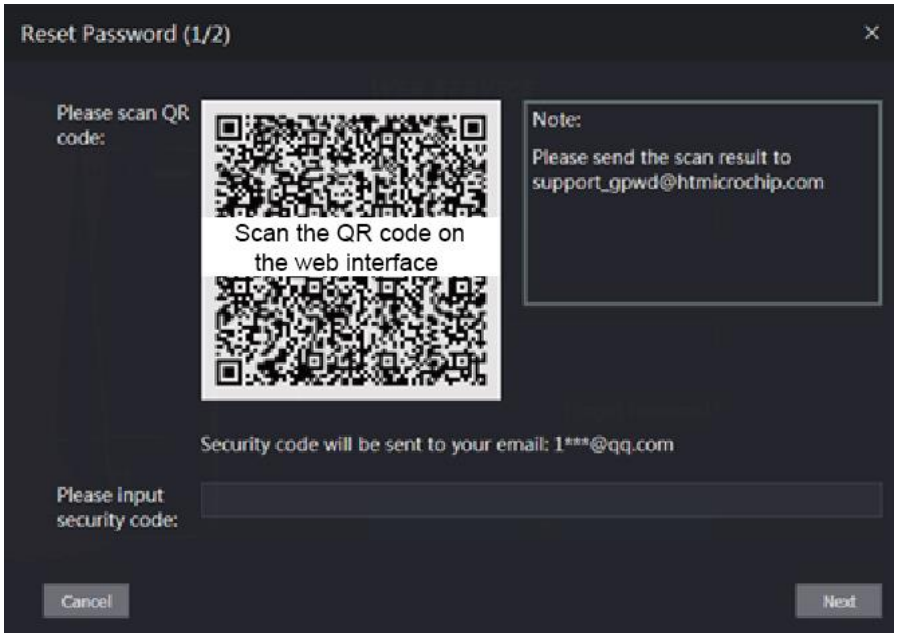


Paso 2 Lee los consejos.

Paso 3 Haga clic en Aceptar.

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

Figura 4-6 Restablecer contraseña



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

- Como máximo se generarán dos códigos de seguridad escaneando el mismo código QR. Si los códigos de seguridad 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, se invalidará.
- Si se ingresan códigos de seguridad incorrectos por cinco veces consecutivas, el administrador se congelará por cinco minutos. Ingrese el código de seguridad que recibió.

Paso 5

Paso 6 Hacer clic **Próximo.**

los **Restablecer la contraseña** Se muestra la interfaz. Restablecer y

Paso 7 confirmar la nueva contraseña.

La contraseña debe constar de 8 a 32 caracteres no en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo '";: &). Haga clic en **OKAY,** y se completa el reinicio.

Paso 8

4.4 Enlace de alarma

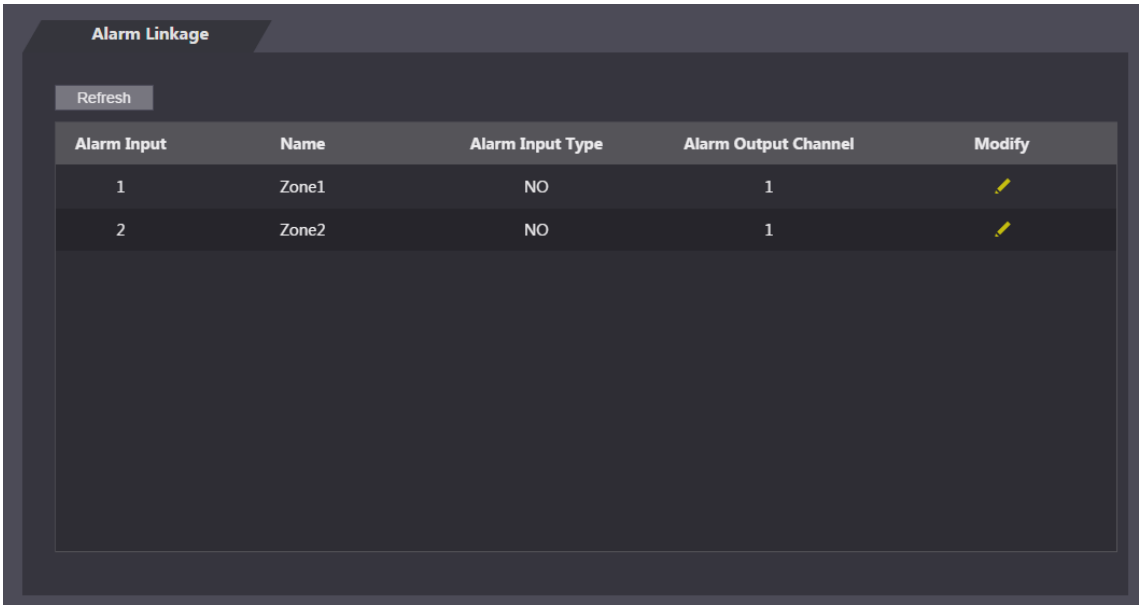
4.4.1 Configuración del enlace de alarma

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.

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

los **Enlace de alarma** Se muestra la interfaz. Ver Figura 4-7.

Figura 4-7 Enlace de alarma



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

4-8 Modificación del parámetro de enlace de alarma Figura

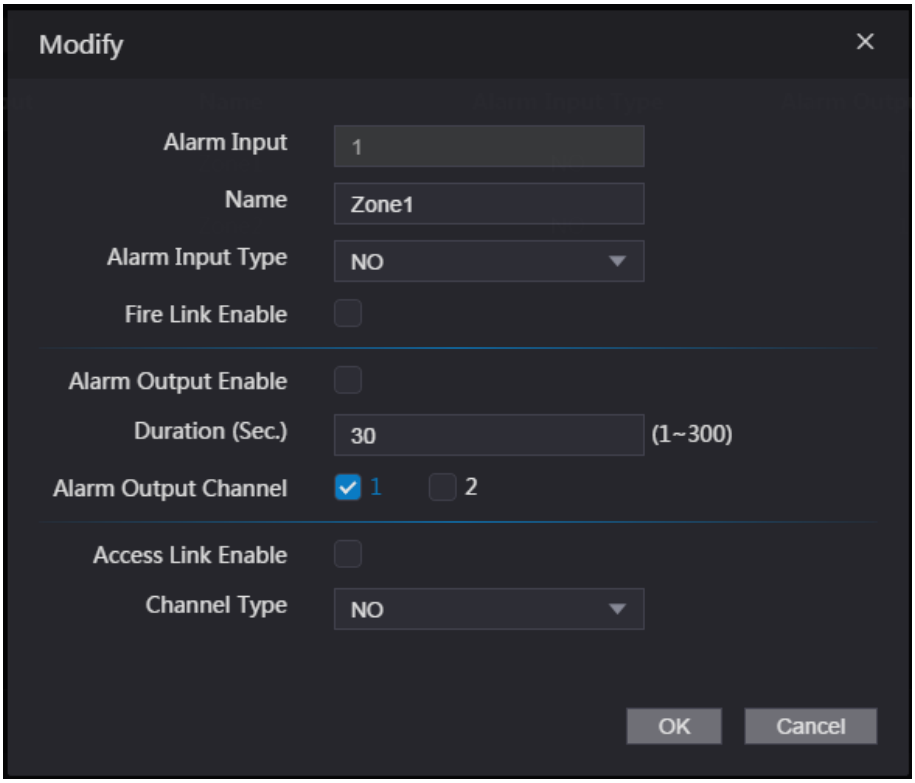


Tabla 4-1 Descripción del parámetro de enlace de alarma

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

Paso 3 Hacer clic **OKAY**, 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.

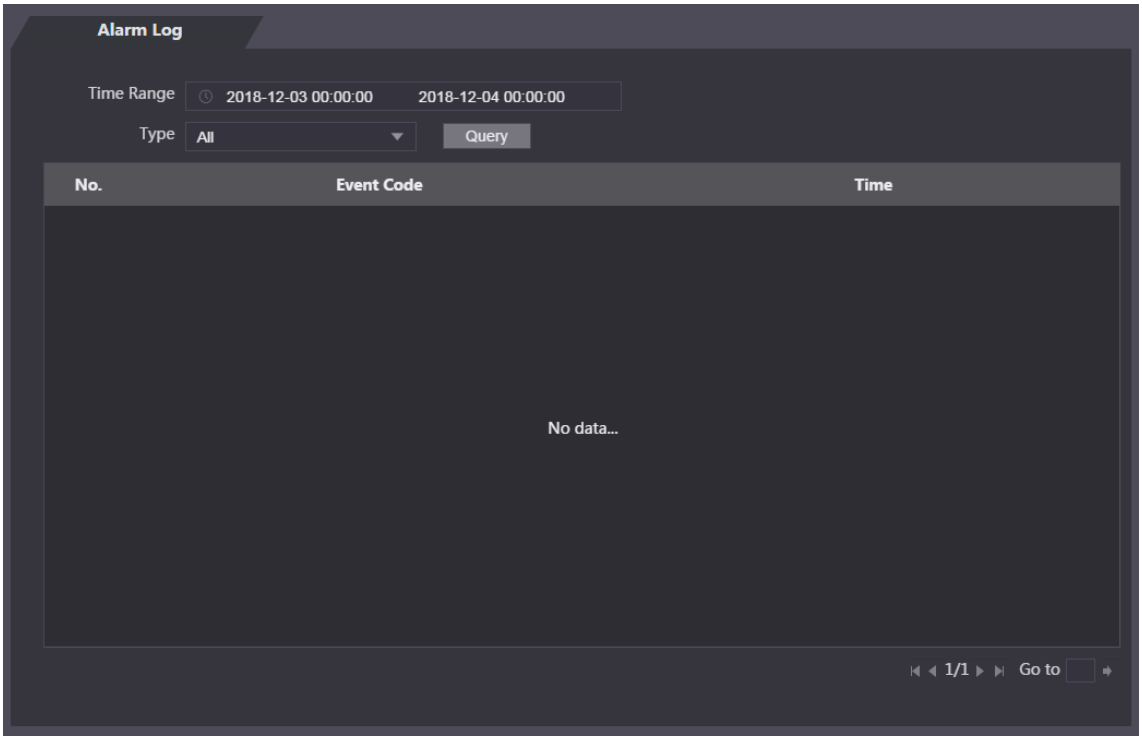
4.4.2 Registro de alarmas

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

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

los **Registro de alarma** Se muestra la interfaz. Ver Figura 4-9.

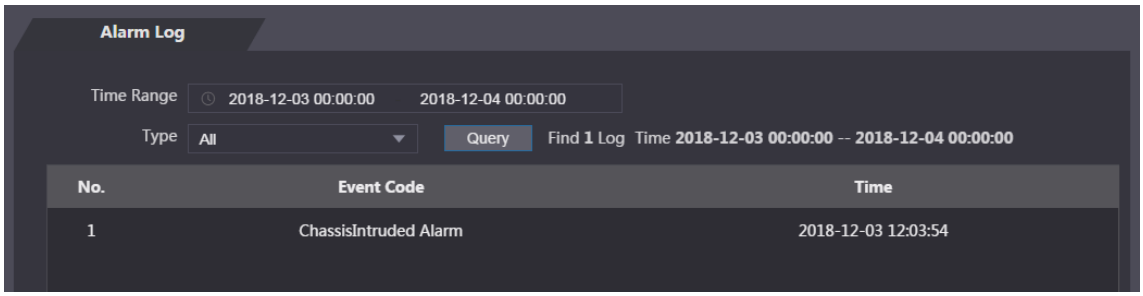
alarmas Registro de



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

Se muestran los resultados de la consulta. Ver Figura 4-10.

