

Unidad VTO (Versión 4.6)

Manual del usuario








Prefacio

Este manual presenta la estructura y configuración de la unidad VTO. Lea atentamente antes de usar la unidad VTO y consérvelo para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de señal	Significado
 DANGER	Indica un peligro potencial alto que, si no se evita, provocará la muerte o lesiones graves.
 WARNING	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 CAUTION	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, reducciones en el rendimiento o resultados impredecibles.
	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
 NOTE	Proporciona información adicional como complemento al texto.

Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
Versión 1.0.0	Primer lanzamiento.	Mayo de 2023

Aviso de protección de la privacidad

Como usuario del dispositivo o responsable del tratamiento de datos, podría recopilar datos personales de otras personas, como su rostro, huellas dactilares y número de matrícula. Debe cumplir con las leyes y normativas locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: proporcionar una identificación clara y visible para informar a las personas sobre la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del manual

- Este manual es solo de referencia. Podrían existir ligeras diferencias entre el manual y el producto.
- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas que no cumplan con el manual.
- El manual se actualizará según las últimas leyes y regulaciones de las jurisdicciones pertinentes. Para obtener información detallada, consulte el manual de usuario impreso, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. Este manual es solo de referencia. Podrían existir ligeras diferencias entre la versión electrónica y la versión impresa.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto podrían generar diferencias entre el producto real y el manual. Para obtener el programa más reciente y la documentación complementaria, póngase en contacto con el servicio de atención al cliente.

- Podría haber errores de impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. En caso de duda o controversia, nos reservamos el derecho de ofrecer una explicación definitiva.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de empresas en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta información sobre el manejo adecuado del dispositivo, la prevención de riesgos y la prevención de daños materiales. Lea atentamente antes de usar el dispositivo y siga las instrucciones al usarlo.

Requisitos de operación



- Compruebe si la fuente de alimentación es correcta antes de usarlo.
- No desconecte el cable de alimentación del costado del dispositivo mientras el adaptador esté encendido.
- Utilice el dispositivo dentro del rango nominal de entrada y salida de energía.
- Transporte, utilice y almacene el dispositivo en las condiciones de humedad y temperatura permitidas.
- Si el dispositivo permanece apagado durante más de un mes, debe guardarse en su embalaje original y sellarse. Asegúrese de mantenerlo alejado de la humedad y almacenarlo en las condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquido sobre el dispositivo y asegúrese de que no haya ningún objeto lleno de líquido sobre el dispositivo que evite que el líquido fluya hacia él.
- No desmonte el dispositivo sin instrucciones profesionales.

Requisitos de instalación



- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- Cumpla estrictamente con las normas y códigos de seguridad eléctrica locales. Asegúrese de que el voltaje ambiente sea estable y cumpla con los requisitos de alimentación del dispositivo.
- No conecte el dispositivo a dos o más tipos de fuentes de alimentación, para evitar dañar el dispositivo.
- El uso inadecuado de la batería podría provocar un incendio o una explosión.



- El personal que trabaja en altura debe tomar todas las medidas necesarias para garantizar su seguridad personal, incluido el uso de casco y cinturones de seguridad.
- No coloque el dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- Instale el dispositivo sobre una superficie estable para evitar que se caiga.
- Instale el dispositivo en un lugar bien ventilado y no bloquee su ventilación.
- Utilice un adaptador o fuente de alimentación de gabinete proporcionado por el fabricante.
- Utilice los cables de alimentación recomendados para la región y que cumplan con las especificaciones de potencia nominal.
- La fuente de alimentación debe cumplir con los requisitos de ES1 de la norma IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de la fuente de alimentación se indican en la etiqueta del dispositivo.
- El dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectada a una toma de corriente con conexión a tierra.

目录

Prólogo.....	I
Precauciones y advertencias importantes.....	III
1 Descripción general del producto.....	1
1.1 Introducción.....	1
1.2 Función.....	1
1.3 Panel frontal.....	2
1.3.1 Serie 65.....	2
1.3.2 Serie 75.....	4
1.3.3 Serie 95.....	5
1.4 Panel trasero.....	5
1.4.1 Serie 65.....	6
1.4.2 Serie 75.....	8
1.4.3 Serie 95.....	10
2 Operación VTO.....	12
2.1 Serie 65.....	12
2.1.1 Pantalla de inicio.....	12
2.1.2 Entorno de ingeniería.....	13
2.2 Serie 75/95.....	27
2.2.1 Pantalla de inicio.....	28
2.2.2 Entorno de ingeniería.....	29
2.2.3 Registro del propietario.....	43
2.2.4 Desbloqueo.....	47
2.2.5 Llamada.....	49
2.2.6 Mensajes.....	50
3 Operaciones de la página web.....	51
3.1 Inicio de sesión en la página web.....	51
3.2 Restablecimiento de la contraseña.....	51
3.3 Introducción a la página de inicio.....	52
3.4 Cambiar el mensaje del usuario.....	53
3.5 Importar/Exportar la información del dispositivo.....	54
3.5.1 Importación de la información del dispositivo.....	54
3.5.2 Exportación de la información del dispositivo.....	54
3.6 Importar/Exportar la información del usuario.....	54
3.6.1 Importación de la información del usuario.....	54
3.6.2 Exportación de la información del usuario.....	55
3.7 Configuración local.....	55

3.7.1 Configuración de parámetros de vídeo y audio.....	55
3.7.2 Configuración de parámetros de control de acceso.....	59
3.7.3 Configuración de parámetros del sistema.....	61
3.7.4 Configuración de la gestión de seguridad.....	63
3.7.5 Configuración de parámetros Wiegand.....	64
3.7.6 Configuración de parámetros de detección de rostros.....	64
3.7.7 Agregar usuarios ONVIF.....	66
3.7.8 Configuración de parámetros de reconocimiento de huellas dactilares.....	67
3.7.9 Carga de archivos de audio.....	67
3.7.10 Visualización de la información legal.....	68
3.8 Entorno del hogar.....	68
3.8.1 Adición del VTO.....	68
3.8.2 Adición del VTH.....	68
3.8.3 Adición del VTS.....	68
3.8.4 Adición del IPC.....	69
3.8.5 Visualización de los dispositivos en línea.....	72
3.8.6 Anuncio.....	72
3.8.7 Gestión de personal.....	73
3.9 Red.....	75
3.9.1 Configuración de los parámetros básicos.....	75
3.9.2 Configuración del servicio UPnP.....	82
3.9.3 Configuración del servidor SIP.....	85
3.9.4 Cortafuegos.....	85
3.10 Registros.....	87
3.10.1 Visualización de los registros de llamadas.....	87
3.10.2 Búsqueda de registros de alarmas.....	88
3.10.3 Búsqueda de registros de desbloqueo de la puerta.....	88
3.10.4 Búsqueda en los registros del sistema.....	89
3.11 Reinicio del dispositivo.....	90
3.12 Restauración a los valores predeterminados de fábrica.....	90
3.13 Cerrar sesión.....	90
Apéndice 1 Recomendaciones de ciberseguridad.....	91

1 Descripción general del producto

1.1 Introducción

El portero automático digital (en adelante, "VTO") utiliza una pantalla táctil capacitiva y un marco de aluminio anodizado, y está equipado con una cámara de red de doble lente de 2 MP. El VTO integra un algoritmo de aprendizaje profundo que permite al usuario abrir la puerta mediante la función de reconocimiento. Ofrece múltiples métodos de autenticación, como reconocimiento de código QR, reconocimiento de huellas dactilares y apertura con contraseña. Admite llamadas de emergencia, anuncios, búsqueda de registros y otras funciones. El VTO se utiliza generalmente en zonas residenciales.

1.2 Función

Videollamada y llamada de voz

Realiza llamadas de vídeo y voz al VTH o al VTS.

Llamada grupal

Si el VTO actual funciona como servidor SIP, puede llamar a muchos VTH al mismo tiempo.

Llamada de emergencia

Llama directamente al centro de gestión en caso de emergencia.

Descubrir

- Desbloqueo a través del rostro: el VTO reconoce el rostro utilizando el último algoritmo de aprendizaje profundo y abre la puerta.
- Desbloqueo mediante huella dactilar: El módulo de huella dactilar incorporado reconoce la huella dactilar.
- Desbloqueo a través del código QR: El VTO reconoce el código QR para abrir la puerta.

Siendo monitoreado

El VTH o el centro de gestión pueden supervisar el VTO. El VTO admite hasta seis transmisiones para su supervisión.

Instantánea automática

Toma instantáneas mientras estás en una llamada o desbloqueando la puerta y las almacena en la tarjeta SD.

Control de acceso

Controla directamente las cerraduras.

Gestión de alarmas

El VTO tiene funciones de alarma de manipulación y alarma de detección de detector de puerta.

Conexión con el ascensor

Conéctese con el ascensor para habilitar la función de enlace de control del ascensor.

Iluminación inteligente por infrarrojos

Detecta automáticamente el paisaje real y abre la iluminación.

Operación independiente

Emite las tarjetas, registra las huellas y los rostros a través del dispositivo.

Gestión de sub VTO

El VTO principal puede conectarse con hasta 9 VTO secundarios en la misma unidad.

Anuncio

Envía el anuncio al VTH.

Búsqueda de registros

Admite la búsqueda del registro de llamadas, registro de alarmas y registro de desbloqueo.

1.3 Panel frontal

1.3.1 Serie 65

Los modelos de dispositivo en la primera fila de la siguiente figura son VTO6521F y VTO6521H. Los modelos de dispositivo en la segunda fila de la siguiente figura son VTO6531H y VTO6541H.

Figura 1-1 Panel frontal

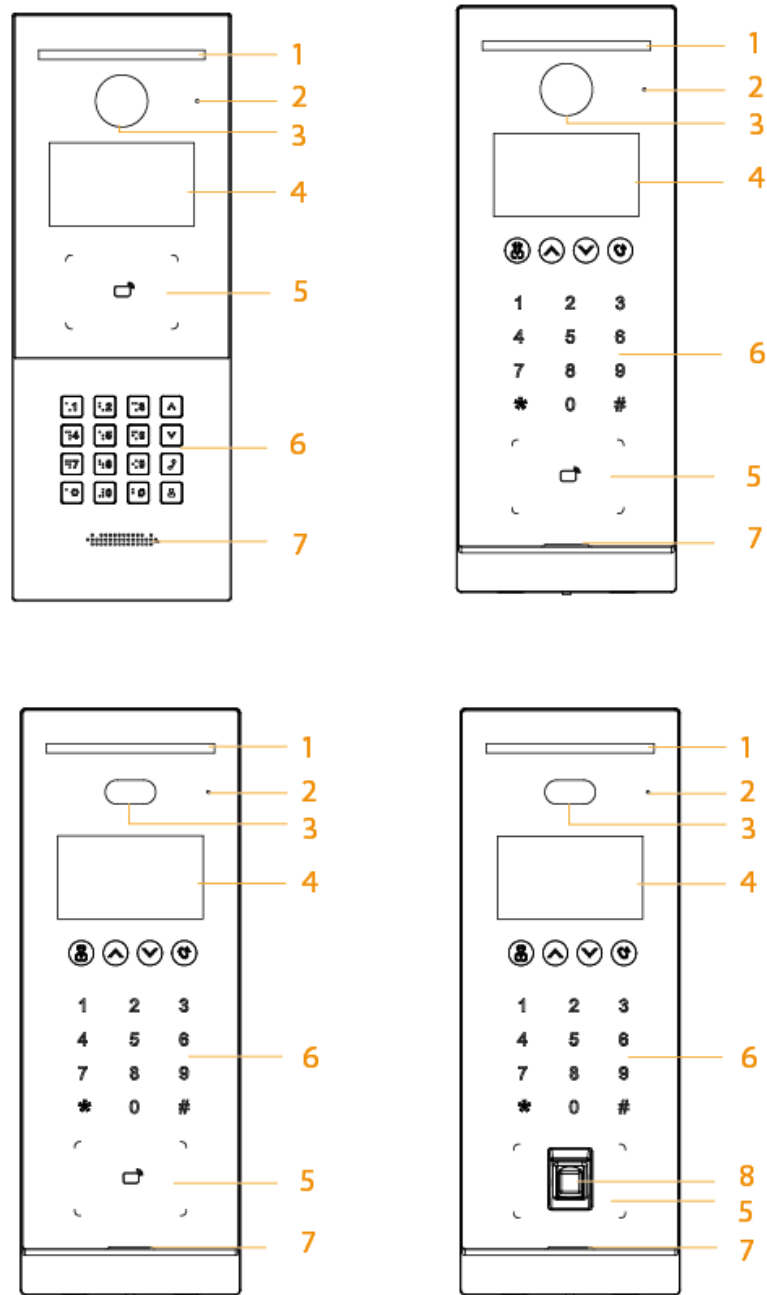


Tabla 1-1 Descripción de componentes

No.	Descripción	No.	Descripción
1	Iluminador blanco	5	Área de deslizamiento de tarjetas
2	micrófono	6	Teclado
3	Cámara	7	Altoparlante
4	Mostrador	8	Sensor de huellas dactilares

1.3.2 Serie 75

Figura 1-2 Panel frontal

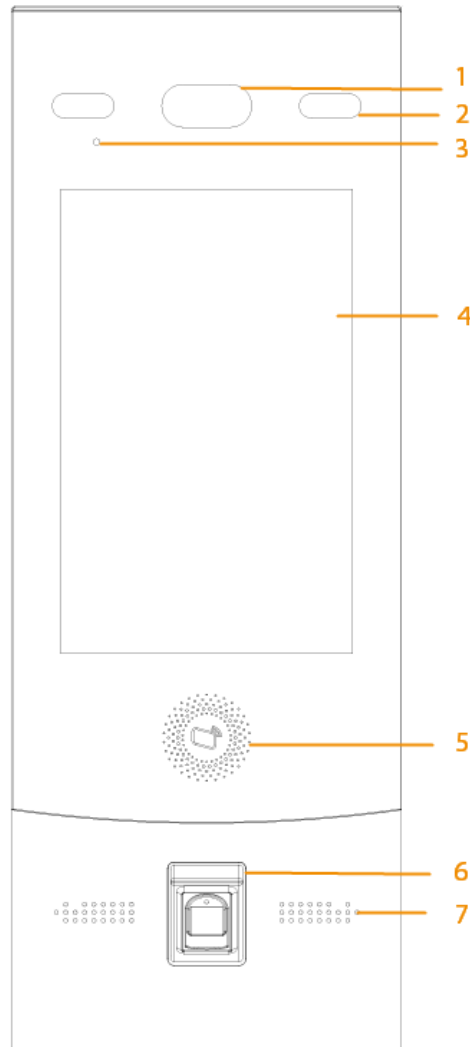


Tabla 1-2 Descripción de los componentes

No.	Descripción	No.	Descripción
1	Cámara	5	Área de deslizamiento de tarjetas
2	Iluminador blanco	6	Sensor de huellas dactilares
3	micrófono	7	Altoparlante
4	Mostrar	—	—

1.3.3 Serie 95

Figura 1-3 Panel frontal

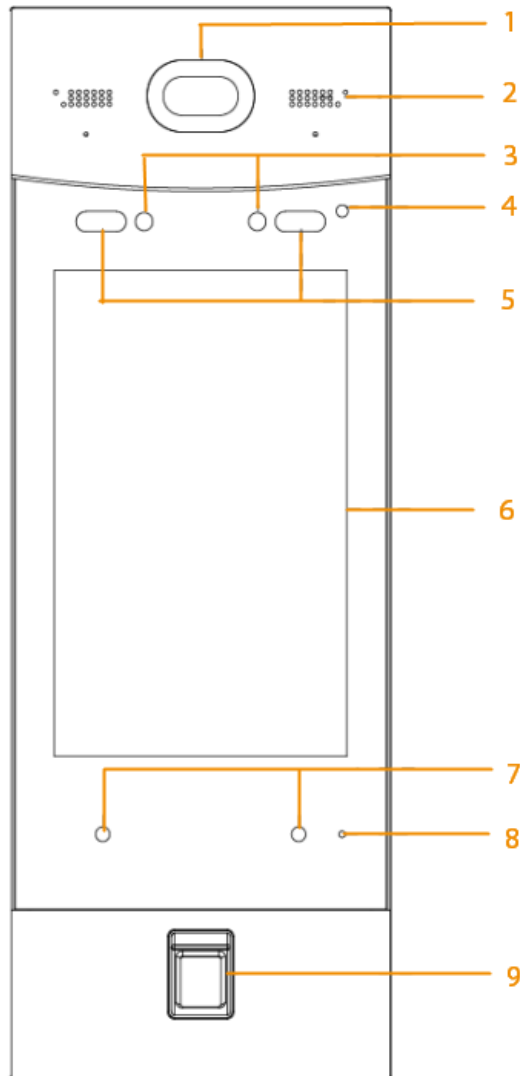


Tabla 1-3 Descripción de los componentes

No.	Descripción	No.	Descripción
1	Cámara	6	Mostrar
2	Altoparlante	7	Sensor de proximidad
3	IR derecha	8	micrófono
4	Fototransistor	9	Sensor de huellas dactilares
5	Iluminador blanco	—	—

1.4 Panel trasero

1.4.1 Serie 65

Figura 1-4 Panel trasero

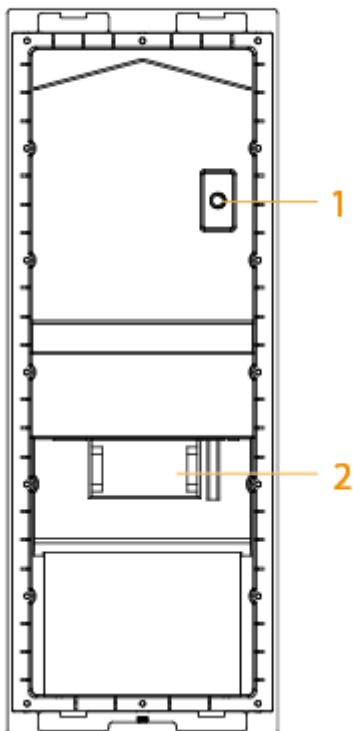


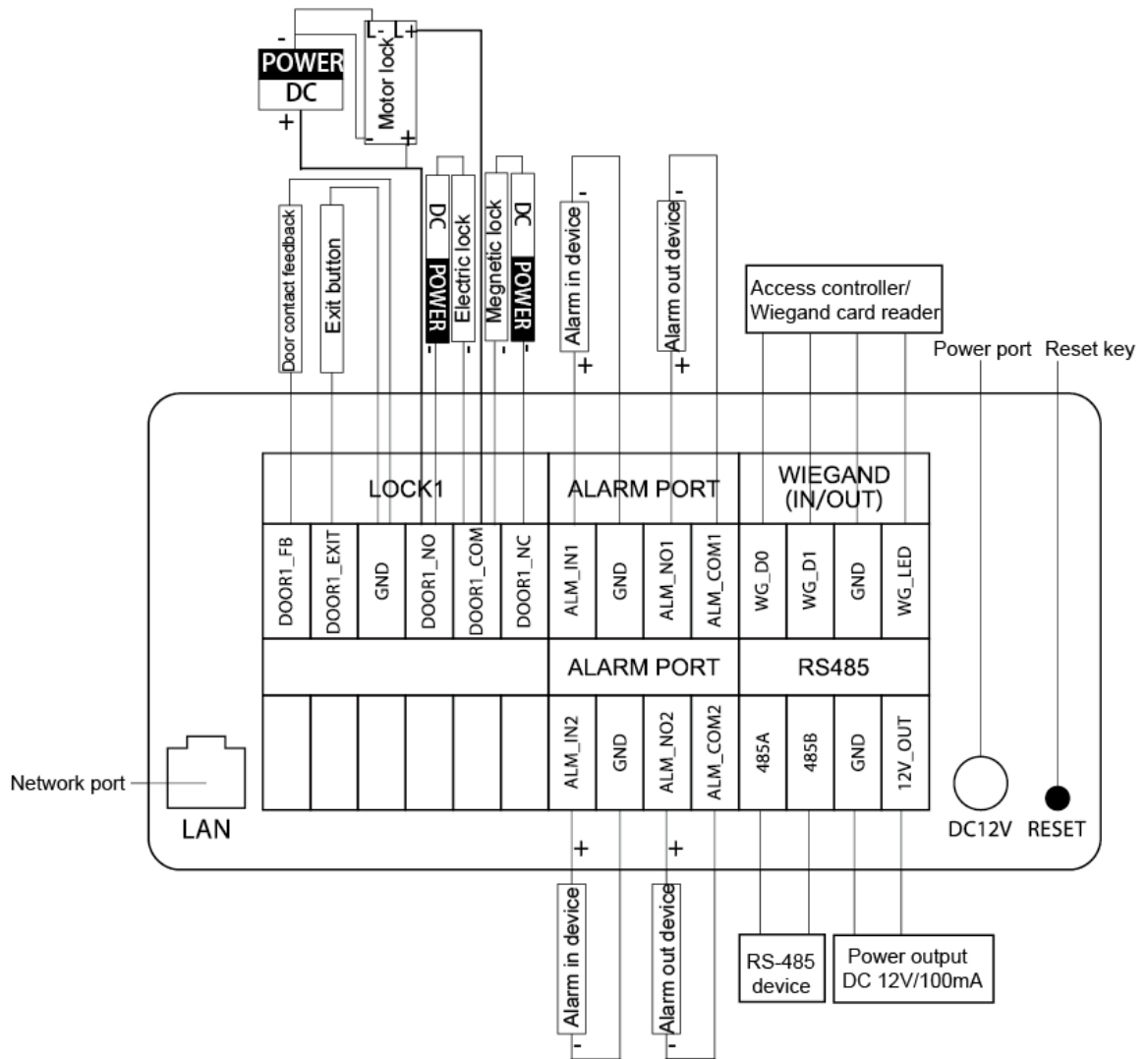
Tabla 1-4 Descripción de los componentes

No.	Descripción
1	Botón de manipulación Dentro de los 5 minutos posteriores a que se enciende el dispositivo, si presiona continuamente el botón de manipulación 5 veces en 8 segundos, el dispositivo emite un pitido y elimina la información de la cuenta.
2	Puertos de funciones (conectados a cerraduras, controladores de acceso, dispositivos de entrada/salida de alarma)



Para obtener detalles sobre el puerto de alimentación, el puerto de red y otros puertos, consulte la Figura 1-5.

Figura 1-5 Conexión del cable



Reiniciar: Pulse el botón de reinicio durante más de 8 segundos para restaurar el dispositivo a la configuración de fábrica. Se eliminarán la IP, la cuenta, la configuración y la información de la base de datos.

1.4.2 Serie 75

Figura 1-6 Panel trasero

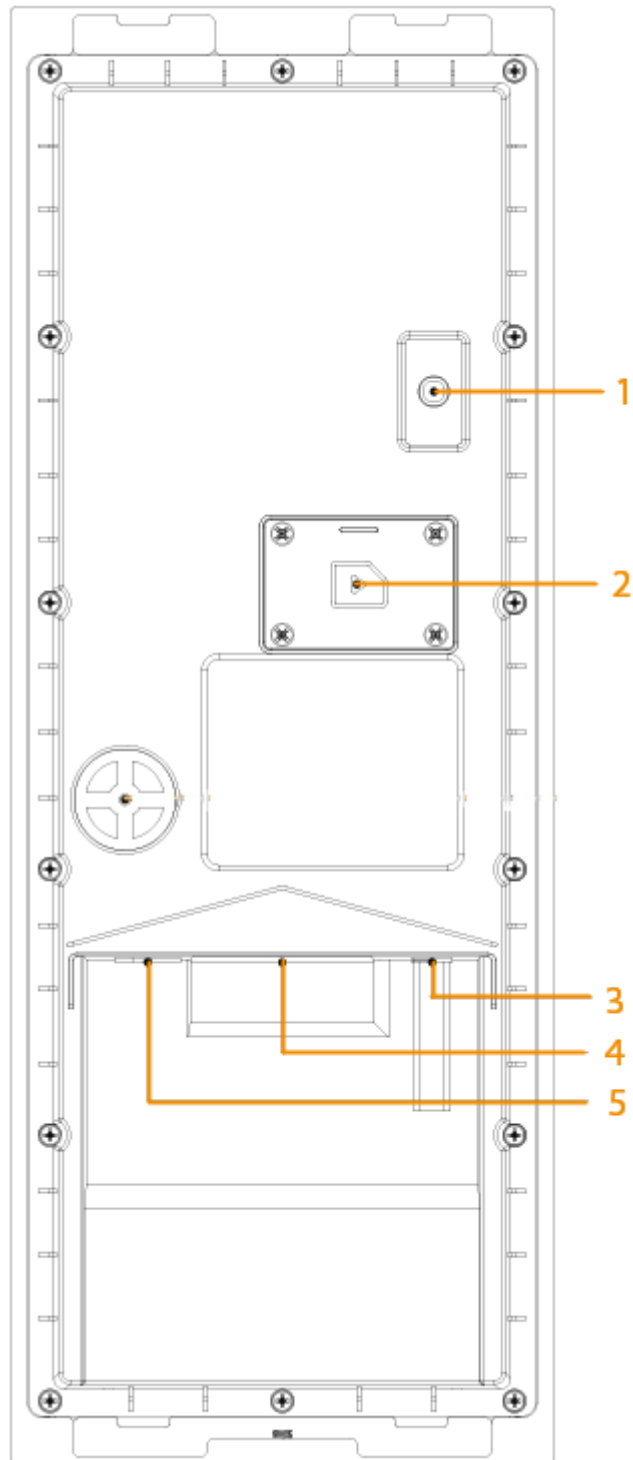


Tabla 1-5 Descripción de componentes

No.	Descripción
1	Botón de manipulación

No.	Descripción
	Dentro de los 5 minutos posteriores a que se enciende el dispositivo, si presiona continuamente el botón de manipulación 5 veces en 8 segundos, el dispositivo emite un pitido y elimina la información de la cuenta.
2	Cubierta de la tarjeta SIM
3	Puerto de alimentación
4	Puertos de función (como puerto de entrada/salida de alarma, puerto de bloqueo y puerto wiegand)
5	Puerto Ethernet

Figura 1-7 Conexión del cable (1)

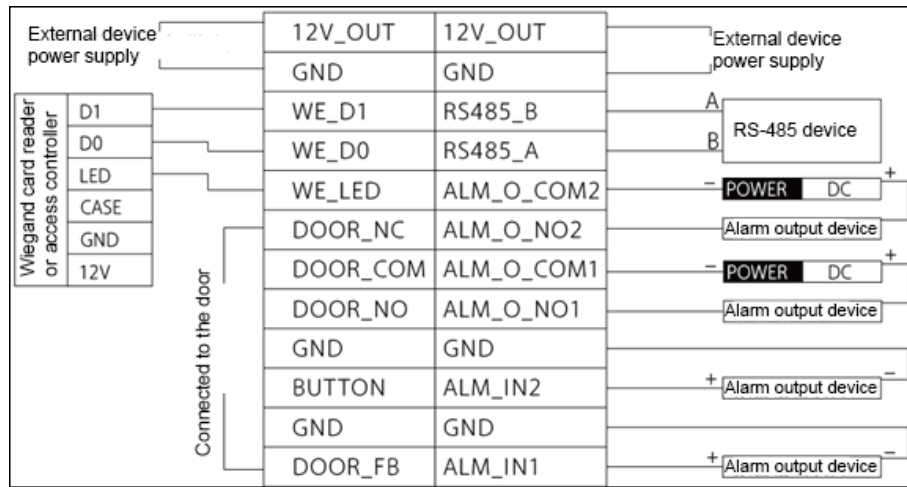
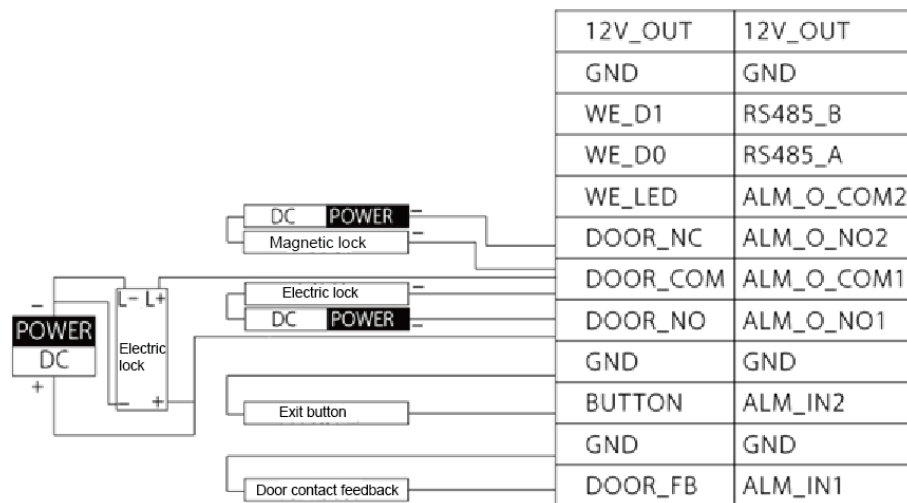


Figura 1-8 Conexión del cable (2)



1.4.3 Serie 95

Figura 1-9 Panel trasero

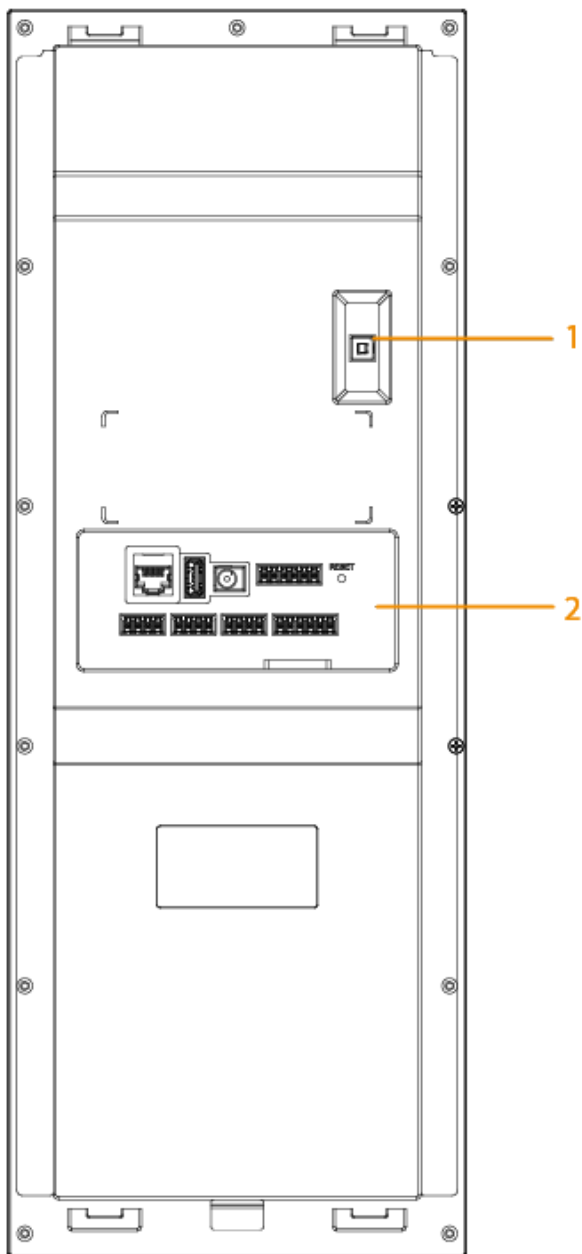


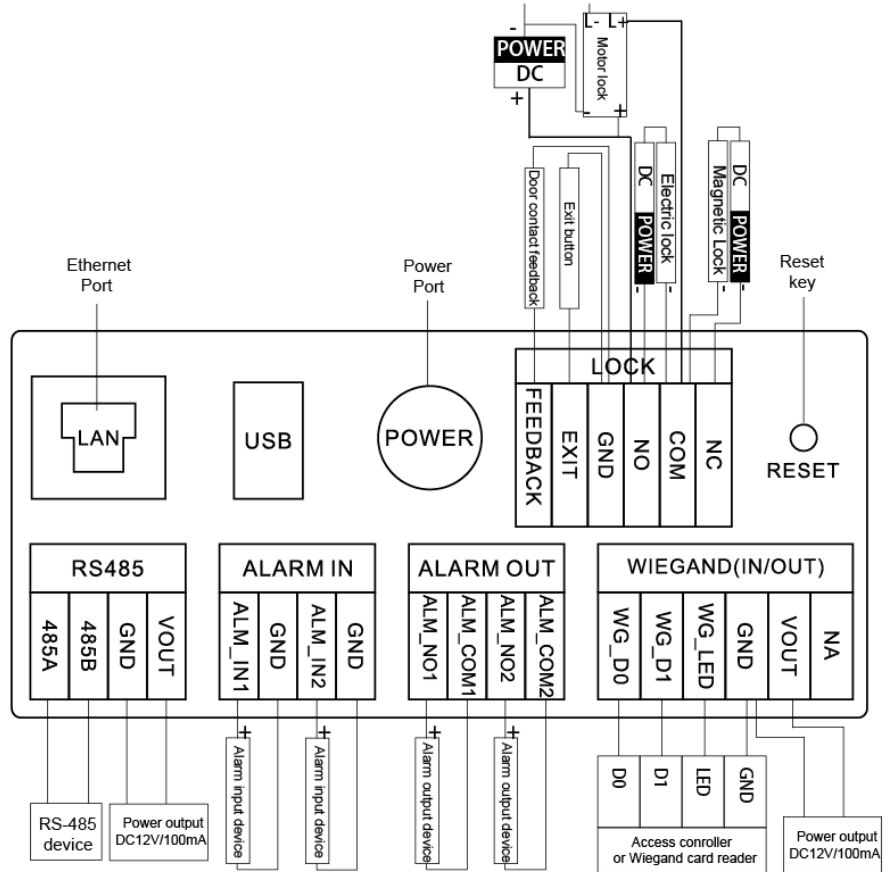
Tabla 1-6 Descripción de los componentes

No.	Descripción
1	Botón de manipulación Dentro de los 5 minutos posteriores a que se enciende el dispositivo, si presiona continuamente el botón de manipulación 5 veces en 8 segundos, el dispositivo emite un pitido y elimina la información de la cuenta.
2	Puertos de función



Para obtener detalles sobre el puerto de alimentación, el puerto de red y otros puertos, consulte la Figura 1-10.

