Controlador de acceso por reconocimiento facial

Manual de usuario

Prefacio

General

Este manual presenta las funciones y operaciones del Controlador de acceso con reconocimiento facial (en adelante, el "Controlador de acceso"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para consultarlo en el futuro.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Significado
	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
	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.
	Proporciona información adicional como complemento al texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	junio 2022

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otras personas, como su rostro, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones 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

- El manual es sólo para referencia. Pueden encontrarse ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas incurridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es sólo para referencia. Es posible que se encuentren ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y software están sujetos a cambios sin previo aviso por escrito. Actualizaciones de Producto

Podría dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Comuníquese con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.

- Pueden existir errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- 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 comerciales registradas y nombres de empresas que aparecen en este manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con 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 dar una explicación final.

Salvaguardias y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del controlador de acceso, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el Controlador de acceso y cumpla con las pautas al usarlo.

Requisito de transporte

Transporte, utilice y almacene el controlador de acceso en condiciones permitidas de humedad y temperatura.

Requisito de almacenamiento

Guarde el controlador de acceso en condiciones permitidas de humedad y temperatura.

requerimientos de instalación

- No conecte el adaptador de corriente al controlador de acceso mientras el adaptador esté encendido.
- Cumpla estrictamente con el código y las normas locales de seguridad eléctrica. Asegúrese de que el voltaje ambiental sea estable y cumpla con los requisitos de suministro de energía del controlador de acceso.
- No conecte el Controlador de acceso a dos o más tipos de fuentes de alimentación para evitar daños al Controlador de acceso.
- El uso inadecuado de la batería podría provocar un incendio o una explosión.

- El personal que trabaja en alturas debe tomar todas las medidas necesarias para garantizar la seguridad personal, incluido el uso de casco y cinturones de seguridad.
- No coloque el controlador de acceso en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el Access Controller alejado de la humedad, el polvo y el hollín.
- Instale el controlador de acceso en una superficie estable para evitar que se caiga.
- Instale el controlador de acceso 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 cumplan con las especificaciones de potencia nominal.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en el estándar IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de suministro de energía están sujetos a la etiqueta del Controlador de acceso.

- El Controlador de Acceso es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del controlador de acceso esté conectada a una toma de corriente con conexión a tierra protectora.

Requisitos de operación

- Compruebe si la fuente de alimentación es correcta antes de su uso.
- No desenchufe el cable de alimentación en el costado del controlador de acceso mientras el adaptador esté encendido.

en.

- Opere el controlador de acceso dentro del rango nominal de entrada y salida de energía.
- Utilice el controlador de acceso en las condiciones permitidas de humedad y temperatura.
- No deje caer ni salpique líquido sobre el Controlador de acceso y asegúrese de que no haya ningún objeto lleno de líquido sobre el Controlador de acceso para evitar que el líquido fluya hacia él.
- No desmonte el controlador de acceso sin instrucción profesional.
- Este producto es un equipo profesional.

Tabla de contenido

1.1 Introducción

El controlador de acceso es un panel de control de acceso que admite desbloqueo mediante rostros, contraseñas, huellas dactilares, tarjetas, código QR y sus combinaciones. Basado en el algoritmo de aprendizaje profundo, presenta un reconocimiento más rápido y una mayor precisión. Puede funcionar con una plataforma de gestión que satisfaga las diversas necesidades de los clientes.

1.2 Características

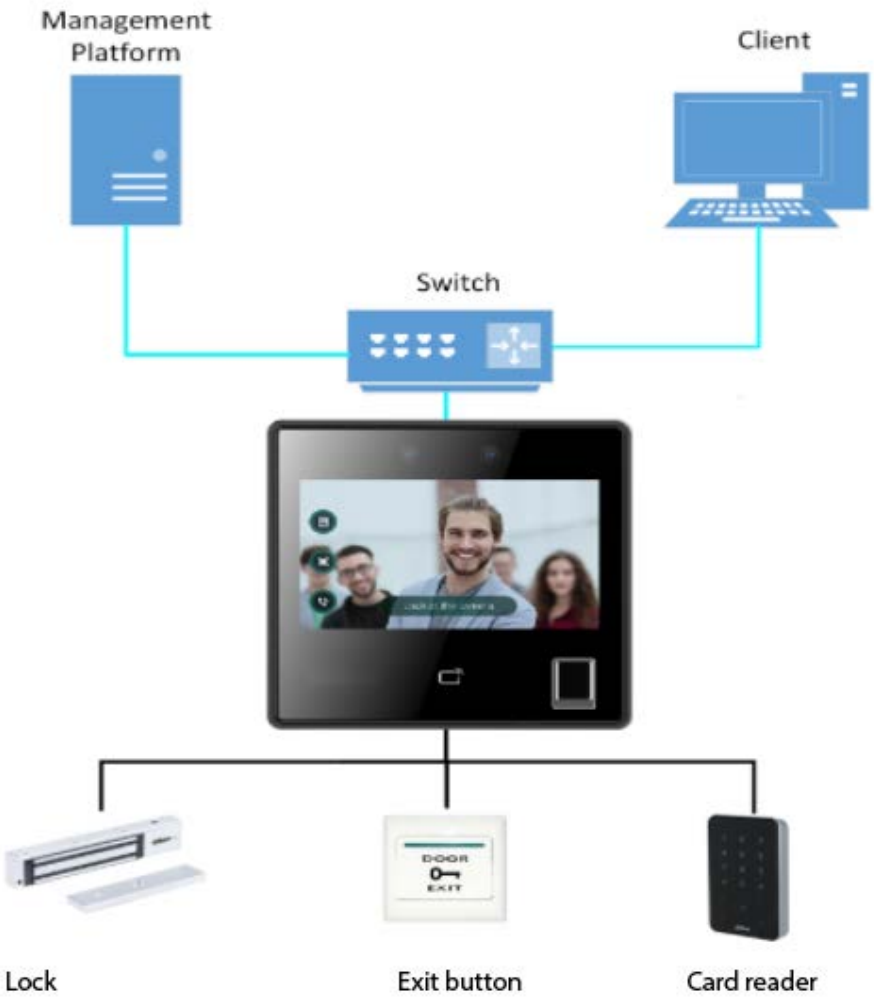
- La carcasa está construida con material PC y ABS, lo que la hace ideal para uso en interiores.
- Pantalla táctil de cristal de 4,3 pulgadas con una resolución de 480×272.
- Cámara de doble lente gran angular de 2 MP con iluminación IR y DWDR.
- Múltiples métodos de desbloqueo que incluyen huella digital, rostro, tarjeta IC y contraseña. También puedes combinarlos para crear tus propios métodos de desbloqueo personales.
- Admite detección de máscaras.
- Admite código QR de visitante con plataforma DSS Pro.
- Reconoce caras a una distancia de 0,3 ma 1,5 m (0,98 pies-4,92 pies) y detecta personas entre la altura de 1,1 m y 2,0 m (3,61 pies-6,56 pies) cuando la cámara está instalada a 1,4 m (4,5 pies).
- Admite 3.000 usuarios, 3.000 rostros, 3.000 contraseñas, 5.000 tarjetas, 5.000 huellas dactilares, 50 administradores y 300.000 registros.
- La detección de vida tiene una tasa de precisión de reconocimiento facial del 99,9 % y el tiempo de comparación 1:N es de 0,2 s por persona.
- Admite lector de tarjetas RS-485, lector de tarjetas Wiegand (26, 34, 66), botón de salida, detector de estado de puerta y un puerto Ethernet de 100 Mbps.
- Se pueden configurar hasta 128 períodos, junto con 128 planes de vacaciones, período normalmente abierto, períodos normalmente cerrado, períodos de desbloqueo remoto y períodos de desbloqueo del primer usuario.
- Ofrece múltiples tipos de alarmas, como coacción, manipulación, intrusión, tiempo de espera de desbloqueo y uso excesivo de tarjeta ilegal.
- Admite usuarios generales, usuarios de patrulla, usuarios de listas de bloqueo, usuarios VIP, usuarios invitados y otros usuarios
- Cuenta con anti-passback, múltiples métodos de verificación, desbloqueo remoto, desbloqueo del primer usuario y admite la visualización de videos en la plataforma.
- Para mejorar la seguridad y proteger contra la apertura forzada del dispositivo, se admite la expansión del módulo de seguridad.
- Conexión TCP/IP y Wi-Fi, registro automático, registro P2P y DHCP.
- Admite realizar videollamadas y usar la aplicación para recibir notificaciones de alarma, desbloquear puertas de forma remota y realizar otras tareas.
- Admite la personalización de indicaciones de voz.
- Actualización online y actualización a través de USB.
- Funciona sin conexión y se comunica con la plataforma de gestión cuando está conectado a una red.
- Admite vigilancia para proteger el sistema contra fallas de software y hardware.

- Soporta SDK.
- Se conecta a DSS Pro y SmartPSS Lite.

1.3 Aplicación

Se utiliza ampliamente en parques, comunidades, centros de negocios y fábricas, y es ideal para lugares como edificios de oficinas, edificios gubernamentales, escuelas y estadios.