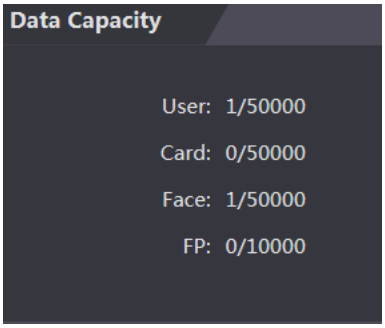
Figura 4-10. Resultados de la consulta



4.5 4.5Capacidad de datos

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

Figura 4-11. Capacidad de datos



4.6 Configuración de vídeo

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

4.6.1 Velocidad de datos

Figura 4-12. Velocidad de datos

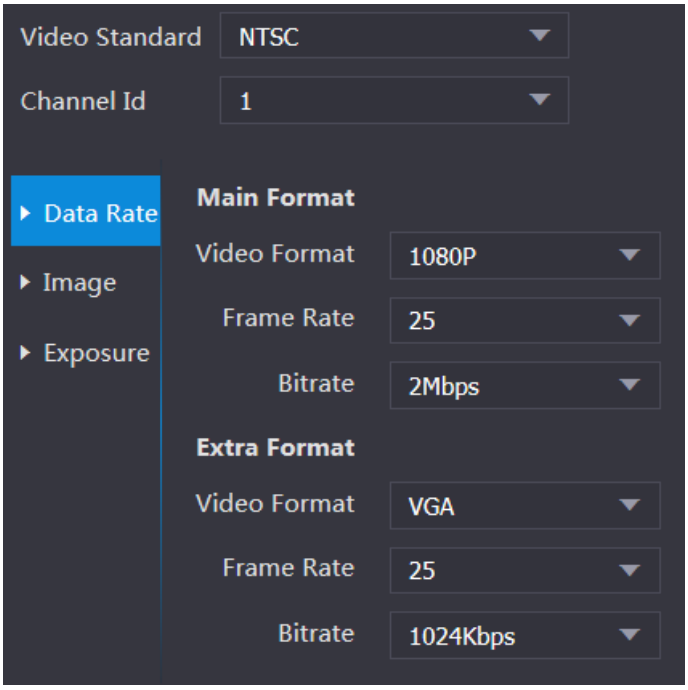


Tabla 4-2 Descripción del parámetro de velocidad de datos

Parámetro		Descripción
Estándar de video		Hay dos opciones: NTSC y PAL. Seleccione un estándar de acuerdo con el estándar de video de su región.
Canal		Hay dos opciones: 1 y 2. 1 es la cámara de luz blanca y 2 es la cámara de luz IR.
Formato principal	Formato de video	Hay cuatro opciones: D1, VGA, 720p y 1080p. Selecciona un opción de acuerdo con la calidad de video que desee.
	Velocidad de cuadros	La velocidad a la que aparecen cuadros consecutivos en una pantalla. los el rango de velocidad de fotogramas es de 1 a 25 fps.

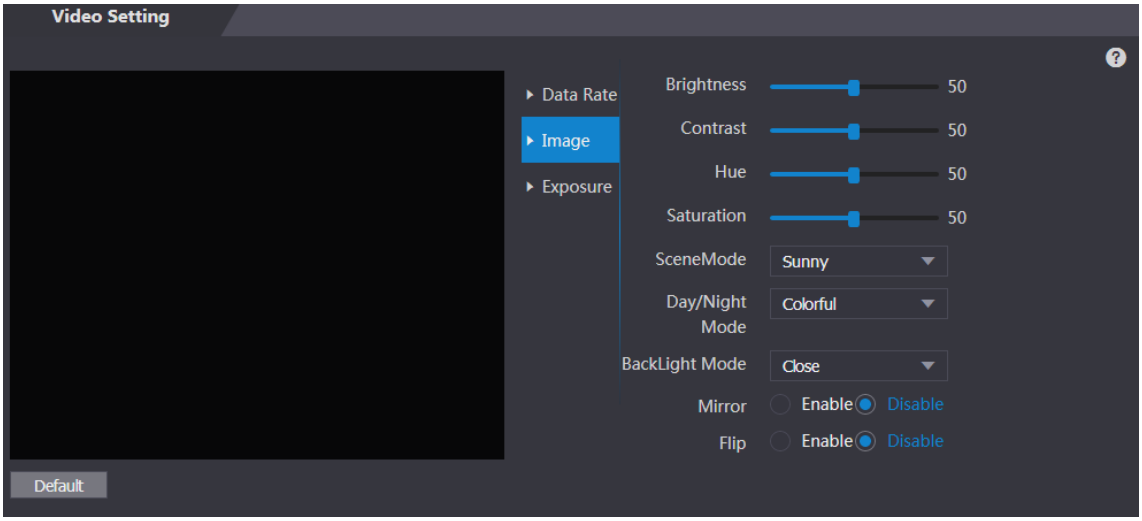
Paramet er		Descripción
	Velocidad de bits	El número de bits que se transportan o procesan por unidad de tiempo. Hay cinco opciones: 1.75Mbps, 2Mbps, 4Mbps, 6Mbps y 8Mbps.
Formato extra	Formato de video	Hay tres opciones: D1, VGA y QVGA.
	Velocidad de cuadros	La velocidad a la que aparecen cuadros consecutivos en una pantalla. los el rango de velocidad de fotogramas es de 1 a 25 fps.
	Velocidad de bits	El número de bits que se transportan o procesan por unidad de tiempo. Hay opciones: 256 Kbps, 320 Kbps, 384 Kbps, 448 Kbps, 512 Kbps, 640 Kbps, 768 Kbps, 896 Kbps, 1024 Kbps, 1,25 Mbps, 1.5Mbps y 1.75Mbps.

4.6.2 Imagen

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

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

Figura 4-13. Imagen



Paso 2 Seleccione Wide Dynamic en el modo de retroiluminación.

Tabla 4-3 Descripción del parámetro de imagen

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

Parámetro	Descripción
Modo escena	• Cerrar: sin modos. • Auto: el sistema ajusta automáticamente los modos de escena. • Soleado: en este modo, el tono de la imagen se reducirá. • Noche: en este modo, el tono de la imagen aumentará.  **Soleado** está seleccionado por defecto.
Modo día / noche	El modo Día / Noche decide el estado de funcionamiento de la luz de relleno. • Auto: el sistema ajusta automáticamente los modos día / noche. • Colorido: en este modo, las imágenes son con colores. • Blanco y negro: en este modo. Las imágenes están en blanco y negro.
Modo de luz de fondo	• Cerrar: sin luz de fondo. • BLC: la compensación de luz de fondo corrige regiones con valores extremadamente altos o bajos niveles de luz para mantener un nivel de luz normal y utilizable para el objeto enfocado. • WDR: en el modo de amplio rango dinámico, el sistema se atenúa áreas y compensa áreas oscuras para garantizar la definición de objetos en las áreas brillantes y áreas oscuras.  Cuando los rostros humanos están en la luz de fondo, debe habilitar Wide Dynamic. • HLC: se necesita una compensación de resaltado para compensar La sobreexposición de reflejos o fuentes de luz intensas, como focos, faros, luces de pórtico, 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.
Dar la vuelta	Cuando esta función está habilitada, los videos se pueden voltear.

4.6.3 Exposición

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

Tabla 4-4 Descripción del parámetro de exposición

Parámetro	Descripción
Contra parpadeo	• 50Hz: cuando la frecuencia de servicio de la corriente alterna es de 50Hz, el la exposición se ajusta automáticamente para asegurarse de que no haya rayas en las imágenes. • 60Hz: cuando la frecuencia de la red de corriente alterna es de 60Hz, el la exposición se ajusta automáticamente para asegurarse de que no haya rayas en las imágenes. Al aire libre: cuando **Al aire libre** está seleccionado, el modo de exposición puede ser • cambiado.

Parámetro	Descripción
Modo de exposición	• Cuando seleccionas **Al aire libre** en la lista desplegable Antiparpadeo, puede seleccionar **Prioridad de obturador** como el modo de exposición. • Los modos de exposición de diferentes dispositivos pueden variar, y el producto real prevalecerá. Puedes seleccionar entre: • Auto: el controlador de acceso ajustará automáticamente el brillo de imágenes • Prioridad de obturador: el controlador de acceso ajustará el brillo de la imagen según el rango de valores de exposición del obturador. Si el brillo de la imagen no es suficiente y el valor del obturador ha alcanzado el límite superior o inferior, el controlador de acceso ajustará automáticamente el valor de ganancia para obtener el brillo ideal. • Manual: puede configurar el valor de ganancia y obturador manualmente para ajustar el brillo de la imagen.
Obturador	Cuanto mayor sea el valor del obturador y más corto sea el tiempo de exposición, más oscuras serán las imágenes.
Rango de valor del obturador	Si seleccionas **Gama personalizada,** Puede personalizar el rango de valores del obturador.
Rango de valor de ganancia	Cuando se establece el rango de valor de ganancia, se mejorará la calidad del video.
Compensación de exposición	Puede aumentar el brillo del video ajustando el valor de compensación de exposición.
NR 3D	Cuando la reducción de ruido 3D (RD) está habilitada, el ruido de video se puede reducir y se producirán videos de alta definición.
Grado	Puede ajustar el valor de 3D NR cuando 3D NR está habilitado. Cuanto mayor sea el valor, menor será el ruido.

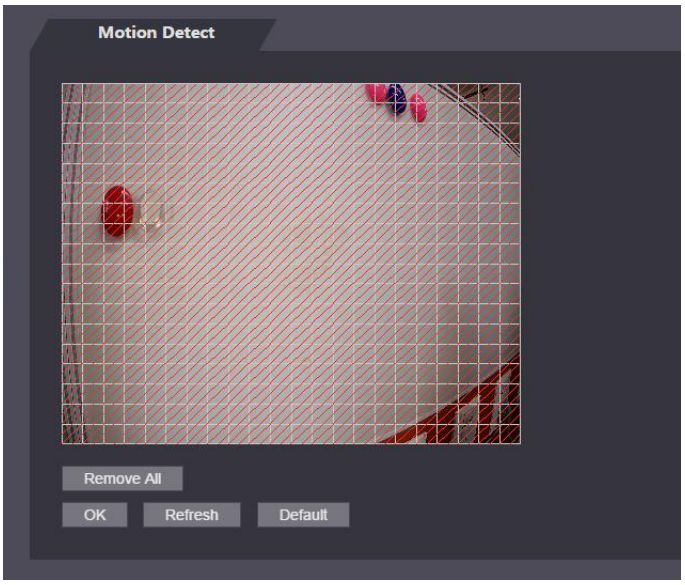
4.6.4 Detección de movimiento

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

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

los **Detección de movimiento** Se muestra la interfaz. Ver Figura 4-14.

Figura 4-14. Detección de movimiento

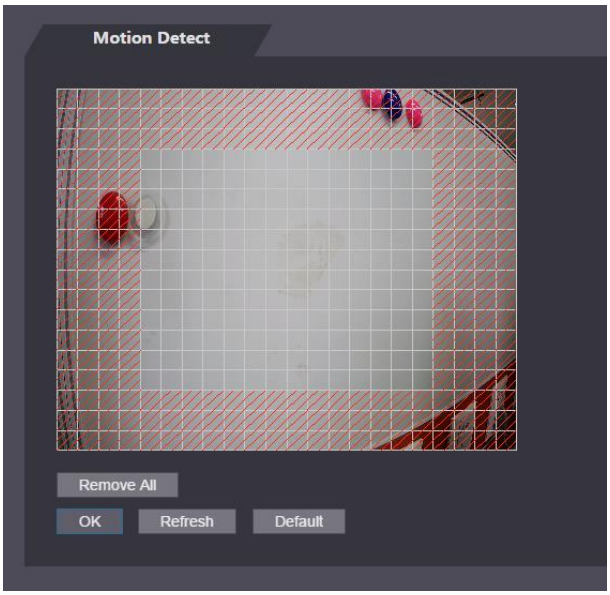


Paso 2 Mantenga presionado el botón izquierdo del mouse y luego arrastre el mouse hacia el área roja. los

Se muestra el área de detección de movimiento. Ver Figura 4-15.