Figura 1-10 Conexión del cable



Reiniciar: Pulse el botón de reinicio durante más de 8 segundos para restaurar el dispositivo a la configuración de fábrica. Se eliminarán la IP, la cuenta, la configuración y la información de la base de datos.

Operación 2 VTO

Este capítulo presenta las operaciones en los dispositivos y utiliza 2 tipos como ejemplos según la pantalla mostrada.

Serie 2.1 65

Los dispositivos de la serie 65 utilizan el siguiente estilo de pantalla.



Las siguientes instantáneas de los dispositivos son solo de referencia y es posible que se encuentren ligeras diferencias en la pantalla de operación del VTO, según su modelo.

2.1.1 Pantalla de inicio

Figura 2-1 Pantalla de inicio

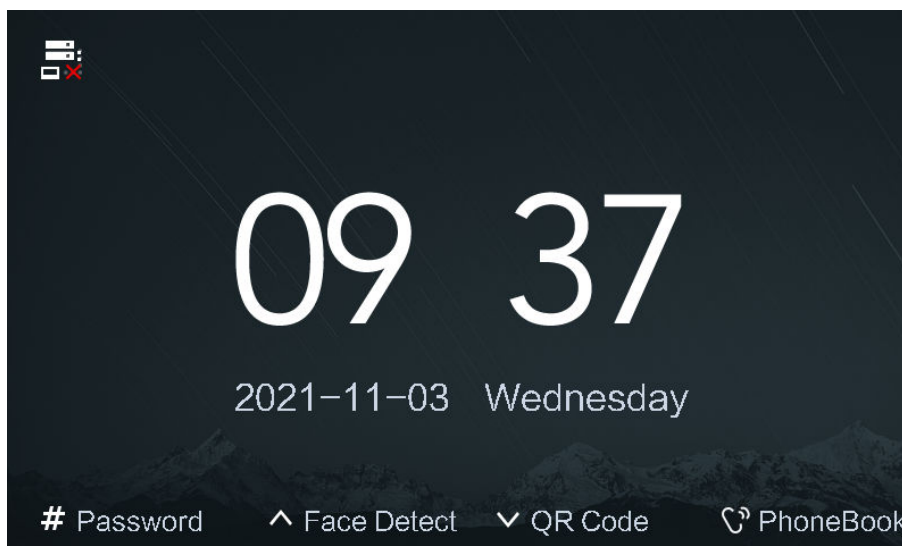


Tabla 2-1 Descripción de las instrucciones de la pantalla de inicio

Instrucción	Descripción
	Muestra el estado del servidor SIP.
# Password	Presione # y luego ingrese la contraseña para abrir la puerta.
^ Face Detect	Presione ^ y el VTO detectará la cara para abrir la puerta.
v QR Code	Presione v y luego escanee el código QR para abrir la puerta.
PhoneBook	Prensa para ver la agenda telefónica.

2.1.2 Configuración de ingeniería

La configuración de ingeniería está diseñada para que los administradores realicen configuraciones avanzadas en el VTO, incluida la emisión de tarjetas de acceso, la modificación de la dirección IP del dispositivo y la adición de personas.

Procedimiento

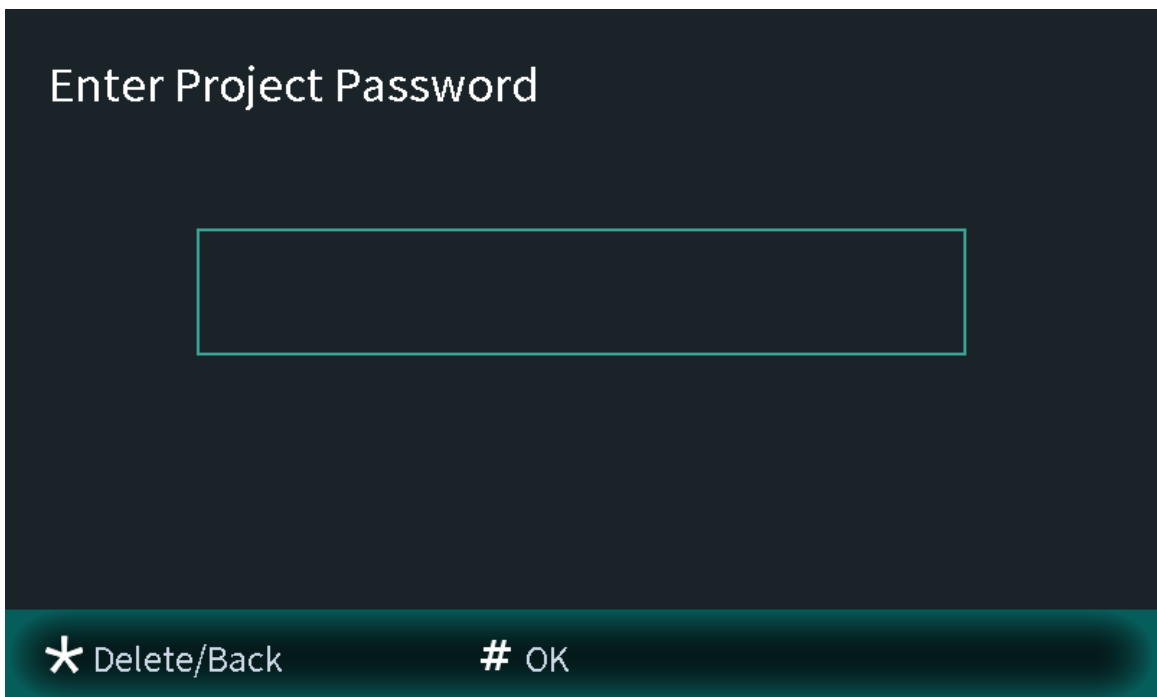
Paso 1 Prensas*En el VTO, cuando se muestre la pantalla de inicio,

Paso 2 introduzca la contraseña del proyecto.



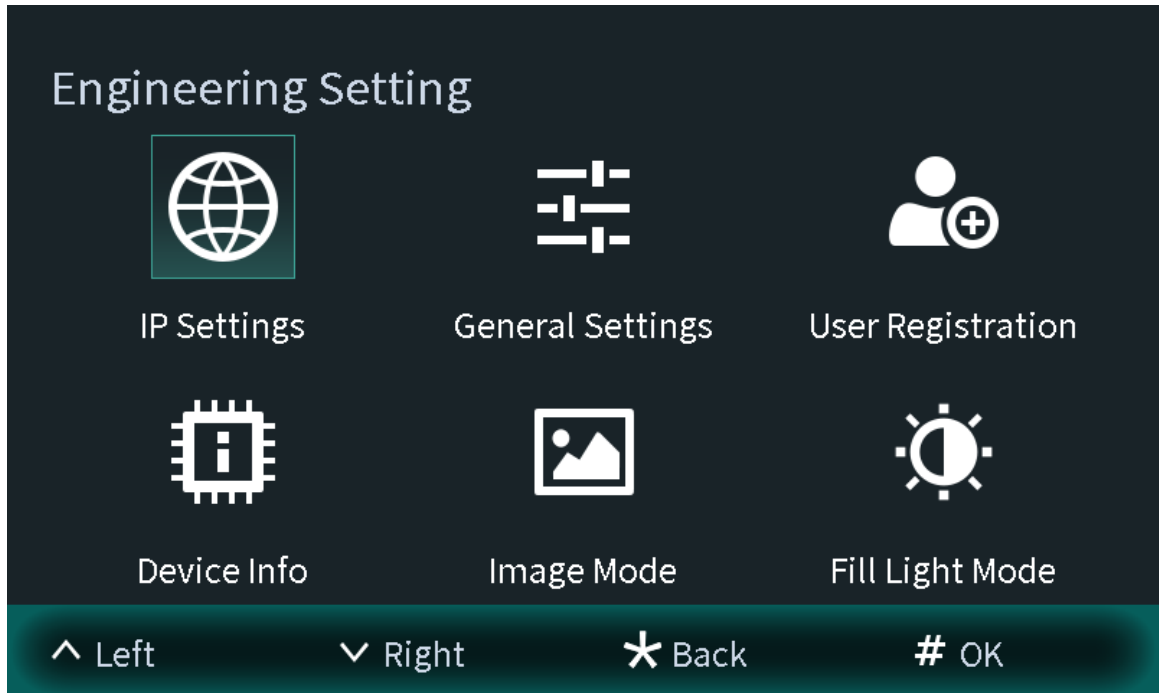
Debes configurar la contraseña del proyecto seleccionando **Configuración local** > **Control de acceso** > **Local** en la página web de la VTO.

Figura 2-2 Ingrese la contraseña



Paso 3 Prensas#para ingresar al entorno de ingeniería.

Figura 2-3 Configuración de ingeniería



2.1.2.1 Configuración de la dirección IP

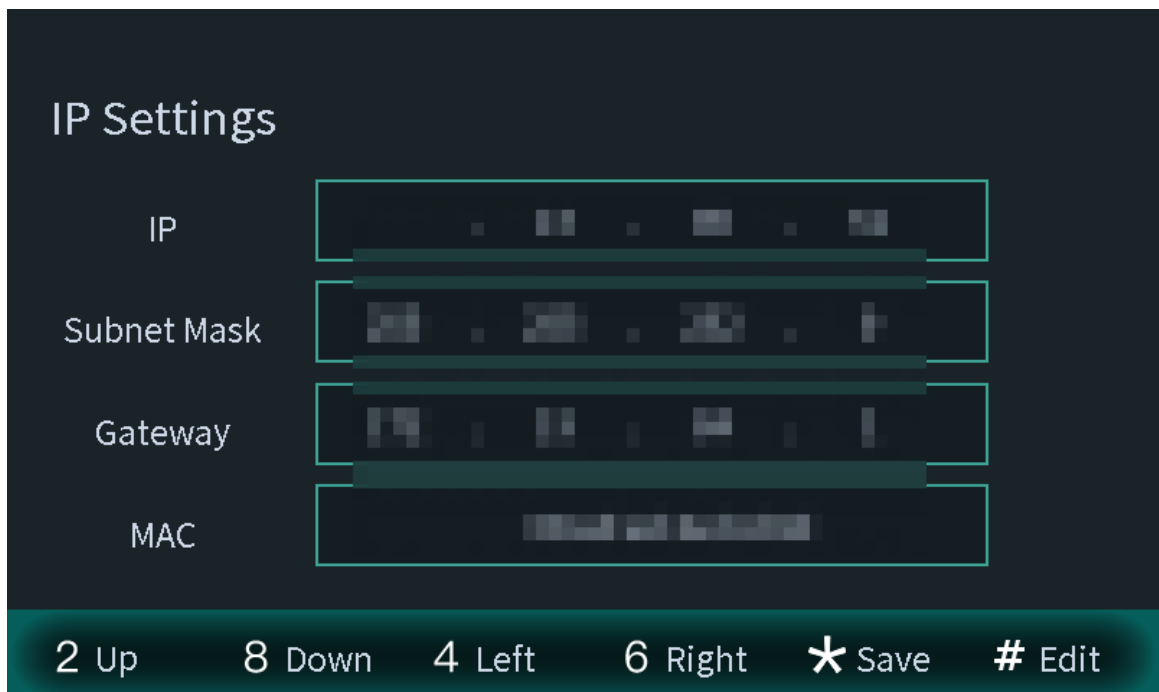
Configurar la dirección IP del VTO.

Procedimiento

Paso 1 Seleccionar **Configuración de IP** en el **Configuración de ingeniería** pantalla.

Paso 2 Ingrese la dirección IP, la máscara de subred y la puerta de enlace.

Figura 2-4 Configurar la IP




Paso 3 Presiona * para completar la configuración.

2.1.2.2 Configuración general

Seleccionar **Configuración general** Para configurar el volumen, la duración del protector de pantalla y el brillo. Después de la configuración, pulse * para guardar y volver a **Configuración general** pantalla.

Volumen

Prensa  para aumentar el volumen.


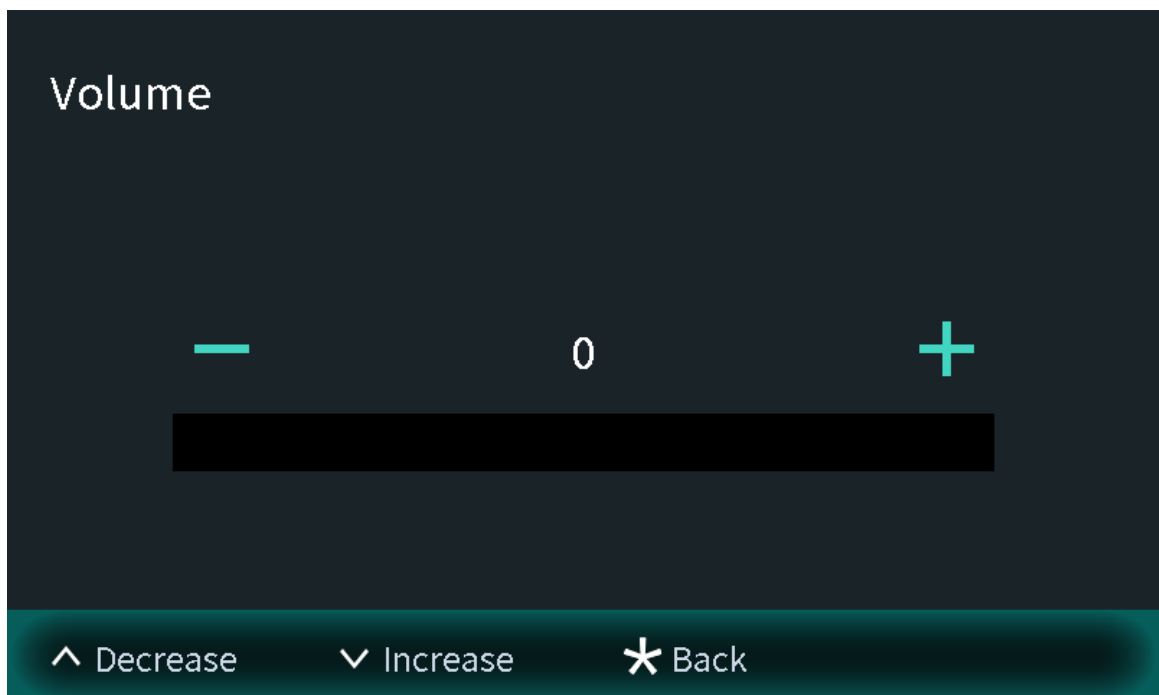

Prensa  para disminuir el volumen.

Figura 2-5 Configuración del volumen



Tiempo de protector de pantalla

Prensa  para aumentar el tiempo del protector de pantalla.


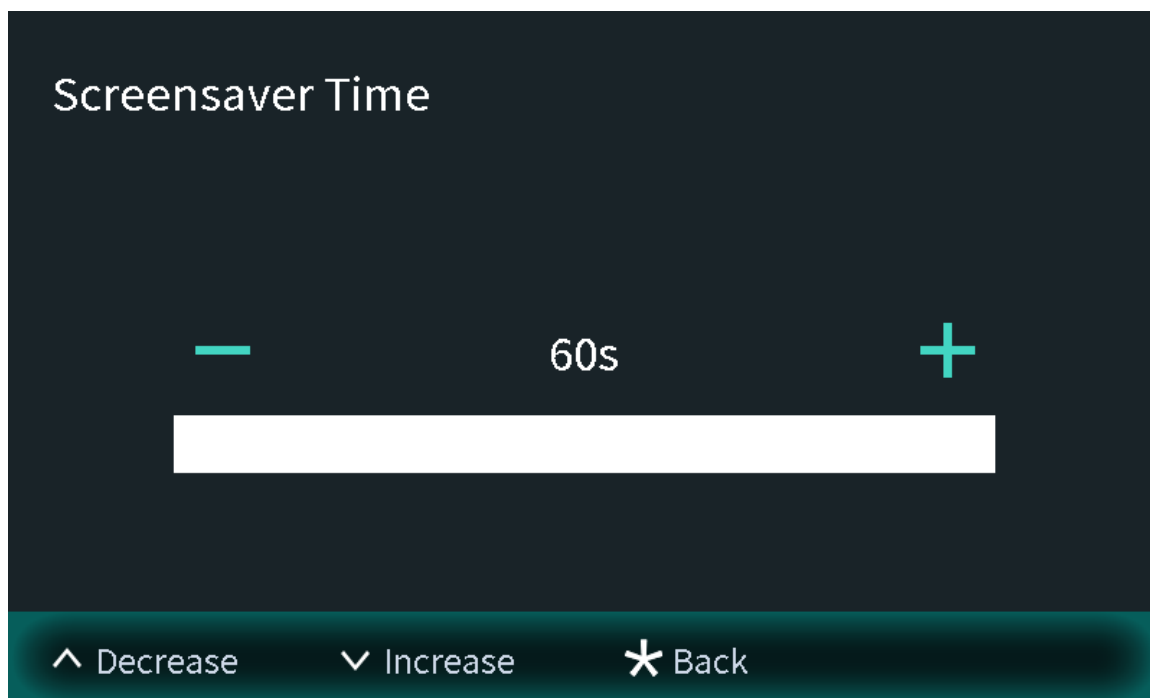

Prensa  para disminuir el tiempo del protector de pantalla.

Figura 2-6 Tiempo del protector de pantalla



Tiempo de brillo

Prensa  para aumentar el tiempo de brillo.


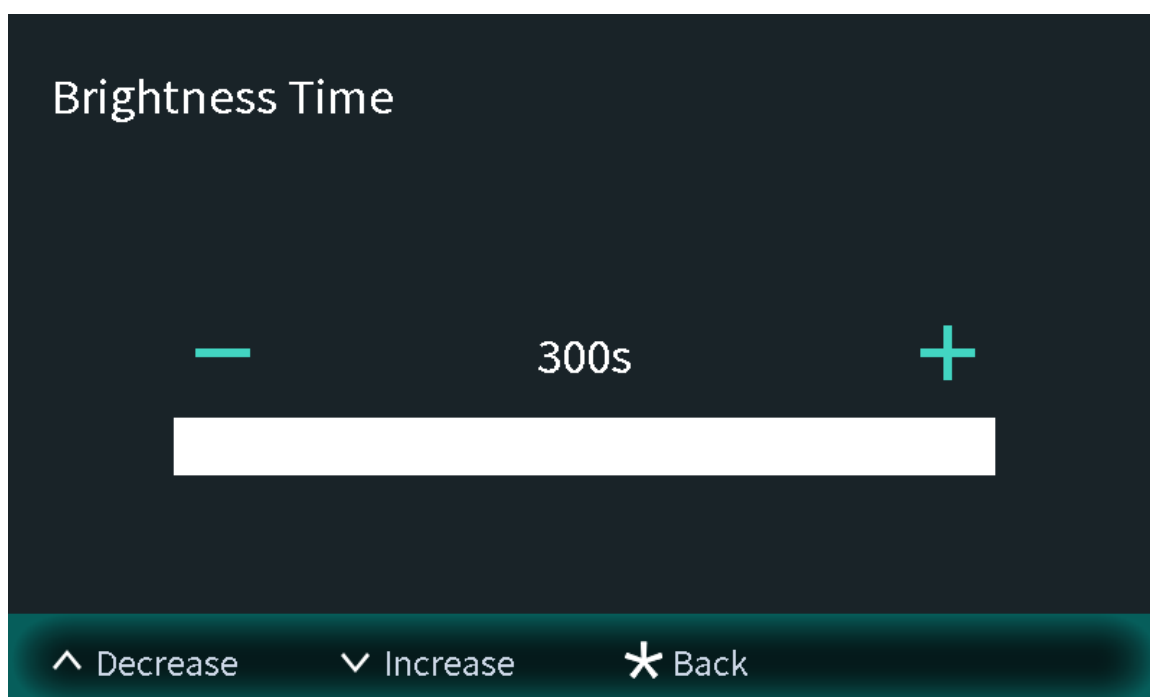
Prensa  para disminuir el tiempo de brillo.

Figura 2-7 Tiempo de brillo



2.1.2.3 Registro de usuario

Debe registrar usuarios para desbloquear puertas. Los métodos de desbloqueo incluyen tarjeta, reconocimiento facial, huella dactilar, código QR y contraseña. Puede agregar métodos de desbloqueo después de configurar la información del personal.

- Si el VTO actual u otro VTO funciona como servidor SIP, registre al usuario en el VTO.
- Si la plataforma funciona como servidor SIP, la plataforma envía la información de imágenes faciales, huellas dactilares y tarjetas al VTO.



Los métodos de desbloqueo pueden variar según el producto. Algunos métodos están disponibles en algunos modelos.

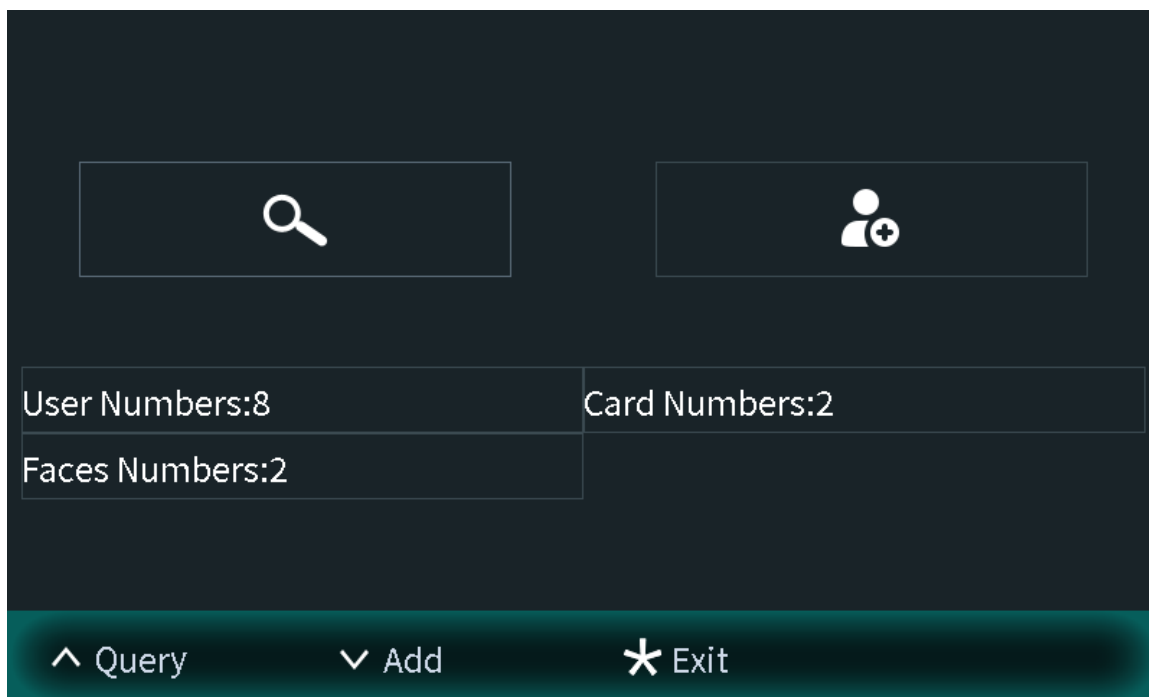
2.1.2.3.1 Agregar el usuario

La información básica incluye número de personal, número de habitación y nombre de usuario.

Procedimiento

Paso 1 Seleccionar **Registro de usuario** en el **Configuración de ingeniería** pantalla.

Figura 2-8 Registro de usuario



Paso 2 Prensa  para agregar el usuario.

Figura 2-9 Agregar el usuario

Please input user information

User ID 0 *

Room No. *

Lock Local Second Lock

^ Switch v Delete # OK * Back

Paso 3 Ingrese el ID de usuario y el número de habitación, configure las cerraduras y luego presione#para guardar la información.

2.1.2.3.2 Agregar caras

Añade caras de usuarios registrados para desbloquear la puerta.

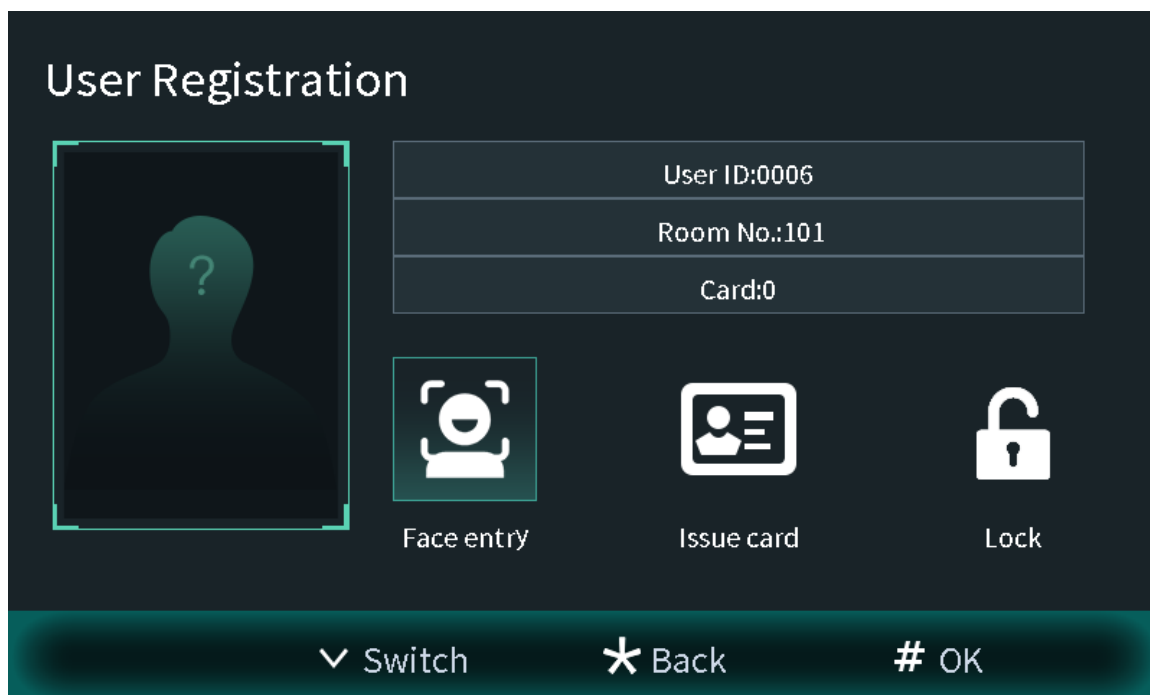


El reconocimiento facial está disponible en modelos seleccionados.

Procedimiento

Paso 1 Seleccionar**Entrada de cara**en el**Registro de usuario** pantalla.

Figura 2-10 Entrada de rostro



Paso 2 Coloca tu cara en el centro del marco y la imagen de tu cara se tomará automáticamente.

La imagen del rostro se tomará automáticamente. Si no está satisfecho con la imagen, pulse * para cancelar la foto.

Figura 2-11 Registro facial



Paso 3 Prens # para guardar la foto.

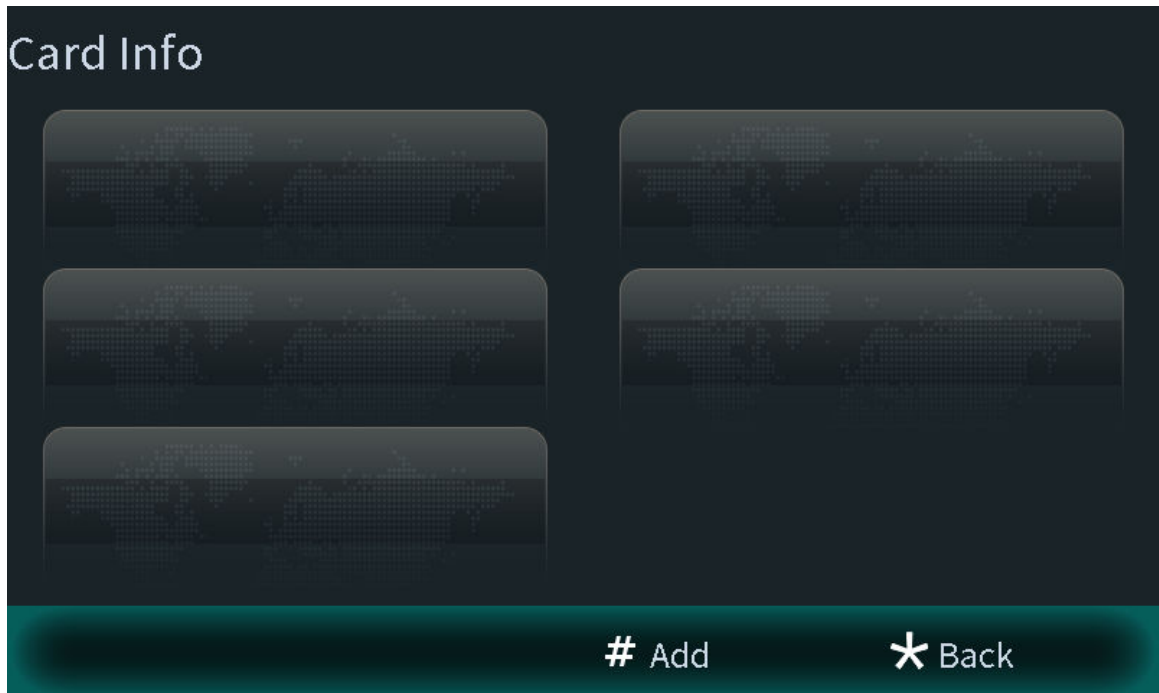
2.1.2.3.3 Emisión de tarjetas

Puedes emitir hasta 5 tarjetas para cada usuario.

Procedimiento

Paso 1 Seleccionar **Tarjeta de emisión** en el **Registro de usuario** pantalla y luego presione **#** para agregar la tarjeta.

Figura 2-12 Información de la tarjeta



Paso 2 Seleccionar **Tarjeta principal** o **contraseña** para emitir tarjetas.

1. Seleccionar **Tarjeta principal** Si desea emitir tarjetas a través de la tarjeta principal, luego deslice su tarjeta principal en el lector de tarjetas para continuar con el proceso de emisión de tarjetas.