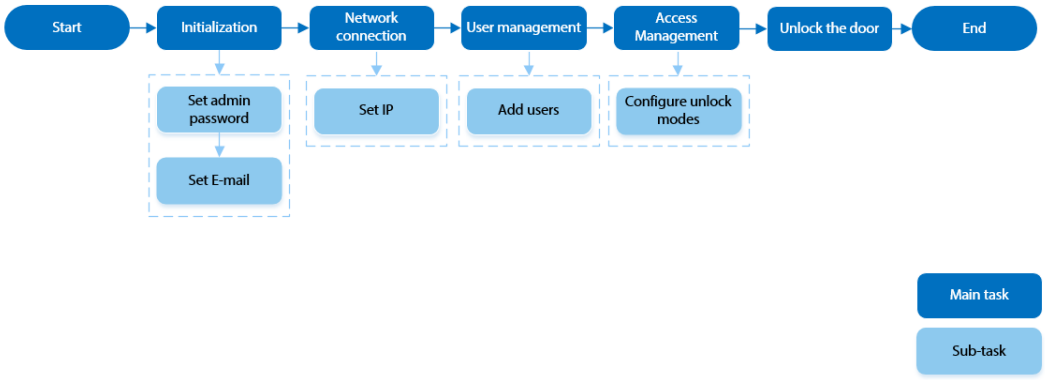
Figura 1-1 Redes



2 operaciones locales

2.1 Procedimiento de configuración básica

Figura 2-1 Procedimiento de configuración básica



2.2 Iconos comunes

Tabla 2-1 Descripción de iconos

Icono	Descripción
	Icono del menú principal.
	Icono de confirmación.
	Pase a la primera página de la lista.
	Pase a la última página de la lista.
o	Pase a la página anterior de la lista.
o	Pase a la siguiente página de la lista.
	Volver al menú anterior.
	Encendido.
	Apagado.
	Borrar
	Buscar

2.3 Pantalla de espera

Puede desbloquear la puerta mediante rostros, contraseñas y códigos QR. También puedes realizar llamadas a través de la función de intercomunicador.

- Si no se realiza ninguna operación en 30 segundos, el controlador de acceso pasará al modo de espera.
- Este manual es sólo para referencia. Es posible que se encuentren ligeras diferencias entre la pantalla de espera en este manual y en el dispositivo real.

Figura 2-2 Página de inicio

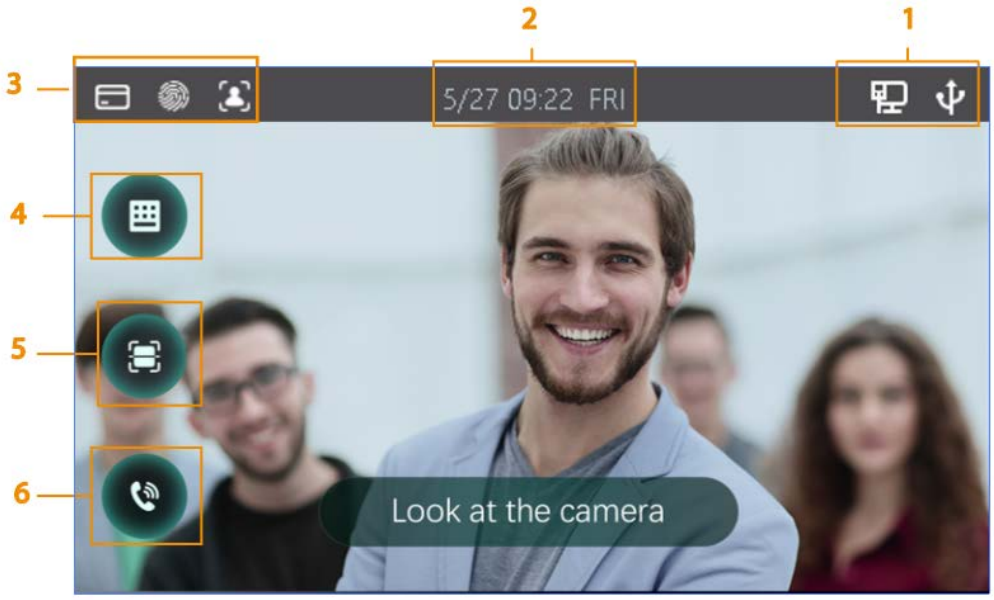


Tabla 2-2 Descripción de la pantalla de inicio

No.	Nombre	Descripción
1	Indicación de estado	Muestra el estado de Wi-Fi, red y USB, y más.
2	Fecha y hora	Muestra la fecha y hora actual.
3	Métodos de verificación	Muestra los métodos de verificación disponibles.
4	Contraseña	Ingrese la contraseña de usuario o la contraseña de administrador para desbloquear la puerta.
5	Código QR	Toque el ícono del código QR y escanee el código QR para desbloquear la puerta.
6	Intercomunicador	Cuando el controlador de acceso funciona como servidor, puede llamar al VTO y al VTH. Cuando el DSS funciona como servidor, el controlador de acceso puede llamar al VTO, VTS y DSS. Toque el ícono, ingrese el número de habitación para llamar al propietario de la casa.

2.4 Inicialización

Para el uso por primera vez o después de restaurar los valores predeterminados de fábrica, debe seleccionar un idioma en Access Controller y luego configurar la contraseña y la dirección de correo electrónico para la cuenta de administrador. Puede utilizar la cuenta de administrador para iniciar sesión en el menú principal del Access Controller y en la página web.

- Si olvida la contraseña de administrador, envíe una solicitud de restablecimiento a su dirección de correo electrónico registrada.
- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &).

2.5 Iniciar sesión

Inicie sesión en el menú principal para configurar el controlador de acceso. Solo la cuenta de administrador y la cuenta de administrador pueden ingresar al menú principal del controlador de acceso. Para el primer uso, use la cuenta de administrador para ingresar a la pantalla del menú principal y luego podrá crear las otras cuentas de administrador.

- Cuenta de administrador: puede iniciar sesión en la pantalla del menú principal del controlador de acceso, pero no tiene permiso de acceso a la puerta.
- Cuenta de administración: puede iniciar sesión en el menú principal del controlador de acceso y tiene permisos de acceso a la puerta.

Paso 1 Mantenga presionada la pantalla de espera durante 3 segundos. seleccione

Paso 2 un método de verificación para ingresar al menú principal.

- Rostro: Ingrese al menú principal mediante reconocimiento facial.
- Huella digital: ingrese al menú principal usando la huella digital.

  La función de huella digital solo está disponible para el modelo de huella digital de Access Controller.
- Card Punch: ingrese al menú principal deslizando la tarjeta.

  La función Card Punch solo está disponible para el modelo de tarjeta deslizante de Access Controller.
- PWD: Ingrese el ID de usuario y la contraseña de la cuenta de administrador.
- admin: Ingrese la contraseña de administrador para ingresar al menú principal.

2.6 Comunicación de red

Configure la red, el puerto serie y el puerto Wiegand para conectar el controlador de acceso a la red.

El puerto serie y el puerto wiegand pueden diferir según los modelos de Access Controller.

2.6.1 Configuración de IP

Configure la dirección IP del controlador de acceso para conectarlo a la red. Después de eso, puede iniciar sesión en la página web y en la plataforma de administración para administrar el Controlador de acceso.

Paso 1 Sobre el**Menú principal**, seleccionar**Conexión**>**Red**>**Dirección IP**.

Paso 2 Configurar la dirección IP.