- Los rectángulos rojos son área de detección de movimiento. El rango de detección de movimiento predeterminado es 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 de detección sin movimiento si dibuja en el área de detección de movimiento predeterminada.

Figura 4-15 Área de detección de movimiento

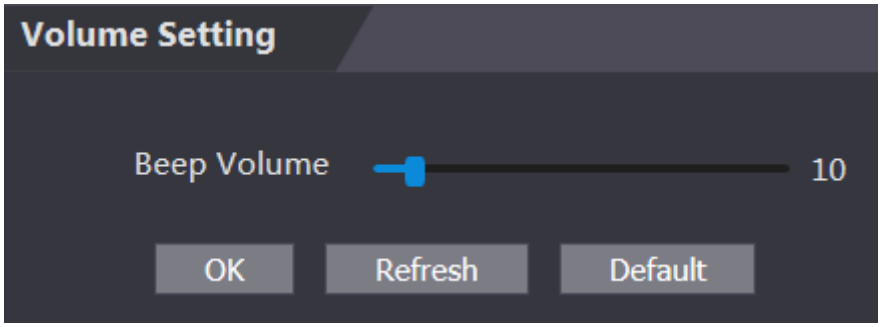


Paso 3 **Hacer clic Okay para terminar la configuración.**

4.6.5 Configuración de volumen

Puede ajustar el volumen del altavoz del controlador de acceso.

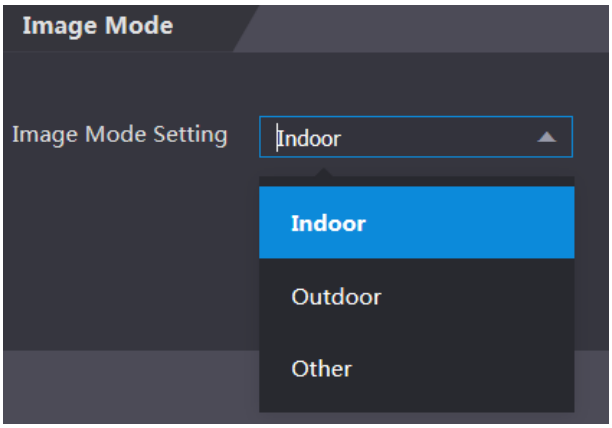
Figura 4-16. Ajuste de volumen



4.6.6 Modo de imagen

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

Figura 4-17 Modo de imagen



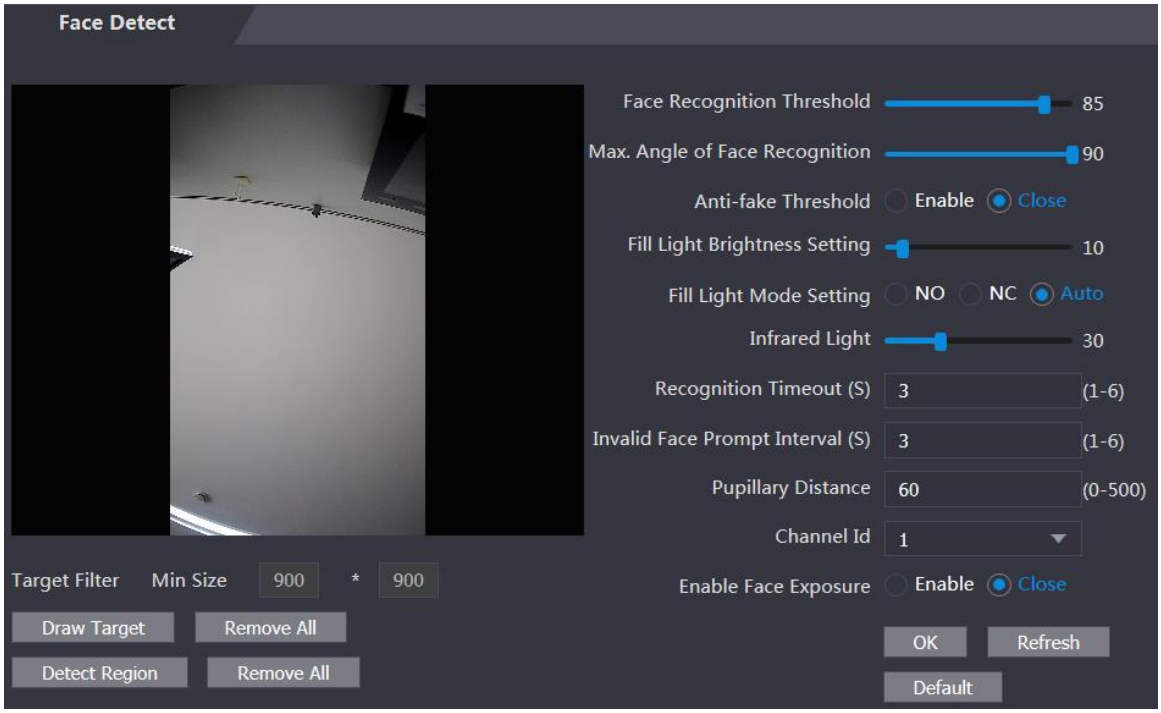
4.7 Detección de rostro

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

Paso 1 Seleccione **Detección de rostro.**

los **Detección de rostro** Se muestra la interfaz. Ver Figura 4-18.

Figura 4-18 Detección de la cara



Paso 2 Configurar parámetros. Ver tabla 4-5.

Tabla 4-5 Descripción del parámetro de detección de cara

Parámetro	Descripción
Umbral de reconocimiento facial	Cuanto mayor sea el valor, mayor será la precisión.
Max. Ángulo de reconocimiento facial	Cuanto mayor sea el ángulo, se reconocerá el rango más amplio de los perfiles.
Umbral antifalsificación	Hay dos opciones: **Habilitar** y **Cerca.**
Ajuste de brillo de luz de relleno	Puede configurar el brillo de la luz de relleno.
Llenar Ajuste de modo de luz	Hay tres modos de luz de relleno. • NO: La luz de relleno está normalmente encendida. • NC: la luz de relleno está normalmente cerrada. • Automático: la luz de relleno se encenderá automáticamente cuando se detecte movimiento Se activa el evento. **Cuando Auto está seleccionado, la luz de relleno no estará encendida incluso si el valor de Luz infrarroja es mayor que 19.**
Luz infrarroja	Ajuste las luces brillantes IR arrastrando la barra de desplazamiento.
Tiempo de espera de reconocimiento	Cuando una persona que no tiene la autoridad de acceso se para frente al controlador de acceso y se le reconoce el rostro, el controlador le indicará que el reconocimiento de rostro falló. El intervalo de solicitud se denomina tiempo de espera de reconocimiento.
Intervalo de aviso de cara no válido	Cuando una cara no tiene autoridad de acceso frente al controlador de acceso, el controlador le indicará que la cara no es válida. El intervalo de solicitud no es válido.
Distancia pupilar	La distancia pupilar es el valor de píxel de la imagen entre los centros de Las pupilas en cada ojo. Debe establecer un valor apropiado para que el

Parámetro	Descripción
	El controlador de acceso puede 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 será el valor. Si un adulto está a 1.5 metros de la lente, el valor de la distancia pupilar puede estar entre 50 y 70.
Habilitar Cara Exposición	Después de habilitar la exposición facial, el rostro humano será más claro cuando el controlador de acceso se instale en exteriores.
Canal ID	Hay dos opciones: 1 y 2. 1 es la cámara de luz blanca y 2 es la cámara de luz IR.
Draw Target	Hacer clic **Draw Target,** y luego puedes dibujar el marco mínimo de detección de rostros. Hacer clic **Eliminar todo,** y puedes eliminar todos los marcos que dibujaste.
Detectar región	Hacer clic **Detectar región,** mueva el mouse y podrá ajustar la región de detección de rostros. Hacer clic **Eliminar todo,** y puedes eliminar todas las regiones de detección.

Paso 3 Hacer clic **Okay** para terminar la configuración.

4.8 Configuración de red

4.8.1 TCP / IP

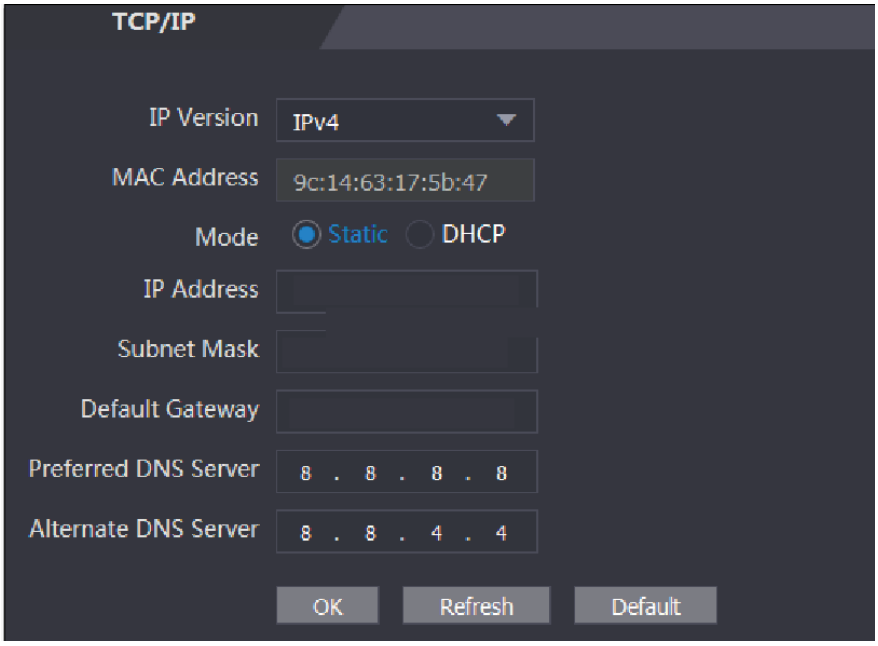
Debe configurar la dirección IP y el servidor DNS para asegurarse de que el controlador de acceso pueda comunicarse con otros dispositivos.

Condición previa

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

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

Figura 4-19 TCP / IP



Paso 2 Configurar parámetros.

Tabla 4-6 TCP / IP

Parámetro	Descripción
Versión IP	Hay una opción: IPv4.
Dirección MAC	Se muestra la dirección MAC del controlador de acceso.
Modo	• Estático Establezca la dirección IP, la máscara de subred y la dirección de la puerta de enlace manualmente. • DHCP • Después de habilitar DHCP, la dirección IP, la máscara de subred y la dirección de la puerta de enlace no se pueden configurar. • Si DHCP es efectivo, la dirección IP, la máscara de subred y la dirección de la puerta de enlace se mostrarán automáticamente; Si DHCP no es efectivo, la dirección IP, la máscara de subred y la dirección de la puerta de enlace serán cero. • Si desea ver la IP predeterminada cuando DHCP es efectivo, debe deshabilitar DHCP.
Dirección local de enlace	La dirección local de enlace solo está disponible cuando se selecciona IPv6 en la versión IP. Se asignarán direcciones locales de enlace únicas al controlador de interfaz de red en cada local red de área para permitir comunicaciones La dirección local de enlace 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.
Servidor DNS preferido	Establezca la dirección IP del servidor DNS preferido.
Servidor DNS alternativo	Establezca la dirección IP del servidor DNS alternativo.