Si no tiene una tarjeta principal, emita una en la VTO mediante contraseña. Luego, vaya a la página web de la VTO y seleccione **Entorno del hogar > Gestión de personal**, y



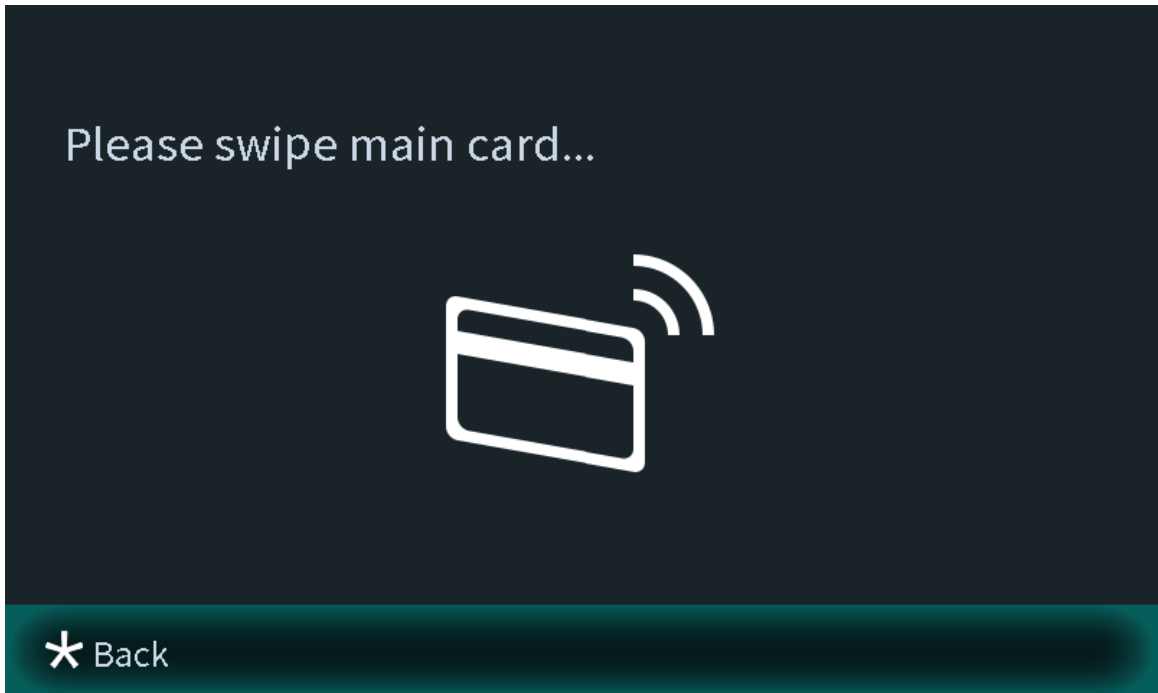
Haga clic en  luego configure una tarjeta como su tarjeta principal haciendo clic en .

Figura 2-13 Deslizar la tarjeta principal

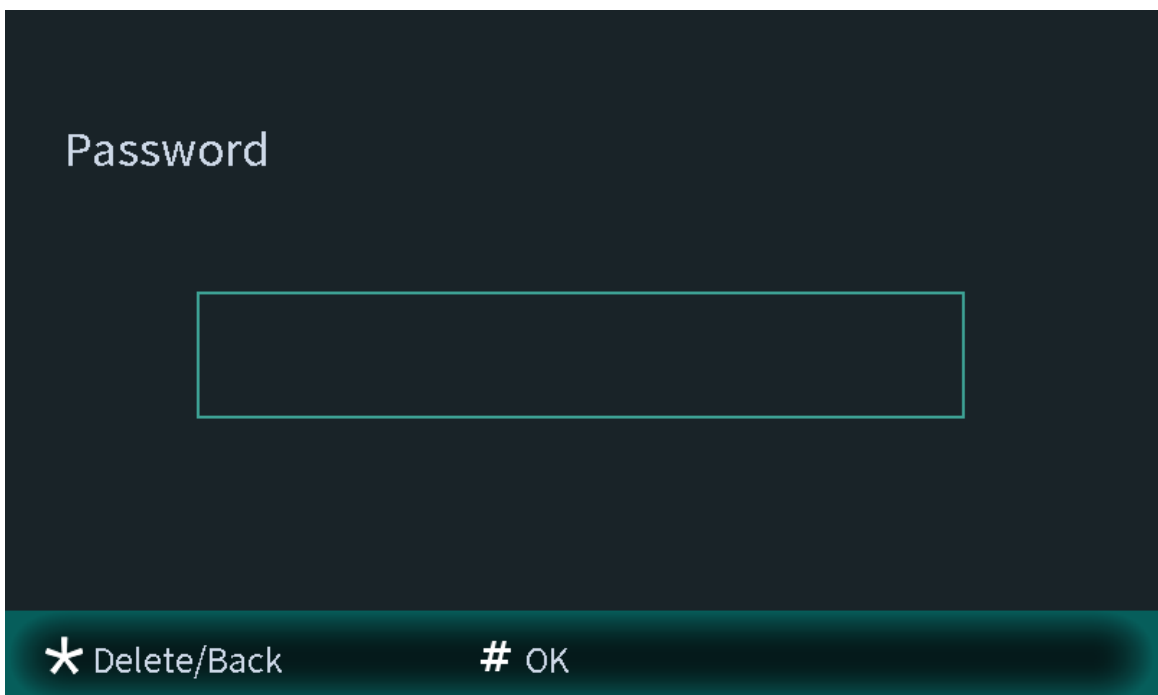


2. Seleccionar **Contraseña** Si desea emitir tarjetas mediante contraseña, introdúzcala y pulse #.



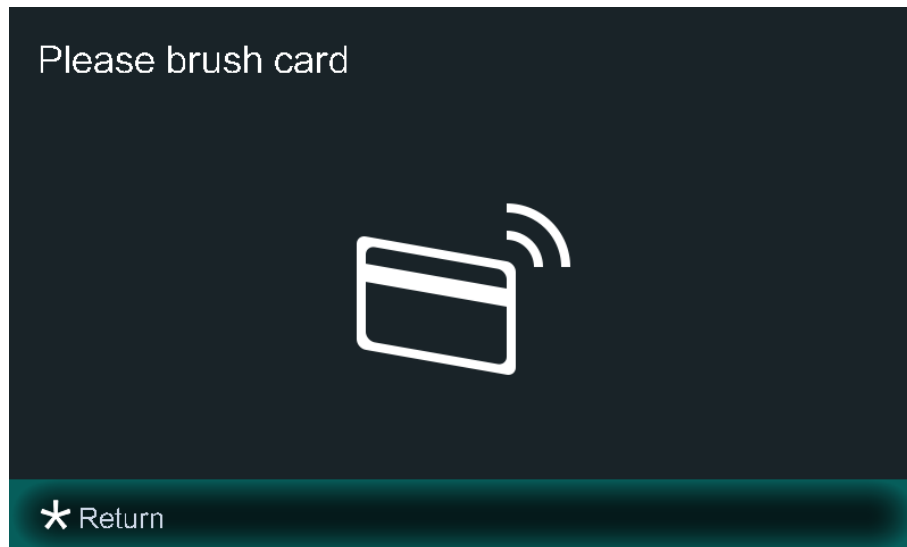
Es necesario introducir la contraseña en **Contraseña de la tarjeta de emisión** cuadro de texto que usted planeó en la página web del VTO a través de **Configuración local > Control de acceso > Local**.

Figura 2-14 Contraseña de la tarjeta principal



Paso 3 Pase la tarjeta por el lector y los números de tarjeta se reconocerán automáticamente.

Figura 2-15 Registro de nueva tarjeta

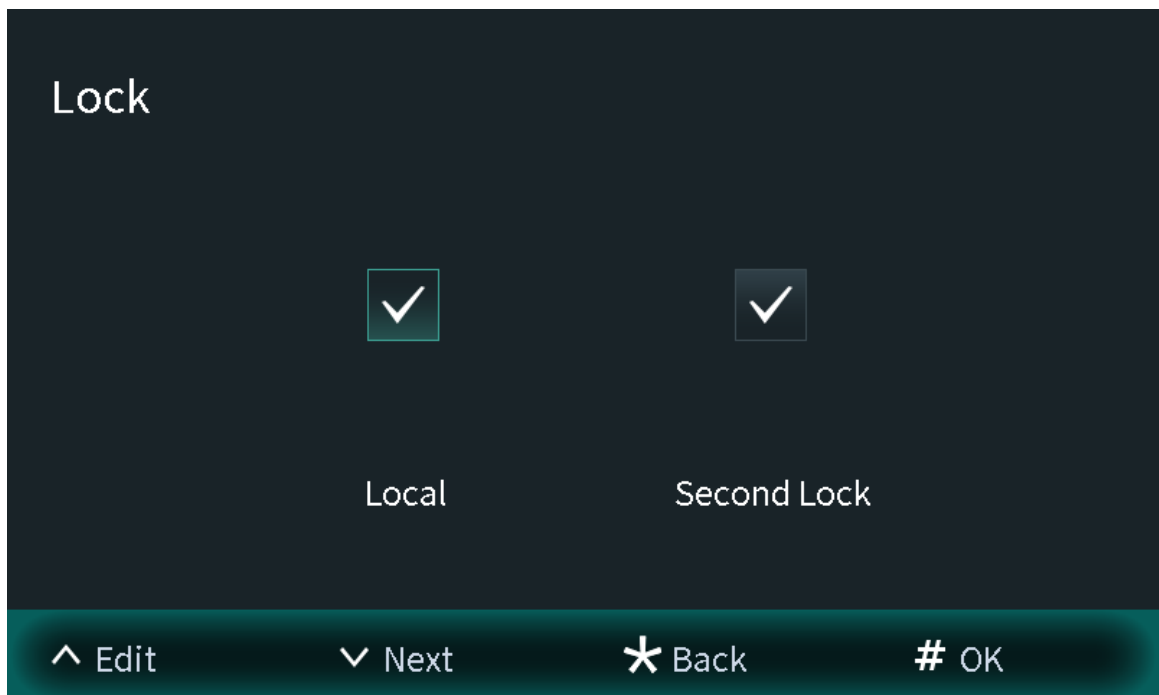


2.1.2.3.4 Configuración de las cerraduras

Seleccionar **Cerrar** en el **Registro de usuario** Pantalla para configurar la autoridad para abrir la cerradura local y la segunda cerradura.

- Seleccionar **Local**, y el usuario tendrá autoridad para abrir la cerradura local.
- Seleccionar **Segunda cerradura**, y el usuario tendrá autoridad para abrir la segunda cerradura que se conecta al VTO a través del puerto de función.

Figura 2-16 Bloqueo



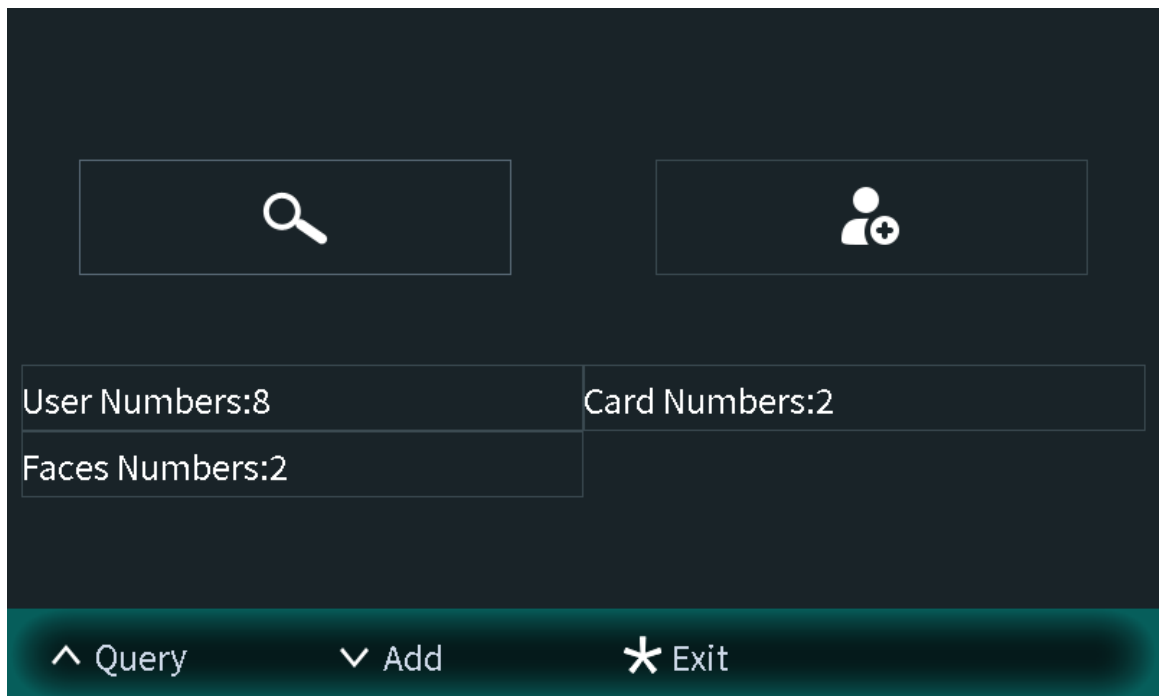
2.1.2.3.5 Búsqueda del usuario

Vea la información del usuario según su ID o número de habitación. Puede configurarla.

Procedimiento

Paso 1 Seleccionar **Registro de usuario** en el **Configuración de ingeniería** pantalla.

Figura 2-17 Registro de usuario




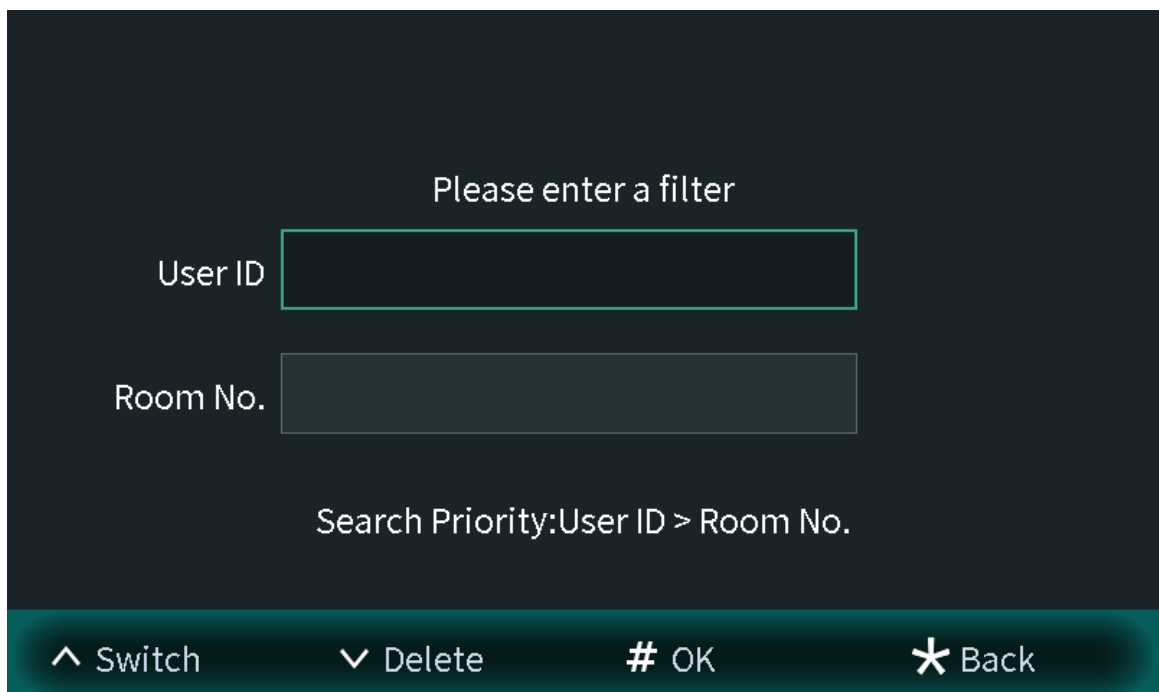
Paso 2 Presione  luego ingrese el número de identificación de usuario o el número de habitación.

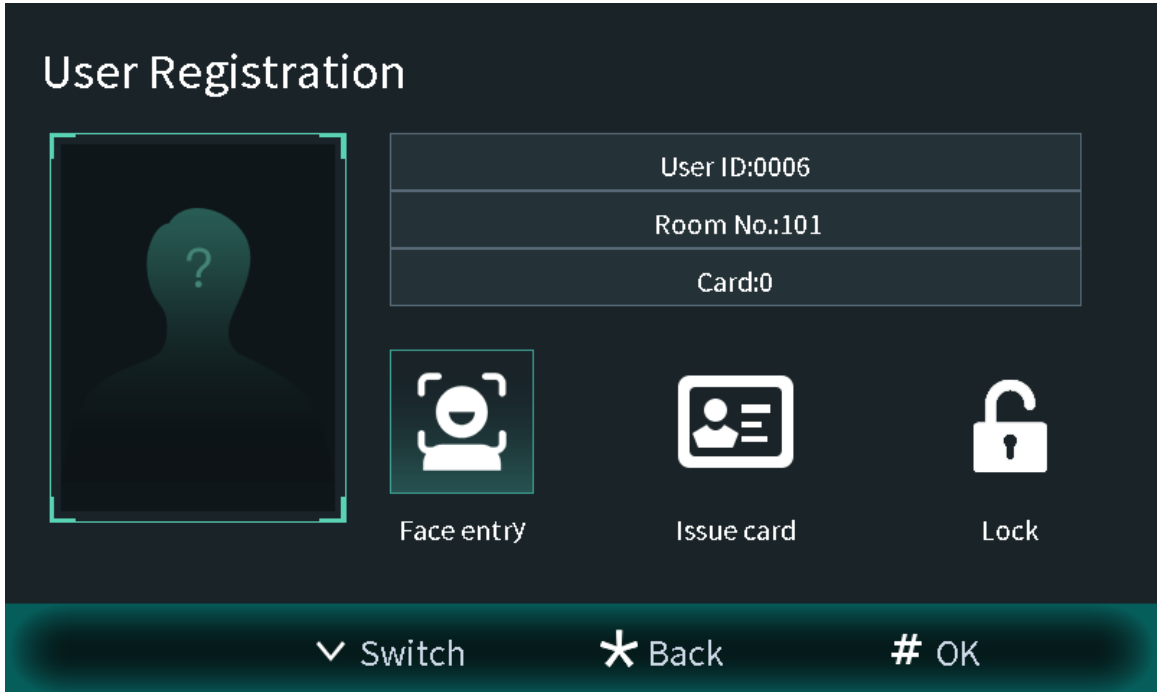
Figura 2-18 Búsqueda del usuario



Paso 3 Prensas# para ver la información del usuario.

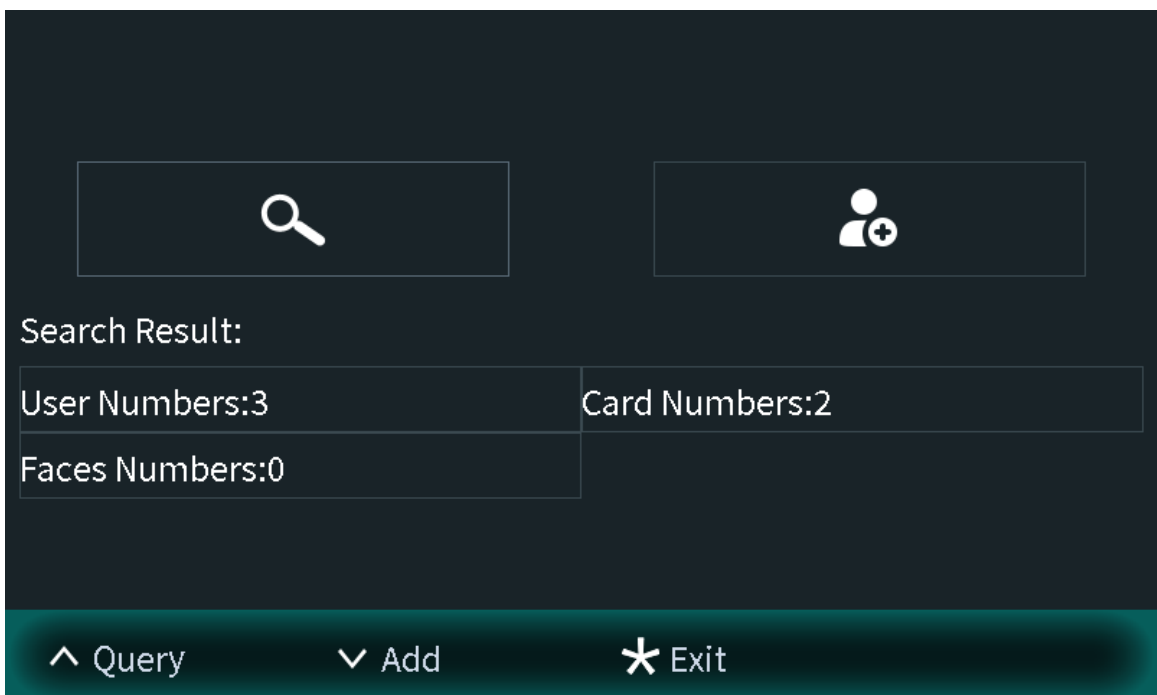
- Ingrese el ID de usuario para ver su información. También puede configurar las imágenes faciales, las tarjetas y los candados.

Figura 2-19 Información del usuario



- Ingrese el número de habitación para ver los números de usuario, números de tarjeta y números de imagen facial de la habitación.

Figura 2-20 Resultado de la búsqueda



2.1.2.4 Visualización de la información del dispositivo

Puede ver el número de puerto web, la versión del software, la versión de MCU y la versión del algoritmo.

Procedimiento

Paso 1 Seleccionar **Información del dispositivo** en el **Configuración de ingeniería**

Paso 2 Pantalla  /  para cambiar las páginas.

Figura 2-21 Información del dispositivo (1)

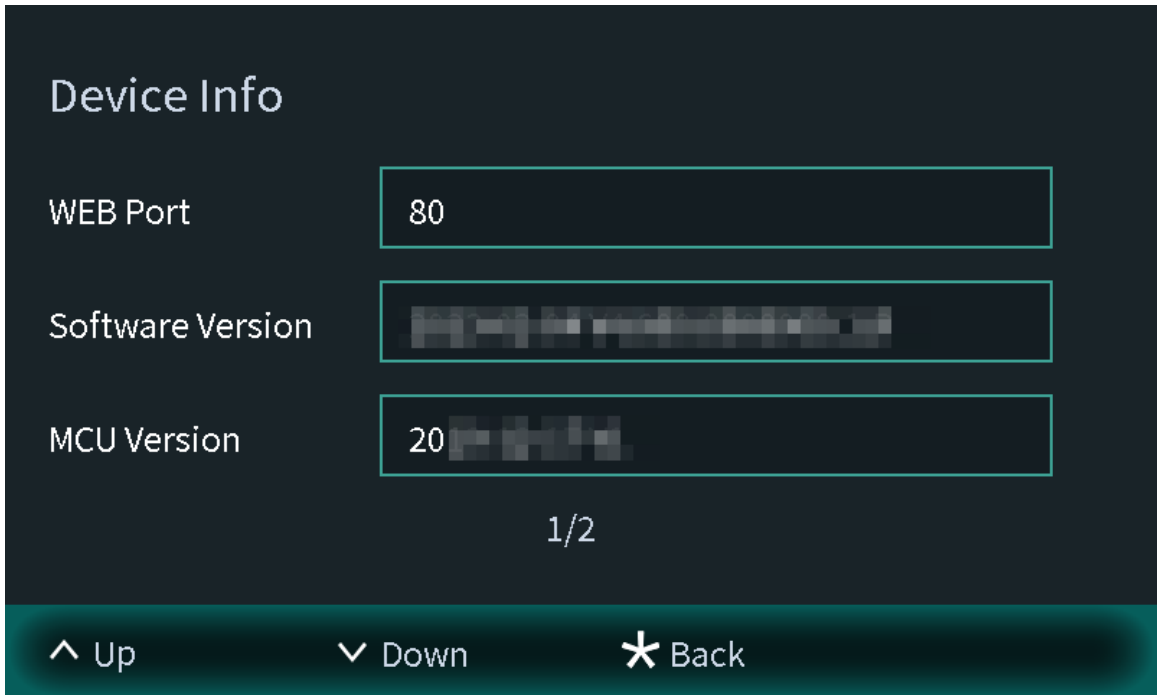
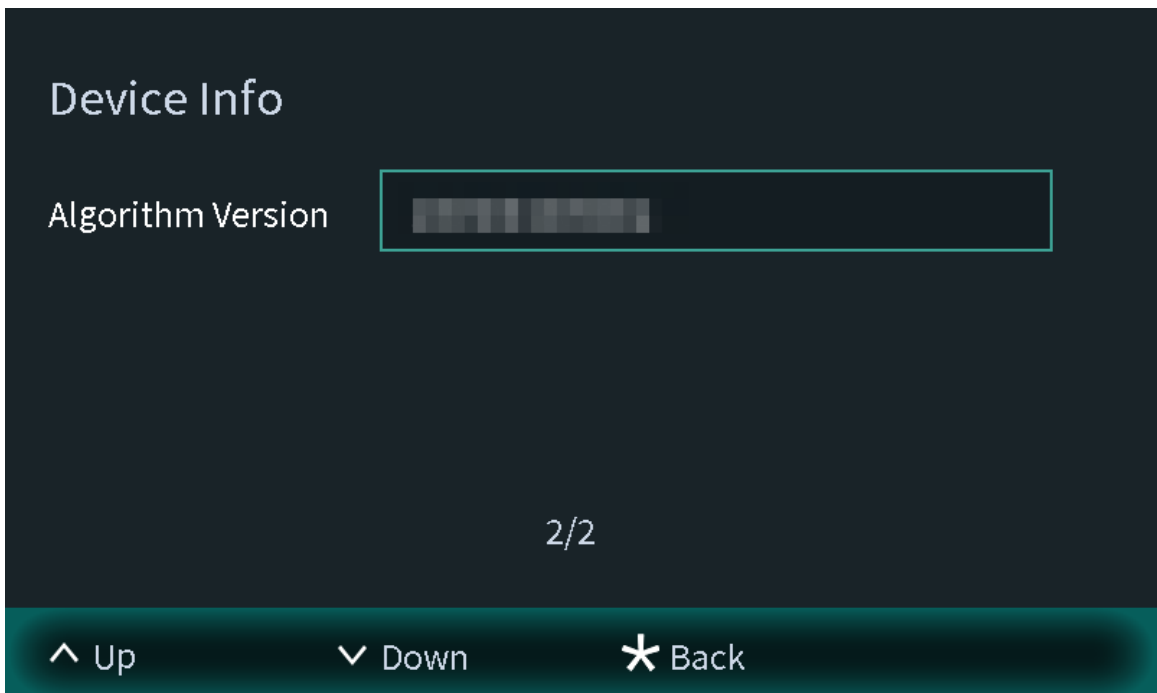


Figura 2-22 Información del dispositivo (2)



2.1.2.5 Configuración del modo de imagen

Configure el modo de imagen según su situación. Los valores de los parámetros de imagen varían según el modo de imagen.

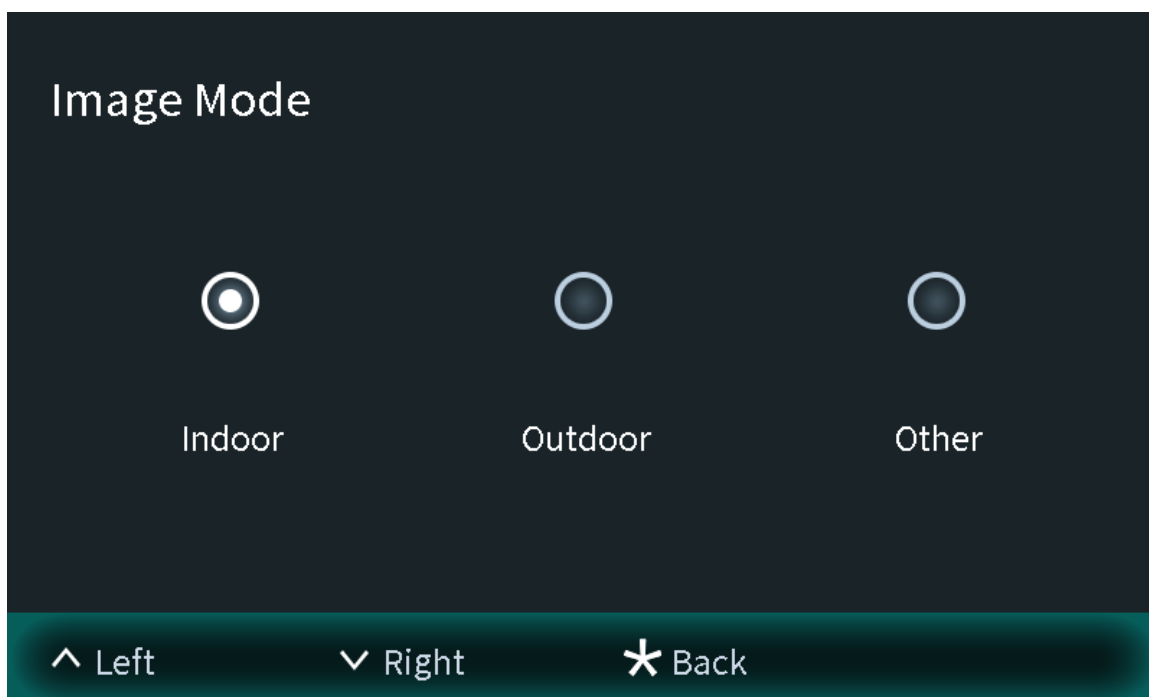
Procedimiento

Paso 1 Seleccionar **Modo de imagen** en el **Configuración de ingeniería**

Paso 2 pantalla. Seleccione de **Interior**, **Exterior** y **Otro**.

- Seleccione el modo interior cuando instale el dispositivo en la escena interior.
- Seleccione el modo exterior cuando instale el dispositivo en la escena exterior.
- Seleccione el otro modo cuando instale el dispositivo en una escena con luz de fondo, como por ejemplo en el pasillo.

Figura 2-23 Modo de imagen



Paso 3 Prensas para guardar y volver a **Configuración de ingeniería** pantalla.

2.1.2.6 Configuración del modo de luz de relleno

Configure el modo de luz de relleno para cambiar el estado del iluminador según su situación real.

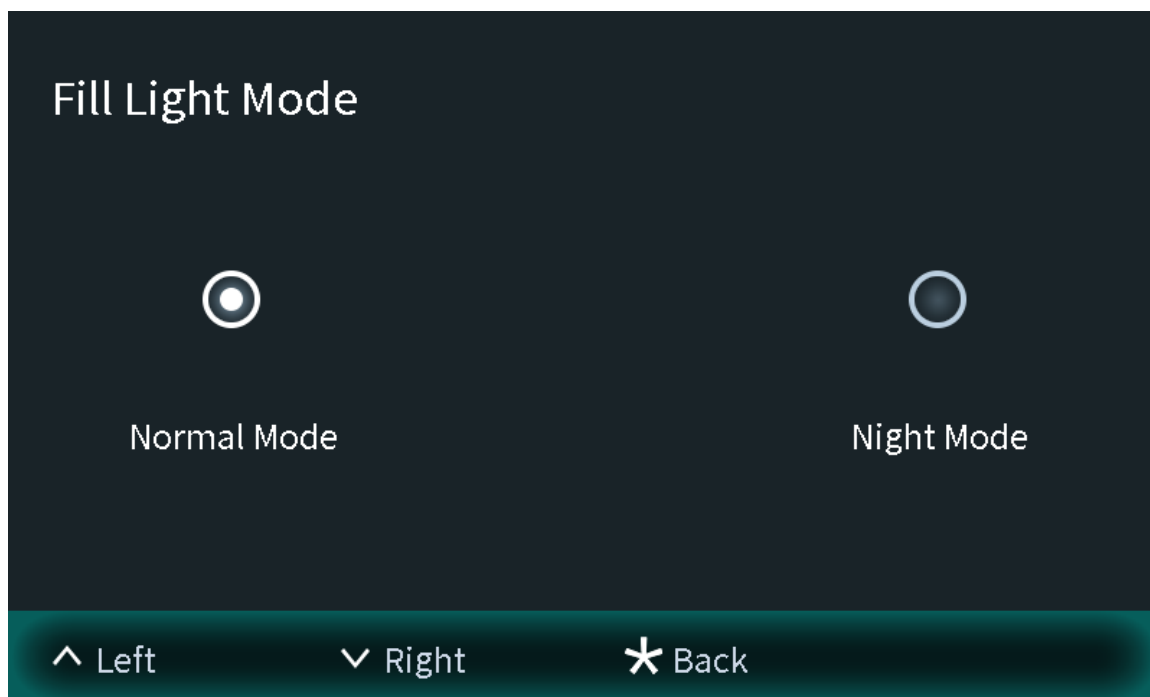
Procedimiento

Paso 1 Seleccionar **Modo de luz de relleno** en el **Configuración de ingeniería**

Paso 2 pantalla. Seleccione de **Modo normal** y **Modo nocturno**.