Figura 2-3 Configuración de la dirección IP

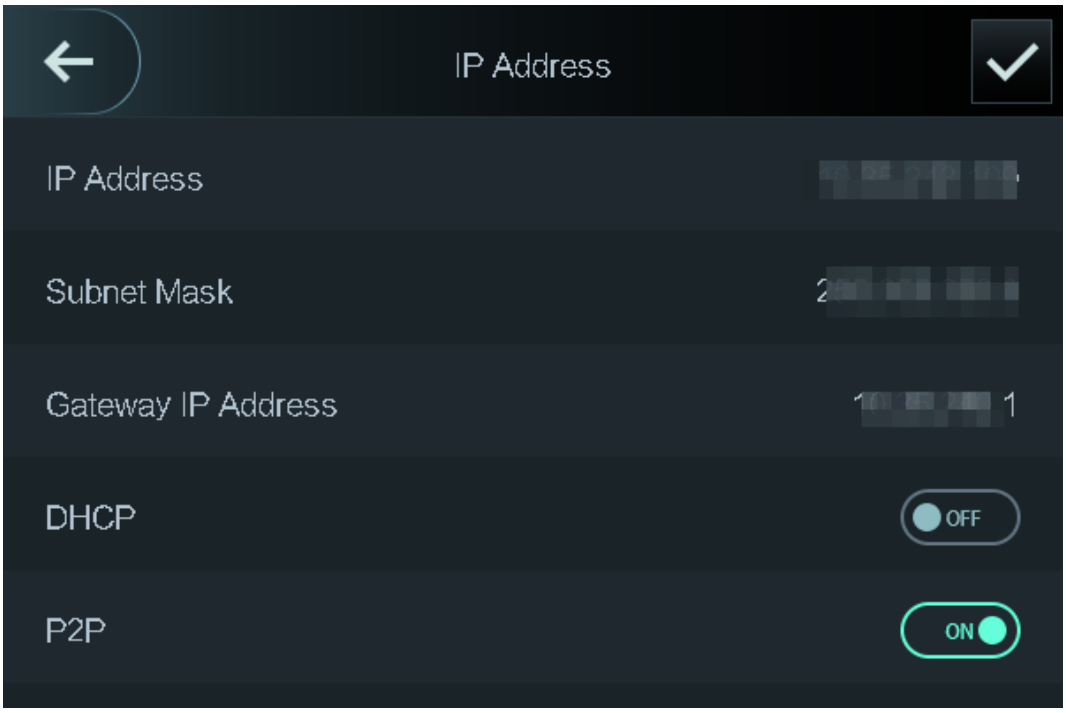


Tabla 2-3 Parámetros de configuración IP

Parámetro	Descripción
Dirección IP/Máscara de subred/Dirección de puerta de enlace	La dirección IP, la máscara de subred y la dirección IP de la puerta de enlace deben estar en el mismo segmento de red.
DHCP	Significa Protocolo de configuración dinámica de host. Cuando DHCP está activado, al controlador de acceso se le asignará automáticamente la dirección IP, la máscara de subred y la puerta de enlace.
P2P	La tecnología P2P (peer-to-peer) permite a los usuarios administrar dispositivos sin solicitar DDNS, configurar el mapeo de puertos o implementar un servidor de tránsito.

2.6.2 Registro activo

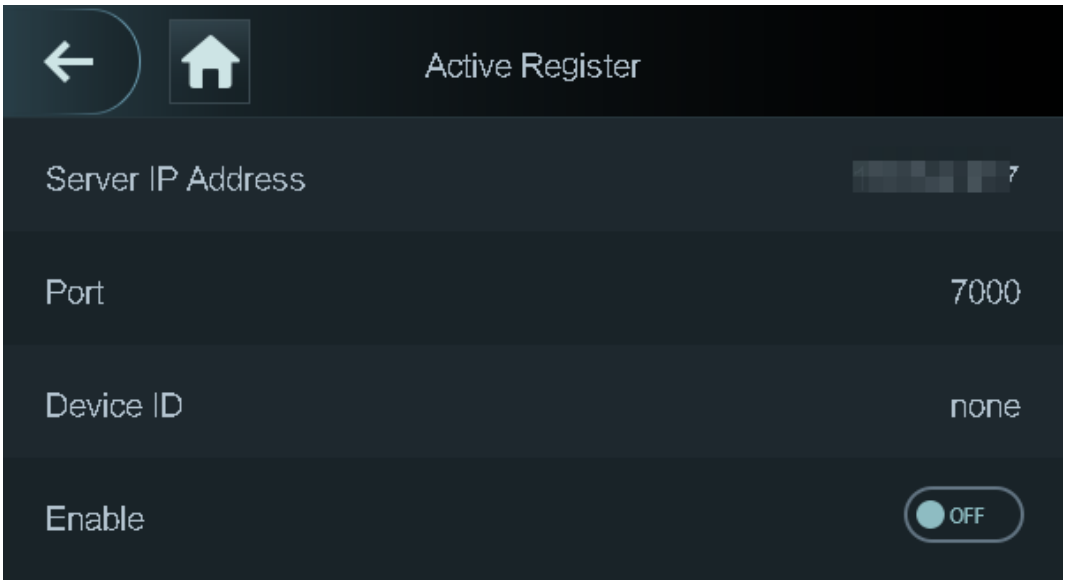
Puede activar la función de registro automático para acceder al Controlador de acceso a través de la plataforma de gestión.

La plataforma de gestión puede borrar todas las configuraciones del personal e inicializar el controlador de acceso.

Para evitar la pérdida de datos, mantenga correctamente los permisos de la plataforma de gestión.

Paso 1 Sobre el**Menú principal**, seleccionar**Conexión**>**Red**>**Registro activo**.

Figura 2-4 Registro automático



Paso 2 Active la función de registro automático y configure los parámetros.

Tabla 2-4 Registro automático

Parámetro	Descripción
Dirección del servidor	La dirección IP de la plataforma de gestión.
Puerto	El número de puerto de la plataforma de gestión.
ID del dispositivo	Ingrese la ID del dispositivo (definida por el usuario). Cuando agrega el controlador de acceso a la administración plataforma, el ID del dispositivo en la plataforma de gestión debe conforme al ID del dispositivo definido en el controlador de acceso.

Paso 3 Habilite la función de registro activo.

2.6.3 Configuración de Wi-Fi

Puede conectar el Access Controller a la red a través de una red Wi-Fi.

La función Wi-Fi solo está disponible para ciertos modelos de Access Controller.

Paso 1 Sobre el**Menú principal**, seleccionar**Conexión**>**Red**>**Wifi**.

Paso 2 Enciende el wifi.

Paso 3 Toque para buscar redes inalámbricas disponibles.

Etapa 4 Seleccione una red inalámbrica e ingrese la contraseña.

Si no se busca ninguna red Wi-Fi, toque**SSID**para ingresar el nombre de Wi-Fi.

Paso 5 Grifo .

2.6.4 Configurar el puerto serie

Paso 1 Sobre el**Menú principal**, seleccionar**Conexión**>**Puerto serial**.

Paso 2 Seleccione un tipo de puerto.

- Seleccionar**Lector**cuando el controlador de acceso se conecta a un lector de tarjetas.
- Seleccionar**Controlador**cuando el Controlador de acceso funciona como un lector de tarjetas, y el Controlador de acceso enviará datos al Controlador de acceso para controlar el acceso.

  Tipo de datos de salida:

  ◇ Tarjeta: genera datos basados en el número de tarjeta cuando los usuarios deslizan la tarjeta para desbloquear la puerta; genera datos basados en el primer número de tarjeta del usuario cuando utiliza otros métodos de desbloqueo.

  ◇ No.: genera datos basados en la identificación del usuario.
- Seleccionar**Lector (OSDP)**cuando el controlador de acceso está conectado a un lector de tarjetas basado en el protocolo OSDP.
- Módulo de seguridad: cuando se conecta un módulo de seguridad, el botón de salida y el bloqueo no serán efectivos.

2.6.5 Configuración de Wiegand

El controlador de acceso permite el modo de entrada y salida Wiegand. Paso

1 Sobre el**Menú principal**, seleccionar**Conexión**>**Wiegand**.

Paso 2 Seleccione un Wiegand.

- Seleccionar**Entrada Wiegand**cuando conecta un lector de tarjetas externo al controlador de acceso.
- Seleccionar**Salida Wiegand**cuando el Controlador de Acceso funciona como un lector de tarjetas y necesita conectarlo a un controlador u otro terminal de acceso.

Figura 2-5 Salida Wiegand

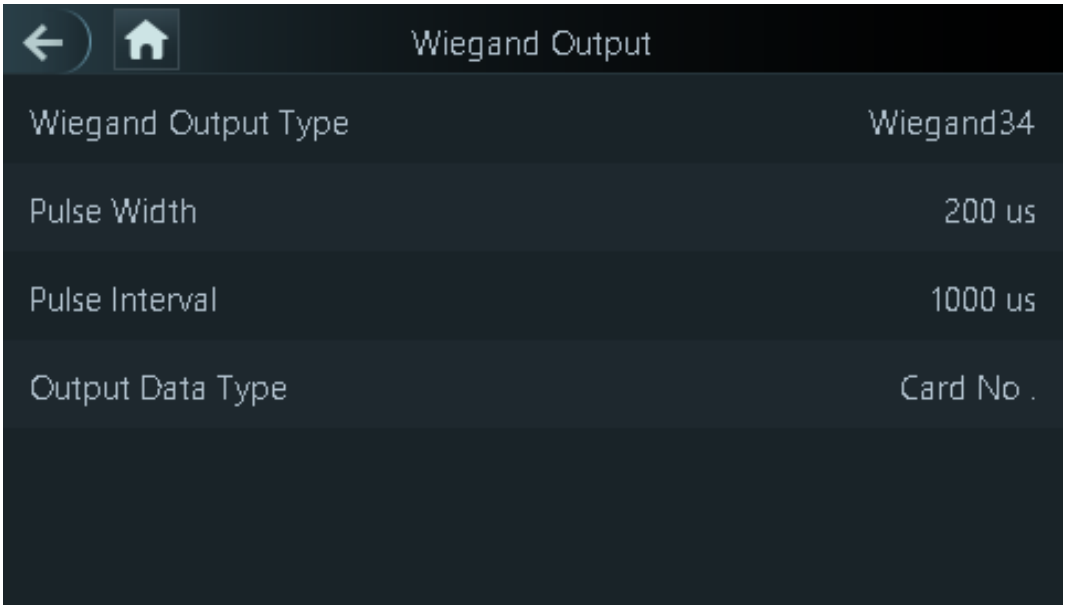


Tabla 2-5 Descripción de la salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	Seleccione un formato Wiegand para leer números de tarjetas o números de identificación. ● **Wiegand26**: Lee tres bytes o seis dígitos. ● **Wiegand34**: Lee cuatro bytes u ocho dígitos. ● **Wiegand66**: Lee ocho bytes o dieciséis dígitos.
Ancho de pulso	Ingrese el ancho del pulso y el intervalo de pulso de la salida Wiegand.