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

4.8.2 Puerto

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

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

los **Puerto** Se muestra la interfaz.

Paso 2 Configurar números de puerto. Ver 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 4-7 Descripción del puerto

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

Paso 3 clic en **Okay** para completar la configuración.

4.8.3 Registrarse

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.

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

Paso 2 los **Registro automático** Se muestra la interfaz. Seleccione **Habilitar,** e ingrese la IP del host, el puerto y la ID del dispositivo secundario.

Tabla 4-8 Descripción del registro automático

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

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

4.8.4 P2P

La computación 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 la red externa; de lo contrario, no se puede usar el controlador de acceso.

Figura 4-20 P2P

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

los **P2P** Se muestra la interfaz. Seleccione **Habilitar** para

Paso 2 habilitar la función P2P.

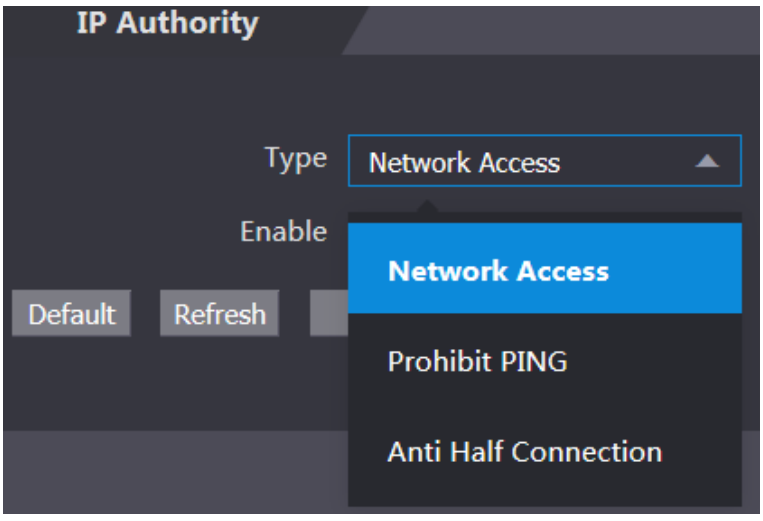
Paso 3 Hacer clic **Okay** para completar la configuración.

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

4.9 Administración de Seguridad

4.9.1 Autoridad de PI

Figura 4-21. Autoridad de propiedad intelectual



Seleccione un modo de seguridad cibernética según sea necesario.

4.9.2 Sistemas

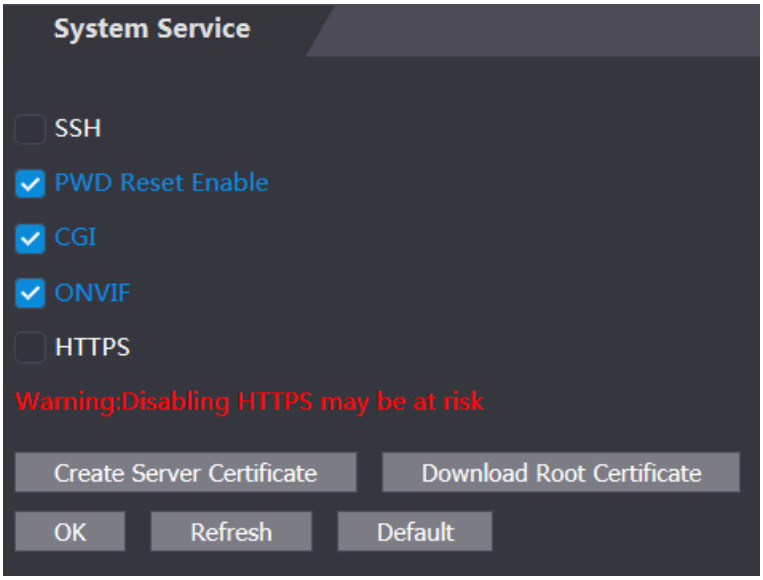
4.9.2.1 Servicio del sistema

Hay cuatro opciones: SSH, PWD Reset Enable, CGI y HTTPS. Consulte "3.9.4 Características" para seleccionar una o más de una de ellas.

La configuración del servicio del sistema realizada en la página web y la configuración en el **Caracteristicas**

La interfaz del controlador de acceso se sincronizará.

Figura 4-22. Servicio del sistema



4.9.2.2 Crear certificado de servidor

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

4.9.2.3 Descargar certificado raíz

Paso 1 Hacer clic **Descargue el certificado raíz.**

Seleccione una ruta para guardar el certificado en **Guardar el archivo** caja de diálogo. Haga doble clic en el **Certificado de**

Paso 2 **raíz** que ha descargado para instalar el certificado.

Instale el certificado siguiendo las instrucciones en pantalla.

4.9.3 Gestión de usuarios

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

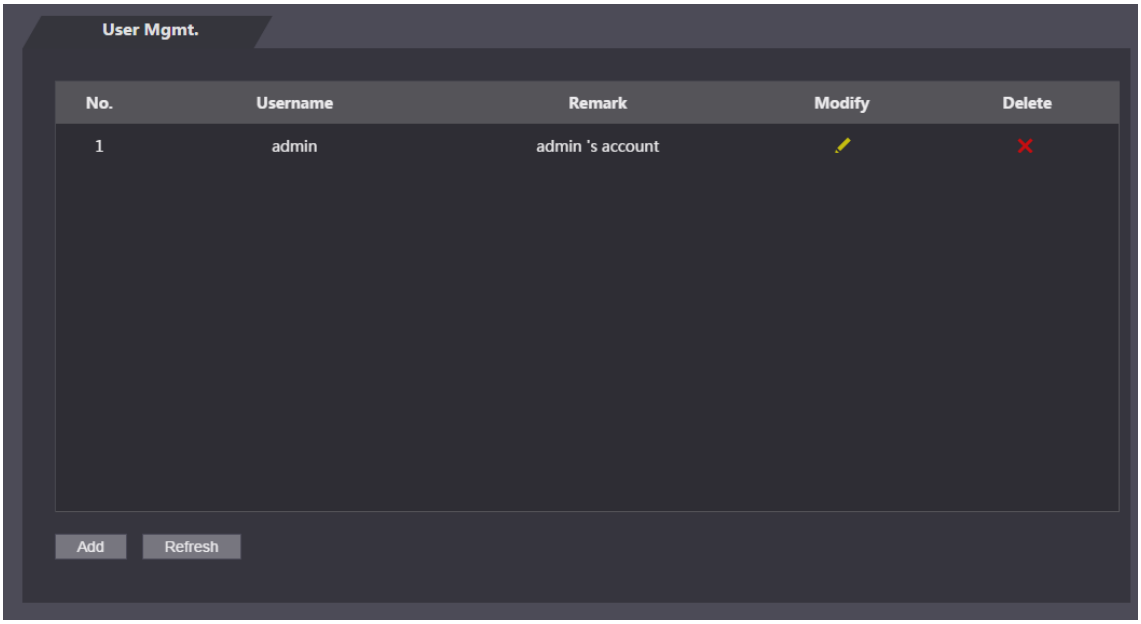
4.9.3.1 Agregar usuarios

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

4.9.3.2 Modificar información del usuario

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

Figura 4-23. usuarios

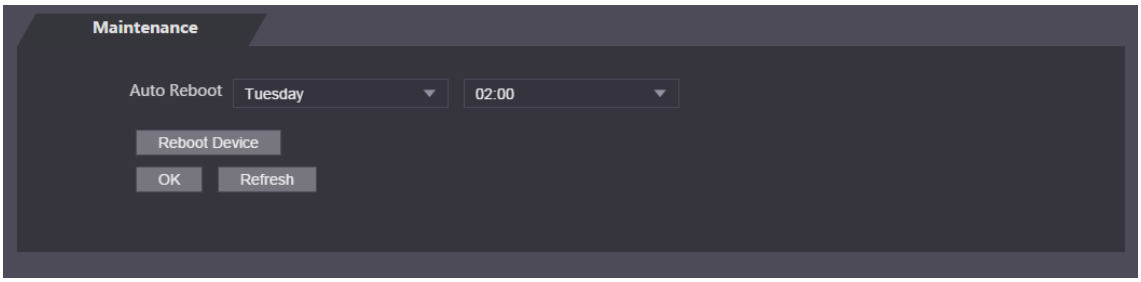


4.9.4 Mantenimiento

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.

El tiempo de reinicio predeterminado es a las 2 en punto de la mañana del martes. Hacer clic **Reiniciar dispositivo,** el controlador de acceso se reiniciará de inmediato. Hacer clic **OKAY,** el controlador de acceso se reiniciará a las 2 en punto de la mañana todos los martes. Ver Figura 4-24.

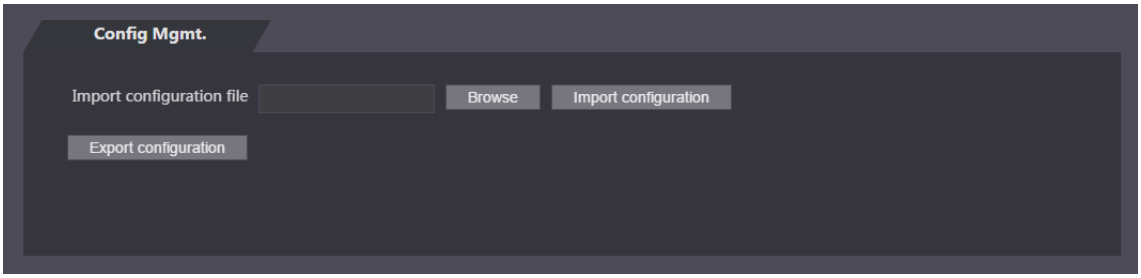
Figura 4-24. Mantenimiento



4.9.5 Gestión de configuración

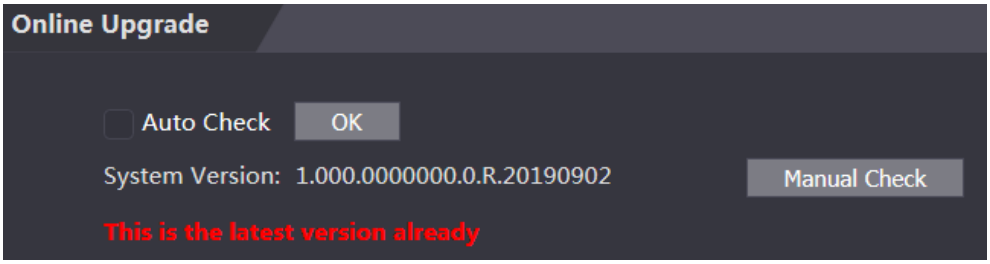
Cuando más de un controlador de acceso necesita la misma configuración, puede configurar parámetros para ellos importando o exportando archivos de configuración. Ver Figura 4-25.

Figura 4-25. Gestión de la configuración



4.9.6 Actualización

Puedes elegir Verificación automática para actualizar el sistema automáticamente. También puedes seleccionar Verificación manual para actualizar el sistema manualmente.