- **Modo normal:** Cuando el dispositivo detecta personas, el iluminador se activa. Si no hay personas, se apaga automáticamente.
- **Modo nocturno:** Selecciona el modo nocturno, especialmente por la noche. El iluminador estará siempre encendido.

Figura 2-24 Modo de luz de relleno



Paso 3 Prensas* para guardar e ir a **Configuración de ingeniería** pantalla.

Serie 2.2 75/95

Los dispositivos de las series 75 y 95 utilizan el siguiente estilo de pantalla.



Las siguientes instantáneas de los dispositivos son solo de referencia y es posible que se encuentren ligeras diferencias en la pantalla de operación del VTO, según su modelo.




2.2.1 Pantalla de inicio

Figura 2-25 Pantalla de inicio



Tabla 2-2 Descripción de las instrucciones de la pantalla de inicio

Instrucción	Descripción
	Muestra el estado del servidor SIP.
	Llame o ingrese la contraseña para ir a la pantalla de configuración del ingeniero.
	Escanee el código QR para abrir la puerta.
	Reconoce la cara para abrir la puerta.

Instrucción	Descripción
	Ver la agenda telefónica.
	Registrar la información del propietario.
	Ver la información publicada.

2.2.2 Configuración de ingeniería

Información de fondo

- Configurar la contraseña del proyecto a través de **Configuración local**>**Control de acceso**>**Local** en la página web.
- Sólo el administrador o el ingeniero pueden operar en la pantalla de configuración de ingeniería.

Procedimiento

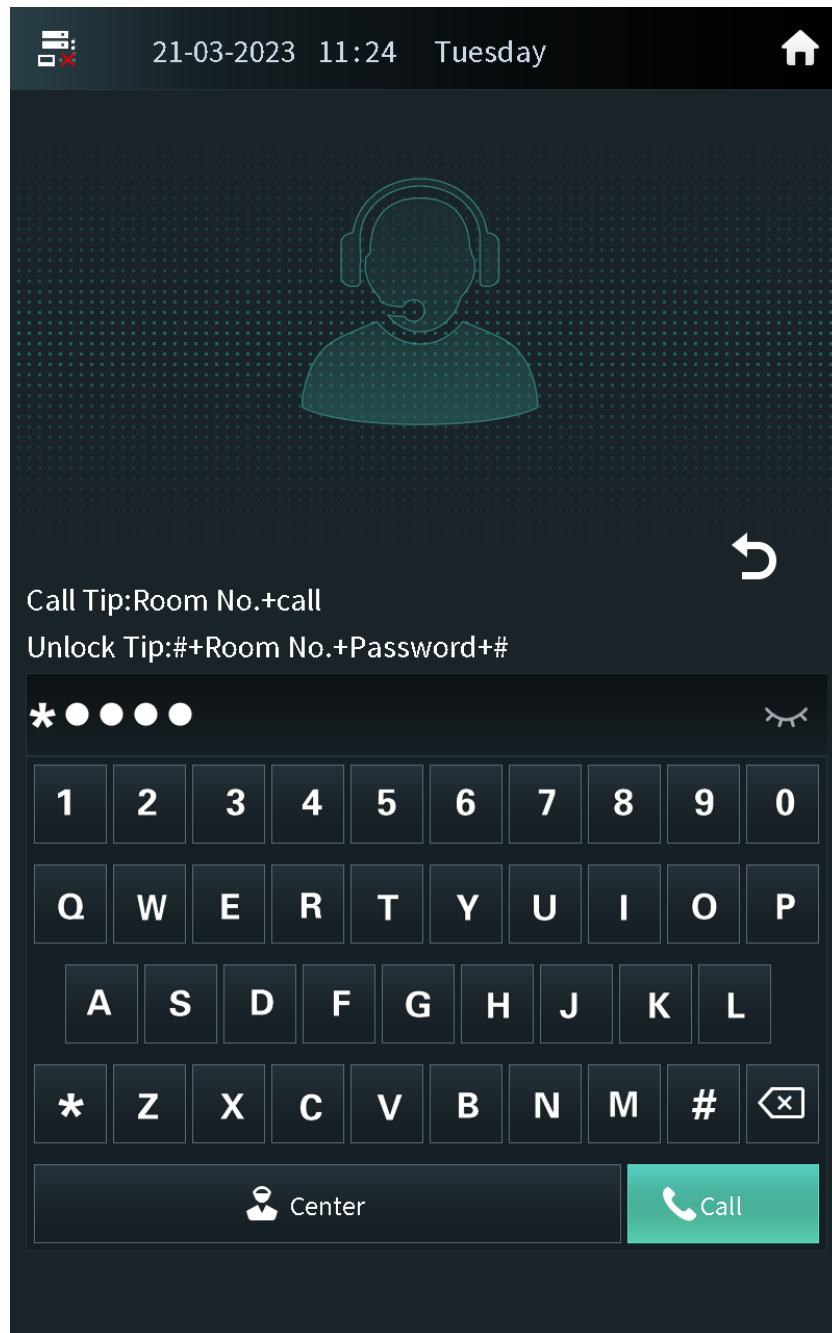
Paso 1 Encienda el VTO.

Paso 2 Toque  en la pantalla de inicio.

Paso 3 Introduzca la contraseña para ir a la pantalla de configuración de ingeniería.

La contraseña es *+contraseña del proyecto+#. Por ejemplo, si configura la contraseña del proyecto como 888888 en la página web, introduzca *888888# para acceder a la pantalla de configuración de ingeniería.

Figura 2-26 Ingrese la contraseña



2.2.2.1 Configuración de la dirección IP

Configure la dirección IP del VTO de acuerdo con su plan de red actual.

Procedimiento

- Paso 1 Prensa **Configuración de IP** En la pantalla de configuración del ingeniero,
- Paso 2 introduzca la dirección IP, la máscara de subred y la puerta de enlace.

Figura 2-27 Configuración de IP

21-03-2023 11:24 Tuesday

IP Settings General Settings User Registration Device Info

IP:

MSK:

Gateway:

MAC:

OK Cancel

Paso 3 Prensa **DE ACUERDO**.

2.2.2.2 Configuración general

Configura el volumen, el tiempo de brillo y otros parámetros.

Procedimiento

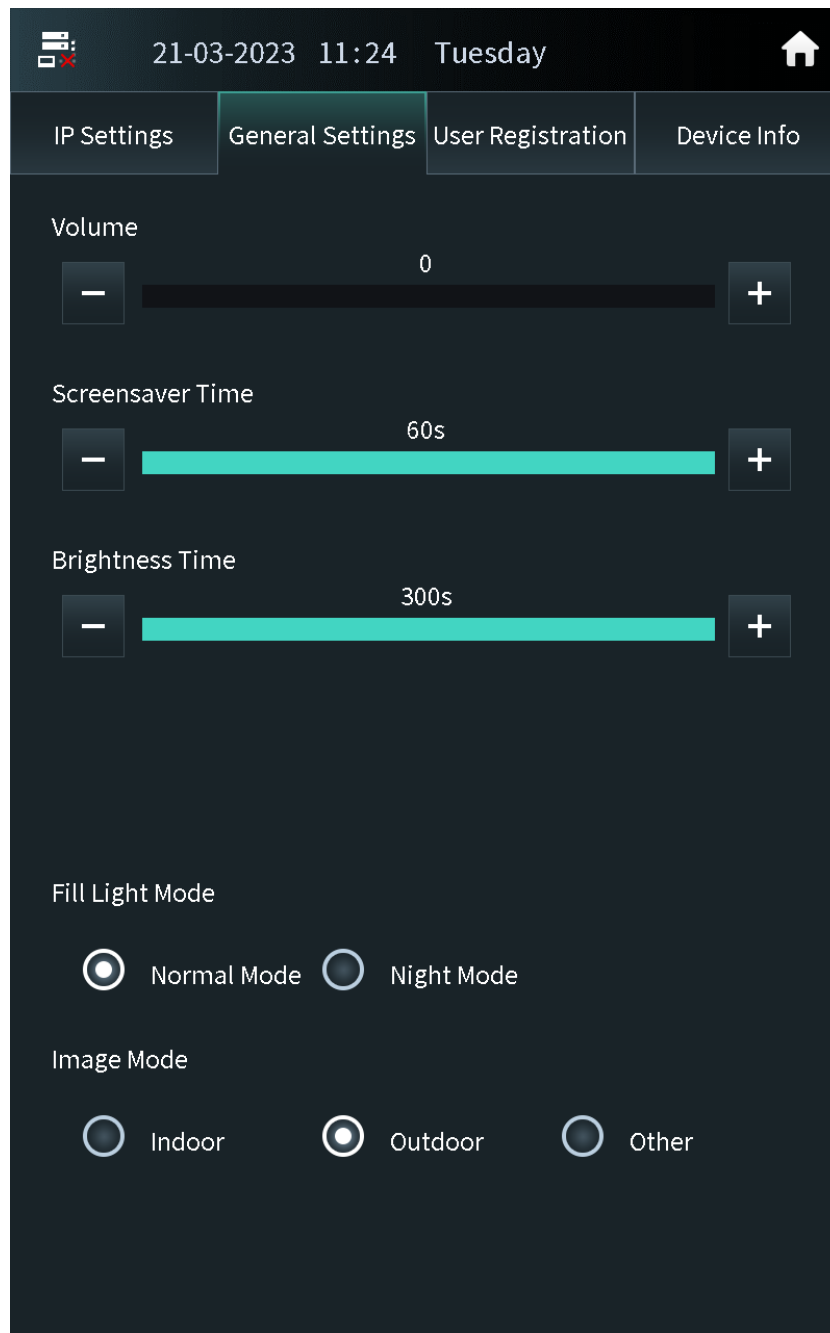
Paso 1 Prensa **Configuración general** en la pantalla de configuración del ingeniero.

Paso 2 Prensa **+o-** para ajustar el volumen, el tiempo del protector de pantalla y el tiempo de brillo.

- Volumen: El volumen de operación del VTO o de llamada del VTO.
- Tiempo de protector de pantalla: la cantidad de tiempo de inactividad que debe transcurrir antes de que se active el protector de pantalla.

- Tiempo de brillo: la pantalla se apaga automáticamente después de dejar el VTO inactivo durante el tiempo que configure.

Figura 2-28 Configuración general



Paso 3 Configure el modo de luz de relleno y el modo de imagen.

Otro En el modo de imagen se entienden otras escenas con retroiluminación como el pasillo o el semiexterior.

2.2.2.3 Registro de usuario

Si el VTO actual u otro VTO funciona como servidor SIP, el administrador puede registrar la información del usuario y agregar rostros, huellas dactilares y tarjetas. El VTO también permite configurar la tarjeta principal e informar sobre su pérdida.



- Los rostros, huellas y tarjetas que se registren solo serán válidos para el VTO vigente.
- Si la plataforma funciona como servidor SIP, la plataforma envía la información de rostros, huellas dactilares y tarjetas al VTO.

2.2.2.3.1 Agregar usuarios

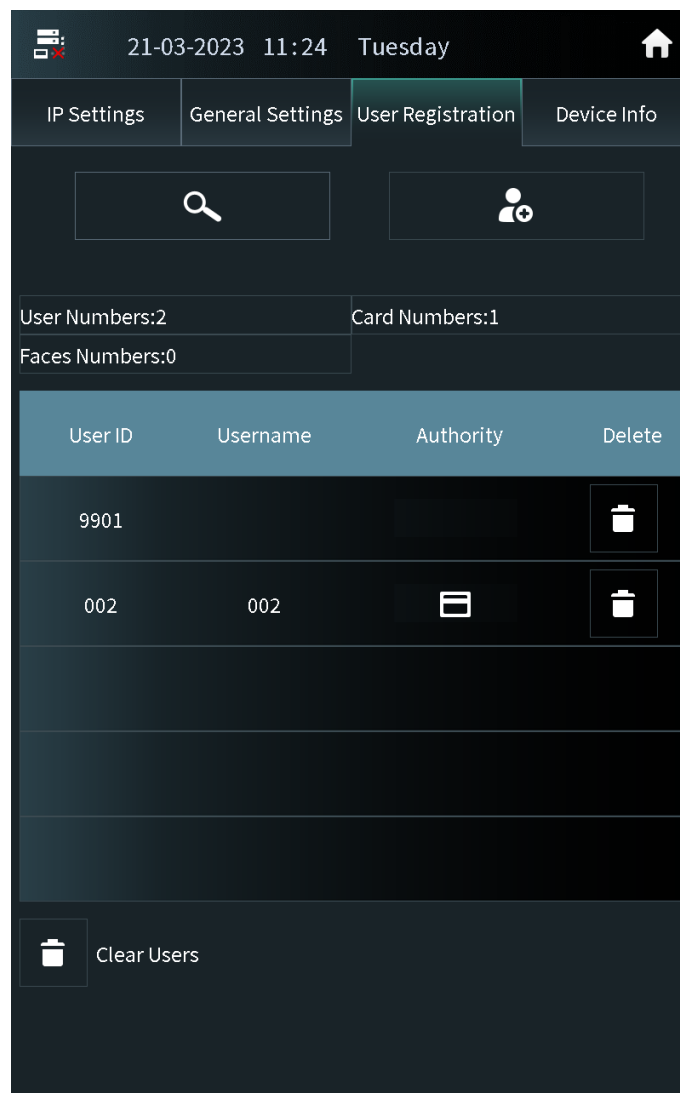
Agrega el usuario y luego registra la información del rostro, la huella dactilar y la tarjeta.

Procedimiento

Paso 1 Grifo **Registro de usuario** en la pantalla de configuración del ingeniero.

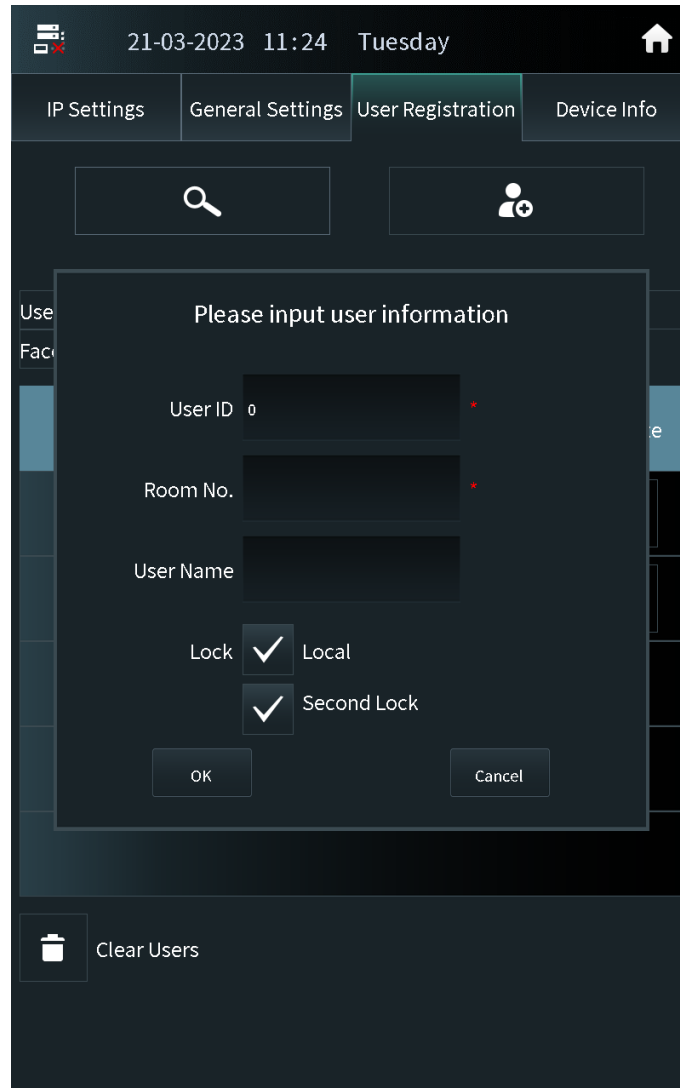
- : El usuario ha registrado la cara.
- : El usuario ha registrado la tarjeta.
- : El usuario ha registrado la huella dactilar.

Figura 2-29 Registro de usuario



Paso 2 Toque Ingrese el ID de usuario, el número de habitación y el nombre de usuario, y luego configure la cerradura local y la segunda cerradura.

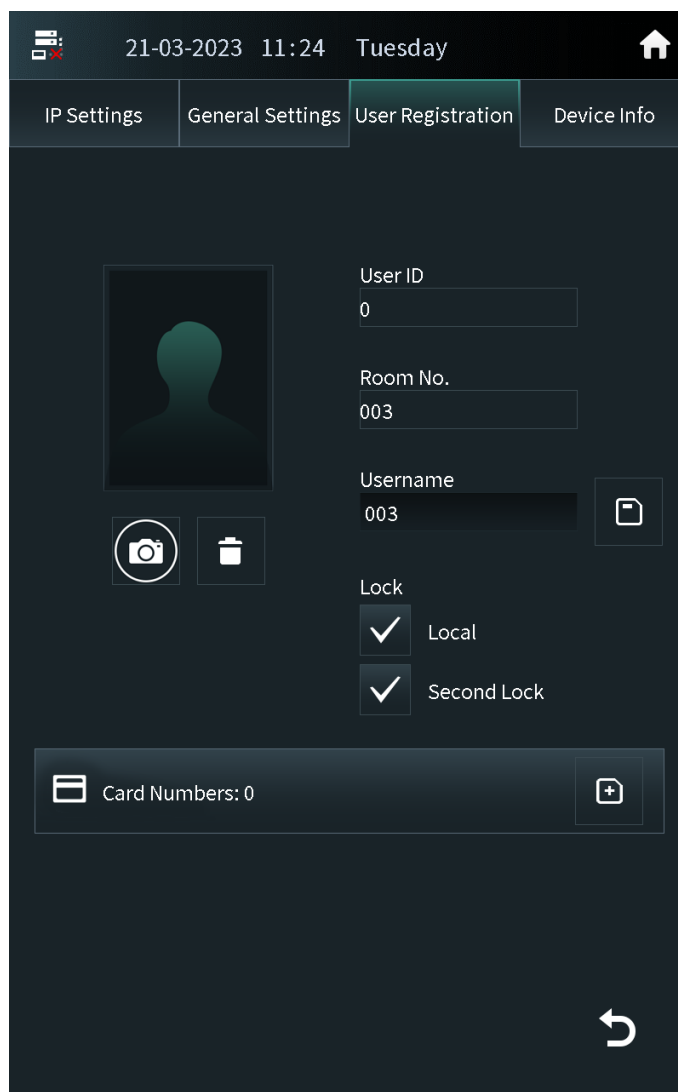
Figura 2-30 Agregar el usuario



Paso 3

Grifo DE ACUERDO.

Figura 2-31 Información del usuario





Paso 4 Añade la cara, la huella dactilar y la tarjeta.

- Para obtener detalles sobre cómo agregar la imagen de la cara, consulte "2.2.2.3.2 Agregar caras".
- Para obtener detalles sobre cómo agregar la huella digital, consulte "2.2.2.3.3 Agregar huellas digitales".
- Para obtener detalles sobre cómo agregar la tarjeta, consulte "2.2.2.3.4 Emisión de tarjetas".

2.2.2.3.2 Agregar caras

Procedimiento

Paso 1  Grifo  en la pantalla de información del usuario.

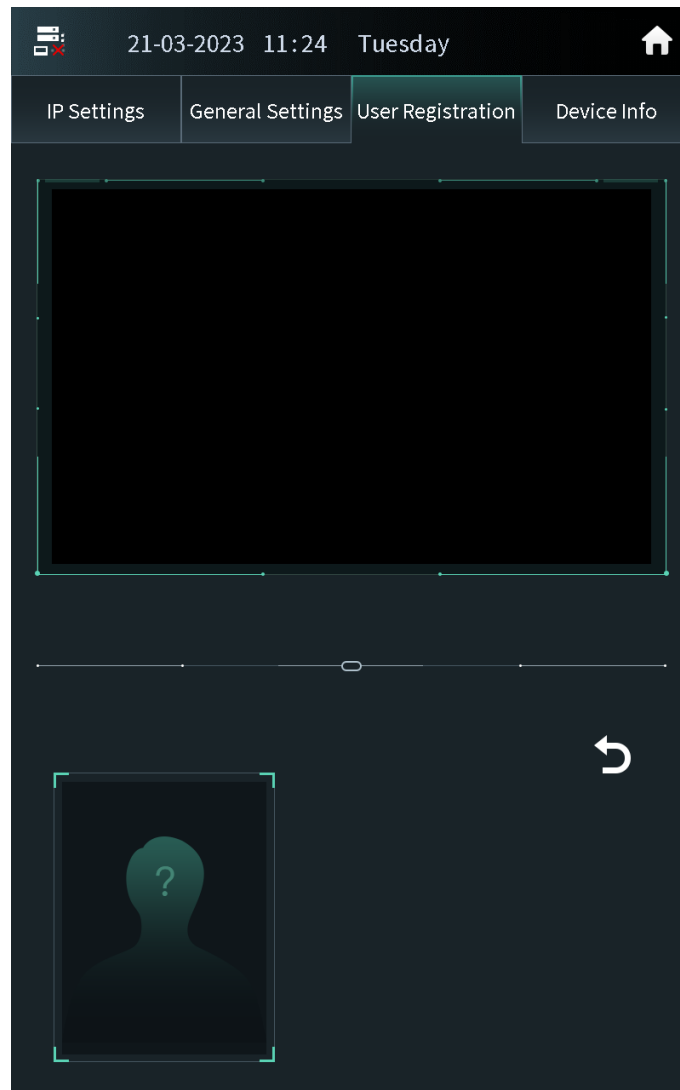


Si está en la pantalla de registro de usuario, seleccione el usuario para ir a la pantalla de información del usuario.

Paso 2 Asegúrate de que tu cara esté en el centro del marco y la imagen de tu cara se tomará automáticamente.

Grifo **Cancelar** registrarse nuevamente si no desea la foto.


Figura 2-32 Registro de rostros



Paso 3 Grifo **DE ACUERDO** después de confirmar la imagen de la cara.

2.2.2.3.3 Agregar huellas dactilares

Procedimiento


Paso 1 Grifo  junto a los números de huellas dactilares en la pantalla de información del usuario.



Si está en la pantalla de registro de usuario, seleccione el usuario para ir a la pantalla de información del usuario.

Paso 2 Presione el sensor de huellas dactilares y luego mueva el dedo después de la indicación de voz o pantalla.

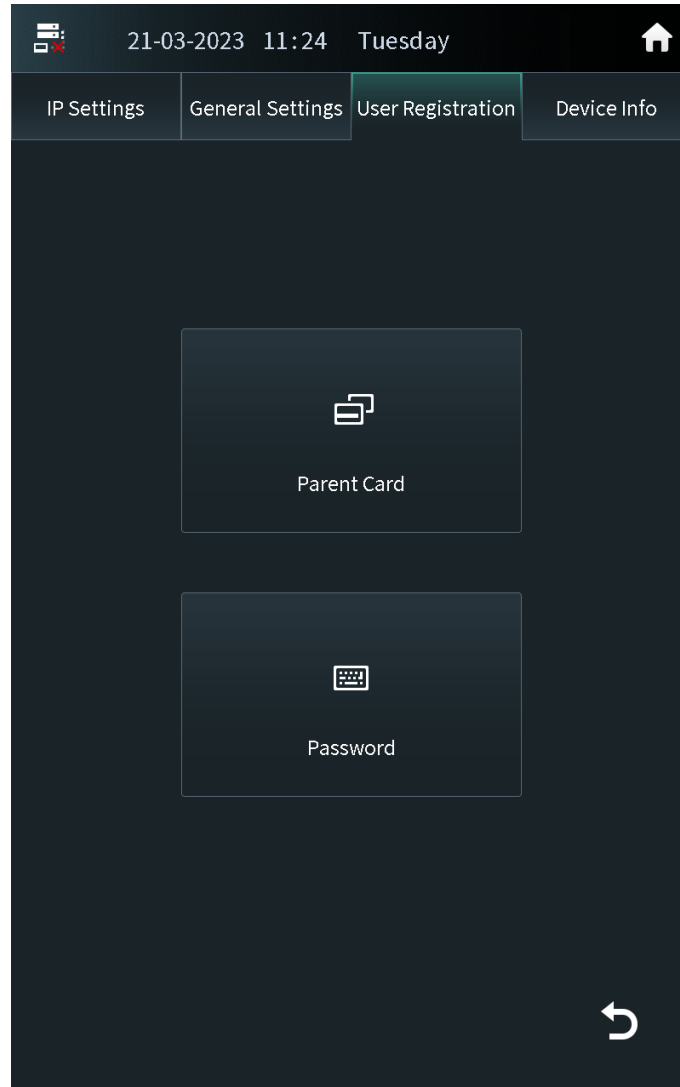
2.2.2.3.4 Emisión de tarjetas

Presiona  junto a los números de tarjeta en la pantalla de información del usuario.



Si está en la pantalla de registro de usuario, seleccione el usuario para ir a la pantalla de información del usuario.

Figura 2-33 Tarjetas de problemas



Emisión de tarjetas por parte de la tarjeta principal

Utilice la tarjeta principal autorizada para registrar la nueva tarjeta.

Prerrequisitos

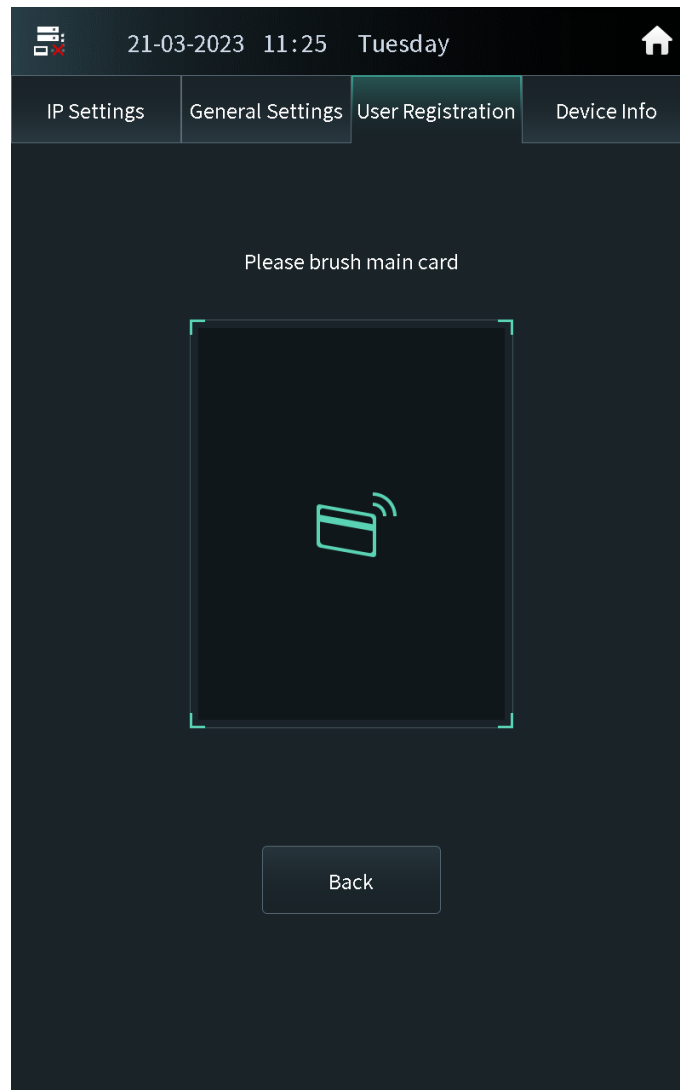
Asegúrese de que la tarjeta principal esté presente. Si no la hay, regístrela con la contraseña y configúrela como principal.

Procedimiento

Paso 1 Seleccionar **Tarjeta para padres** En la pantalla de emisión de tarjetas,

Paso 2 pase la tarjeta principal.

Figura 2-34 Tarjeta principal



Paso 3 Pase la nueva tarjeta.

El VTO muestra **Éxito de la tarjeta de emisión**. Puedes pasar otras tarjetas para registrarte continuamente. Toca **Atrás** Si no es necesario agregar otras tarjetas.

Emisión de tarjetas por contraseña

Utilice la contraseña de la tarjeta emitida para registrar la nueva tarjeta.



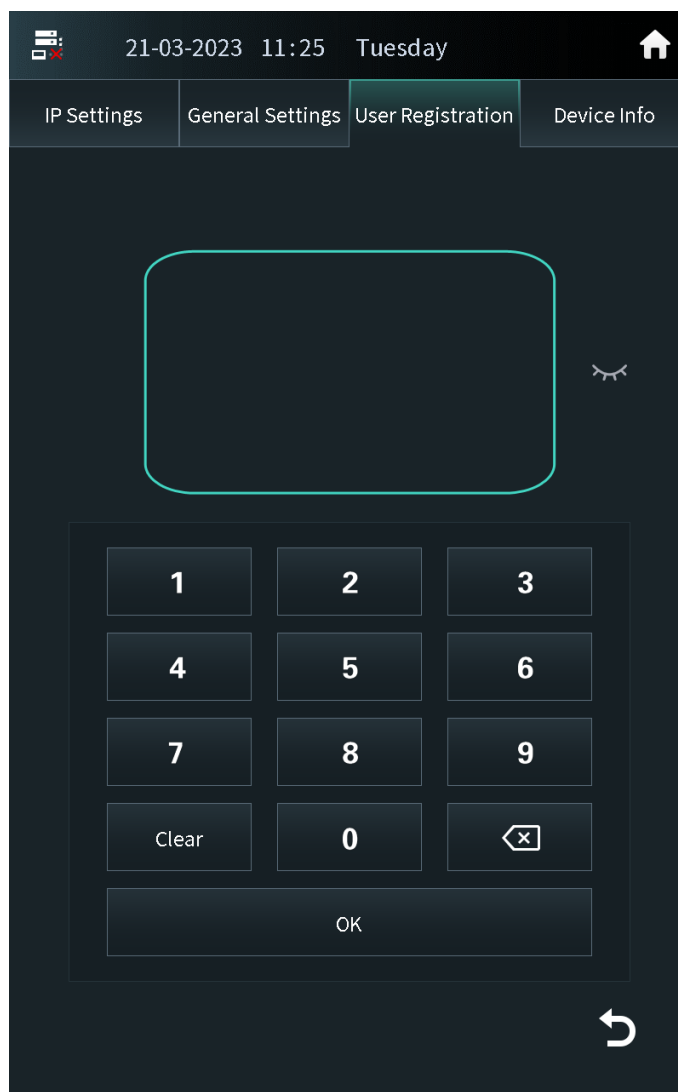
Puede configurar la contraseña a través de **Configuración local > Control de acceso > Gestión de contraseñas**. Para obtener más detalles, consulte Configurar bloqueo local.

Procedimiento

Paso 1 Seleccionar **Contraseña** En la pantalla de la tarjeta de emisión, introduzca

Paso 2 la contraseña de la tarjeta de emisión y pulse **DE ACUERDO**.