Parámetro	Descripción
Intervalo de pulso	
Tipo de datos de salida	Seleccione el tipo de datos de salida. ● **ID de usuario**: genera datos basados en el ID de usuario. ● **Número de tarjeta**: Genera datos basados en el primer número de tarjeta del usuario y el formato de datos es hexadecimal o decimal.

2.7 Gestión de usuarios

Puede agregar nuevos usuarios, ver la lista de usuarios/administradores y editar la información del usuario.

Las imágenes de este manual son solo de referencia y pueden diferir del producto real.

2.7.1 Agregar nuevos usuarios

Paso 1 Sobre el**Menú principal**, seleccionar**Usuario**>**Nuevo**

Paso 2 **Usuario**. Configure los parámetros en la interfaz.

Figura 2-6 Nuevo usuario (1)

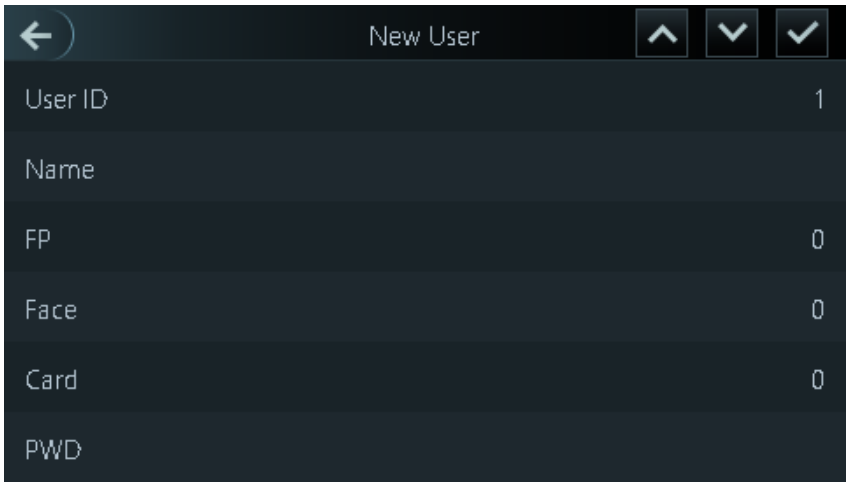


Figura 2-7 Nuevo usuario (2)

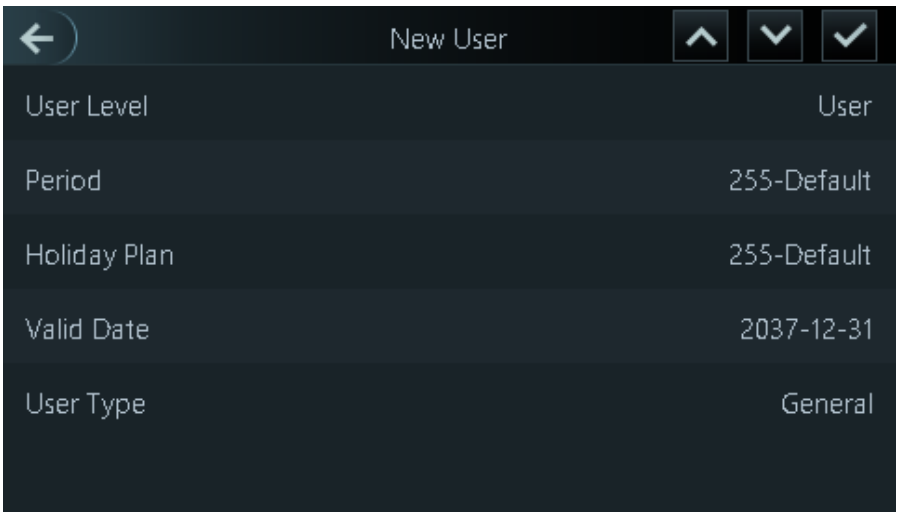


Tabla 2-6 Descripción de nuevos parámetros de usuario

Parámetro	Descripción
ID de usuario	Introduzca los ID de usuario. Los ID pueden ser números, letras y sus combinaciones, y la longitud máxima del ID es de 32 caracteres. Cada identificación es única.
Nombre	Ingrese el nombre con un máximo de 32 caracteres (incluidos números, símbolos y letras).
FP	Registrar huellas dactilares. Un usuario puede registrar hasta 3 huellas digitales y usted puede configurar una huella digital para la huella digital de coacción. Se activará una alarma cuando se utilice la huella digital de coacción para desbloquear la puerta. Sólo ciertos modelos admiten el desbloqueo por huella digital.
Rostro	Asegúrese de que su rostro esté centrado en el marco de captura de imágenes, y se capturará y analizará automáticamente una imagen del rostro.
Tarjeta	Un usuario puede registrar cinco tarjetas como máximo. Ingrese su número de tarjeta o pase su tarjeta y luego el controlador de acceso leerá la información de la tarjeta. Puedes habilitar el**Tarjeta de coacción**función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta. Sólo ciertos modelos admiten el desbloqueo de tarjetas.
PCD	Ingrese la contraseña de usuario. La longitud máxima de la contraseña es de 8 dígitos.
Nivel de usuario	Puede seleccionar un nivel de usuario para nuevos usuarios. ● **Usuario**: Los usuarios solo tienen permiso de acceso a la puerta. ● **Administración**: Los administradores pueden desbloquear la puerta y configurar el controlador de acceso.
Período	Las personas pueden desbloquear la puerta sólo durante el período definido.
Plan de vacaciones	Las personas pueden desbloquear la puerta sólo durante el plan de vacaciones definido.
Fecha válida	Establezca una fecha en la que expirarán los permisos de acceso de la persona.
Tipo de usuario	● **General**: Los usuarios generales pueden desbloquear la puerta. ● **Lista de bloqueos**: Cuando los usuarios en la lista de bloqueo desbloquean la puerta, el personal de servicio recibirá una notificación. ● **Invitado**: Los huéspedes pueden desbloquear la puerta dentro de un período definido o durante una determinada cantidad de veces. Una vez transcurrido el período definido o los tiempos de desbloqueo, no pueden desbloquear la puerta. ● **Patrulla**: Se realizará un seguimiento de la asistencia de los usuarios de Patrol, pero no tendrán permisos de desbloqueo. ● **VIP**: Cuando VIP abra la puerta, el personal de servicio recibirá un aviso. ● **Otros**: Cuando desbloqueen la puerta, la puerta permanecerá desbloqueada durante 5 segundos más. ● Usuario personalizado 1/Usuario personalizado 2: Lo mismo con los usuarios generales.

Paso 3 Grifo .

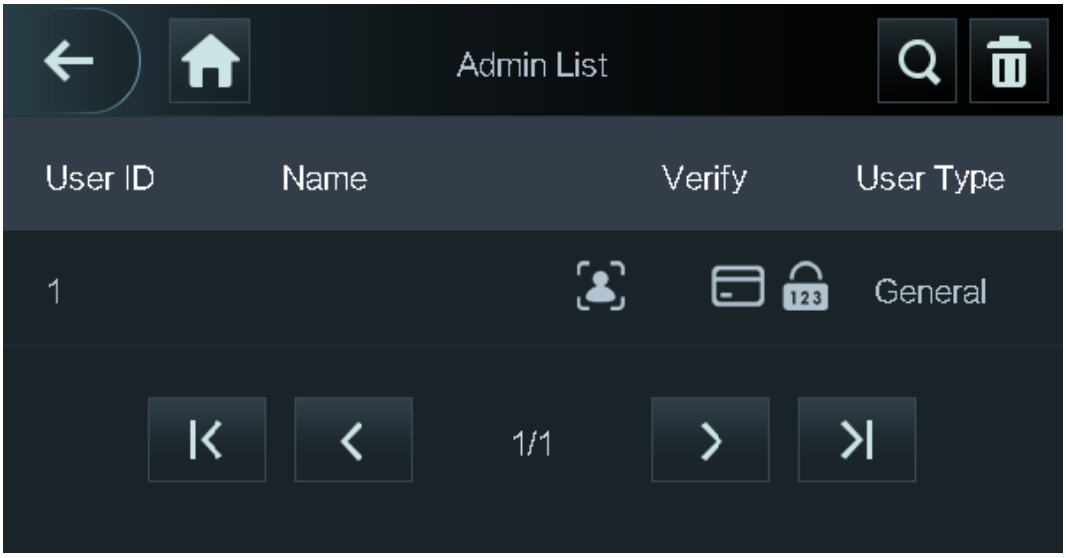
2.7.2 Ver información del usuario

Puede ver la lista de usuarios/administradores y editar la información del usuario.