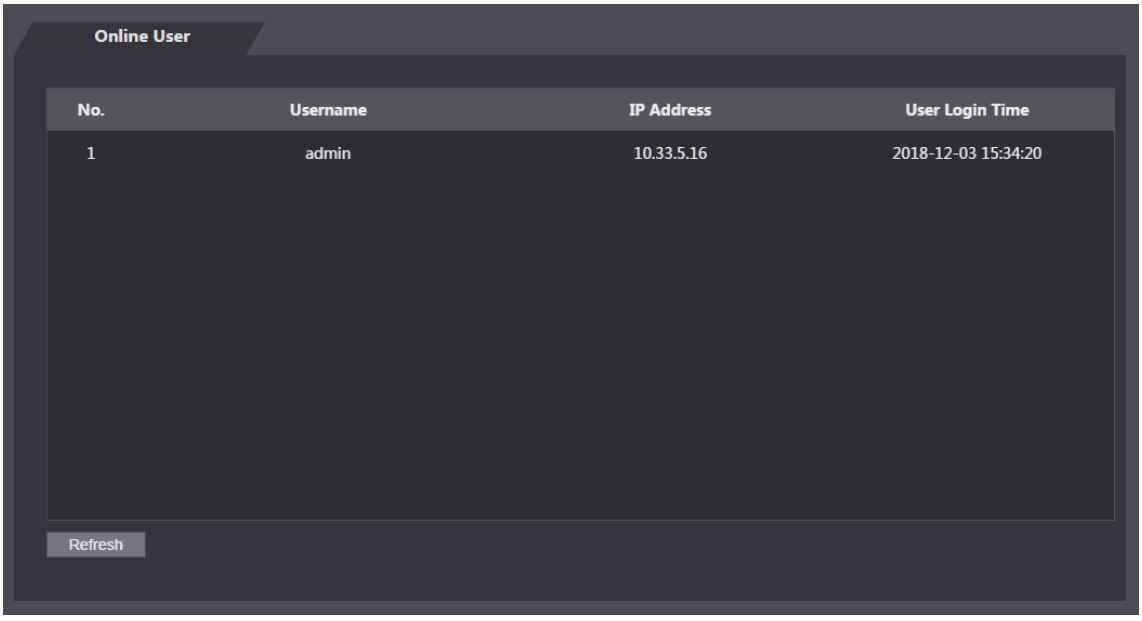
4.9.7 Información de versión

Puede ver información que incluye dirección MAC, número de serie, versión de MCU, versión web, versión de línea de base de seguridad y versión del sistema.

4.9.8 Usuario en línea

Puede ver el nombre de usuario, la dirección IP y el tiempo de inicio de sesión del usuario en Usuario en línea interfaz. Ver Figura 4-26.

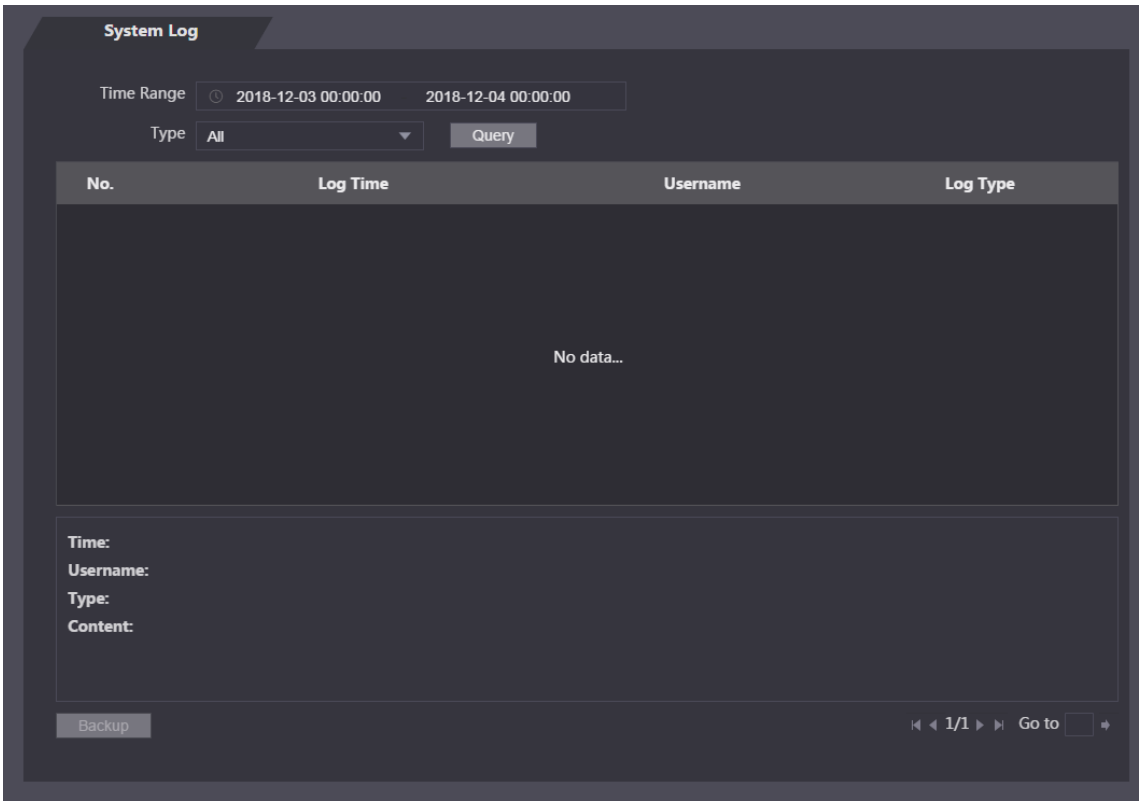
Figura 4-26. Usuario en línea



4.10 Registro del sistema

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

Figura 4-27. Registro del sistema



4.10.1 Consultar registros

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

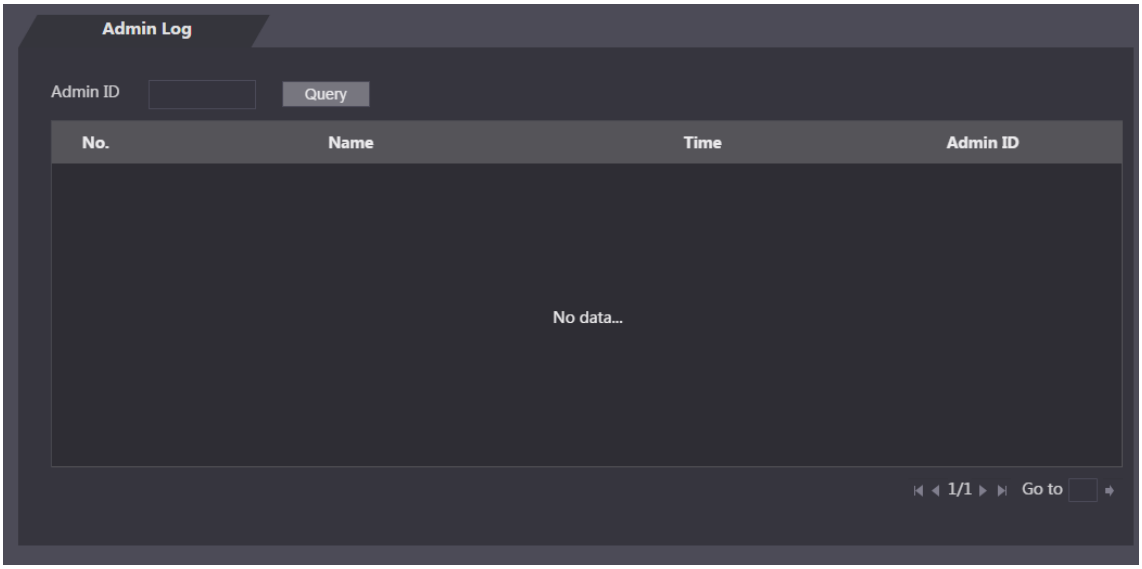
4.10.2 Copia de seguridad de registros

Hacer clic **Apoyo** para hacer una copia de seguridad de los registros que se muestran.

4.11 Registro de administrador

Ingrese ID de administrador en el **Registro de administrador** interfaz, haga clic **Consulta,** y luego verá los registros de operación del administrador. Ver Figura 4-28.

Figura 4-28. Registro de administrador



Pase el cursor del mouse sobre , y luego puedes ver información detallada del actual usuario.

4.12 Salida

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

5 5 Configuración inteligente de PSS

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

Las interfaces de PSS inteligentes pueden variar con las versiones, y prevalecerá la interfaz real.

5.1 Iniciar sesión

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

5.2 Agregar dispositivos

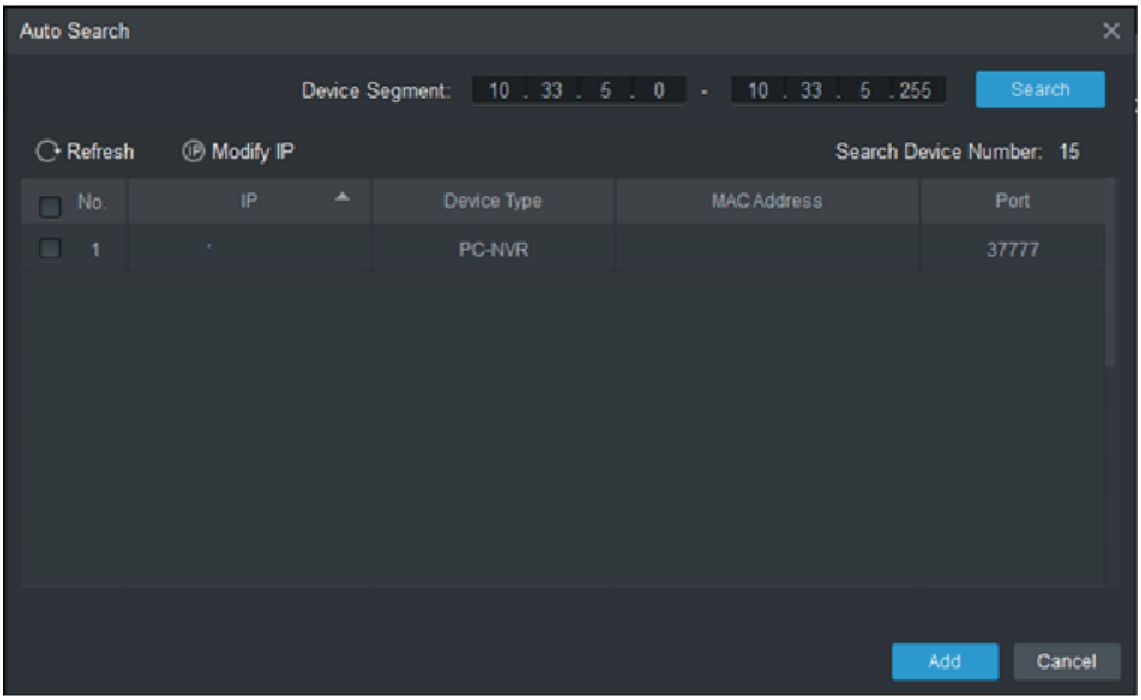
Debe agregar controladores de acceso al Smart PSS. Puedes hacer clic Auto búsqueda para agregar y hacer clic Añadir para agregar dispositivos manualmente.

5.2.1 Búsqueda automática

Puede buscar y agregar controladores de acceso en el mismo segmento de red al Smart PSS. Ver Figura 5-1 y Figura 5-2.

Figura 5Dispositivos

Figura 5-2 Búsqueda automática



Paso 1 Hacer clic **Auto búsqueda,** ingrese el segmento de red y luego haga clic en Buscar. Una lista será desplegado.

Paso 2 Seleccione los controladores de acceso que desea agregar a Smart PSS y luego haga clic en Agregar, se mostrará el cuadro de diálogo de información de inicio de sesión. Ingrese el nombre de

Paso 3 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 Smart PSS.

5.2.2 Agregar manual

Debe conocer las direcciones IP y los nombres de dominio de los controladores de acceso que desea agregar. Ver Figura 5-3 y Figura 5-4.