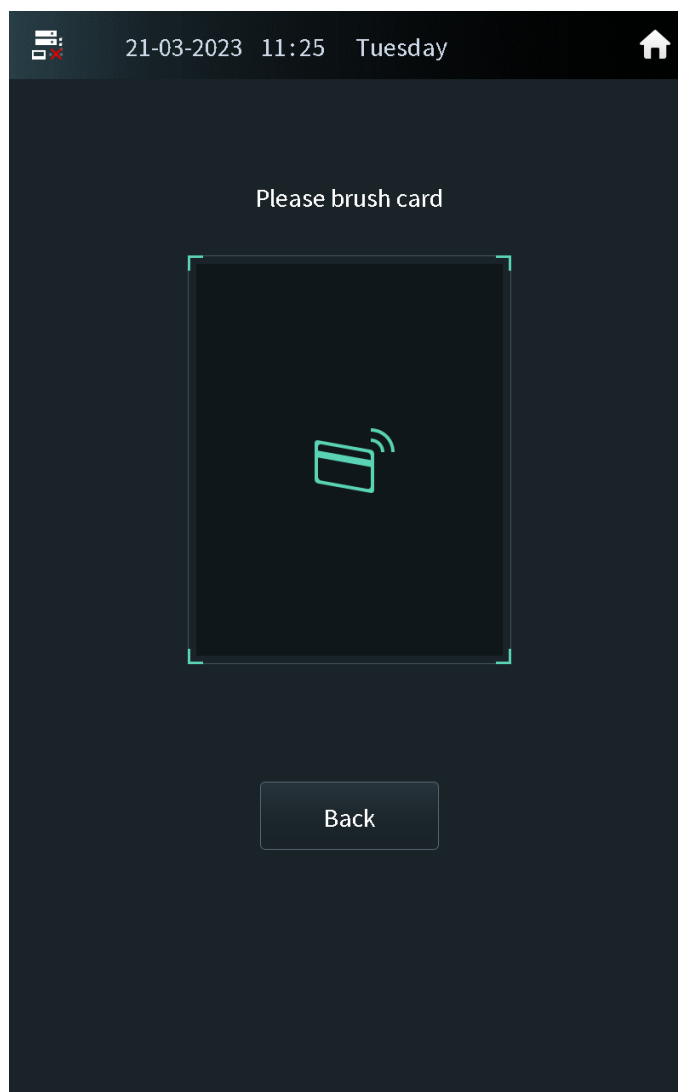
Figura 2-35 Contraseña de la tarjeta de emisión



Paso 3 Pase la nueva tarjeta.

El VTO muestra **Éxito de la tarjeta de emisión**. Puedes pasar otras tarjetas para registrarte continuamente. Toca **Atrás** Si no es necesario agregar otras tarjetas.

Figura 2-36 Registro de nueva tarjeta



2.2.2.3.5 Gestión de tarjetas

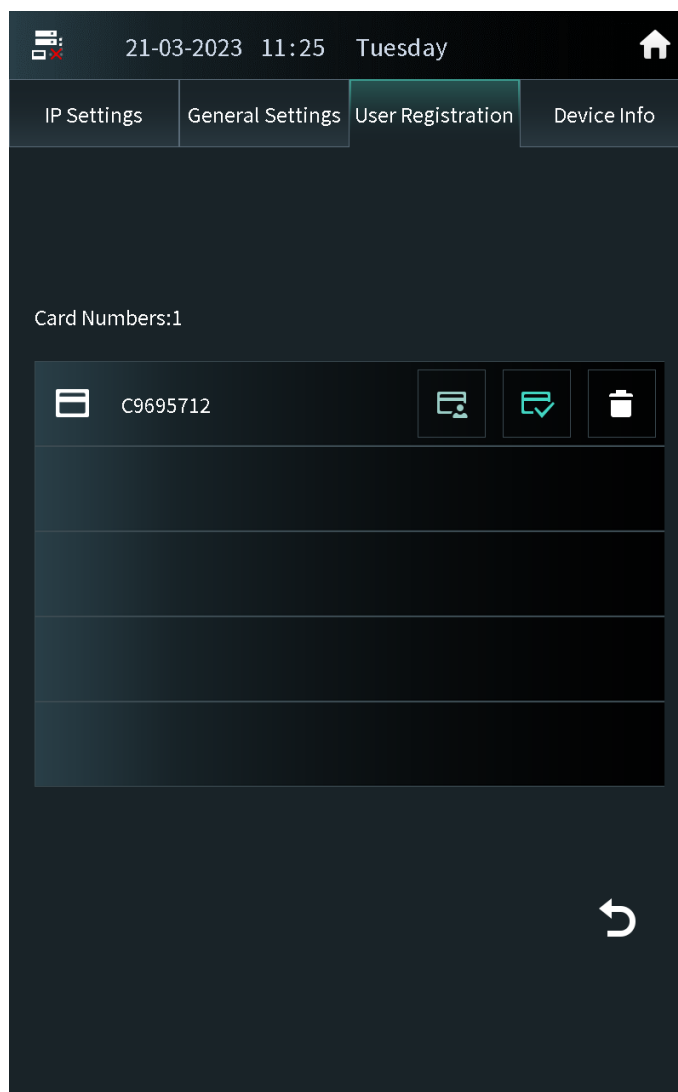
Configuración de la tarjeta principal

La tarjeta principal se utiliza para registrar otras tarjetas nuevas.

Procedimiento

- Paso 1** Seleccione el usuario en la pantalla de registro de usuario.
- Paso 2** Presione **Números de tarjeta**.

Figura 2-37 Lista de tarjetas



Paso 3

Prensa



, y el icono gira



La tarjeta está configurada como tarjeta principal.



Prensa



para cancelar la tarjeta principal.

Informar sobre la pérdida de la tarjeta

Si reporta la pérdida de la tarjeta común, no podrá usarla para abrir la puerta. Si reporta la pérdida de la tarjeta principal, esta no podrá usarla para abrir la puerta ni registrar la nueva tarjeta.

Procedimiento

Paso 1

Seleccione el usuario en la pantalla de registro de usuario.

Paso 2

Toque **Números de tarjeta**.

Paso 3

Grifo



, y el icono gira



La tarjeta se reporta como perdida y no se puede usar para abrir la puerta.




Grifo



Para cancelar el reporte de pérdida. La tarjeta puede usarse para abrir la puerta nuevamente.

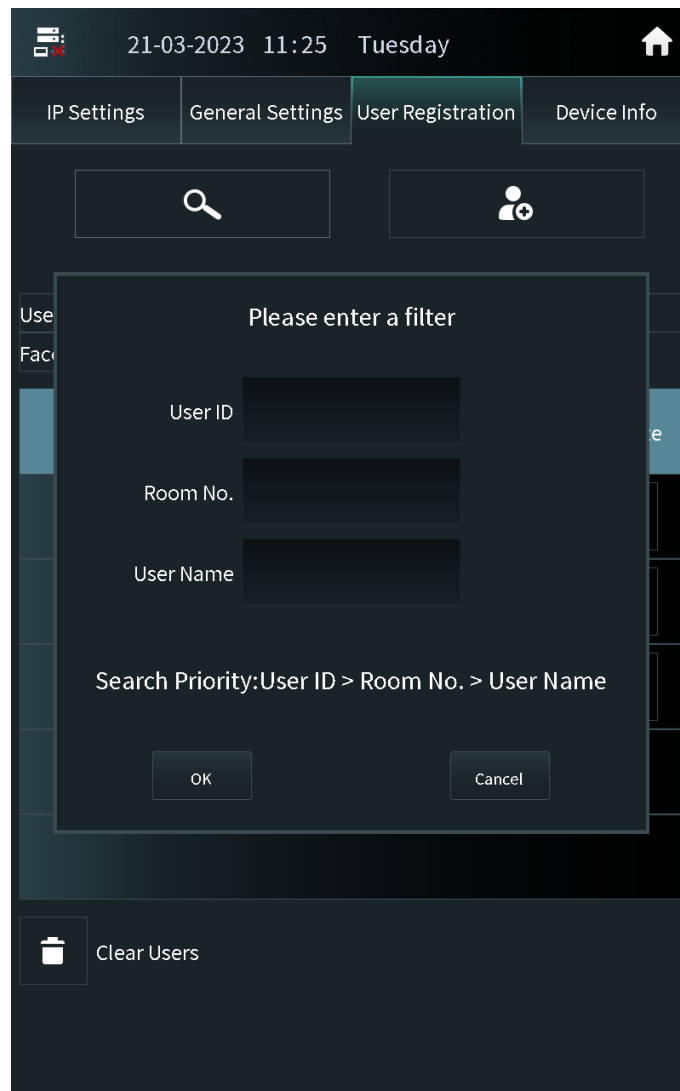
2.2.2.3.6 Búsqueda de un usuario

Procedimiento

Paso 1 Grifo  en la pantalla de registro de usuario.

Paso 2 Ingrese el ID de usuario, el número de habitación o el nombre de usuario y luego toque **DE ACUERDO**.

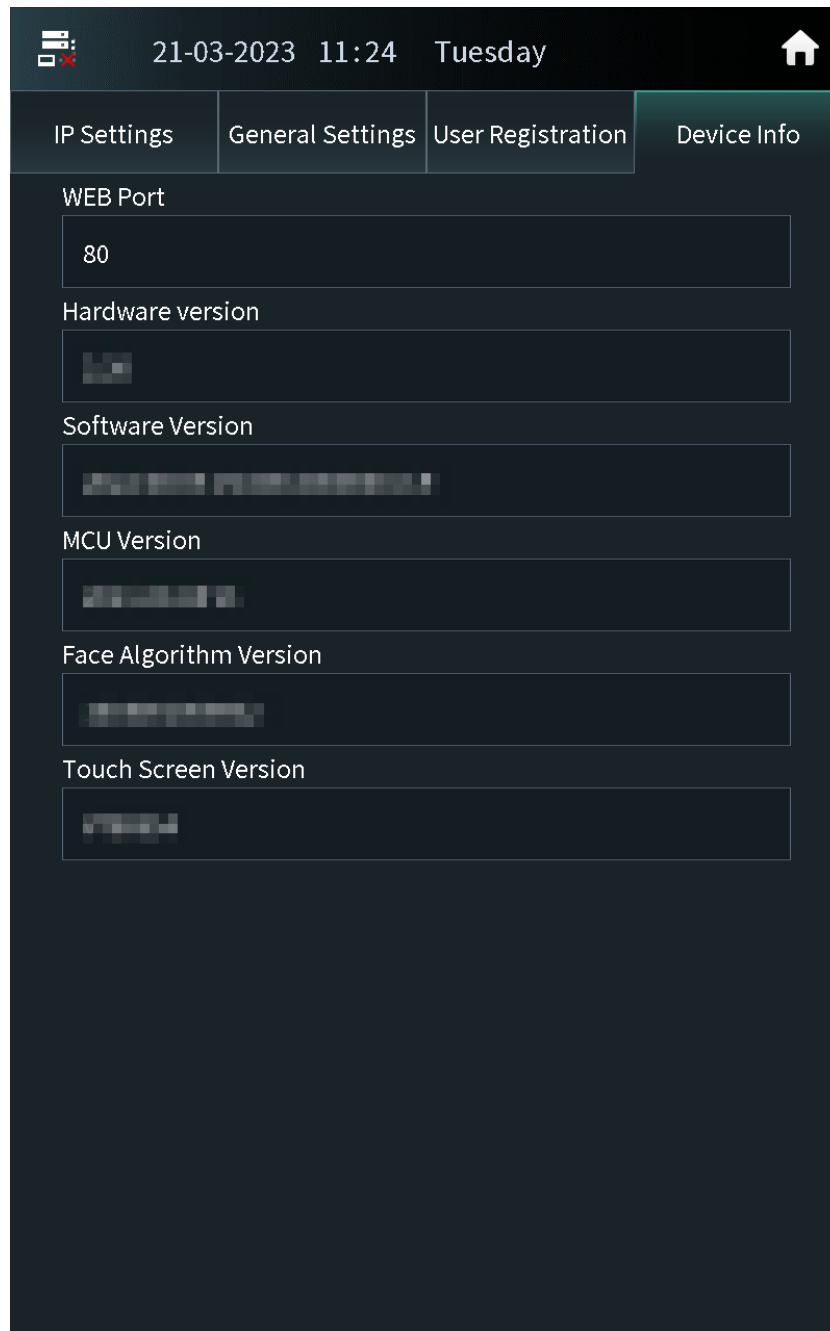
Figura 2-38 Búsqueda del usuario



2.2.2.4 Visualización de la información del dispositivo

Prensa **Información del dispositivo** en la pantalla de configuración del ingeniero para ver los detalles del VTO.

Figura 2-39 Ver la información del dispositivo



2.2.3 Registro del propietario

El titular únicamente podrá registrar y mantener la información, imágenes faciales y huellas dactilares de las personas ante el VTH.

2.2.3.1 Agregar propietarios

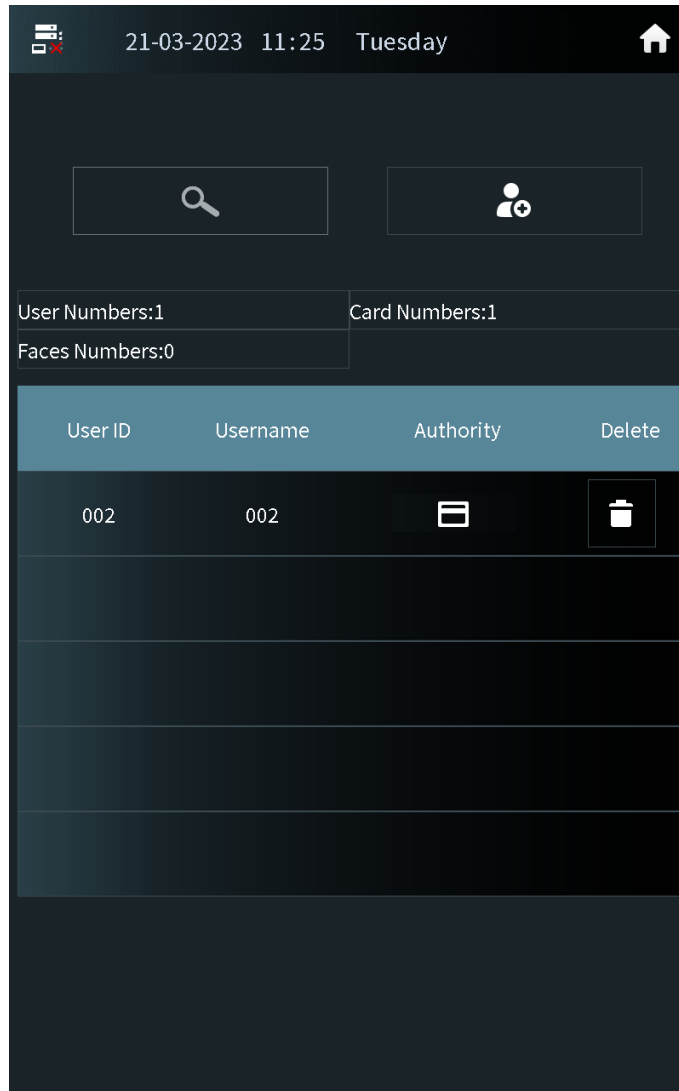
Agregue el propietario y luego registre la cara y la huella digital.

Procedimiento

Paso 1 Grifo **Dueño** en la pantalla de inicio.

Paso 2 Pase la tarjeta registrada para ingresar a la lista de propietarios.

Figura 2-40 Lista de usuarios



Paso 3 Grifo para agregar el usuario.

Figura 2-41 Agregar el usuario

The screenshot shows a mobile application interface with a dark theme. At the top, there is a status bar with the date '21-03-2023', time '11:26', and day 'Tuesday'. Below this, there are two buttons: a search icon and a plus icon. A modal dialog titled 'Please input user information' is open, containing the following fields and options:

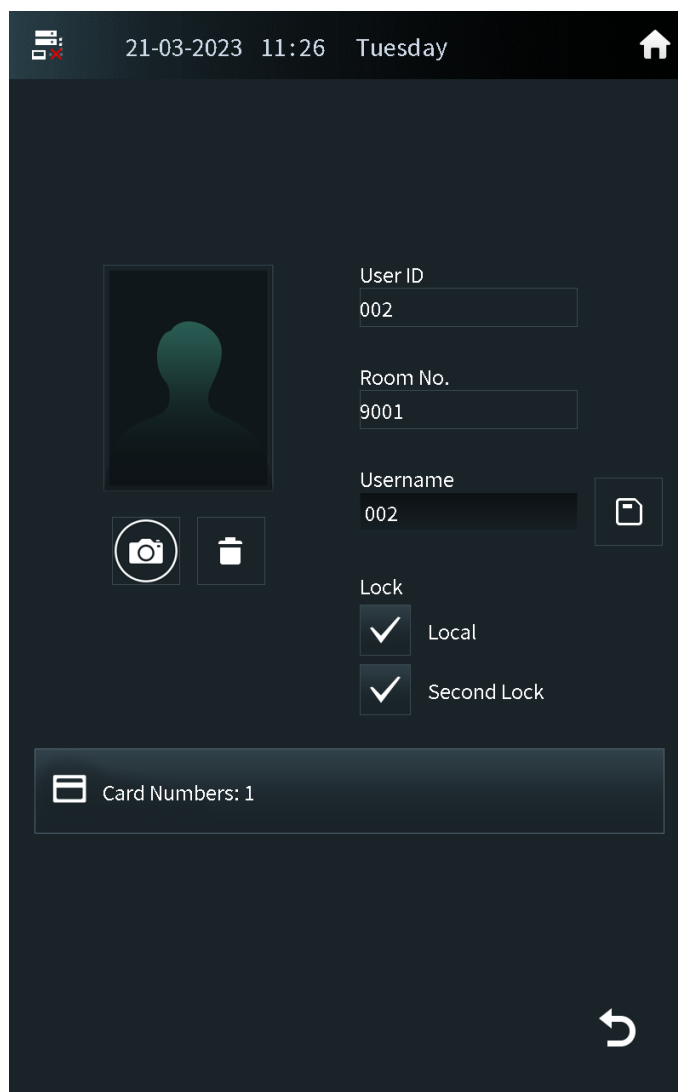
- User ID: 1
- Room No.: 9001
- User Name: (empty)
- Lock: Local
- Second Lock: Second Lock

At the bottom of the modal are two buttons: 'OK' and 'Cancel'.

Paso 4 Ingrese el ID de usuario, el número de habitación y el nombre de usuario. Configure la

Paso 5 cerradura local o la segunda cerradura y luego toque **DE ACUERDO**.

Figura 2-42 Información del usuario




Paso 6 Registra la imagen del rostro y la huella dactilar.

- Para obtener detalles sobre cómo agregar la imagen de la cara, consulte "2.2.3.2 Agregar caras".
- Para obtener detalles sobre cómo agregar la huella digital, consulte "2.2.3.3 Agregar huellas digitales".

2.2.3.2 Agregar caras

Procedimiento

Paso 1  Grifo en la pantalla de información del usuario.

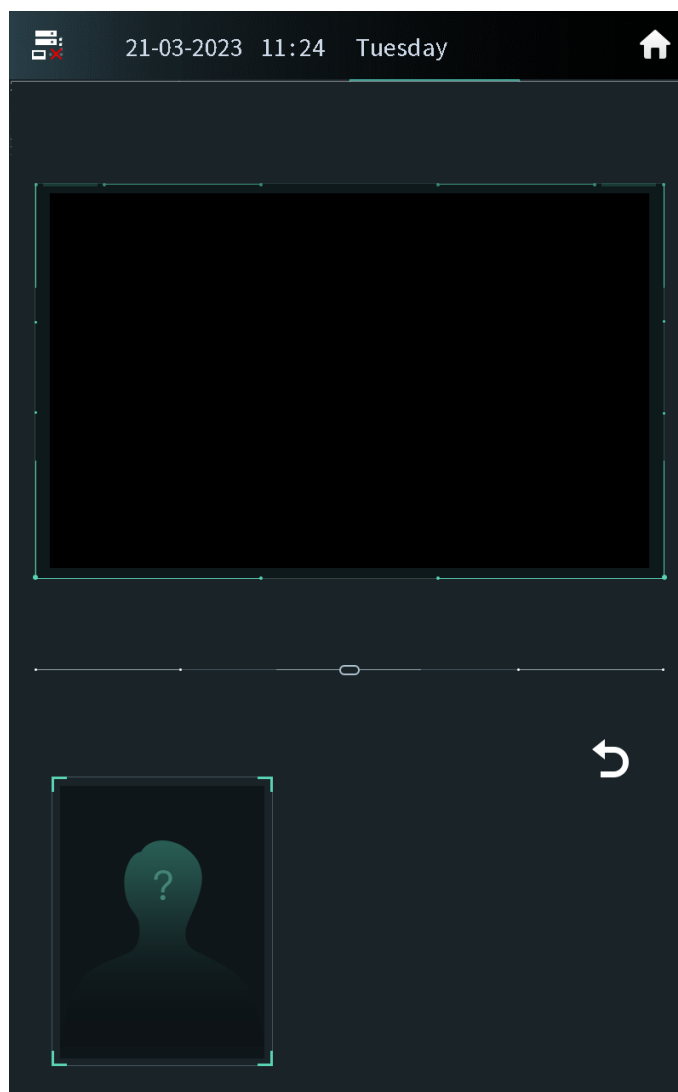


Si está en la pantalla del propietario, seleccione el usuario para ir a la pantalla de información del usuario.

Paso 2 Coloca tu cara en el centro del marco.

La imagen del rostro se tomará automáticamente. Si no está satisfecho con la foto, toque **Cancelar** para cancelar la foto y registrarse nuevamente.


Figura 2-43 Registro facial



Paso 3 Grifo **DE ACUERDO** después de confirmar la imagen de la cara.

2.2.3.3 Agregar huellas dactilares

Procedimiento

Paso 1 Grifo  junto a los números de huellas dactilares en la pantalla de información del usuario.



Si está en la pantalla del propietario, seleccione el usuario para ir a la pantalla de información del usuario.

Paso 2 Presione el sensor de huellas dactilares y luego mueva el dedo después de la indicación de voz o pantalla.

2.2.4 Desbloquear

2.2.4.1 Desbloqueo mediante identificación del rostro

Cuando alguien se acerca al VTO, este muestra automáticamente la pantalla de detección facial y detecta el rostro. Las indicaciones de voz y del dispositivo...**Éxito de puertas abiertas** significa que la puerta se abre y puedes entrar. Si el dispositivo muestra **No autorizado**, registre primero la cara.

2.2.4.2 Desbloqueo mediante escaneo del código QR

Escanee el código QR para abrir la puerta. La plataforma envía el código QR. Para más información, consulte el manual de usuario de la plataforma correspondiente.

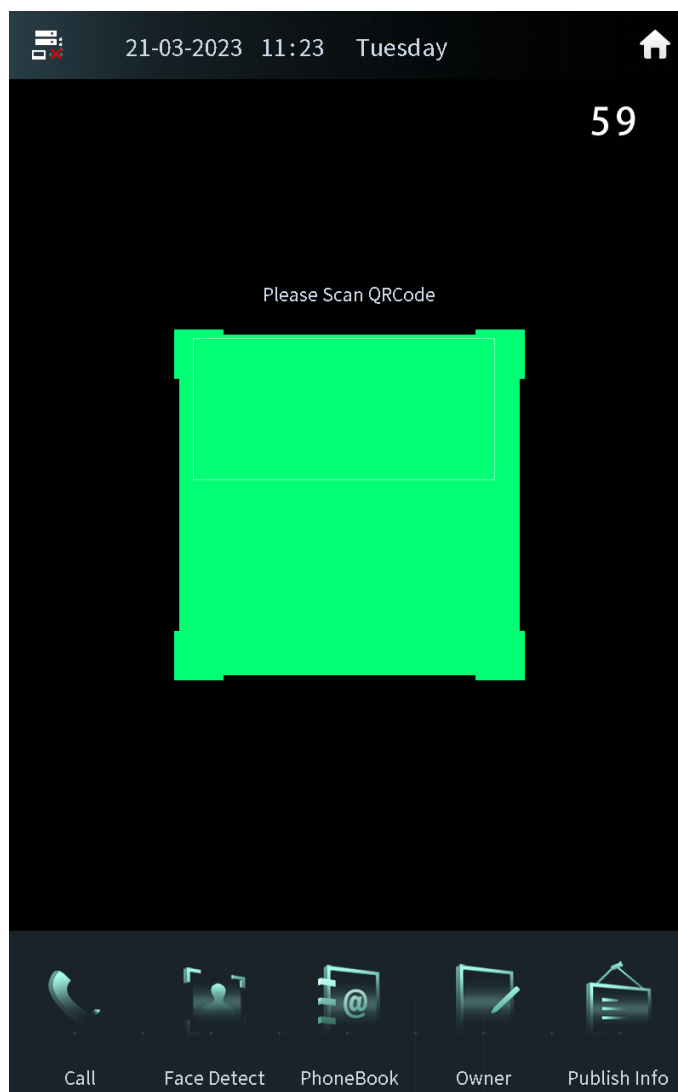
Procedimiento

Paso 1  Prensa  en la pantalla de inicio.

Paso 2 Muestre el código QR y luego asegúrese de que el código QR aparezca en el visor.

El mensaje de voz y el mensaje del dispositivo **Abierto exitosamente** significa que la puerta se abre y puedes entrar. Si el dispositivo muestra **Inválido**, verifique el código QR.

Figura 2-44 Escanee el código QR



2.2.4.3 Desbloqueo por contraseña

Procedimiento

Paso 1  Grifo en la pantalla de inicio.

Paso 2 Introduzca la contraseña para abrir la puerta.

- **# *Contraseña+#**: La contraseña aquí se configura a través de **Configuración local > Control de acceso > Gestión de contraseñas** en la página web. Por ejemplo, si la contraseña es 123456, introduzca "#123456#" para abrir la puerta.
- **# *Número de habitación + Contraseña + #**: La contraseña se configura en el VTH. Si el número de habitación tiene menos de 6 dígitos, debe introducir un 0 antes. Por ejemplo, si el número de habitación es 9901 y la contraseña es 112233, introduzca "#009901112233#" para abrir la puerta.



Primero debes cambiar la contraseña predeterminada en el VTH si deseas utilizar este método para abrir la puerta.

El mensaje de voz y el mensaje del dispositivo **Abierto exitosamente** significa que la puerta se abre y puedes entrar. Si el dispositivo muestra **Error de contraseña**, verifique la contraseña.

2.2.4.4 Desbloqueo mediante tarjeta

Cepille la tarjeta autorizada. La indicación de voz y la del dispositivo **Éxito de puertas abiertas** significa que la puerta se abre y puedes entrar. Si el dispositivo muestra **No autorizado**, registre la tarjeta.

2.2.4.5 Desbloqueo por huellas dactilares

Presiona la huella dactilar. La instrucción de voz y la del dispositivo **Éxito de puertas abiertas** significa que la puerta se abre y puedes entrar. Si el dispositivo muestra **No autorizado**, registra la huella dactilar.

2.2.4.6 Desbloqueo a través del VTH

Cuando el VTO llama al VTH o este lo monitorea, puede presionar el botón de desbloqueo en el VTH para el visitante. El mensaje de voz y el mensaje del dispositivo... **Éxito de puertas abiertas** significa que la puerta se abre y puedes entrar.



2.2.4.7 Desbloqueo a través del VTS

Cuando el VTO llama al VTS o este lo monitorea, puede presionar el botón de desbloqueo del VTS para el visitante. El mensaje de voz y el mensaje del dispositivo... **Éxito de puertas abiertas** significa que la puerta se abre y puedes entrar.

2.2.5 Llamada



2.2.5.1 Llamada al VTH

Procedimiento

- Paso 1 Grifo  en la pantalla de inicio.
- Paso 2 Ingrese el número de habitación y luego toque **Llamar**.
- Paso 3 Grifo  en el VTH para recibir la llamada.

2.2.5.2 Llamada a la Administración de la Propiedad (VTS)

Procedimiento

- Paso 1 Grifo  en la pantalla de inicio.
- Paso 2 Grifo . Hay un mensaje de voz **Llamando, por favor**
- Paso 3 **espere** El VTS recibe la llamada.

2.2.6 Mensajes

Si el VTO llama al VTH y este no responde la llamada, el VTO muestra un mensaje. Presione **1** Para dejar un mensaje. El VTO guarda los mensajes en la tarjeta SD del VTH. El usuario del VTH puede verlos en **Mensaje del invitado**.

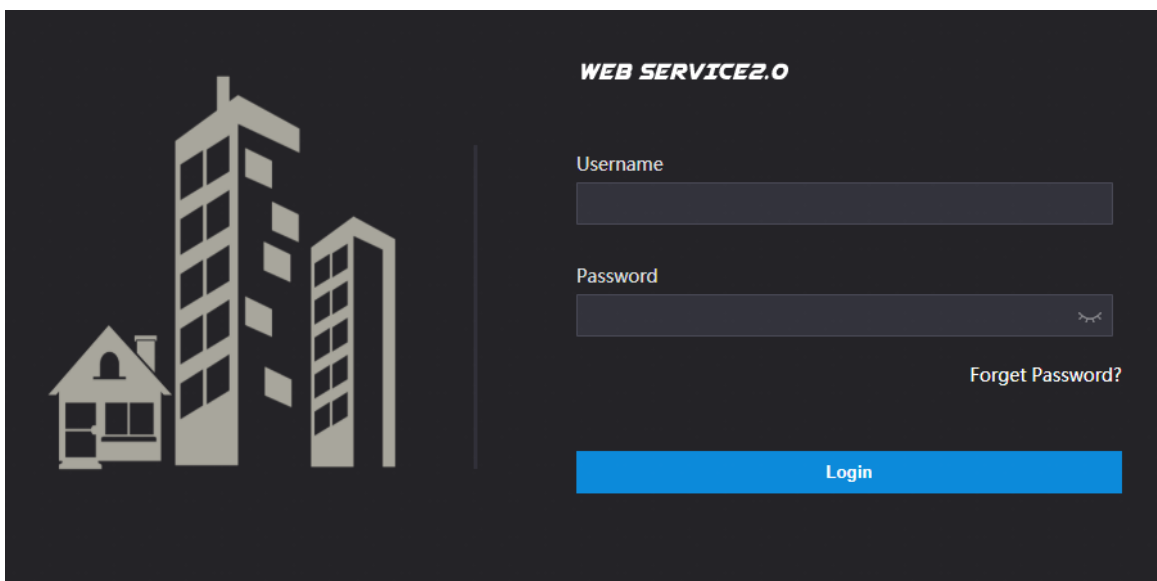
3 Operaciones de página web

3.1 Iniciar sesión en la página web

Procedimiento

- Paso 1 Ingrese la dirección IP del VTO en la barra del navegador para ir a la página de inicio de sesión y luego presione la tecla Enter.
- Paso 2 Introduzca el nombre de usuario (admin por defecto) y la contraseña que configuró durante la inicialización.

Figura 3-1 Inicio de sesión



- Paso 3 Hacer clic **Acceso**.

3.2 Restablecimiento de la contraseña

Si olvida la contraseña de inicio de sesión de la cuenta de administrador, escanee el código QR para restablecerla.

Prerrequisitos

Asegúrese de tener habilitado **Restablecer contraseña** a través de **Configuración local > Seguridad**.



Si no configuró la dirección de correo electrónico durante la inicialización, el sistema informará un error. Para obtener ayuda, póngase en contacto con el distribuidor local o el soporte técnico.

Procedimiento

- Paso 1 Hacer clic **Olvidó su contraseña?** en la página de inicio de sesión y luego haga clic en
- Paso 2 **Próximo** Obtener el **Código de seguridad** según las instrucciones.



- Puedes obtener hasta dos códigos de seguridad con el mismo código QR. Si necesitas más, actualiza el código QR y escanéalo de nuevo.

- El código de seguridad se enviará a tu correo electrónico. Debes usarlo en un plazo de 24 horas. De lo contrario, no será válido.
- La cuenta se bloqueará durante 5 minutos si ingresa el código de seguridad incorrecto 5 veces seguidas.

Paso 3 Ingrese el código de seguridad que recibió y luego haga clic en **Próximo** Ingrese la

Paso 4 nueva contraseña, confírmela y luego haga clic en **DE ACUERDO**.

3.3 Introducción a la página de inicio

El sistema va automáticamente a la página de inicio después de iniciar sesión.