Paso 1 Sobre el**Menú principal**, seleccionar**Usuario**>**Lista de usuarios**, o seleccione**Usuario**>**Lista de administradores**. Ver

Paso 2 todos los usuarios y cuentas de administrador agregados.

Figura 2-8 Lista de administradores



- : Desbloquear mediante contraseña.
- : Desbloqueo mediante tarjeta magnética.
- : Desbloqueo mediante reconocimiento facial.
- : Desbloqueo mediante huella digital.

Operaciones relacionadas

Sobre el**Usuario**pantalla, puede administrar los usuarios agregados.

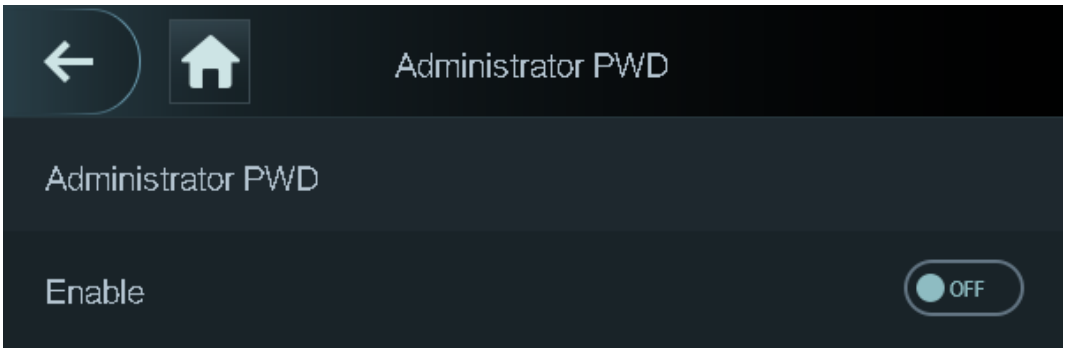
- Buscar usuarios: toque y luego ingrese el nombre de usuario.
- Editar usuarios: toque el usuario para editar la información del usuario.
- Eliminar usuarios
  - ◇ Eliminar individualmente: seleccione un usuario y luego toque .
  - ◇ Eliminar en lotes:
    - ○ Sobre el**Lista de usuarios**pantalla, toque para eliminar a todos los usuarios.
    - ○ Sobre el**Lista de administradores**pantalla, toque para eliminar todos los usuarios administradores.

2.7.3 Configurar la contraseña del administrador

Puede desbloquear la puerta ingresando únicamente la contraseña de administrador. La contraseña de administrador no está limitada por tipos de usuarios. Solo se permite una contraseña de administrador para un dispositivo.

Paso 1 Sobre el**Menú principal**pantalla, seleccione**Usuario**>**Administrador PCD**.

Figura 2-9 Establecer contraseña de administrador



Paso 2 Grifo**Administrador PCD**y luego ingrese la contraseña de administrador.

Paso 3 Grifo ☑

Etapa 4 Active la función de administrador.

2.8 Gestión de acceso

Puede configurar los parámetros de acceso a la puerta, como modos de desbloqueo, vinculación de alarmas y horarios de puertas.

2.8.1 Configurar combinaciones de desbloqueo

Utilice tarjeta, huella digital, rostro o contraseña o sus combinaciones para desbloquear la puerta.

Los modos de desbloqueo pueden diferir según el producto real.

Paso 1 Seleccionar**Acceso**>**Modo de desbloqueo**>**Modo de desbloqueo**.

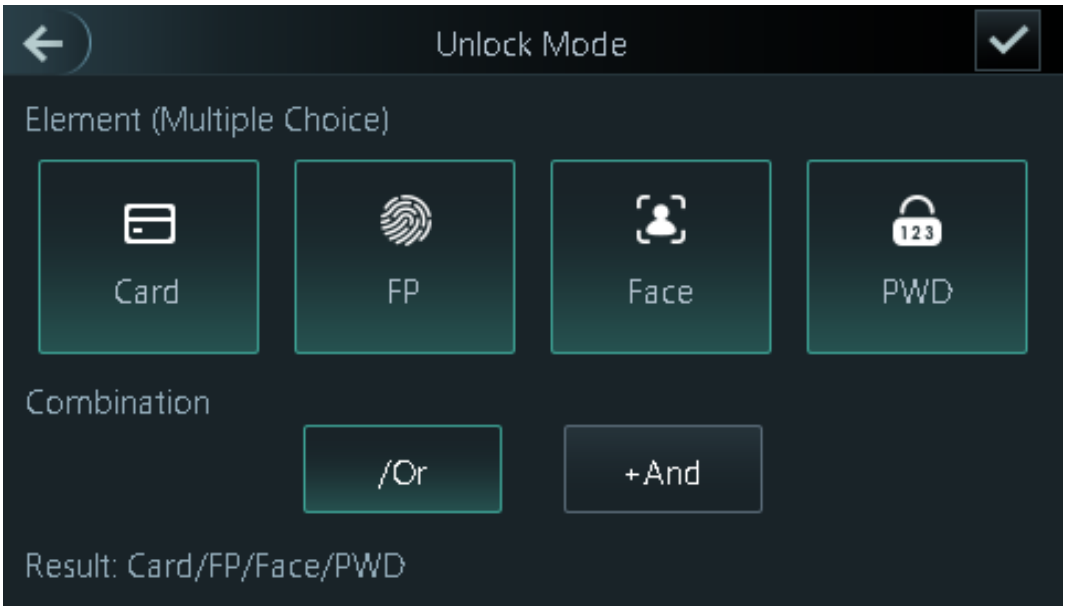
Paso 2 Seleccione métodos de desbloqueo.

Para cancelar su selección, toque el método seleccionado nuevamente.

Paso 3 Toca +**Y**o**/O**para configurar combinaciones.

- **+Y**: Verifique todos los métodos de desbloqueo seleccionados para abrir la puerta.
- **/O**: Verifique uno de los métodos de desbloqueo seleccionados para abrir la puerta.

Figura 2-10 Elemento (opción múltiple)



Etapa 4 Grifo para guardar los cambios.

2.8.2 Configuración de alarma

Se activará una alarma cuando se produzcan eventos de acceso anormales.

Paso 1 Seleccionar**Acceso**>**Alarma**.

Paso 2 Habilite el tipo de alarma.