Figura 5-3 Dispositivos

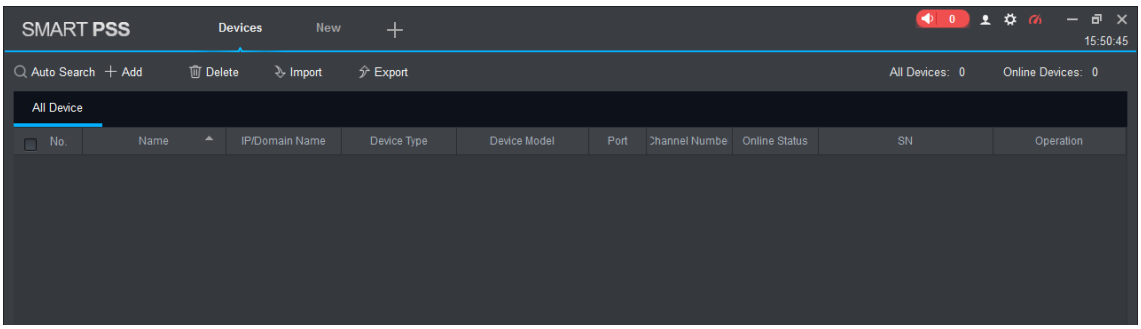
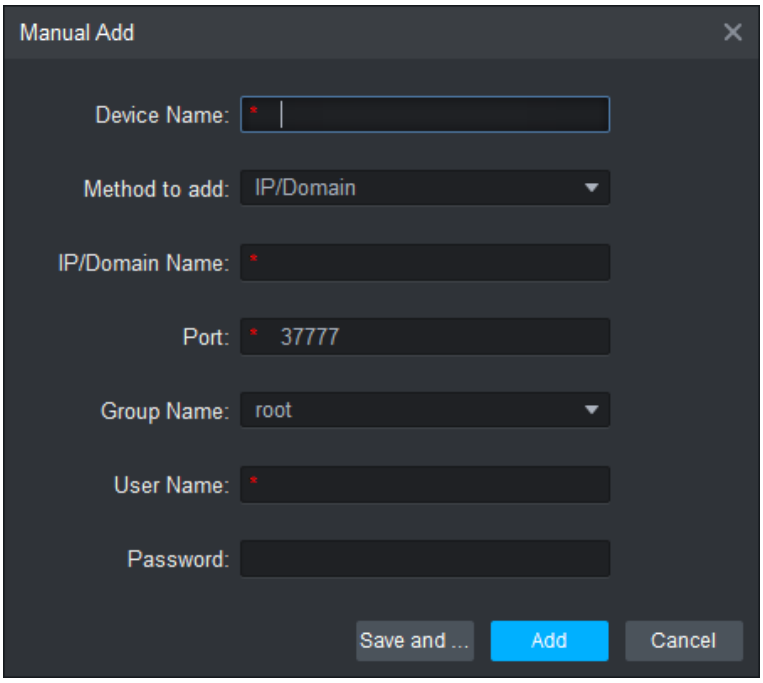


Figura 5-4 Agregar manual



Paso 1 Hacer clic **Añadir** en la interfaz Dispositivos, y se mostrará la interfaz Agregar manual.

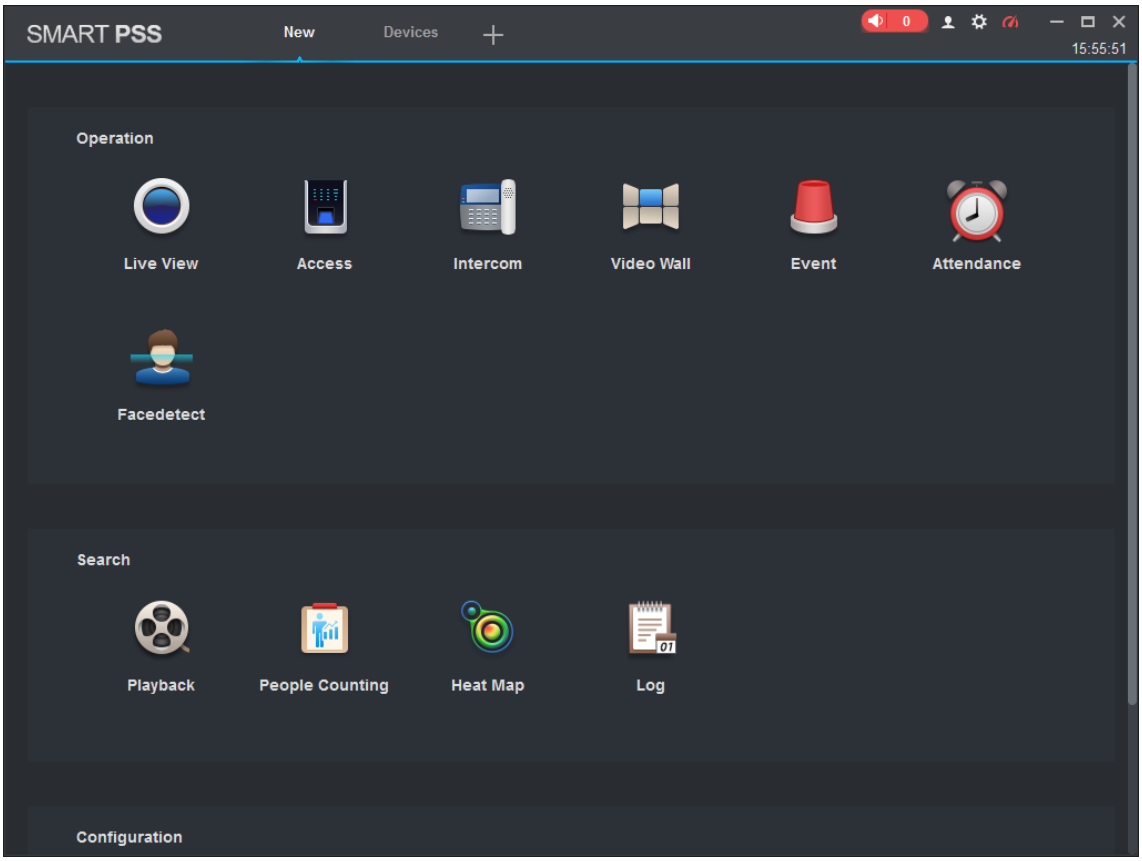
Paso 2 Ingrese el Nombre del dispositivo, seleccione un método para agregar, ingrese el IP / Nombre de dominio, Puerto número (37777 por defecto), Nombre del grupo, Nombre de usuario y Contraseña. Hacer clic **Añadir,** y luego puede ver el

Paso 3 controlador de acceso agregado en la interfaz Dispositivos.

5.3 Agregar usuarios

Los usuarios están obligados con tarjetas. Después de agregar usuarios a Smart PSS, puede configurar los permisos de acceso de los usuarios en **Nuevo> Acceso.** Ver Figura 5-5.

figura 5-5 Nueva

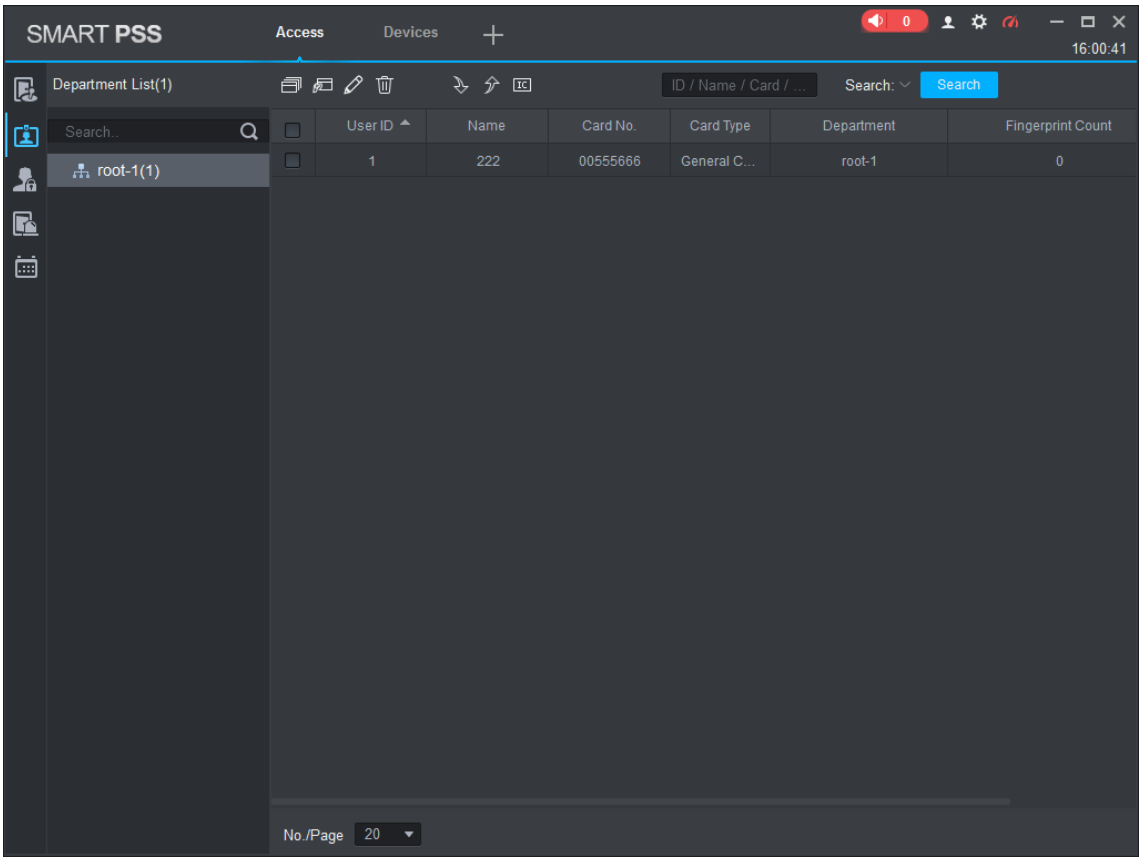


5.3.1 Selección del tipo de tarjeta

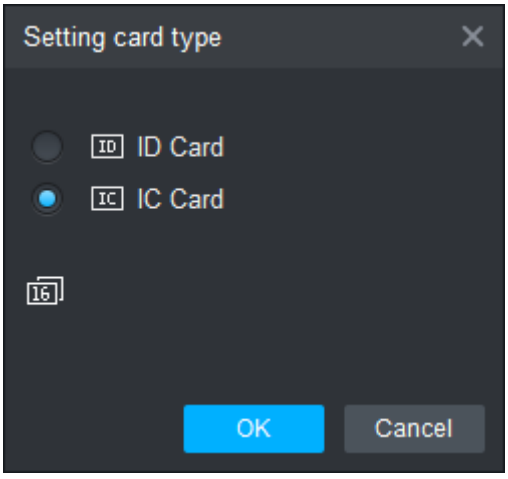
Los tipos de tarjeta deben ser los mismos que los del emisor de la tarjeta; de lo contrario, no se pueden leer los números de tarjeta.

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

Figura 5-6cceda a la



tarjeta Figuración 5-7 Configuración del tipo de



5.3.2 Agregar un usuario

Puede agregar usuarios uno por uno.