Figura 3-2 Página de inicio

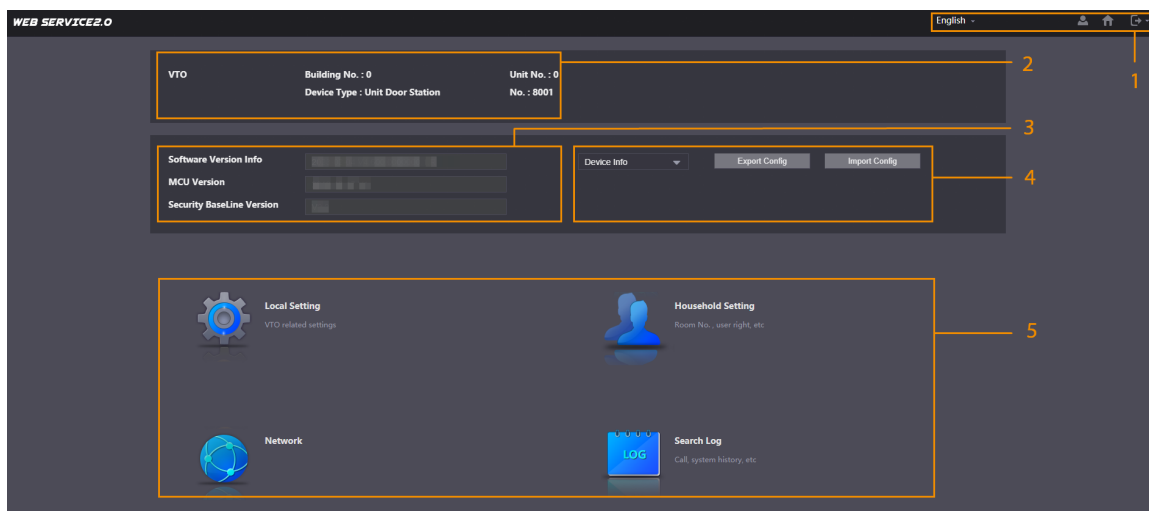


Tabla 3-1 Descripción de la página de inicio

No.	Parámetro	Descripción	
1	Barra de navegación	English -	Seleccione un idioma
			Cambiar la contraseña y la dirección de correo electrónico.
			Haga clic en el icono para ir a la página de inicio.
			Salga de la página web, reinicie el dispositivo o restáurelo a la configuración de fábrica. Para más información, consulte "3.11 Reinicio del dispositivo", "3.12 Restablecimiento de la configuración de fábrica" y "3.13 Cierre de sesión".
2	Información del dispositivo	Ver el número de edificio, el número de unidad, el tipo de dispositivo y el número de dispositivo.	
3	Información de la versión	Vea la versión del software, la versión de MCU y la versión de referencia de seguridad.	
4	Exportación/Importación	Exportar o importar la información del dispositivo o la información del usuario.	

No.	Parámetro	Descripción
5	Configuración local	Configurar la información básica, parámetros de vídeo y audio, control de acceso, sistema, seguridad y Wiegand.
	Entorno del hogar	Gestionar la información de los VTO, VTH, VTS, IPC y enviar el anuncio.
	Red	Configure los parámetros de red, como TCP/IP, FTP, UPnP, servidor SIP y personal. Configure... anuncio.
	Registro de búsqueda	Busque registros de llamadas, registros de alarmas, registros de desbloqueo y registros del sistema.

3.4 Cambiar el mensaje del usuario

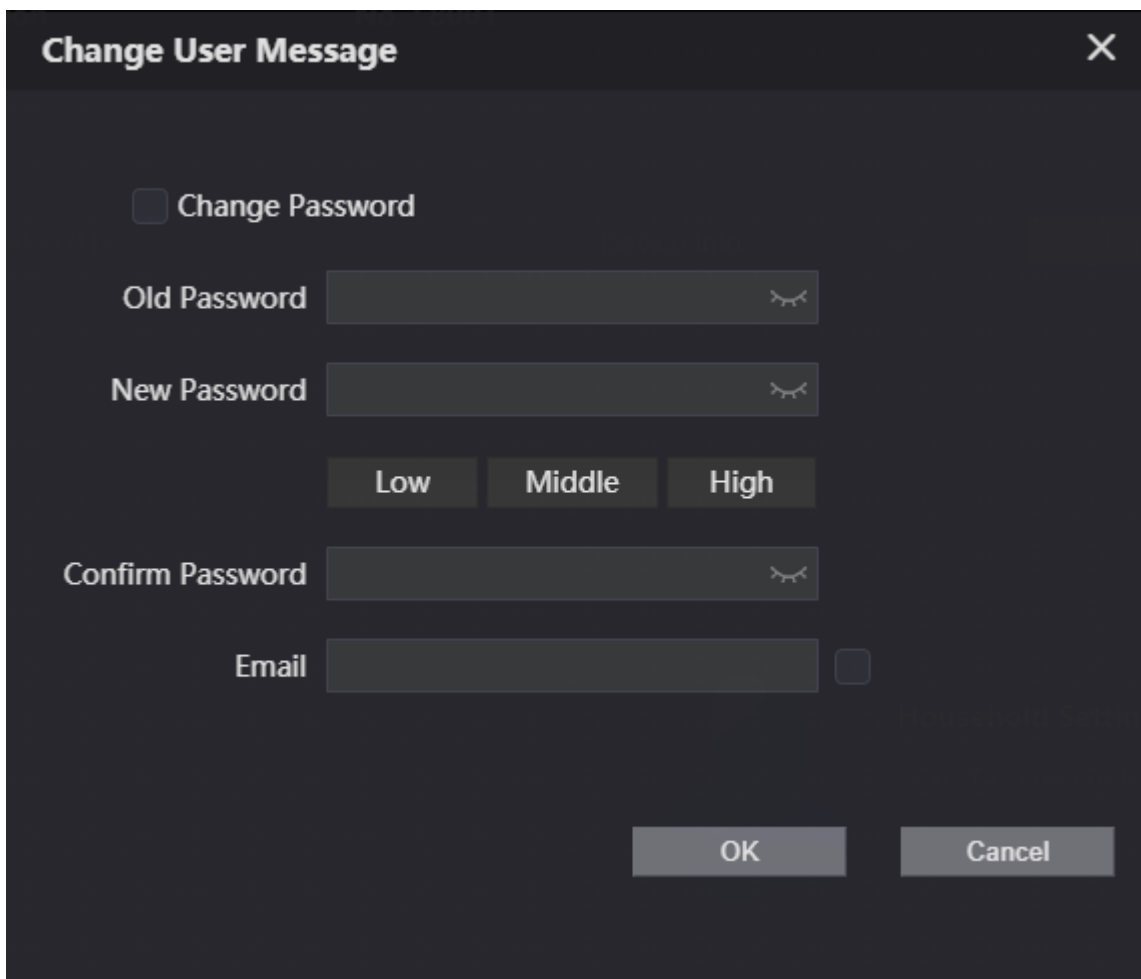
Cambiar la contraseña de inicio de sesión y la dirección de correo electrónico del usuario.

Procedimiento

Paso 1 Hacer clic  en la página de inicio.

Paso 2 Seleccione la información.

Figura 3-3 Cambiar el mensaje del usuario



Paso 3 Configure los parámetros y luego haga clic en **DE ACUERDO**.

3.5 Importar/Exportar la información del dispositivo

3.5.1 Importación de la información del dispositivo

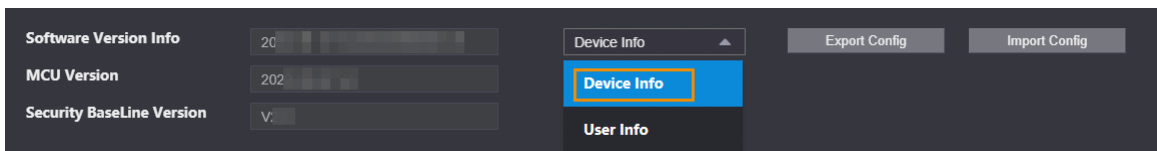
Importar la información del dispositivo al sistema.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccione

Paso 2 Información del dispositivo.

Figura 3-4 Seleccione la información del dispositivo

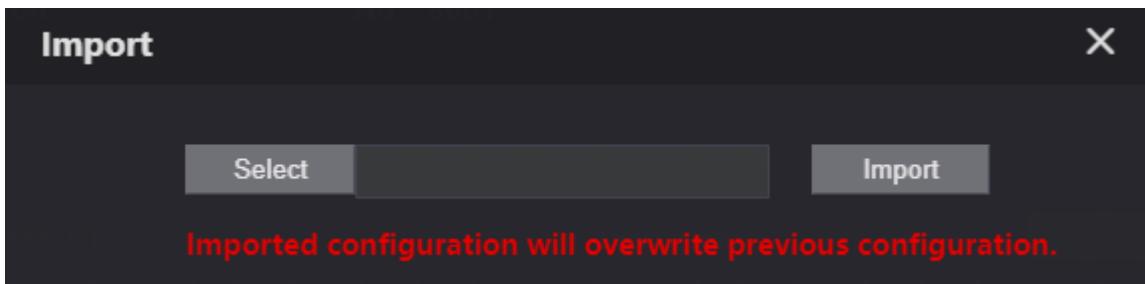


Paso 3 Hacer clic **Importar configuración**.

Paso 4 Hacer clic **Seleccionar** Para seleccionar el archivo de información del dispositivo,

Paso 5 haga clic en **Importar**.

Figura 3-5 Importar la información del dispositivo



3.5.2 Exportación de la información del dispositivo

Inicie sesión en la página web, seleccione **Información del dispositivo**, y luego haga clic **Exportar configuración** para exportar la información del dispositivo actual a la computadora local.

3.6 Importar/Exportar la información del usuario

3.6.1 Importación de la información del usuario

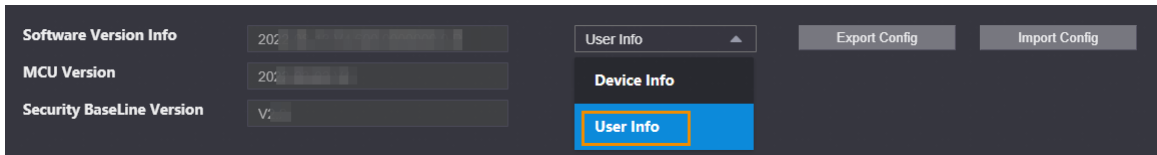
Importar la información del usuario al sistema.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccione

Paso 2 Información del usuario.

Figura 3-6 Seleccionar la información del usuario



Paso 3 Hacer clic **Importar configuración**.

Paso 4 Introduzca la contraseña y haga clic en **Ahorrar**.

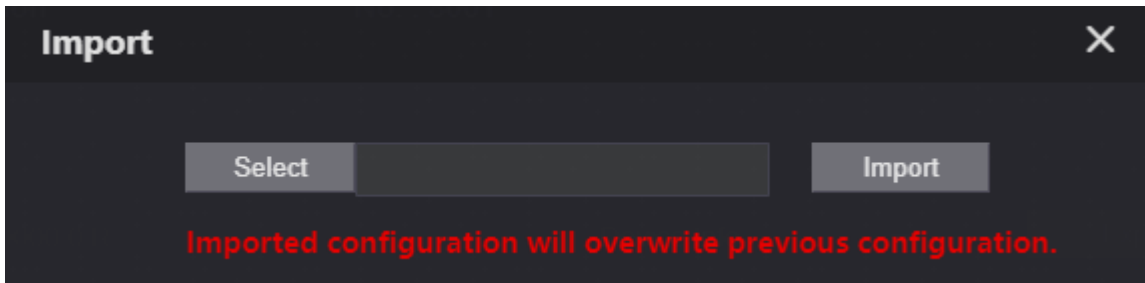


La contraseña se configura durante la configuración de la exportación.

Paso 5 Hacer clic **Seleccionar** Para seleccionar el archivo de información del usuario,

Paso 6 haga clic en **Importar**.

Figura 3-7 Importar la información del usuario



3.6.2 Exportación de la información del usuario

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar **Información del usuario**, y luego haga clic **Exportar**

Paso 3 **configuración**. Configure la contraseña.



La contraseña se utiliza para importar la información del usuario.

Paso 4 Hacer clic **Ahorrar** para guardar el archivo de información del usuario en la computadora local.

3.7 Configuración local

3.7.1 Configuración de parámetros de vídeo y audio

3.7.1.1 Configuración de parámetros de vídeo

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar **Configuración local**>**Vídeo y audio**>**Vídeo**.

Paso 3 Configurar los parámetros de vídeo.

Figura 3-8 Parámetros de vídeo

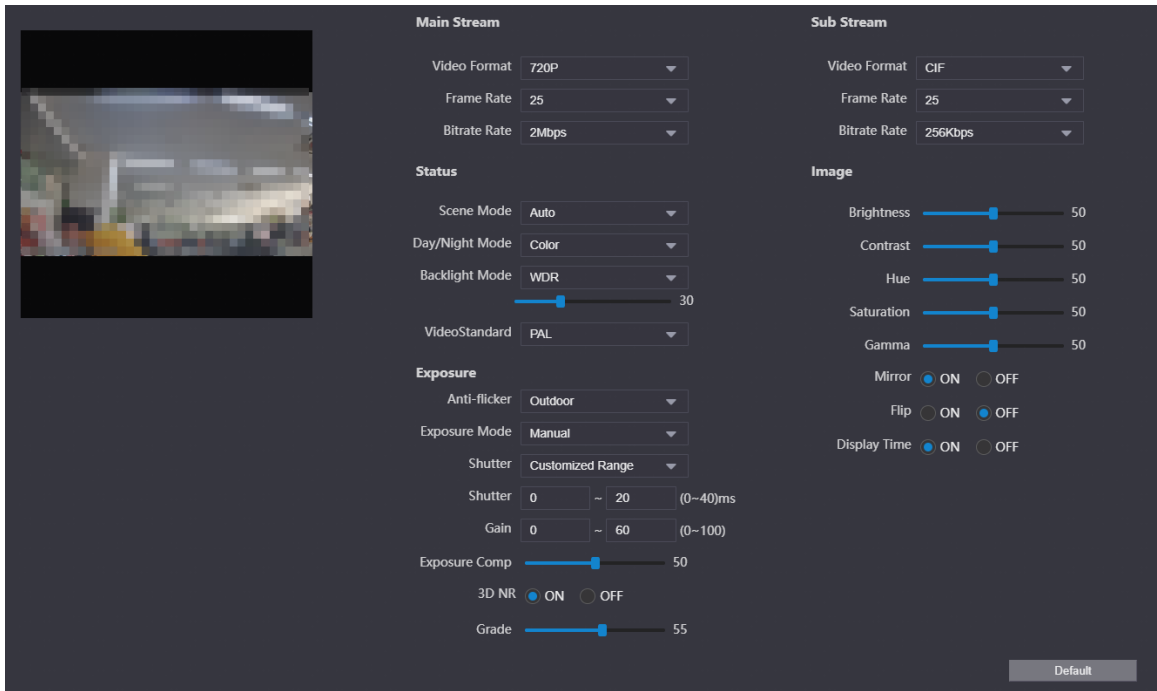


Tabla 3-2 Descripción de los parámetros de vídeo

Parámetro		Descripción
Corriente principal	Formato de vídeo	Ajusta la resolución del vídeo. Puedes seleccionar entre 720P,WVGA,yD1 .
	Velocidad de cuadros	El número de fotogramas por segundo de vídeo. Si selecciona CAMARADA Como estándar de vídeo, puede configurar la velocidad de cuadros hasta 25. Si selecciona NTSC Como estándar de vídeo, puede configurar la velocidad de cuadros hasta 30.
	Tasa de bits	Seleccione de 1024 kbps,1,25 Mbps,1,5 Mbps,1,75 Mbps,2 Mbps,y4 Mbps según la situación real.
Subtransmisión	Formato de vídeo	Ajusta la resolución del vídeo. Puedes seleccionar entre WVGA,D1,QVGA,CIF,y1080P .
	Velocidad de cuadros	El número de fotogramas por segundo de vídeo. Si selecciona CAMARADA Como estándar de vídeo, puede configurar la velocidad de cuadros hasta 25. Si selecciona NTSC Como estándar de vídeo, puede configurar la velocidad de cuadros hasta 30.
	Tasa de bits	Seleccione de 256 kbps,320 kbps,384 kbps,448 kbps,512 kbps,640 kbpsy768 kbps según la situación real.
Estado	Modo de escena	Seleccione de Auto,Soleado,NocheyDesactivado
	Modo día/noche	<ul style="list-style-type: none"> ● Auto:El sistema cambia entre color y blanco y negro según las condiciones reales. ● Color:El sistema muestra la imagen en color. ● Blanco y negro:El sistema muestra imágenes en blanco y negro.

Parámetro		Descripción
	Modo de luz de fondo	<ul style="list-style-type: none"> ● Desactivado:No habrá luz de fondo. ● BLC:El sistema obtiene una imagen más clara de las áreas oscuras del objetivo cuando se dispara contra la luz. ● Amplio rango dinámico (WDR):El sistema atenúa las áreas brillantes y compensa las áreas oscuras para garantizar la claridad de todas las áreas. ● Centro de salud de alto nivel:El sistema atenúa las luces fuertes y reduce el tamaño de la zona de Halo para disminuir el brillo de toda la imagen.
	Estándar de vídeo	Seleccione de CAMARADA y NTSC .
Exposición	Antiparpadeo	<ul style="list-style-type: none"> ● 50 Hz:El sistema ajusta automáticamente la exposición según la luz ambiental para garantizar que no aparezcan rayas. ● 60 Hz:El sistema ajusta automáticamente la exposición según la luz ambiental para garantizar que no aparezcan rayas. ● Exterior:Si seleccionas Exterior, el modo de exposición se puede configurar en Ganar prioridad, Prioridad de obturador y Prioridad del iris. Diferentes dispositivos admiten distintos modos de exposición.
	Modo de exposición	<ul style="list-style-type: none"> ● Auto:La exposición se ajusta automáticamente según el brillo de la escena si el brillo general de las imágenes está dentro del rango de exposición normal. ● Manual:Puedes ajustar el Ganar y Obturador valor manualmente.
	Obturador	Establezca el tiempo de exposición efectivo. Cuanto menor sea el valor, menor será el tiempo de exposición.
	Rango de obturación	Si seleccionas Manual como modo de exposición y seleccione Gama personalizada . Al igual que el obturador, puede configurar el rango del obturador en unidades ms.
	Rango de ganancia	Si seleccionas Manual Como modo de exposición, puede configurar el rango de ganancia para aumentar automáticamente la ganancia del dispositivo cuando la iluminación es baja, obteniendo así una imagen clara.
	Compensación de exposición	Puede configurar el valor de compensación de exposición. El valor varía de 0 a 100. Cuanto mayor sea el valor, más brillante será la imagen.
	Reducción de ruido 3D	Reduzca el ruido de imágenes de varios fotogramas (al menos dos) utilizando la información interfotograma entre dos fotogramas adyacentes en un vídeo. Cuanto mayor sea el nivel, menor será el ruido y mayor la mancha de arrastre.
	Calificación	Grado de reducción de ruido. El valor varía de 0 a 100. Cuanto mayor sea el valor, menor será el ruido.
Imagen	Brillo	Cambia el brillo general de la imagen. Cuanto mayor sea el valor, más brillante será la imagen.

Parámetro		Descripción
	Contraste	Cambie el contraste de la imagen. Cuanto mayor sea el valor, mayor será el contraste entre las áreas brillantes y oscuras. Si el valor es demasiado alto, el área oscura se verá demasiado oscura y el área brillante será más vulnerable a la sobreexposición.
	Matiz	Aclara o intensifica el color. El valor predeterminado lo determina el sensor de luz y es el recomendado.
	Saturación	Establezca la intensidad de los colores. Cuanto mayor sea el valor, más intenso será el color. El valor de saturación no modifica el brillo de la imagen.
	Gama	Cambia el brillo y el contraste de la imagen de forma no lineal. Cuanto mayor sea el valor, más brillante será la imagen.
	Espejo	Si seleccionas EN , la imagen se gira hacia la izquierda y hacia la derecha.
	Voltear	Si seleccionas EN , la imagen se mueve hacia arriba y hacia abajo.
	Tiempo de visualización	Si seleccionas EN , la hora actual se muestra en la imagen de vídeo.

3.7.1.2 Configuración de parámetros de audio

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Configuración local > Vídeo y audio > Audio**.
- Paso 3** Configurar los parámetros de audio.

Figura 3-9 Parámetros de audio

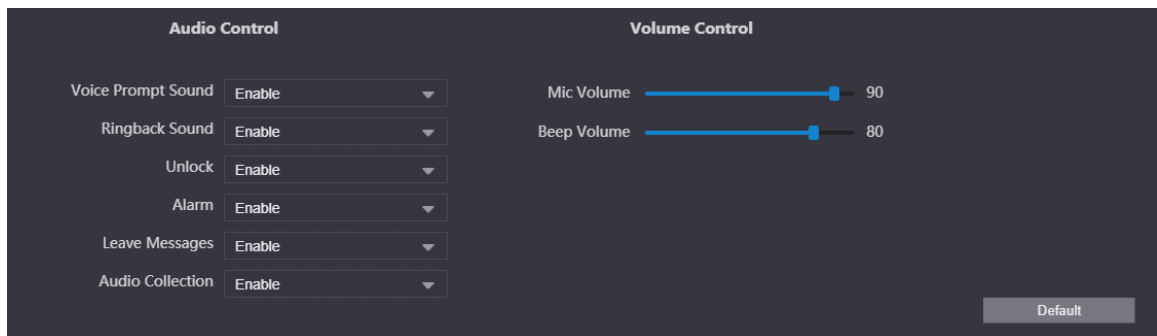


Tabla 3-3 Descripción de los parámetros de audio

Parámetro		Descripción
Control de audio	Aviso de voz Sonido	Si está habilitado, se oirá un sonido de aviso cuando llamas.
	Sonido de retorno de llamada	Si está habilitado, se escucha un sonido de llamada cuando llama.
	Descubrir	Si está habilitado, se oye un sonido de aviso.
	Alarma	Si está habilitado, hay un sonido de alarma.
	Dejar mensajes	Si está habilitado, cuando nadie responde la llamada del visitante, el sistema reproduce un sonido de aviso para los mensajes.

Parámetro		Descripción
	Colección de audio	Si está habilitado, se guardará el audio.
Control de volumen	Volumen del micrófono	Ajuste el volumen del micrófono del VTO. Cuanto mayor sea el valor, mayor será el volumen.
	Volumen del pitido	Ajuste el volumen del pitido del VTO. Cuanto mayor sea el valor, más alto será el volumen.

3.7.2 Configuración de parámetros de control de acceso

3.7.2.1 Configuración del bloqueo local

La cerradura local se refiere a la cerradura conectada al puerto de función del VTO. Puede configurar el intervalo de respuesta, el periodo de desbloqueo, la contraseña y otros parámetros. Para obtener más información sobre la conexión del puerto de función, consulte "1.4 Panel trasero".

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Configuración local**>**Control de acceso**>**Local**.
- Paso 3** Configurar los parámetros del bloqueo local.

Figura 3-10 Bloqueo local

Tabla 3-4 Descripción de los parámetros del bloqueo local

Parámetro	Descripción
Desbloquear intervalo de respuesta	El intervalo para desbloquear nuevamente después del desbloqueo anterior.
Periodo de desbloqueo	La duración durante la cual el bloqueo permanece abierto después del desbloqueo.
Compruebe la señal de la puerta antes de bloquearla	Si seleccionas EN Configure el tiempo de verificación. Cuando el tiempo de desbloqueo supere el tiempo de verificación configurado, se activará la alarma del sensor de puerta y se enviará al VTS.
Tiempo de verificación del sensor de puerta	
Contraseña de la tarjeta de emisión	Se utiliza para emitir nuevas tarjetas. Para más detalles, consulte "2.2.2.3.4 Emisión de Tarjetas" o "2.1.2.3.3 Emisión de Tarjetas".

Parámetro	Descripción
Contraseña del proyecto	Se utiliza para ir a la pantalla de configuración del ingeniero en el VTO.
Tipo de contacto de puerta	<ul style="list-style-type: none"> ● NC: Normalmente cerrado. ● NO: Normalmente abierto.
Cerrar	Seleccione de Local y Segunda cerradura para configurar la autoridad para abrir la cerradura local y la segunda cerradura.
Contraseña de amenaza	Configure la contraseña de amenaza. Si la introduce cuando se le fuerza, se enviará una alarma al centro de administración.
Confirmar contraseña de amenaza	
Tarjeta IC	Cuando está habilitada, se puede utilizar la tarjeta IC para abrir la puerta.
Cifrado y verificación de tarjetas IC	Al activarse, la tarjeta IC se cifra. Deslice la tarjeta correcta con detección de cifrado correcta para abrir la puerta.

Paso 4 Hacer clic **Ahorrar**.

3.7.2.2 RS485

La cerradura se puede conectar a través del puerto RS-485.

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Configuración local** > **Control de acceso** > **RS485**.
- Paso 3** Seleccionar **Cerrar** como el tipo de interfaz.

Figura 3-11 Bloqueo RS-485

Tabla 3-5 Descripción de parámetros del bloqueo RS-485

Parámetro	Descripción
Desbloquear intervalo de respuesta	El intervalo de tiempo para desbloquear nuevamente después del desbloqueo anterior.
Periodo de desbloqueo	El tiempo que el bloqueo permanece abierto después del desbloqueo.
Cerrar	Seleccione de Local y Segunda cerradura para configurar la autoridad para abrir la cerradura local y la segunda cerradura.

Paso 4 Hacer clic **Ahorrar**.

3.7.2.3 Configuración de la contraseña

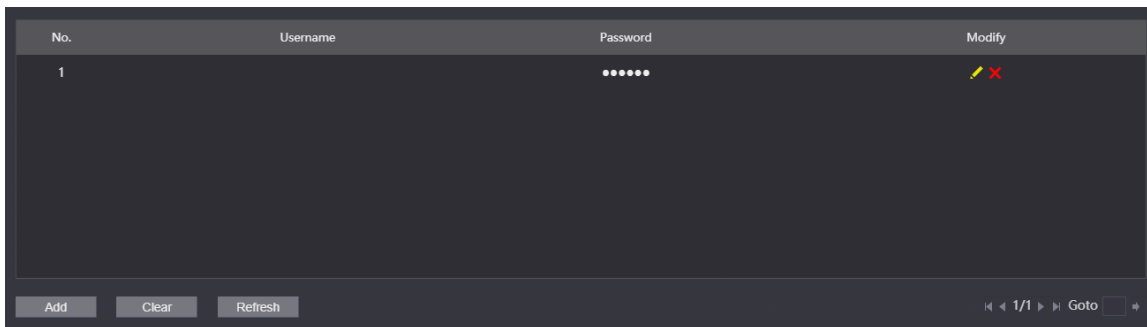
Configurar la contraseña de apertura de la puerta.

Procedimiento

Paso 1 Inicie sesión en la página web.

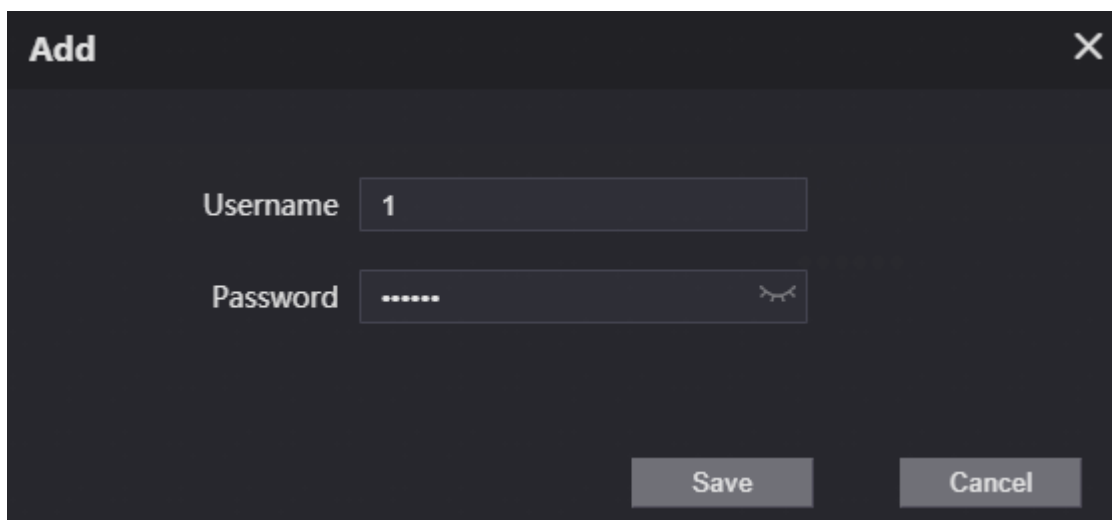
Paso 2 Seleccione **Configuración local > Control de acceso > Gestión de contraseñas**.

Figura 3-12 Gestión de contraseñas





Paso 3 Haga clic en **Agregar**.

Figura 3-13 Agregar la contraseña



Paso 4 Configure el nombre de usuario y la contraseña y luego haga clic en **Ahorrar**.

Operaciones relacionadas

- Editar: Haga clic  para editar la contraseña.
- Eliminar: Haga clic en  para eliminar la contraseña.
- Borrar: Haga clic en **Clar** para borrar todas las contraseñas.
- Actualizar: Haga clic en **Refrescar** para actualizar la página.

3.7.3 Configuración de parámetros del sistema

Configure el formato de fecha, formato de hora, hora del sistema, servidor NTP y otros parámetros.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccione

Paso 2 **Configuración local > Sistema**.

Paso 3 Configurar los parámetros del sistema.

Figura 3-14 Parámetros del sistema

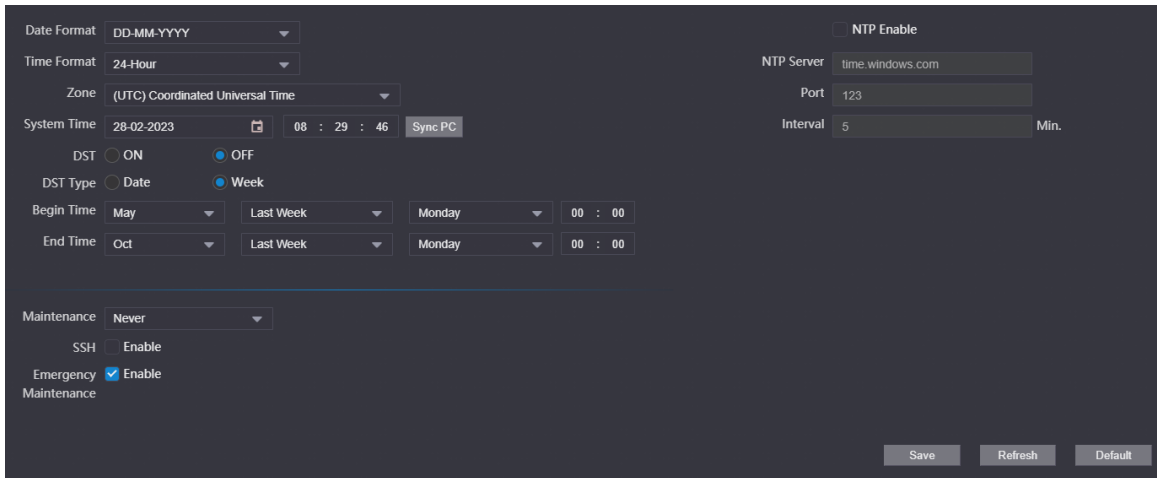


Tabla 3-6 Descripción de los parámetros del sistema

Parámetro	Descripción
Formato de fecha	Configure el formato de fecha, el formato de hora y la zona.
Formato de hora	
Zona	
Hora del sistema	Configurar manualmente la hora del sistema. También puede hacer clic en Sincronizar PC para sincronizar la hora del VTO con la computadora local.
Horario de verano	Seleccione de ENYAPAGADO .
Tipo de horario de verano	Seleccione de FechaySemana .
Hora de inicio	Configure la hora de inicio y la hora de finalización del horario de verano.
Fin de los tiempos	
Habilitar NTP	Si se selecciona, el sistema sincronizará su hora con el servidor NTP que usted configure.
Servidor NTP	Configurar la dirección del servidor NTP.
Puerto	El número de puerto del servidor NTP. El valor predeterminado es 123.
Intervalo	El intervalo en el que el VTO sincroniza la hora con el servidor NTP.
Mantenimiento	Seleccione el tiempo de mantenimiento. El dispositivo se reiniciará automáticamente para mantener la velocidad de funcionamiento.
SSH	Si está habilitado, puede iniciar sesión en el VTO a través de SSH.
Emergencia Mantenimiento	Cuando esta función está habilitada, si el dispositivo no se reinicia 5 veces seguidas, se activará automáticamente un puerto de servicio utilizado por el soporte técnico para realizar actualizaciones y recuperaciones.

Paso 4 Hacer clic **Ahorrar**.

3.7.4 Configuración de la gestión de seguridad

Procedimiento

- Paso 1** Inicie sesión en la página web. Seleccione
- Paso 2** **Configuración local>Seguridad**. Configurar
- Paso 3** los parámetros de seguridad.