Figura 2-11 Alarma

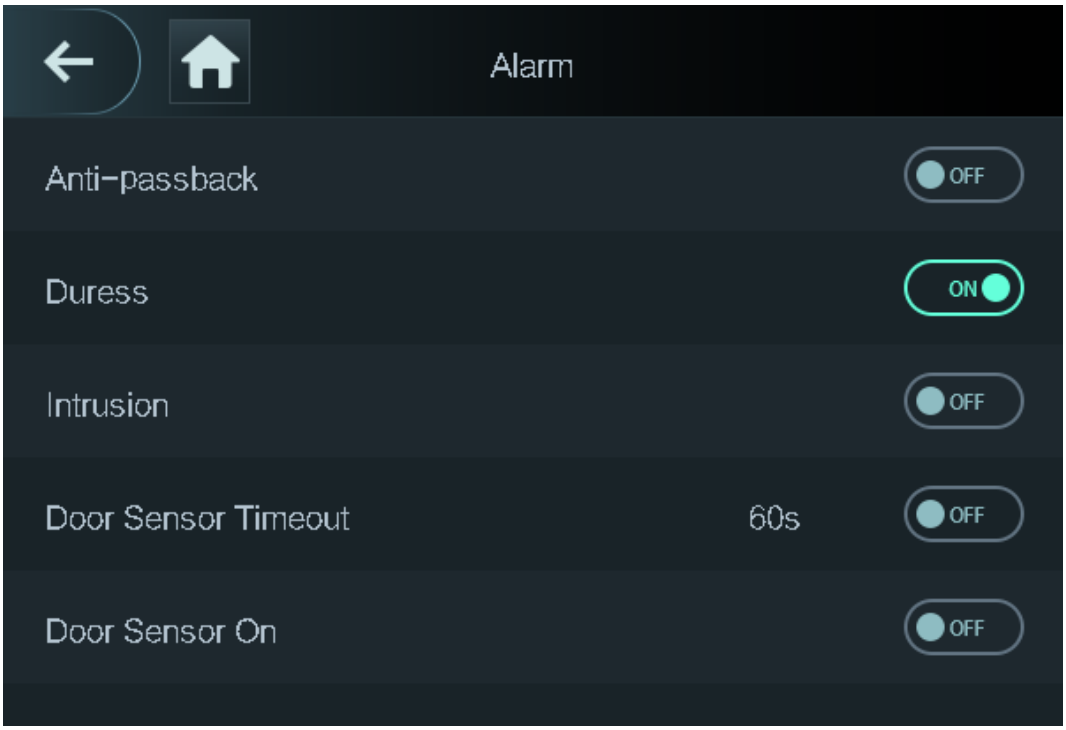


Tabla 2-7 Descripción de los parámetros de alarma

Parámetro	Descripción
Anti-passback	Los usuarios deben verificar sus identidades tanto para entrar como para salir; de lo contrario se activará una alarma. Ayuda a evitar que el titular de una tarjeta le pase una tarjeta de acceso a otra persona para que pueda entrar. Cuando el antipassback está habilitado, el titular de la tarjeta debe abandonar el área segura a través de un lector de salida antes de que el sistema le permita otra entrada. ● Si una persona entra sin autorización y sale sin autorización, se activará una alarma cuando intente volver a entrar y al mismo tiempo se le negará el acceso. ● Si una persona entra sin autorización y sale sin autorización, se activará una alarma cuando intente volver a entrar y al mismo tiempo se le negará el acceso.
Coacción	Se activará una alarma cuando se utilice una tarjeta de coacción, una contraseña de coacción o una huella digital de coacción para desbloquear la puerta.
Intrusión	Cuando el sensor de puerta está habilitado, se activará una alarma de intrusión si la puerta se abre de manera anormal.
Tiempo de espera del sensor de puerta	Se activará una alarma de tiempo de espera si la puerta permanece desbloqueada por más tiempo que el tiempo de espera definido del sensor de puerta, que varía de 1 a 9999 segundos.
Sensor de puerta encendido	Las alarmas de intrusión y tiempo de espera solo se pueden activar después de que se habilita el sensor de puerta.

2.8.3 Configurar el estado de la puerta

Paso 1 Sobre el**Menú principal**pantalla, seleccione**Acceso**>**Estado de la puerta**. Establecer el

Paso 2 estado de la puerta.

- **NO**: La puerta permanece desbloqueada todo el tiempo.
- **CAROLINA DEL NORTE**: La puerta permanece cerrada todo el tiempo.
- **Normal**: Si**Normal**Si selecciona , la puerta se desbloqueará y bloqueará según su configuración.

2.8.4 Configuración del tiempo de retención de bloqueo

Después de que se le conceda acceso a una persona, la puerta permanecerá desbloqueada durante un tiempo definido para que pueda pasar.

Paso 1 Sobre el**Menú principal**, seleccionar**Acceso**>**Tiempo de retención de bloqueo.**

Paso 2 Ingrese la duración del desbloqueo. Toque para guardar los cambios.

Paso 3 ☑

2.9 Gestión de asistencia

Puede activar la función de control de asistencia y los empleados pueden hacer un seguimiento de su asistencia mediante

el controlador de acceso al mismo tiempo que desbloquean la puerta.

Requisitos previos

En la pantalla del menú principal, toque**Asistencia**y luego active la función de tiempo y asistencia.

Procedimiento

Paso 1 En la pantalla del menú principal, seleccione**Asistencia**>**Configuración de modo**.

Figura 2-12 Modo de asistencia

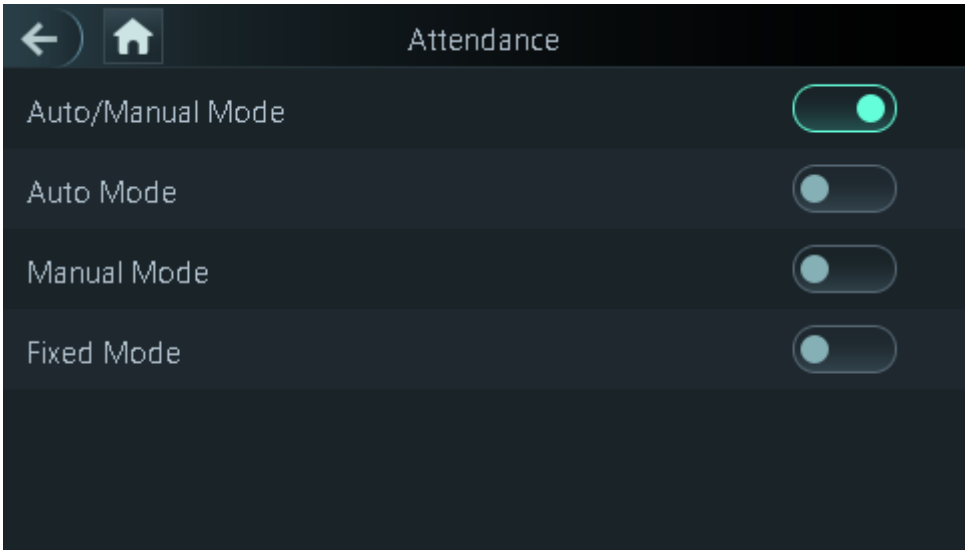


Tabla 2-8 Modo de asistencia

Parámetro	Descripción
Modo automático/manual	Después de marcar la entrada/salida, puede seleccionar manualmente el estado de asistencia o la pantalla muestra el estado del tiempo de asistencia automáticamente.
Modo automático	La pantalla muestra el estado de asistencia automáticamente después de marcar la entrada/salida.
Modo manual	Pinche/despinche y luego toque**Estado de asistencia**para seleccionar varonilmente el estado de asistencia.
Modo fijo	Cuando usted marca su entrada/salida, la pantalla mostrará el estado de asistencia preconfigurado todo el tiempo.

Paso 2 Seleccione un modo de asistencia.

Paso 3 Configure los parámetros para el modo de asistencia.

Figura 2-13 Modo automático/modo manual

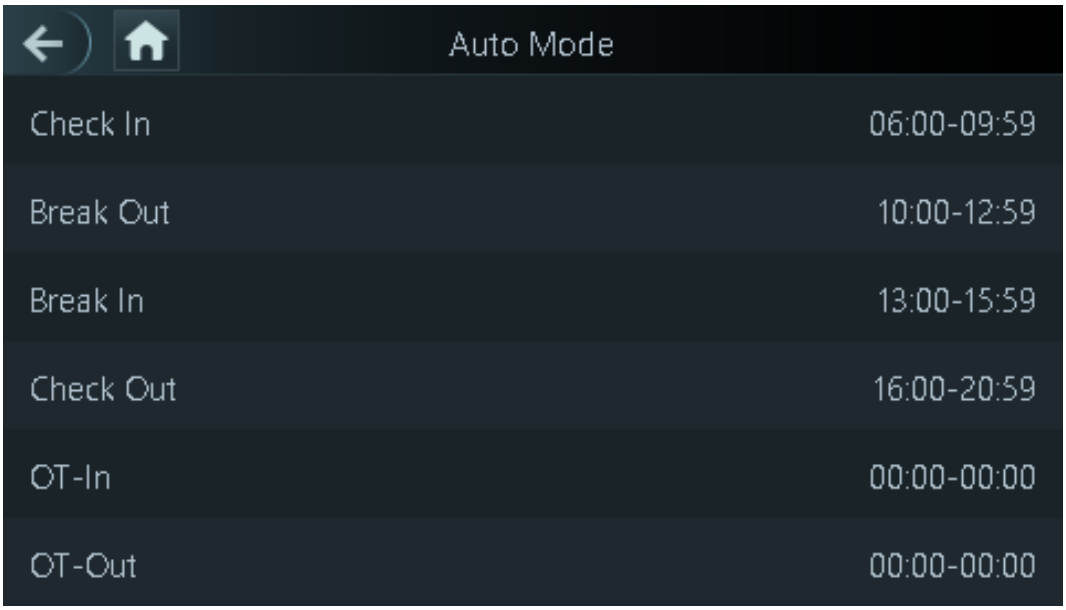


Figura 2-14 Modo fijo

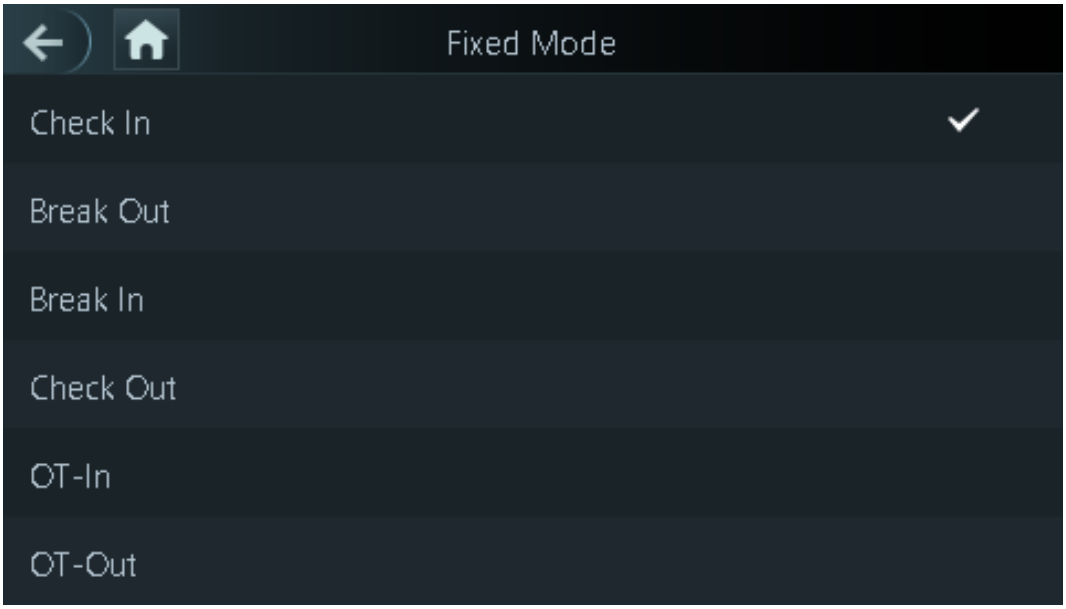


Tabla 2-9 Parámetros del modo de asistencia

Parámetros	Descripción
Registrarse	Marque cuando comience su jornada laboral normal.
Fugarse	Finaliza cuando termine tu excedencia.
Interrumpir	Marque cuando comience su licencia.
Verificar	Termine cuando comience su jornada laboral normal.
Entrada OT	Marque cuando comiencen sus horas extras de trabajo.
OT-fuera	Marque cuando finalicen sus horas extras de trabajo.