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

Figura 5-8 Acceda a la

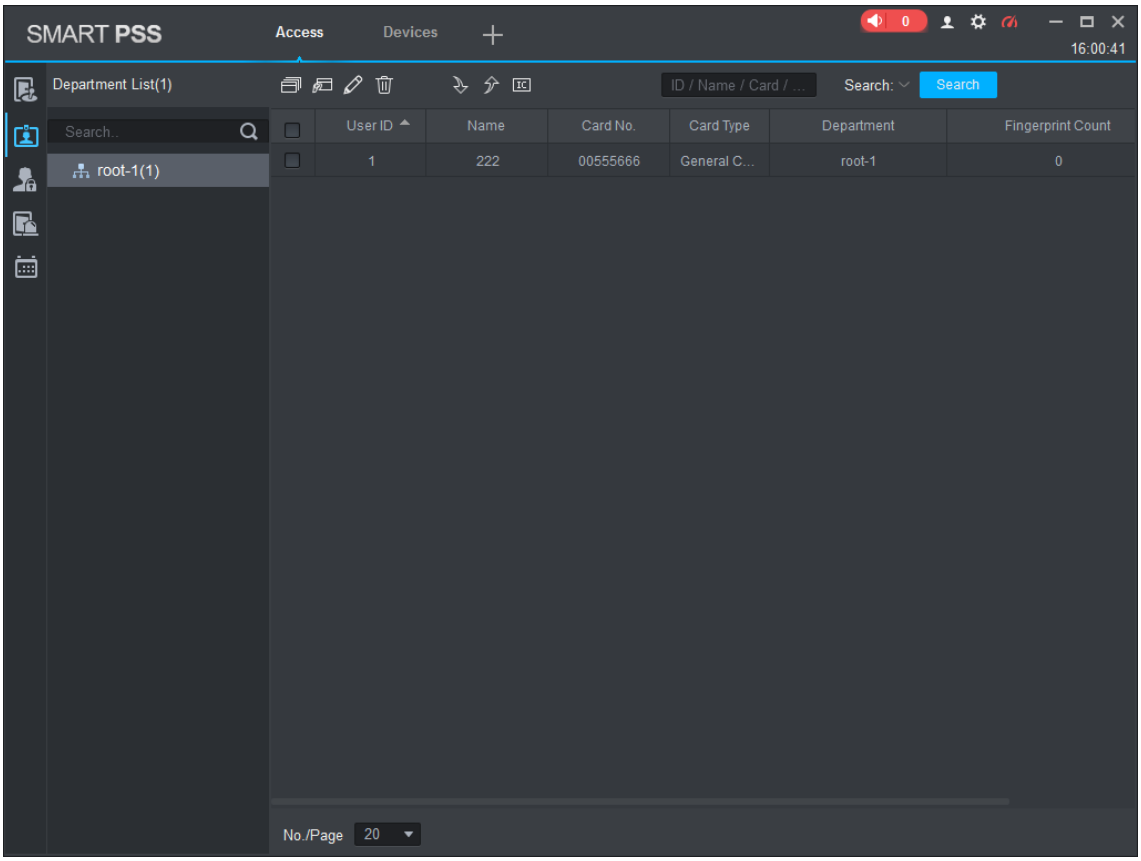
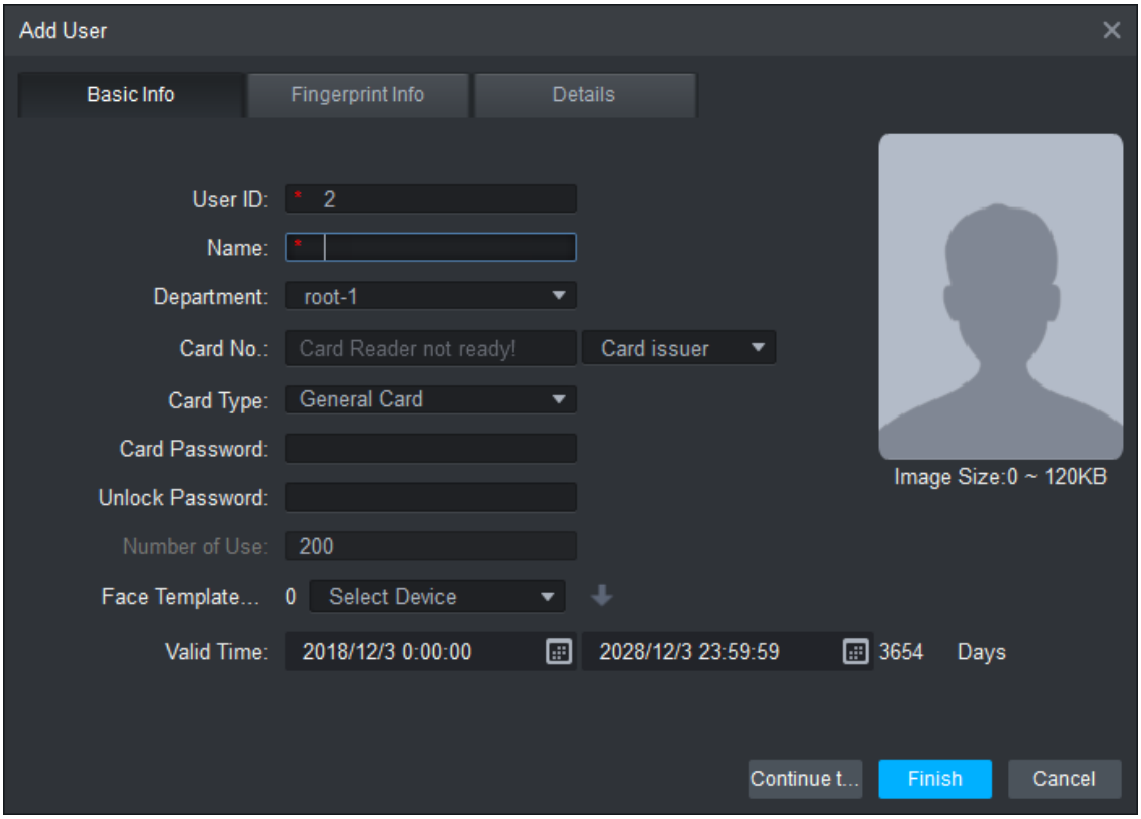


Figura 5-9 Agregar usuario



5.4 Agregar grupo de puertas

Puede gestionar puertas agrupando puertas.

Sobre el **Acceso** interfaz, haga clic  haga clic **Añadir,** ingrese el nombre del grupo de puerta y luego seleccione una hora zona. Hacer clic **Terminar** para completar el usuario agregando. Ver Figura 5-10 y Figura 5-11.

Figura 5-10 Acceso

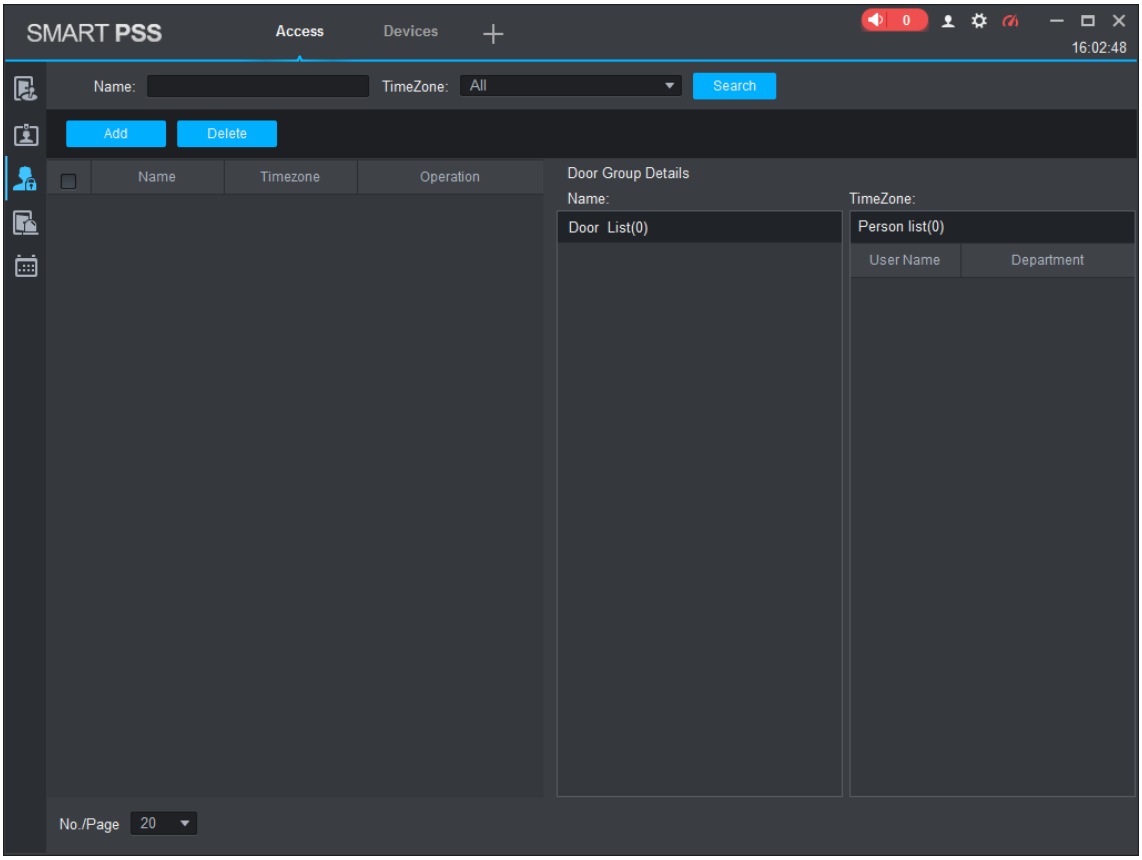
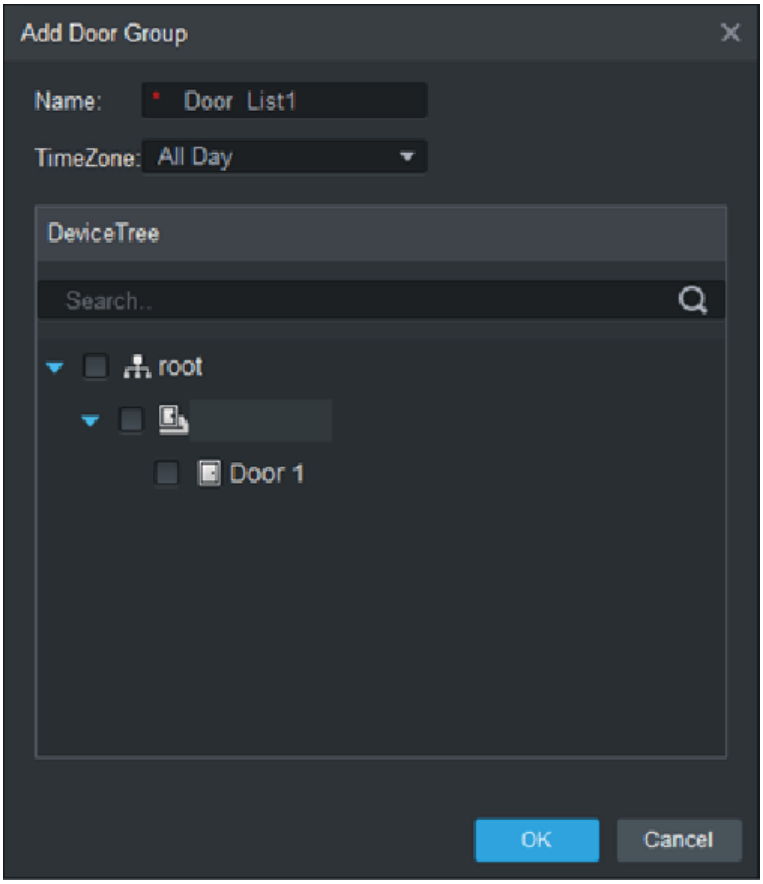


Figura 5-11 Agregar grupo de puertas



5.5 Configuración de permisos de acceso

Puede hacer la configuración de permisos de acceso. Hay dos opciones: permiso de acceso de grupo de puerta y permiso de acceso de usuario. La información de los usuarios que tienen permiso de acceso en Smart PSS y los controladores de acceso se sincronizarán.

5.5.1 Dar permiso por grupo de puerta

Seleccione un grupo de puertas, agregue usuarios a la lista de puertas, y luego los usuarios en la lista de puertas obtienen permisos de acceso de todas las puertas en la lista de puertas. Ver Figura 5-12 y Figura 5-13.