Figura 3-15 Gestión de seguridad

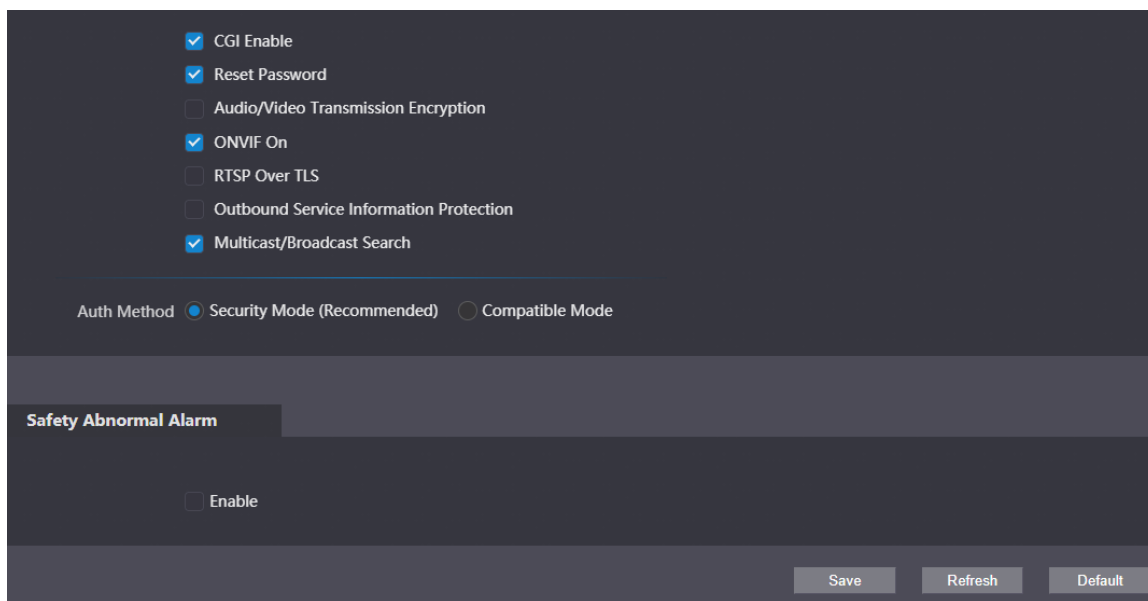


Tabla 3-7 Descripción de los parámetros de seguridad

Parámetro	Descripción
Habilitar CGI	Habilitado por defecto. El VTO se puede conectar con otros productos de video mediante el protocolo CGI (Interfaz de Puerta de Enlace Común).
Restablecer contraseña	Habilitado por defecto. Habilite la función y luego configure la dirección de correo electrónico. Después de la configuración, puede hacer clic en Olvidó su contraseña? en la página de inicio de sesión para restablecer la contraseña.
Cifrado de transmisión de audio y vídeo	Transfiera los datos de audio y video de forma cifrada.
ONVIF activado	Habilitado por defecto. El VTO se puede conectar con otros productos de video mediante el protocolo ONVIF.
RTSP sobre TLS	Transfiera los datos RTSP de forma cifrada.
Protección de la información del servicio de salida	Si está habilitado, la contraseña del dispositivo no se puede obtener a través de la herramienta de tercer protocolo.
Búsqueda de multidifusión/difusión	Si está habilitado, puede buscar el dispositivo a través del protocolo de multidifusión/difusión.
Método de autenticación	Configurar el método de autenticación. Puede seleccionar entre Modo de seguridad (recomendado) y Modo compatible .

Paso 4 Hacer clic **Ahorrar**.

3.7.5 Configuración de parámetros Wiegand

Compatible con dispositivos Wiegand, como lectores y controladores de acceso. Configure el modo y el modo de transmisión según sus dispositivos.

Procedimiento

- Paso 1** Inicie sesión en la página web. Seleccione
- Paso 2** **Configuración local>Wiegand**. Configurar
- Paso 3** los parámetros Wiegand.

Figura 3-16 Parámetros Wiegand

Tabla 3-8 Descripción de los parámetros de Wiegand

Parámetro	Descripción
Modo	Selección de Aporte y Producción según los dispositivos que conectes.
TransMode	Selección de Transformación de 34 bits , Transformación de 66 bits y Transformación de 26 bits . Cuanto mayor sea el valor, más rápida será la transmisión.
Paso de pulso	La frecuencia de la señal Wiegand es 1000 por defecto.
Ancho de pulso	El valor máximo de la señal Wiegand es 200 por defecto.

Paso 4 Hacer clic **Ahorrar**.

3.7.6 Configuración de parámetros de detección de rostros

Configure el umbral, el ángulo de detección y otros parámetros.



La detección de rostro está disponible en modelos seleccionados.

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Configuración local de detección de rostros**
- Paso 3** Configurar los parámetros de detección de rostro.

Figura 3-17 Parámetros de detección de rostros

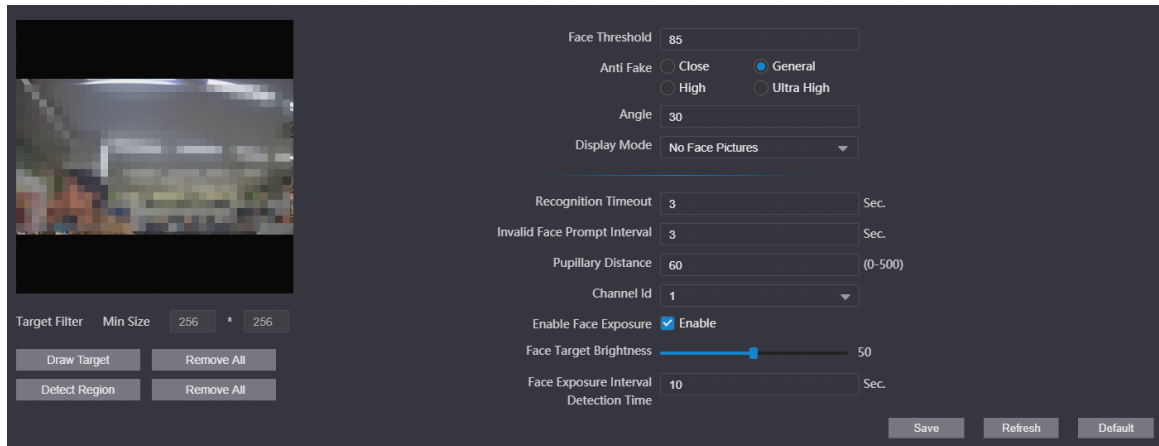


Tabla 3-9 Descripción de parámetros de detección de rostros

Parámetro	Descripción
Umbral facial	Ajuste la precisión de la detección de rostros. Un umbral más alto implica mayor precisión.
Anti-falsificación	Selecciona el nivel para evitar usar la foto o el vídeo de las personas autorizadas para abrir la puerta.
Ángulo	Establezca el ángulo máximo de pose facial para la detección facial. Un valor mayor significa un rango de ángulo facial más amplio.
Modo de visualización	<ul style="list-style-type: none"> ● Sin imágenes de rostro: muestra indicaciones del personaje. ● Sólo imágenes de rostros: muestra la imagen de rostro guardada en la base de datos de rostros. ● Instantáneas y fotografías de rostros: muestra la instantánea y la fotografía de rostros guardadas en la base de datos de rostros.
Tiempo de espera de reconocimiento	Si se reconoce correctamente el rostro de una persona con permiso de acceso, el VTO lo indicará. Configure el intervalo de tiempo para el aviso.
Aviso de rostro no válido Intervalo	Si una persona sin permiso de acceso intenta desbloquear la puerta varias veces dentro del intervalo definido, el VTO mostrará un mensaje de error. Configure el intervalo de tiempo para el mensaje.
Distancia pupilar	Las imágenes faciales requieren la distancia pupilar (píxeles) deseada entre los ojos para un reconocimiento correcto. El píxel varía según el tamaño del rostro y la distancia entre éste y el lente. Si un adulto se encuentra a 1,5 metros del lente, la distancia pupilar puede ser de 50 a 70 px.
Identificación del canal	<ul style="list-style-type: none"> ● 1:Luz blanca. ● 2:Luz infrarroja.
Habilitar exposición facial	Si está habilitado, el VTO aumentará el brillo de acuerdo con el valor configurado solo para el objetivo facial en lugares al aire libre.
Brillo del objetivo facial	
Intervalo de exposición facial Tiempo de detección	Después de la exposición del objetivo facial, si el dispositivo reconoce el rostro nuevamente dentro del tiempo configurado, no hay exposición.

Paso 4 Hacer clic **Ahorrar**.

Operaciones relacionadas

- Dibujar objetivo

Hacer clic **Dibujar objetivo** para configurar el cuadro de detección mínima.

Hacer clic **Eliminar todo** para borrar el cuadro de detección configurado.

- Detectar región

Hacer clic **Detectar región** Para configurar la región de detección, haga clic en los puntos para ajustar la región de detección a un polígono.

Hacer clic **Eliminar todo** para borrar la región de detección configurada.

3.7.7 Agregar usuarios ONVIF

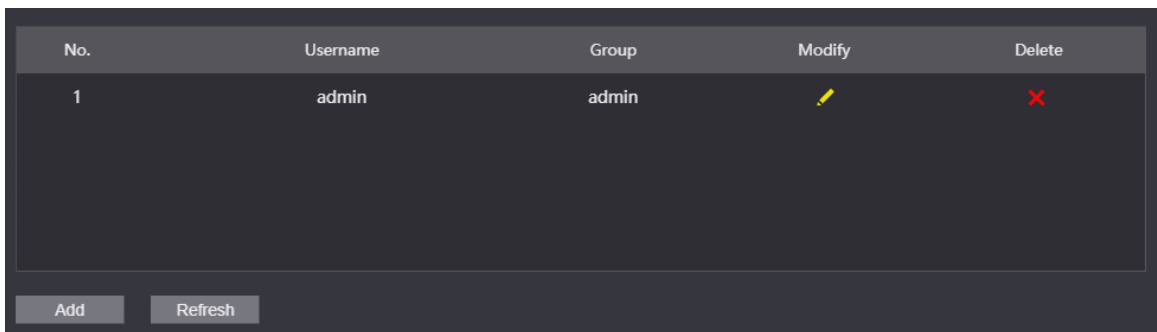
Los usuarios ONVIF se utilizan para el protocolo ONVIF. La información del usuario ONVIF se verificará antes de abrir la puerta.



Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar **Configuración local** > **Usuario de Onvif**.

Figura 3-18 Usuario ONVIF



No.	Username	Group	Modify	Delete
1	admin	admin		

Paso 3 Hacer clic **Agregar**, y luego ingrese el nombre de usuario, la contraseña y confirme la contraseña.

Figura 3-19 Agregar el usuario

Add X

Username

Password

Low Middle High

Confirm password

Save Cancel

Paso 4 Hacer clic **Ahorrar**.

3.7.8 Configuración de parámetros de reconocimiento de huellas dactilares



El reconocimiento de huellas dactilares está disponible en modelos seleccionados.

Procedimiento

- Paso 1 Inicie sesión en la página web.
- Paso 2 Seleccionar **Configuración local** > **Reconocimiento de huellas dactilares**.
- Paso 3 **Configurar el umbral de huella digital**.

Cuanto mayor sea el valor, más preciso será el resultado de la coincidencia.

Figura 3-20 Configurar el parámetro de huella digital

Fingerprint Threshold 3 ▼

Paso 4 Hacer clic **Ahorrar**.

3.7.9 Carga de archivos de audio

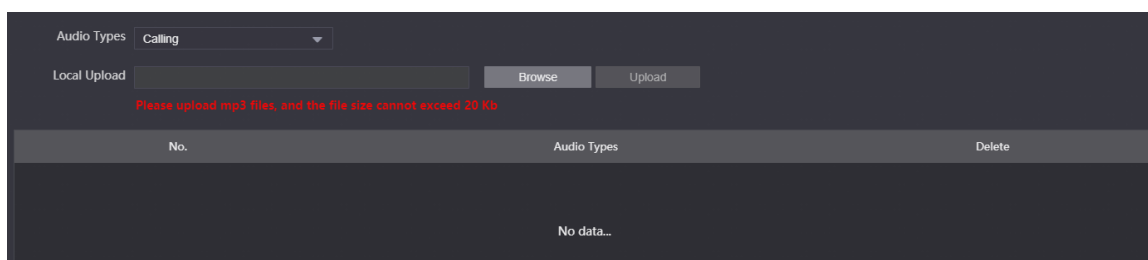
Procedimiento

- Paso 1 Inicie sesión en la página web.
- Paso 2 Seleccionar **Configuración local** > **Subir archivo**.
- Paso 3 Seleccione el tipo de audio.

Paso 4 Hacer clic **Navegar** y luego seleccione el archivo de audio del equipo local. Haga

Paso 5 clic en **Subir**.

Figura 3-21 Subir el archivo



3.7.10 Visualización de la información legal

Inicie sesión en la página web. Seleccione **Configuración local** > **Información legal** Para ver **Acuerdo de licencia de software**, **política de privacidad** y **Aviso de software de código abierto**.

3.8 Entorno del hogar

3.8.1 Agregar el VTO

Para más detalles, véase *Videoportero_Guía de inicio rápido*.

3.8.2 Adición del VTH

Para más detalles, véase *Videoportero_Guía de inicio rápido*.

3.8.3 Adición del VTS

Si el VTO actual funciona como servidor SIP, debe agregar el VTS para habilitar el intercomunicador de video entre el VTO y el VTS.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar **Entorno del hogar** > **Configuración de VTS**.

Paso 3 Hacer clic **Agregar** y luego configure los parámetros.

Figura 3-22 Agregar el VTS

- El número VTS varía entre 888888101 y 888888999.
- Deje la contraseña de registro predeterminada. Si desea registrarla, asegúrese de que coincida con la contraseña de registro del VTS.
- La dirección IP es la dirección del VTS. Haga clic

Paso 4 en **Ahorrar**.

3.8.4 Adición del IPC

Si el VTO actual funciona como servidor SIP, puede agregar los dispositivos IPC en su página web. Los VTH con el mismo servidor SIP en línea obtienen la información de IPC.



- Admite agregar el dispositivo con hasta 32 canales.
- Permite añadir directamente dispositivos IPC. Puede obtener el canal IPC añadiendo NVR/XVR/HCVR.

3.8.4.1 Agregar el IPC uno por uno

Agregue la información del dispositivo de monitoreo de video uno por uno.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar **Entorno del hogar > Configuración del IPC**.

Figura 3-23 Configuración de IPC

IPC Name	IP Addr.	Username	Port	Protocol	Stream	Channel	Device Type	Stream Encry...	Modify	Delete
	0.0.0.0	admin	554	Local	Extra1	1	IPC	OFF		
	0.0.0.0	admin	554	Local	Extra1	1	IPC	OFF		
	0.0.0.0	admin	554	Local	Extra1	1	IPC	OFF		
	0.0.0.0	admin	554	Local	Extra1	1	IPC	OFF		
	0.0.0.0	admin	554	Local	Extra1	1	IPC	OFF		
	0.0.0.0	admin	554	Local	Extra1	1	IPC	OFF		


Paso 3  para configurar los parámetros.

Figura 3-24 Configurar los parámetros

Tabla 3-10 Descripción de parámetros del dispositivo de monitoreo de video

Parámetro	Descripción
Nombre del IPC	Introduzca el nombre del dispositivo IPC/VNR/XVR/HCVR.
Dirección IP.	Introduzca la dirección IP del dispositivo IPC/VNR/XVR/HCVR.
Nombre de usuario	Ingrese el nombre de usuario y la contraseña que utilizó para iniciar sesión en la página web del dispositivo IPC/VNR/XVR/HCVR.
Contraseña	
Puerto	El valor es 554 por defecto.
Protocolo	Seleccione de Local y ONVIF según el dispositivo que agregues.

Parámetro	Descripción
Arroyo	El valor es Extra1 por defecto.
Canal	<ul style="list-style-type: none"> ● Si agrega el IPC, es 1 por defecto. ● Si agrega el NVR/XVR/HCVR, es el canal de IPC que se configuró en el dispositivo VNR/XVR/HCVR.
Tipo de dispositivo	Seleccione el tipo según los dispositivos reales.
Cifrado de transmisión	Mantener la coherencia con el estado de cifrado del dispositivo terminal.

Paso 4 Hacer clic **Ahorrar**.

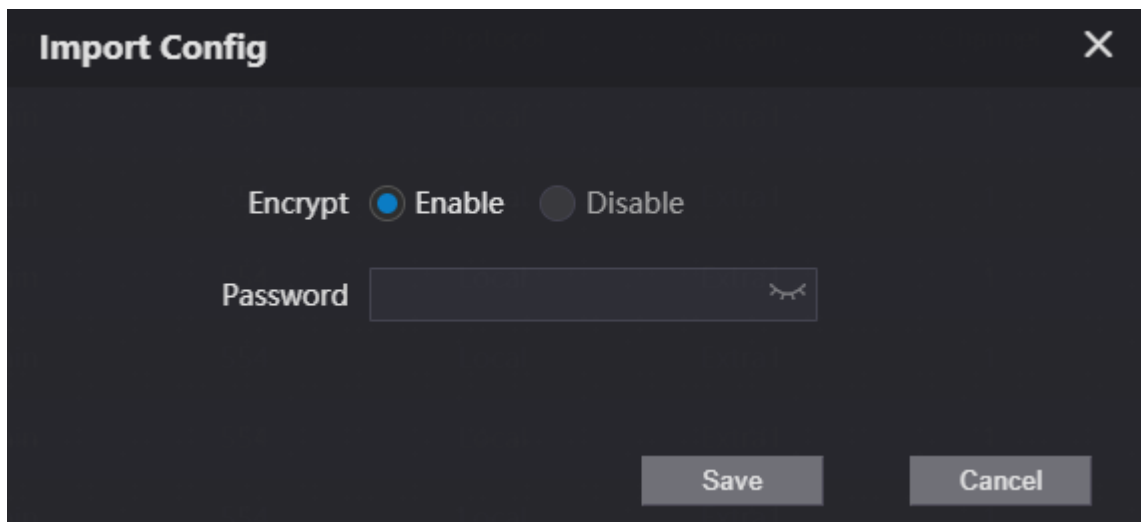
3.8.4.2 Importación de la información de IPC en lotes

Importar la información de IPC al sistema.

Procedimiento

Paso 1 Hacer clic **Importar configuración**.

Figura 3-25 Configuración de importación



Paso 2 Introduzca la contraseña y haga clic en **Ahorrar**.



La contraseña se configura durante la configuración de la exportación.

3.8.4.3 Exportación de la información del IPC en lotes

Exportar la información de IPC y guardarla en la computadora local.

Procedimiento

Paso 1 Hacer clic **Exportar configuración**.

Paso 2 Configure la contraseña y luego haga clic en **Ahorrar**.



La contraseña se utiliza para importar la información del usuario.

Paso 3 Hacer clic **Ahorrar** para guardar el archivo de configuración de IPC en la computadora local.

3.8.5 Visualización de los dispositivos en línea

Si el VTO actual funciona como servidor SIP, el administrador puede ver la información de los dispositivos en línea que se han conectado al servidor SIP actual.

Figura 3-26 Dispositivos en línea

Room No.	Status	IP:Port	Reg Time	Off Time
8001	Online	[Redacted]	28-02-2023 02:27:11	0
9901#0	Offline	[Redacted]	23-02-2023 07:37:38	23-02-2023 08:31:59
9901#10	Offline	[Redacted]	23-02-2023 07:38:22	23-02-2023 08:31:59

3.8.6 Anuncio

Si el VTO actual funciona como servidor SIP, puede enviar anuncios al VTH a través de la página web. También puede consultar el historial.

3.8.6.1 Envío del anuncio


Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Entorno del hogar>Anuncio>Enviar información**.
- Paso 3** Configurar los parámetros.

Figura 3-27 Enviar el anuncio

The screenshot shows a web interface for sending an announcement. At the top, there are two input fields for 'Validity Period': one for the date (28-02-2023) and one for the time (23:59:59). Below these are three main input areas: 'Send to' (with a checkbox for 'All devices'), 'Title', and 'Content'. At the bottom right, there are two buttons: 'Confirm' and 'Refresh'.

Tabla 3-11 Descripción de los parámetros del anuncio

Parámetro	Descripción
Periodo de validez	<p>Configure el período de validez. Debe enviar el anuncio dentro del período de validez para que el VTH pueda recibirlo.</p>  <p>Los registros históricos mostrarán todos los anuncios enviados por el VTO.</p>
Enviar a	Configurar el receptor del anuncio.
Todos los dispositivos	<ul style="list-style-type: none"> ● Introduzca el número de habitación del receptor para enviar únicamente el anuncio. ● Seleccionar Todos los dispositivos Casilla de verificación para enviar el anuncio a todos los dispositivos.
Título	El título del anuncio.
Contenido	El contenido del anuncio. Puede introducir hasta 256 caracteres.

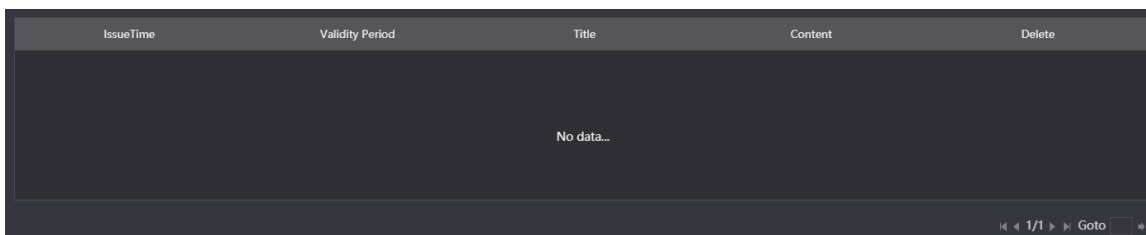
Paso 4 Hacer clic **Confirmar**.

El sistema envía el anuncio al VTH.

3.8.6.2 Visualización del anuncio del historial

Inicie sesión en la página web. Seleccione **Entorno del hogar > Anuncio > Información histórica**. Puede ver o eliminar los registros del historial.

Figura 3-28 Ver los registros del historial



IssueTime	Validity Period	Title	Content	Delete
No data...				

3.8.7 Gestión de personal

Administrar y visualizar la información de las personas, tarjetas y huellas.



La información de la tarjeta y huella dactilar registrada en el VTO se cargará en la gestión de personal en tiempo real.

Inicie sesión en la página web. Seleccione **Entorno del hogar > Gestión de personal**.

Figura 3-29 Gestión de personal

No.	Personnel No.	Room No.	Username	Card/Fingerprint	Modify	Delete
1	9901	9901				

Buttons: Add, Refresh, Clear, Personnel Export, Personnel Import. Page navigation: << 1/1 >> Goto [] +

3.8.7.1 Agregar personas

Añade la información de las personas para gestionar la información en la página web. Permite añadirlas individualmente y por lotes.

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Entorno del hogar > Gestión de personal**. Hacer clic
- Paso 3** **Agregar**.
- Paso 4** Ingrese el número de personal, el número de habitación y el nombre de usuario y luego haga clic en **Ahorrar**.
 - **Número de personal:** Puedes personalizar el número.
 - **Habitación N°:** Introduzca el número de habitación correspondiente del VTH.
 - **Nombre de usuario:** Introduzca el nombre de las personas.

Figura 3-30 Configurar los parámetros

Add [Close X]

Personnel No.

Room No.

Username

Unlock Permission Lock 1 Lock 2




Save Cancel


3.8.7.2 Gestión de tarjetas

El VTO sube la información de la tarjeta a la página web después de registrarse en el dispositivo. Puede consultarla, reportar su pérdida y eliminarla.


3.8.7.2.1 Notificación de la pérdida

Si pierde la tarjeta, le recomendamos que informe la pérdida rápidamente.

Hacer clic  Para acceder a la página de información de la tarjeta, haga clic  el icono se encenderá. . El acceso La autenticación de esta tarjeta deja de ser válida.

Si necesita restaurar la autenticación de acceso, haga clic en  de nuevo.

3.8.7.2.2 Eliminación de la tarjeta

Hacer clic  Para eliminar la tarjeta individualmente, puedes hacer clic **Clarop** para borrar todas las tarjetas.

3.8.7.3 Borrado de huellas dactilares

El VTO sube la información de las huellas dactilares a la página web después de registrarse en el dispositivo. Puede verla y eliminarla.


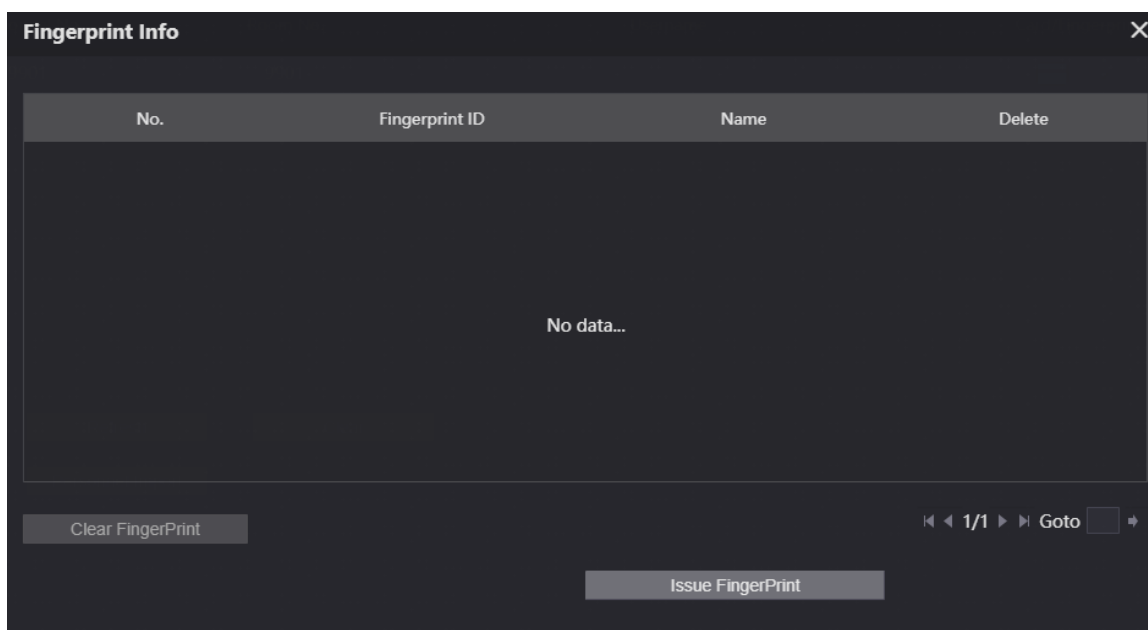
Haga clic  para ver la información de las huellas dactilares de las personas. Haga clic **Huella dactilar clarap** para borrar todas las huellas dactilares de las personas seleccionadas.

Figura 3-31 Información de huellas dactilares



3.9 Red

3.9.1 Configuración de los parámetros básicos

Configure la dirección IP y otros parámetros de red del VTO y los puertos web.

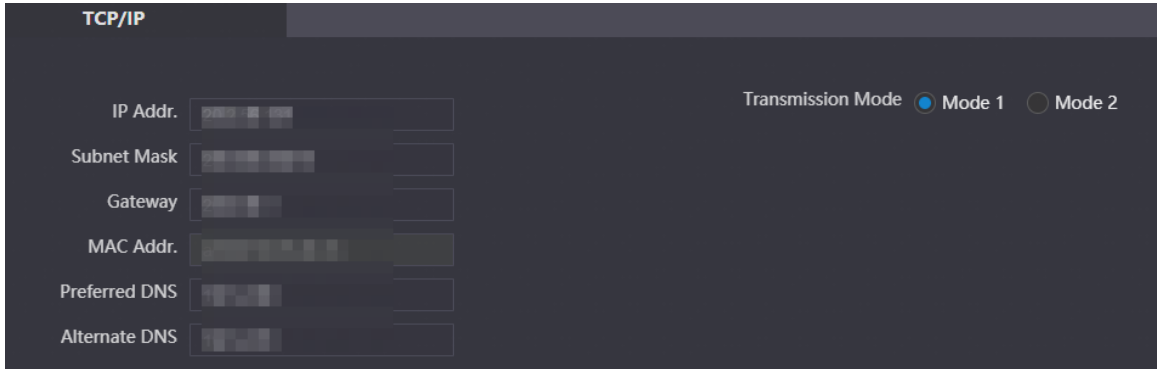
Procedimiento

- Paso 1 Inicie sesión en la página
- Paso 2 web. Seleccione **Red** > **Básico**.

Paso 3 Configurar los parámetros deTCP/IP.

Ingrese la dirección IP, la máscara de subred, la puerta de enlace del VTO y la dirección IP del servidor DNS preferido y el servidor DNS alternativo.

Figura 3-32 Configurar los parámetros TCP/IP



Paso 4 Configurar el webpot.

Figura 3-33 Puerto web

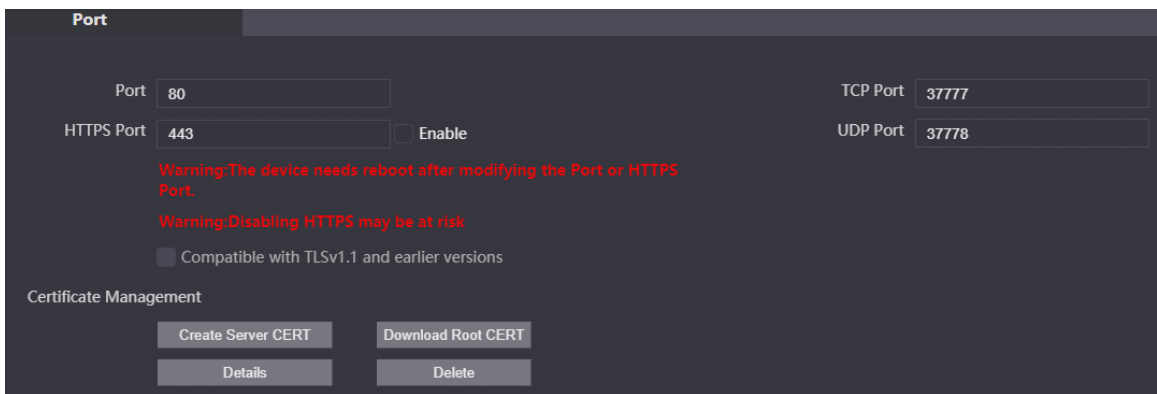


Tabla 3-12 Descripción de los parámetros del puerto web

Parámetro	Descripción	
Puerto	El puerto web predeterminado es el 80. Si cambia el número de puerto, agréguelo después de la dirección IP al iniciar sesión en un navegador web.	
Puerto HTTPS	Introduzca el número de puerto y luego seleccione Permitir Para habilitar la función HTTPS, puede ingresar https://VTO IP: número de puerto HTTPS para ir a la página web de la VTO.	
Puerto TCP	El protocolo TCP proporciona el puerto del servicio. El valor predeterminado es 3777.	
Puerto UDP	El valor predeterminado del puerto de protocolo de datagrama de usuario es 3778.	
Certificado Gestión	Crear certificado de servidor	Si utiliza esta función por primera vez o cambia la IP del dispositivo, haga clic en Crear certificado de servidor .
	Descargar certificado raíz	Si usa HTTPS por primera vez después de cambiar de computadora, haga clic en Descargar certificado raíz .

Parámetro		Descripción
	Detalles	Haga clic para ver la región, provincia, ubicación y otra información detallada.
	Borrar	Eliminar el certificado del servidor.

Paso 5 Hacer clic **Ahorrar**.

3.9.1.1 Creación del certificado del servidor

Instale el certificado de servidor que se creó manualmente para habilitar el inicio de sesión normal y mejorar la seguridad de su sitio web.



- Si utiliza HTTPS por primera vez o se cambia la dirección IP del dispositivo, cree un certificado de servidor y luego instale un certificado raíz.
- Si cambia de computadora para iniciar sesión en la página web, deberá descargar e instalar nuevamente el certificado raíz en la nueva computadora o copiarlo a la nueva computadora.

Procedimiento

Paso 1 En el **Básico** página, haga clic **Crear certificado de**

Paso 2 **servicio**. Ingrese la región, provincia y otra información.

Figura 3-34 Crear el certificado del servidor

Create Server CERT [X]

Region

Province

Location

Organization

Organization Unit

IP/Domain Name

Warning: Reboot the device manually after creating server certificate.

Save Cancel

Paso 3 Hacer clic **Ahorrar**.