2.10 Sistema

2.10.1 Configurar la hora

Configure la hora del sistema, como fecha, hora y NTP.

Paso 1 Sobre el**Menú principal**, seleccionar**Sistema**>**Tiempo**.

Paso 2 Configurar la hora del sistema.

Figura 2-15 Hora

Tabla 2-10 Descripción de los parámetros de tiempo

Parámetro	Descripción
Sistema de 24 horas	La hora se muestra en formato de 24 horas.
Configuración de fecha	Configura la fecha.
Tiempo	Configura la hora.
Formato de fecha	Seleccione un formato de fecha.
Configuración de horario de verano	1. Toque**Configuración de horario de verano** 2. Habilite el horario de verano. 3. Seleccione**Fecha**o**Semana**desde el**horario de verano**Lista de tipos. 4. Ingrese la hora de inicio y la hora de finalización. 5. toque

Parámetro	Descripción
Comprobación NTP	Un servidor de protocolo de hora de red (NTP) es una máquina dedicada como servidor de sincronización de hora para todas las computadoras cliente. Si su computadora está configurada para sincronizarse con un servidor horario en la red, su reloj mostrará la misma hora que el servidor. Cuando el administrador cambia la hora (para el horario de verano), todas las máquinas cliente en la red también se actualizarán. 1. Toque**Comprobación NTP**. 2. Active la función de verificación NTP y configure los parámetros. ● **Dirección IP del servidor**: Introduzca la dirección IP del servidor NTP y el controlador de acceso sincronizará automáticamente la hora con el servidor NTP. ● **Puerto**: Introduzca el puerto del servidor NTP. ● **Intervalo (min)**: Introduzca el intervalo de sincronización horaria.
Zona horaria	Seleccione la zona horaria.

2.10.2 Configuración de parámetros de cara

Paso 1 En el menú principal, seleccione**Sistema**>**Parámetro de cara**.

Paso 2 Configure los parámetros de la cara y luego toque .

Figura 2-16 Parámetro de cara (01)

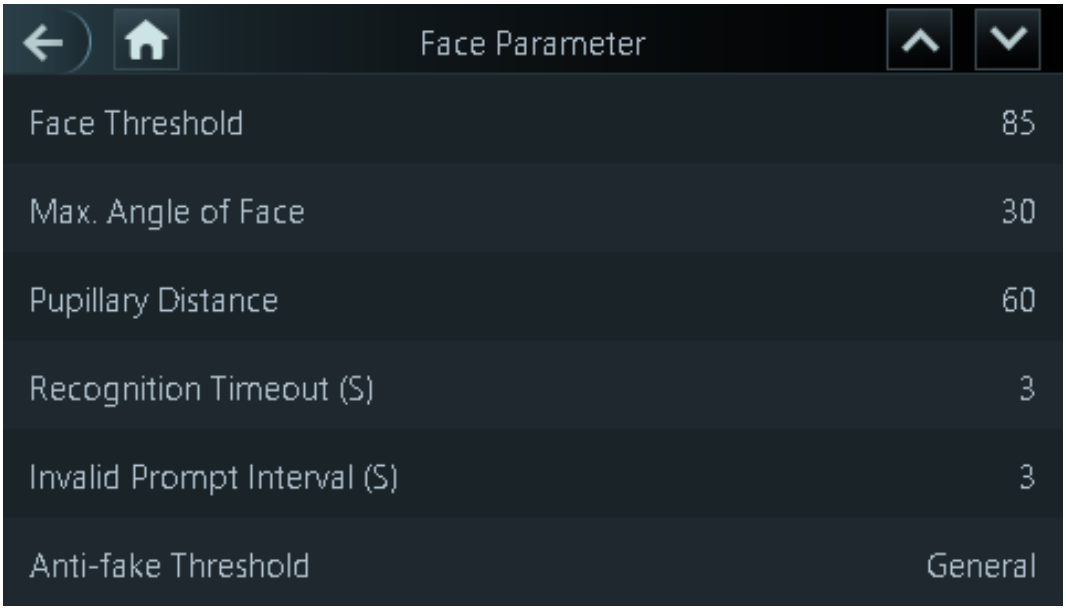


Figura 2-17 Parámetro de cara (02)

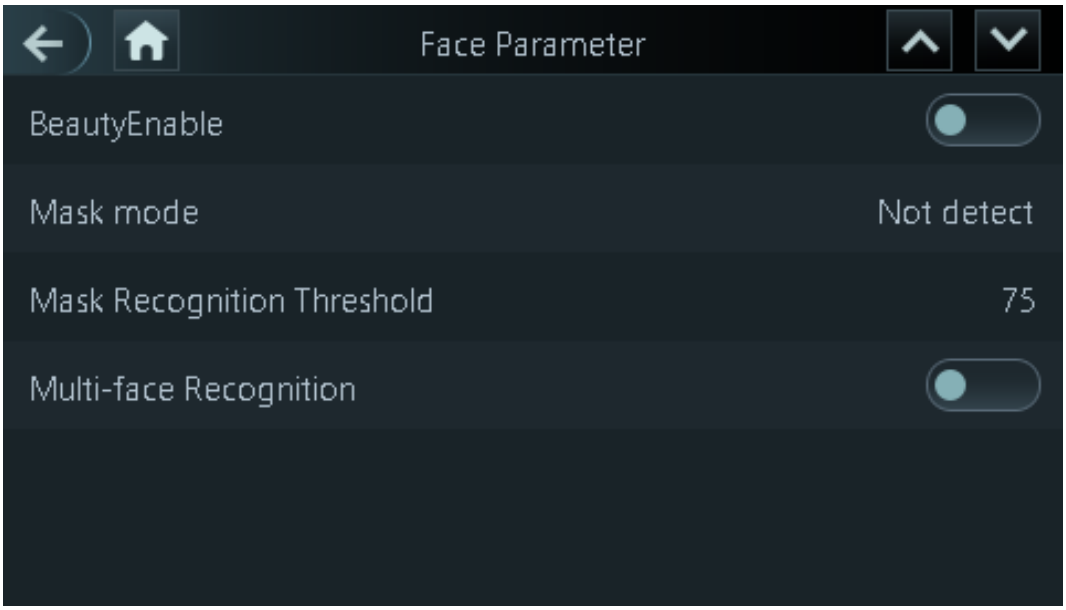


Tabla 2-11 Descripción de los parámetros de la cara

Nombre	Descripción
Umbral facial	Ajuste la precisión del reconocimiento facial. Un umbral más alto significa una mayor precisión.
Máx. Ángulo de la cara	Establezca el ángulo máximo de pose del rostro para la detección de rostros. Un valor mayor significa un rango de ángulo de cara mayor. Si el ángulo de pose de la cara está fuera del rango definido, el cuadro de detección de caras no aparecerá.
Distancia pupilar	Las imágenes de rostros requieren los píxeles deseados entre los ojos (llamado distancia pupilar) para un reconocimiento exitoso. El píxel predeterminado es 45. El píxel cambia según el tamaño de la cara y la distancia entre las caras y la lente. Si un adulto está a 1,5 metros de la lente, la distancia pupilar puede ser de 50 px a 70 px.
Tiempo de espera de reconocimiento (S)	Si se reconoce correctamente el rostro de una persona con permiso de acceso, el controlador de acceso le indicará que el reconocimiento facial se realizó correctamente. Puede ingresar el tiempo del intervalo de solicitud.
Mensaje de cara no válida Intervalo (s)	Si una persona sin permiso de acceso intenta desbloquear la puerta varias veces en el intervalo definido, el controlador de acceso indicará un fallo en el reconocimiento facial. Puede ingresar el tiempo del intervalo de solicitud.
Umbral antifalsificación	Evite el reconocimiento facial falso mediante el uso de una foto, video, máscara o un sustituto diferente del rostro de una persona autorizada. ● Cerrar: Desactiva esta función. ● General: un nivel normal de detección anti-spoofing significa una mayor tasa de acceso a las puertas para personas con máscaras faciales. ● Alto: Un nivel más alto de detección anti-spoofing significa mayor precisión y seguridad. ● Extremadamente alto: un nivel extremadamente alto de detección anti-suplantación de identidad significa una precisión y seguridad extremadamente altas.
BellezaHabilitar	Embellece las imágenes de rostros capturados.