Figura 5-12. Acceso

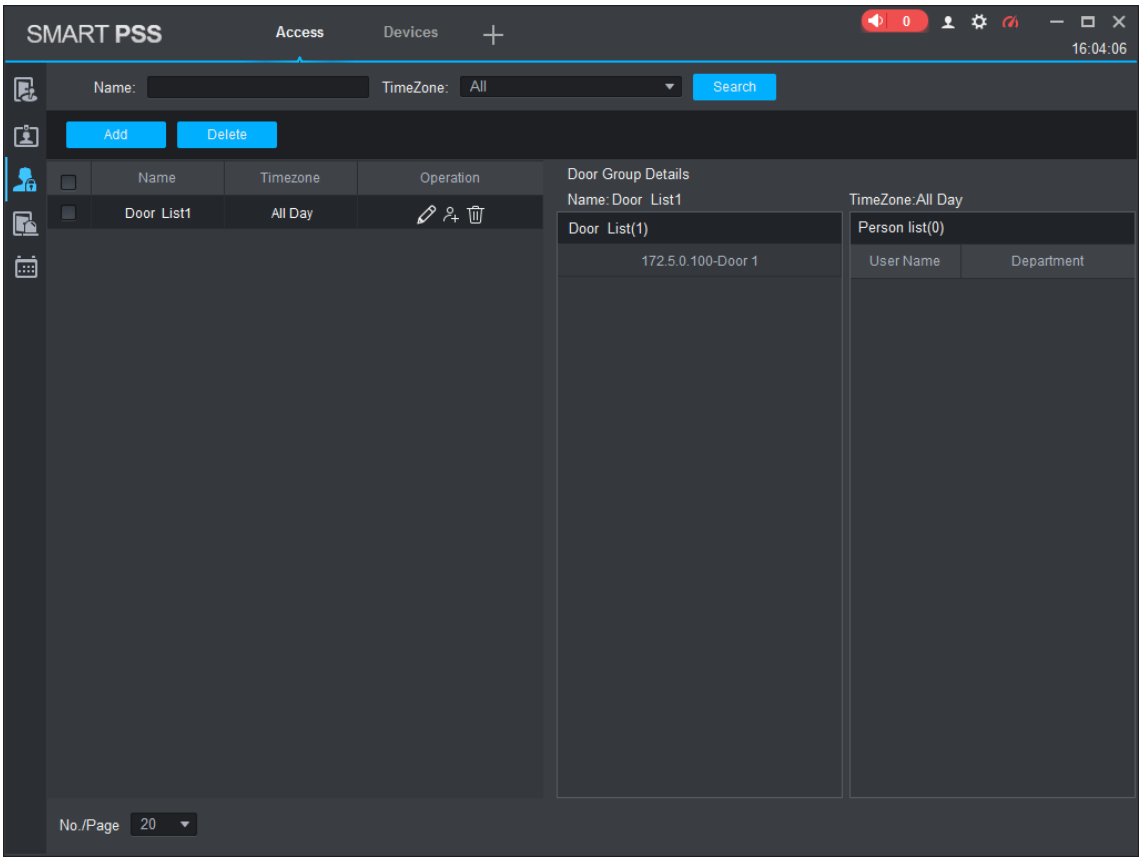
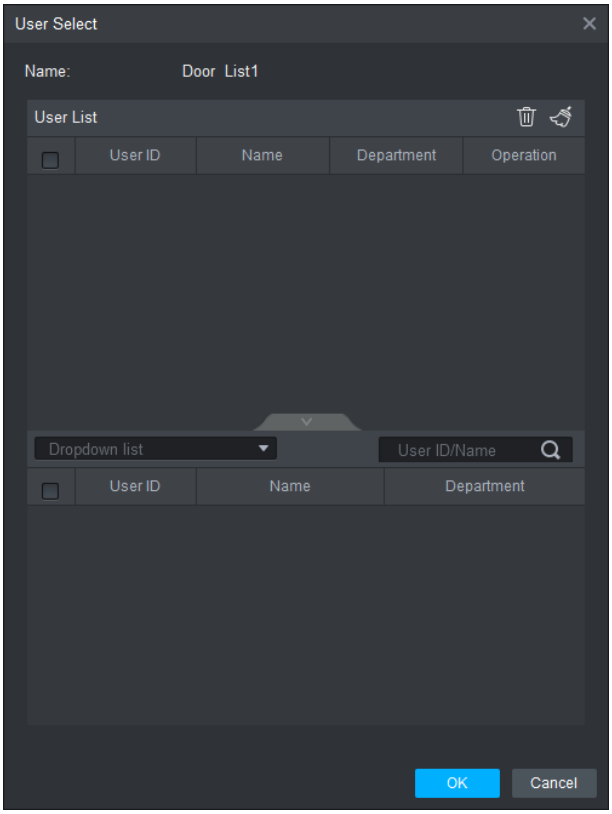


Figura 5-13 Seleccionar usuario



Paso 1 Sobre el **Acceso** interfaz, haga clic  haga clic **Añadir,** y haga clic **Permiso de grupo de puerta.**

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

luego busca usuarios. Seleccione usuarios de los usuarios que encontró. Hacer clic **Terminar**

Paso 3 para completar la configuración.

No se pueden encontrar usuarios sin ID de usuario.

5.5.2 Conceder permiso por ID de usuario

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

Figura 5-14 Acceso

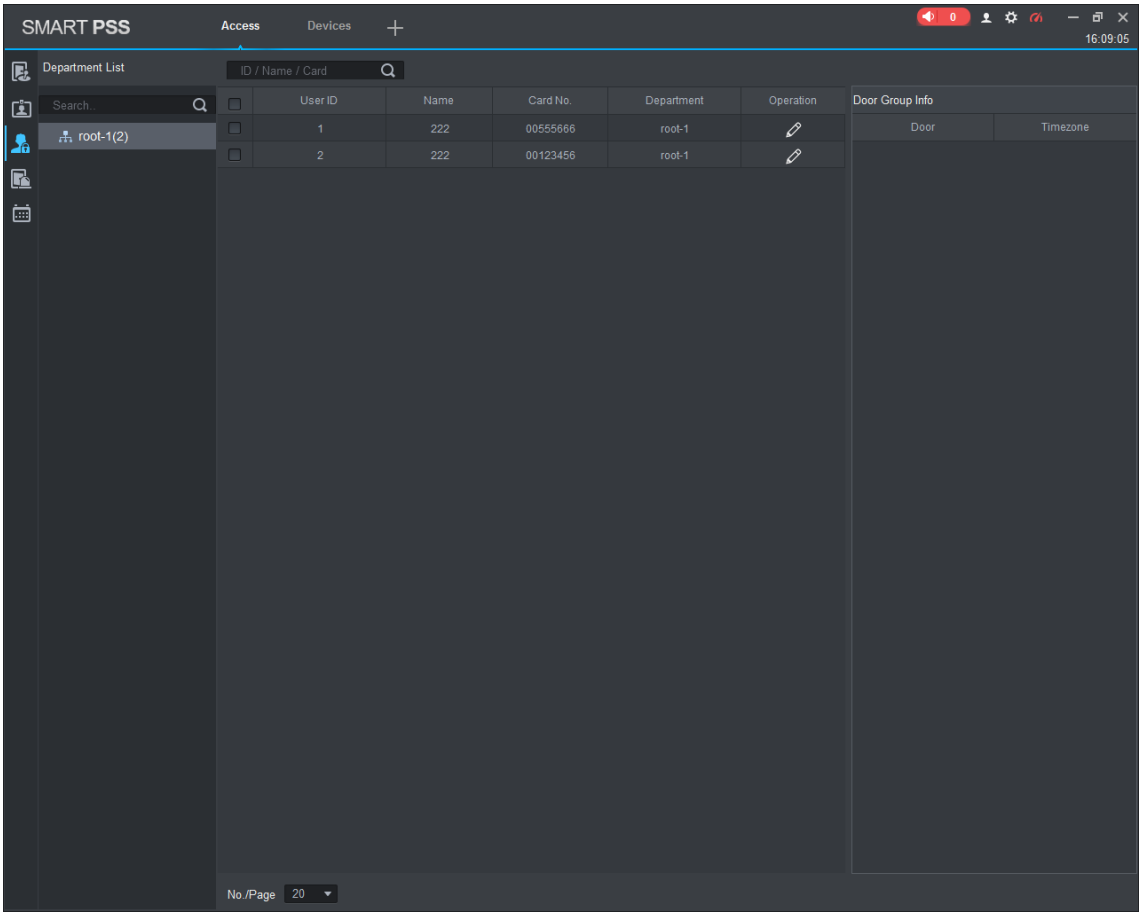
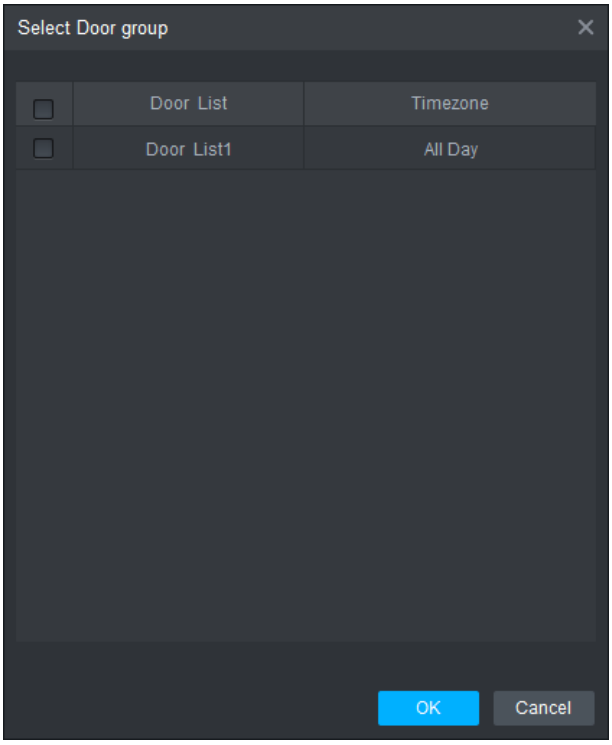


Figura 5-15 Seleccionar grupo de puertas



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

Paso 2 Hacer clic  . Se muestra la interfaz Seleccionar grupo de puertas.

Paso 3 Seleccione el departamento de usuarios en la lista desplegable, o ingrese ID / Nombre de usuario, y luego seleccione un lista de puertas.

Paso 4 Haga clic en Finalizar para completar la configuración.

Apéndice 1 Recomendaciones de ciberseguridad

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

Acciones obligatorias a tomar para la seguridad de la red del equipo básico:

1. Use contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

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

- Sugerimos que descargue y use la última versión del software del cliente.

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

1. Protección física

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

2. Cambie las contraseñas regularmente

Sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinado o descifrado.

3. Establecer y actualizar las contraseñas Restablecer la información a tiempo

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

4. Habilitar bloqueo de cuenta

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

5. Cambiar los puertos HTTP y otros servicios predeterminados

Le sugerimos que cambie los puertos HTTP y otros puertos de servicio predeterminados en cualquier conjunto de números entre 1024 ~ 65535, lo que reduce el riesgo de que personas externas 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. Habilite la lista blanca

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

8. Enlace de dirección MAC

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

9. Asignar cuentas y privilegios razonablemente

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

10. Desactiva los servicios innecesarios y elige 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 seguras y contraseñas de autenticación.
- SMTP: elija TLS para acceder al servidor de buzones.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

11. Transmisión cifrada de audio y video

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

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

12. Auditoría segura

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

13. Registro de red

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

14. Construir un entorno de red seguro

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

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

- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.