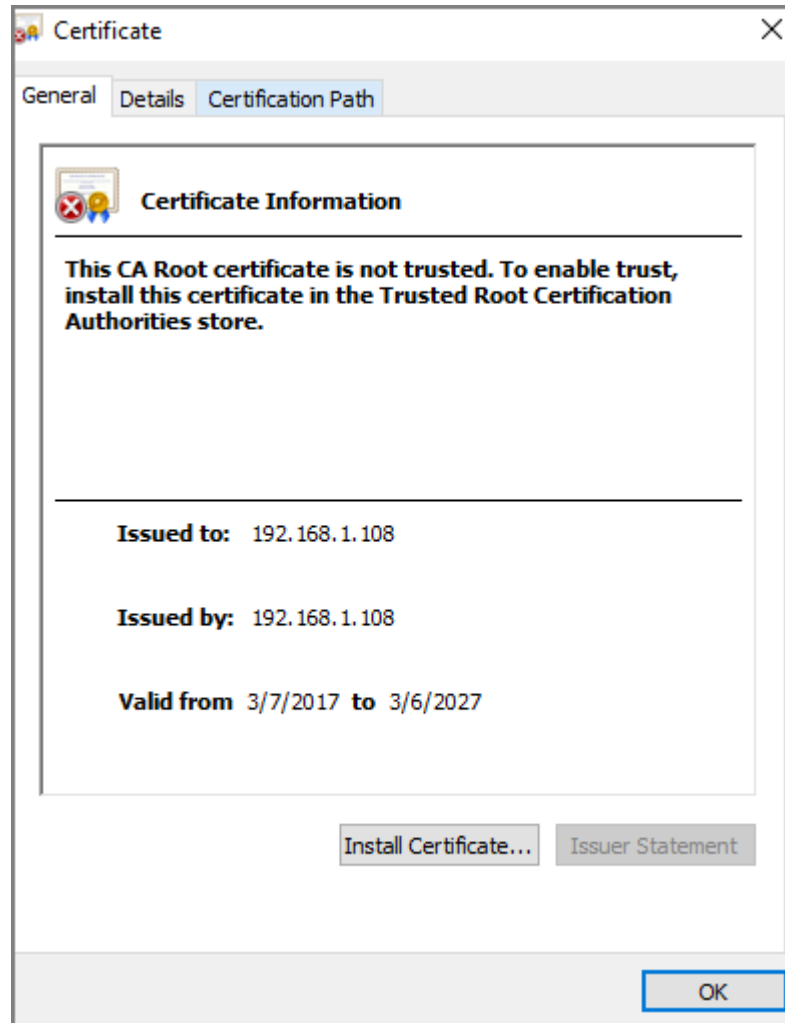
El dispositivo se reiniciará.

3.9.1.2 Descarga e instalación del certificado raíz

Procedimiento

- Paso 1 En el **Básico** página, haga clic **Descargar certificado raíz**
- Paso 2 Haz doble clic en el archivo que has descargado. Haz clic
- Paso 3 en **Instalar certificado**.

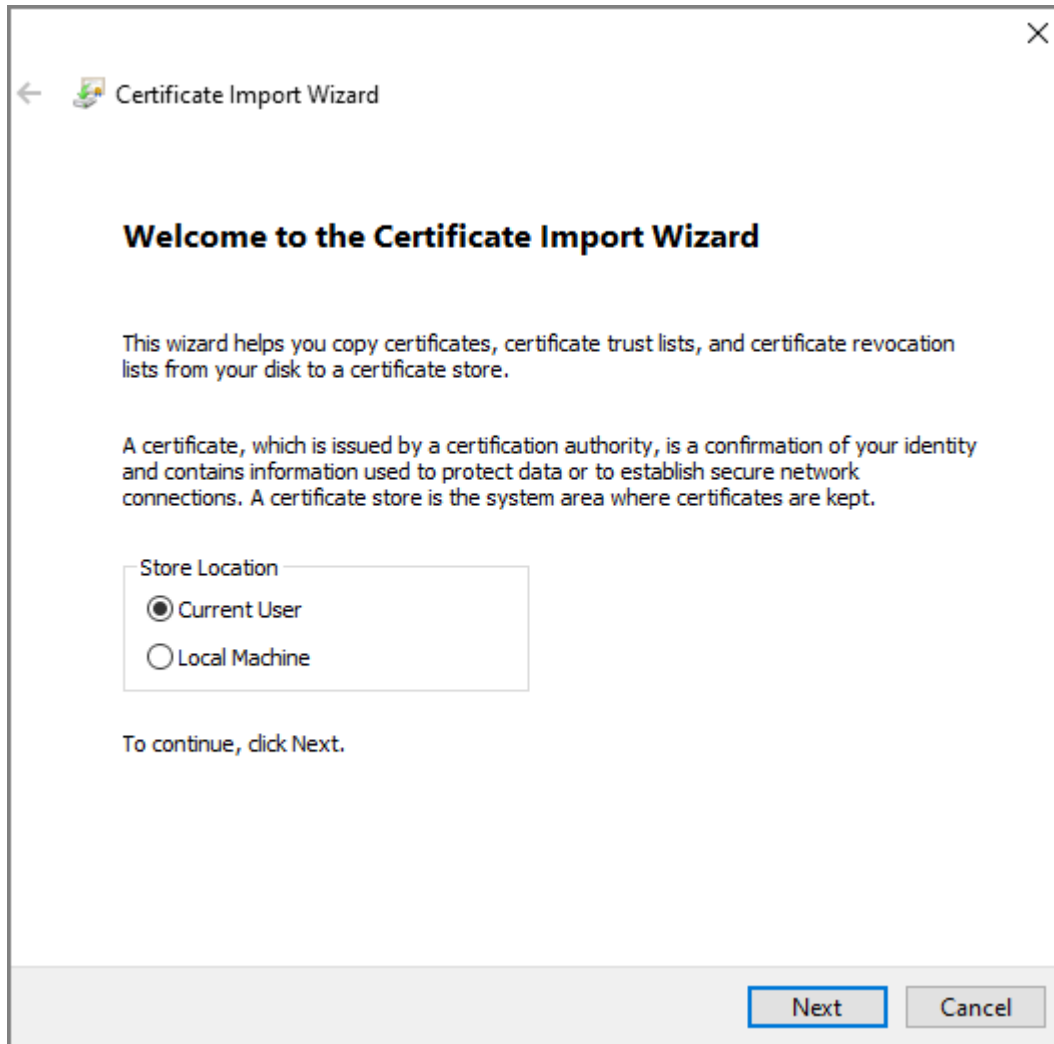
Figura 3-35 Información del certificado



Paso 4 Seleccionar **Usuario actual** o **Máquina local**, y luego haga clic **Próximo**.

- **Usuario actual**: Se aplica al usuario que ha iniciado sesión en la computadora.
- **Máquina local**: Se aplica a todos los usuarios que han iniciado sesión en la computadora.

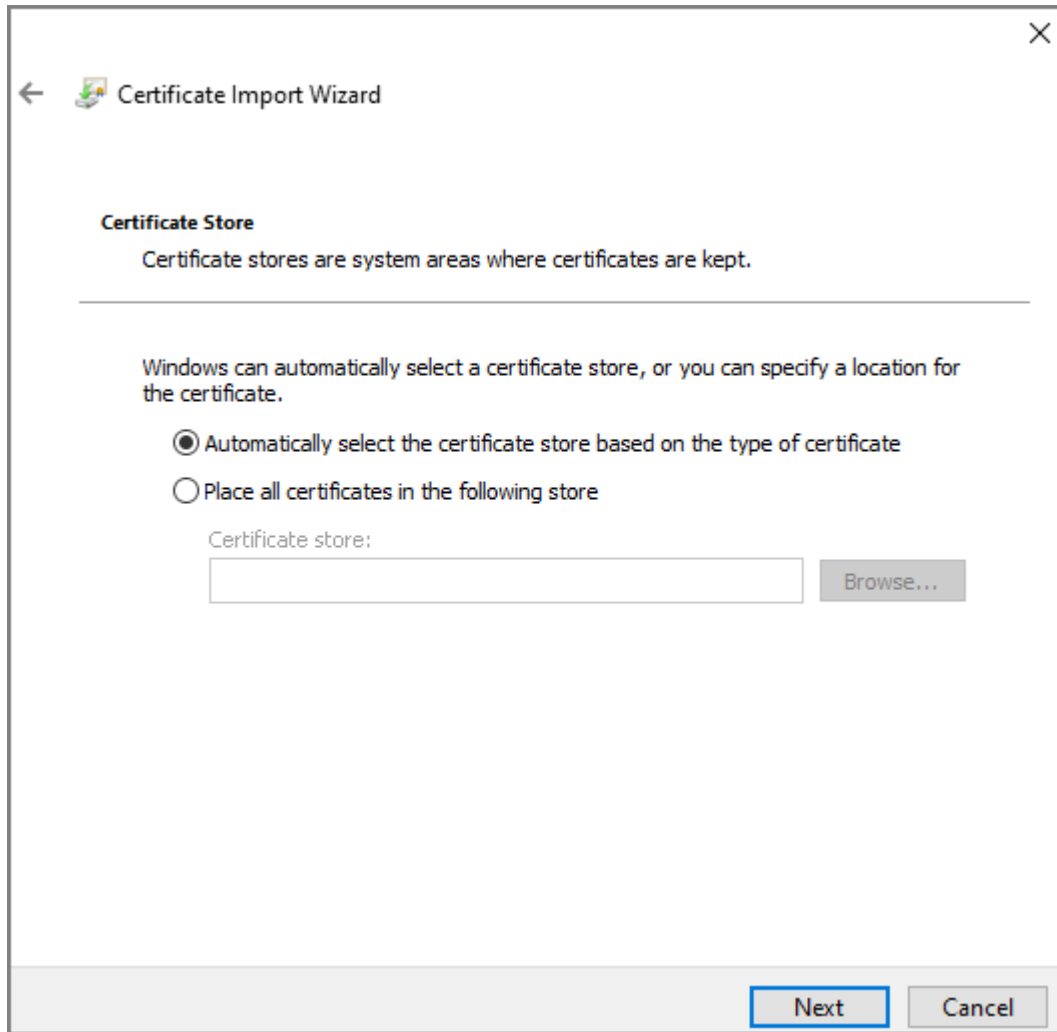
Figura 3-36 Ubicación de la tienda



Paso 5 Seleccione la ubicación adecuada.

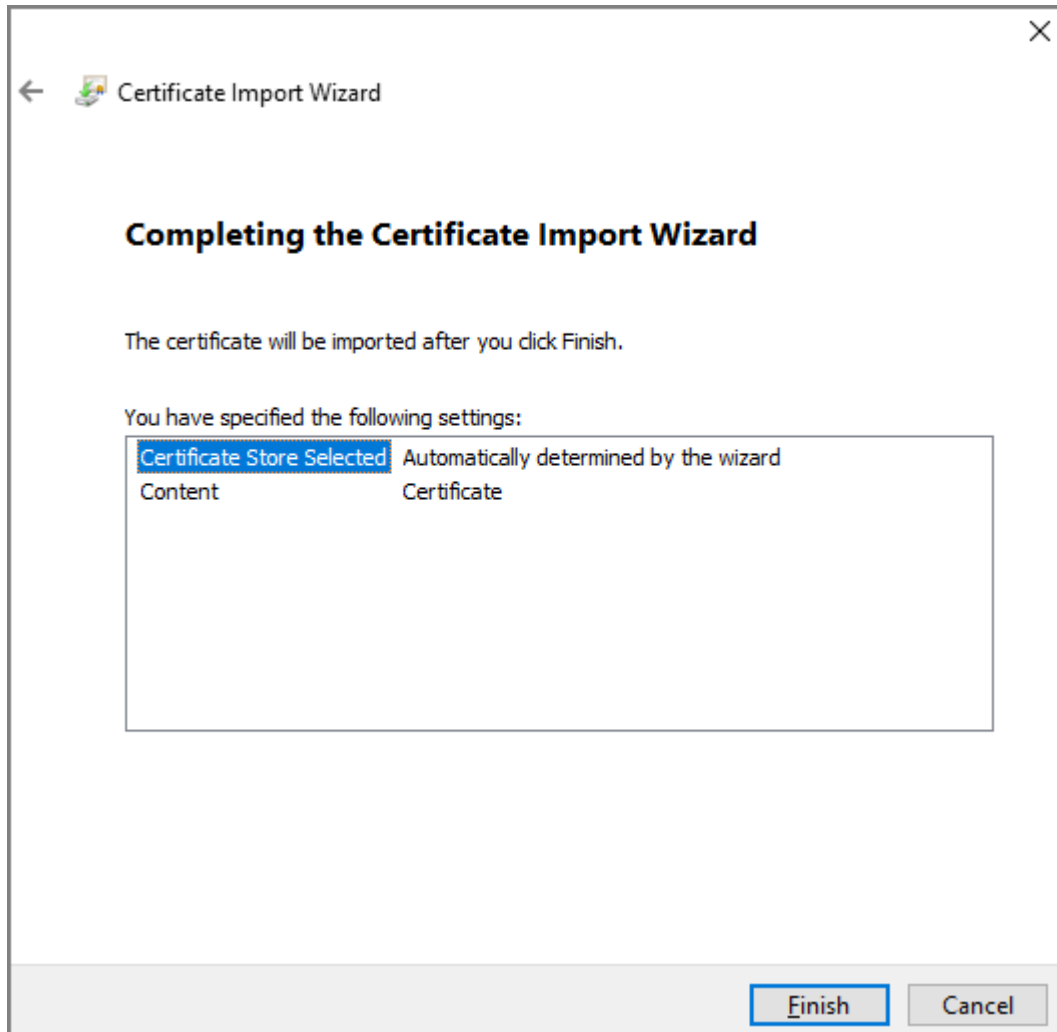
- a. Seleccione **Coloque todos los certificados en el siguiente almacén**.
- b. Haga clic **Navegar** para importar el certificado a la **Tienda de autoridades de certificación raíz de confianza**, y luego haga clic **Próximo**.

Figura 3-37 Almacén de certificados



Paso 6 Hacer clic **Finalizar**.

Figura 3-38 Finalizar la descarga del certificado



3.9.2 Configuración del servicio UPnP

Si el VTO actual funciona como servidor SIP, puede agregar una relación de mapeo entre la intranet y la extranet mediante el protocolo UPnP. Esta función permite conectar dispositivos en la intranet a través de la dirección IP de la extranet.

Prerrequisitos

- Asegúrese de que el VTO se haya conectado al enrutador.
- Habilite la función UPnP del enrutador y luego configure la dirección IP WAN para configurar la conexión a Internet.
- Conecte el VTO al puerto LAN del enrutador.

3.9.2.1 Habilitación de los servicios UPnP

Procedimiento

- Paso 1 Inicie sesión en la página
- Paso 2 web. Seleccione **Red>UPnP**.

Figura 3-39 UPnP

<input checked="" type="checkbox"/>	Service Name	Service Type	Protocol	Internal Port	External Port	Status	Modify	Delete
<input checked="" type="checkbox"/>	HTTP	CustomService	TCP	80	8080	Failed		
<input checked="" type="checkbox"/>	TCP	CustomService	TCP	37777	37777	Failed		
<input checked="" type="checkbox"/>	UDP	CustomService	UDP	37778	37778	Failed		
<input checked="" type="checkbox"/>	RTSP	CustomService	TCP	554	554	Failed		
<input checked="" type="checkbox"/>	PrivService	CustomService	TCP	18877	18877	Failed		
<input checked="" type="checkbox"/>	Rtp	CustomService	UDP	15006	15006	Failed		
<input checked="" type="checkbox"/>	Rtp	CustomService	UDP	15007	15007	Failed		
<input checked="" type="checkbox"/>	Rtp	CustomService	UDP	15008	15008	Failed		

Paso 3 Seleccione los servicios y luego seleccione **Permitir**. Haga

Paso 4 clic **Ahorrar**.

Ingresa **http://IP de extranet: puerto externo** para visitar el dispositivo interno del puerto correspondiente del router.

3.9.2.2 Agregar el servicio UPnP

Añade los nuevos servicios UPnP.

Procedimiento

Paso 1 Inicie sesión en la página

Paso 2 web. Seleccione **Red > UPnP**.

Paso 3 Hacer clic **Agregar** y luego configure los parámetros.

Figura 3-40 Agregar el servicio UPnP

Tabla 3-13 Descripción de los parámetros del servicio UPnP

Parámetro	Descripción	
ENCENDIDO/APAGADO	<ul style="list-style-type: none"> ● EN:Habilitar el servicio. ● APAGADO:Deshabilitar el servicio. 	
Nombre del servicio	El nombre y el tipo del servicio de red.	
Tipo de servicio		
Protocolo	Seleccione de TCP y UDP .	
Puerto interno	El puerto al que se dirige el VTO actual. Necesita mapear.	<ul style="list-style-type: none"> ● Recomendamos usar un número de puerto entre 1024 y 5000 para el puerto externo. Evite usar un número de puerto entre 1 y 255 y un número de puerto del sistema entre 256 y 1023 en caso de conflicto de puertos. ● Si implementa muchos dispositivos en la misma LAN, primero haga un plan del número de puerto para evitar que muchos dispositivos tengan una relación de mapeo con el mismo puerto externo. ● Asegúrese de que el número de puerto pueda funcionar normalmente y no esté restringido. ● El puerto interno y el puerto externo del TCP y del UDP deben ser el mismo y no se pueden modificar.
Puerto externo	El puerto de la enrutador que necesita tener el cartografía relación.	

Paso 4 Hacer clic **Ahorrar**.

3.9.3 Configuración del servidor SIP

Configure el servidor SIP y registre el VTO y el VTH en él para habilitar el videoportero mediante el protocolo SIP. Puede configurar el VTO actual, otro VTO o la plataforma como servidor SIP. Para más detalles, consulte *Videoportero_Guía de inicio rápido*.

3.9.4 Cortafuegos

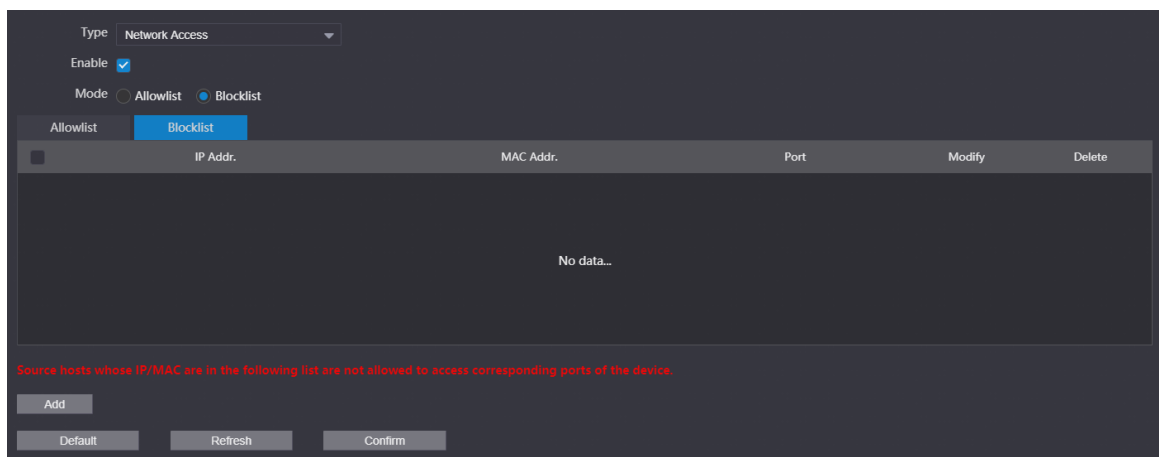
3.9.4.1 Acceso a la red

Configure la lista de permitidos y la lista de bloqueados para administrar los permisos de los usuarios.

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccione **Red > Cortafuegos**.
- Paso 3** Seleccione **Acceso a la red** como el tipo y luego seleccione **Permitir**. Configure
- Paso 4** la lista de permitidos y la lista de bloqueados.


Figura 3-41 Acceso a la red



1. Seleccione entre **Lista de permitidos** y **Lista de bloqueo** como modo. También puedes hacer clic **Lista de permitidos** o **Lista de bloqueo** pestaña.
2. Haga clic **Agregar**.
3. Configure los parámetros.

Figura 3-42 Agregar la dirección IP

Tabla 3-14 Descripción de los parámetros de la dirección IP

Parámetro	Descripción
Tipo	<p>Seleccione de Dirección IP, Sección de propiedad intelectual, Dirección MAC, y Toda la propiedad intelectual.</p> <p></p> <p>Si seleccionas Dirección MAC. Como tipo, ingrese la dirección MAC y luego haga clic en Ahorrar.</p>
Versión IP	La versión predeterminada es IPv4 .
IPv4	Introduzca la dirección IP.
Todos los puertos	Tras habilitarla, la lista de permitidos o bloqueados se aplicará a todos los puertos del dispositivo. Si no selecciona todos los puertos, introduzca el puerto de inicio y el puerto de destino.

4. Haga clic **Ahorrar**.

Paso 5 Hacer clic **Confirmar**.

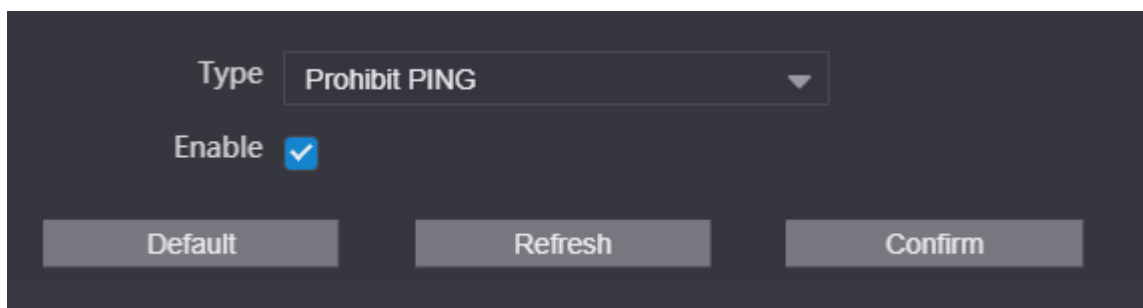
3.9.4.2 Prohibir PING

Después de habilitar **Prohibir PING**, el dispositivo no responderá al PING.

Procedimiento

- Paso 1** Iniciar sesión en la página web
- Paso 2** Seleccionar **Red > Cortafuegos**. Seleccionar
- Paso 3** **Prohibir PING** como el tipo. Habilitar la
- Paso 4** función.

Figura 3-43 Prohibir PING



Paso 5 Hacer clic **Confirmar**.

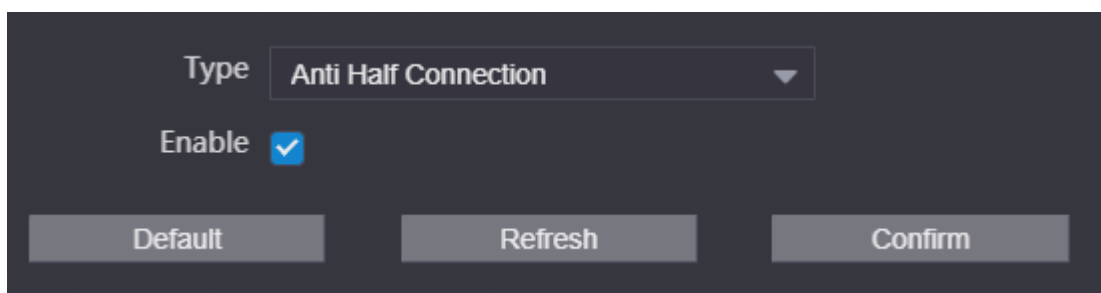
3.9.4.3 Conexión anti-media

Tras la activación, el sistema monitorea el número UDP o TCP que envía la solicitud y no recibe respuesta. La conexión no se permite cuando el número alcanza un valor determinado. Asegúrese de que la conexión normal tenga el recurso y evite las conexiones semiabiertas.

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccione **Red>Cortafuegos**.
- Paso 3** Seleccionar **Anti-Media Conexión** como el tipo.
- Paso 4** Habilitar la función.

Figura 3-44 Conexión anti-mitad



Paso 5 Hacer clic **Confirmar**.

3.10 Registros

3.10.1 Visualización de los registros de llamadas

Consulte los registros de llamadas del VTO. El sistema puede guardar hasta 1024 registros.

Procedimiento

- Paso 1** Inicie sesión en la página web. Seleccione
- Paso 2** **Registro de búsqueda>Llamar**.

Figura 3-45 Registros de llamadas

No.	Call Type	Room No.	Begin Time	Talk Time(Min.)	End State
No data...					

Export Data Please keep unencrypted files well, in order to avoid data leakage risk. 1/1 Goto

Paso 3 (Opcional) Haga clic en **Exportar datos** para exportar los registros de llamadas del VTO.

3.10.2 Búsqueda de registros de alarmas

Consulte los registros de alarmas del VTO. El sistema puede guardar hasta 1024 registros.



Cuando el VTO actual funciona como servidor SIP, el sistema tiene los registros de alarma.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccione

Paso 2 **Registro de búsqueda>Alarma.**

Figura 3-46 Registros de alarmas

No.	Room No.	Event State	Channel	Begin Time
1	8001	Door Sensor	5	28-02-2023 02:27:39
2	8001	Tamper Alarm	1	28-02-2023 02:27:06
3	8001	Door Sensor	5	23-02-2023 12:15:44
4	8001	Tamper Alarm	1	23-02-2023 12:15:11
5	8001	Door Sensor	5	23-02-2023 07:01:48
6	8001	Tamper Alarm	1	23-02-2023 07:01:15
7	8001	Tamper Alarm	1	23-02-2023 06:59:39
8	8001	Door Sensor	5	23-02-2023 06:57:53
9	8001	Tamper Alarm	1	23-02-2023 06:57:21

Export Data Please keep unencrypted files well, in order to avoid data leakage risk. 1/1 Goto

Paso 3 (Opcional) Haga clic en **Exportar datos** para exportar los registros de alarma del VTO.

3.10.3 Búsqueda de registros de desbloqueo de la puerta

Consulte los registros de apertura de puertas. El sistema puede guardar hasta 1024 registros.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccione

Paso 2 **Registro de búsqueda>Descubrir.**

Figura 3-47 Registros

No.	Unlock Type	VTO No.	Personnel No.	Room No.	Username	Card No.	Lock	Unlock Result	Unlock Time
1	Face Detect Unlock	8001					Local	Failed	28-02-2023 11:58:27
2	Face Detect Unlock	8001					Local	Failed	28-02-2023 11:58:23
3	Face Detect Unlock	8001					Local	Failed	28-02-2023 11:58:18
4	Face Detect Unlock	8001					Local	Failed	28-02-2023 11:58:15
5	Face Detect Unlock	8001					Local	Failed	28-02-2023 11:58:07
6	Face Detect Unlock	8001					Local	Failed	28-02-2023 11:58:04
7	Face Detect Unlock	8001					Local	Failed	28-02-2023 11:57:57
8	Face Detect Unlock	8001					Local	Failed	28-02-2023 11:57:43
9	Face Detect Unlock	8001					Local	Failed	28-02-2023 11:57:38

Export Data Please keep unencrypted files well, in order to avoid data leakage risk. 1/68 Goto

Paso 3 (Opcional) Haga clic en **Exportar datos** para exportar los registros de desbloqueo de la puerta.

3.10.4 Búsqueda en los registros del sistema

Ver los registros de operaciones de la página web.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccione

Paso 2 **Registro de búsqueda>Registro.**

Paso 3 Configure el rango de tiempo, seleccione el tipo y luego haga clic en **Buscar** para ver los registros.

Figura 3-48 Registros

Time Range: 28-02-2023 00:00:00 -- 01-03-2023 00:00:00

Type: All

No.	Record Time	Event
No data...		

Log Info
 Record Time:
 Type:
 Detail:

Export Data 1/1 Goto

Please keep unencrypted files well, in order to avoid data leakage risk.


Tabla 3-15 Descripción del tipo de registro

Tipo	Descripción
Todo	Buscar todos los registros.
Sistema	Buscar los registros del sistema.
Registro	Busque los registros de operaciones del registro.
Configuración	Buscar los registros de la configuración.
Cuenta	Busque los registros de registro de todas las cuentas.


Tipo	Descripción
Seguridad	Busque registros de seguridad del sistema, como coacción, antimanipulación y apagado.
Evento	Busque los registros del evento, como los registros de alarma.

Paso 4 (Opcional) Haga clic en **Exportar datos** para exportar los registros.


3.11 Reinicio del dispositivo

Seleccionar  > **Reiniciar**, y luego haga clic **Confirmar** en la ventana emergente. El dispositivo automáticamente se reinicia y la página web va a la página de inicio de sesión.

3.12 Restauración a los valores predeterminados de fábrica

Seleccionar  > **Restaurar**, y luego haga clic **Confirmar** en la ventana emergente. El dispositivo automáticamente se reinicia y restaura todos los parámetros a los valores predeterminados excepto la dirección IP, y la página web va a la página de inicio de sesión.

3.13 Cerrar sesión

Seleccionar  > **Salida**. La página web va a la página de inicio de sesión.

Apéndice 1 Recomendaciones de ciberseguridad

Acciones obligatorias a tomar para la seguridad básica de la red del dispositivo:

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres.
- Incluya al menos dos tipos de caracteres; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos.
- No contenga el nombre de la cuenta ni 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

- Según el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su dispositivo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema cuente con los parches y correcciones de seguridad más recientes. Cuando el dispositivo esté conectado a la red pública, se recomienda activar la función de "búsqueda automática de actualizaciones" para obtener información actualizada sobre las actualizaciones de firmware publicadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones "conviene tener" para mejorar la seguridad de la red de su dispositivo:

1. Protección física

Le sugerimos que proteja físicamente el dispositivo, especialmente los dispositivos de almacenamiento. Por ejemplo, colóquelo en una sala de computadoras y un armario especiales, e implemente un control de acceso y una gestión de claves rigurosos para evitar que personal no autorizado realice contactos físicos, como dañar el hardware o conectar dispositivos extraíbles (como memorias USB o puertos serie), etc.

2. Cambie las contraseñas periódicamente

Le sugerimos que cambie sus contraseñas periódicamente para reducir el riesgo de que sean adivinadas o descifradas.

3. Establecer y actualizar contraseñas Restablecer información oportunamente

El dispositivo admite la función de restablecimiento de contraseña. Configure la información necesaria para el restablecimiento de contraseña, incluyendo el buzón de correo del usuario final y las preguntas de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar preguntas de protección de contraseña, se recomienda no usar aquellas que sean fáciles de adivinar.

4. Habilitar bloqueo de cuenta

La función de bloqueo de cuenta está activada por defecto y recomendamos mantenerla 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 el puerto HTTP predeterminado y otros puertos de servicio

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

6. Habilitar HTTPS

Le sugerimos habilitar HTTPS, para que pueda visitar el servicio web a través de un canal de comunicación seguro.

7. Vinculación de direcciones MAC

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

8. Asignar cuentas y privilegios de manera razonable

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

9.Desactivar servicios innecesarios y elegir modos seguros

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

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

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

10.Transmisión cifrada de audio y vídeo

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

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

11.Auditoría segura

- **Comprobar usuarios en línea:** le sugerimos que compruebe periódicamente los usuarios en línea para ver si el dispositivo ha iniciado sesión sin autorización.
- **Comprobar el registro del dispositivo:** al ver los registros, puede conocer las direcciones IP que se utilizaron para iniciar sesión en sus dispositivos y sus operaciones clave.

12.Registro de red

Debido a la capacidad de almacenamiento limitada del dispositivo, el registro almacenado es limitado. Si necesita guardar el registro durante un periodo prolongado, se recomienda habilitar la función de registro de red para garantizar que los registros críticos se sincronicen con el servidor de registro de red para su seguimiento.

13.Construir un entorno de red seguro

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

- **Deshabilite la función de mapeo de puertos del enrutador** para evitar el acceso directo a los dispositivos de intranet desde la red externa.
- **La red debe particionarse y aislarse según las necesidades reales.** Si no existen requisitos de comunicación entre dos subredes, se recomienda utilizar VLAN, GAP de red y otras tecnologías para particionar la red y lograr el aislamiento.
- **Establecer el sistema de autenticación de acceso 802.1x** para reducir el riesgo de acceso no autorizado a redes privadas.
- **Habilite la función de filtrado de direcciones IP/MAC** para limitar el rango de hosts permitidos para acceder al dispositivo.