Nombre	Descripción
Parámetros de máscara	● Modo máscara: ◇ **No detectar**: La máscara no se detecta durante el reconocimiento facial. ◇ **Recordatorio de mascarilla**: La máscara se detecta durante el reconocimiento facial. Si la persona no lleva mascarilla, el sistema le recordará que la use y se le permitirá el acceso. ◇ **Intercepción de máscara**: La máscara se detecta durante el reconocimiento facial. Si una persona no lleva mascarilla, el sistema le recordará que la use y se le negará el acceso. ● Umbral de reconocimiento de máscara: un umbral más alto significa una mayor precisión de detección de máscara.
Reconocimiento multicara	Admite la detección de 4 imágenes de rostros al mismo tiempo y el modo de combinaciones de desbloqueo deja de ser válido. La puerta se desbloquea después de que cualquiera de ellos obtenga acceso.

2.10.3 Configuración del volumen

Puede ajustar el volumen del altavoz y del micrófono.

Paso 1 Sobre el**Menú principal**, seleccionar**Sistema**>**Volumen**. Seleccionar

Paso 2 **Volumen del pitido**o**Volumen del micrófono**y luego toque + o − para ajustar el volumen.

2.10.4 (Opcional) Configuración de parámetros de huellas digitales

Configure la precisión de la detección de huellas dactilares. Un valor más alto significa un umbral más alto de similitud y una mayor precisión.

Esta función solo está disponible en Access Controller que admite desbloqueo de huellas digitales.

Paso 1 Sobre el**Menú principal**, seleccionar**Sistema**>

Paso 2 **Parámetro FP**Toque + o − para ajustar el valor.

2.10.5 Configuración de pantalla

Configure el tiempo de apagado de la pantalla y el tiempo de cierre de sesión.

Paso 1 Sobre el**Menú principal**, seleccionar**Sistema**>**Ajustes de pantalla**. Grifo**Hora**

Paso 2 **de cerrar sesión**o**Tiempo de espera de pantalla apagada**y luego toque + o − para ajustar la hora.

2.10.6 Restauración de los valores predeterminados de fábrica

Paso 1 Sobre el**Menú principal**, seleccionar**Sistema**>**Restaurar fábrica**. Restaure los

Paso 2 valores predeterminados de fábrica si es necesario.

- **Restaurar fábrica**: Restablece todas las configuraciones y datos.
- **Restaurar fábrica (guardar usuario y registro)**: Restablece las configuraciones excepto la información del usuario.

y troncos.

2.10.7 Reiniciar el dispositivo

Sobre el**Menú principal**, seleccionar**Sistema**>**Reiniciar**y se reiniciará el controlador de acceso.

2.10.8 Configurar el idioma

Cambie el idioma en el controlador de acceso.

Sobre el**Menú principal**, seleccionar**Sistema**>**Idioma**, seleccione el idioma del controlador de acceso.

2.11 Gestión de USB

Puede utilizar un USB para actualizar el controlador de acceso y exportar o importar información del usuario a través de USB.

- Asegúrese de que haya un USB insertado en el controlador de acceso antes de exportar datos o actualizar el sistema. Para evitar fallas, no extraiga el USB ni realice ninguna operación del Access Controlador durante el proceso.
- Tienes que usar un USB para exportar la información de un Access Controller a otros dispositivos. Rostro No se permite importar imágenes a través de USB.

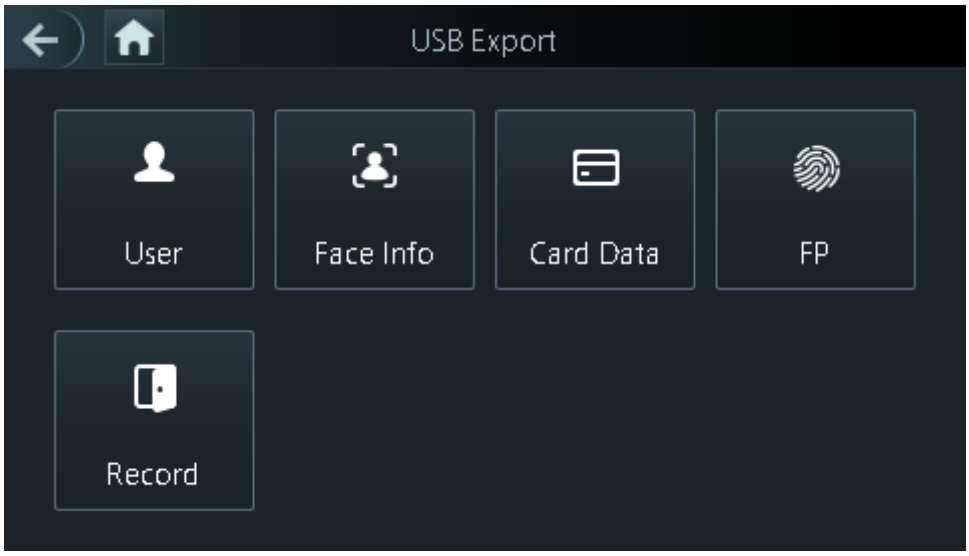
2.11.1 Exportar a USB

Puede exportar datos desde el Access Controller a un USB. Los datos exportados están cifrados y no se pueden editar.

Paso 1 Sobre el**Menú principal**, seleccionar**USB**>**Exportación USB**.

Paso 2 Seleccione el tipo de datos que desea exportar y luego toque**DE ACUERDO**.

Figura 2-18 Exportación USB



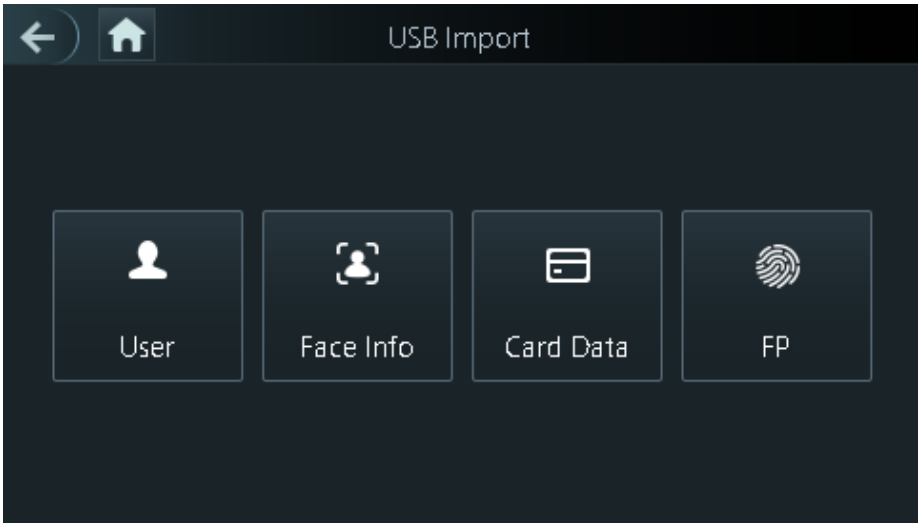
2.11.2 Importar desde USB

Puede importar datos desde USB al Access Controller.

Paso 1 Sobre el**Menú principal**, seleccionar**USB**>**Importación USB**.

Paso 2 Seleccione el tipo de datos que desea exportar y luego toque**DE ACUERDO**.

Figura 2-19 Importación USB



2.11.3 Actualización del sistema

Utilice un USB para actualizar el sistema del Access Controller.

Paso 1 Cambie el nombre del archivo de actualización a "update.bin", colóquelo en el directorio raíz del USB y luego inserte el USB en el Access Controller.

Paso 2 Sobre el**Menú principal**, seleccionar**USB**>**Actualización USB**. Grifo**DE**

Paso 3 **ACUERDO**.

El controlador de acceso se reiniciará cuando se complete la actualización.

2.12 Configuración de funciones

Sobre el**Menú principal**pantalla, seleccione**Características**.

Figura 2-20 Características

Tabla 2-12 Descripción de características

Parámetro	Descripción
Entorno privado	● Habilitar restablecimiento de PWD: puede habilitar esta función para restablecer la contraseña. La función PWD Reset está habilitada de forma predeterminada. ● HTTPS: El Protocolo seguro de transferencia de hipertexto (HTTPS) es un protocolo para la comunicación segura a través de una red informática. Cuando HTTPS está habilitado, HTTPS se utilizará para acceder a los comandos CGI; de lo contrario, se utilizará HTTP. Cuando HTTPS está habilitado, el controlador de acceso se reiniciará automáticamente. ● CGI: Common Gateway Interface (CGI) ofrece un protocolo estándar para que los servidores web ejecuten programas de manera similar a las aplicaciones de consola que se ejecutan en un servidor que genera páginas web dinámicamente. El CG I está habilitado de forma predeterminada. ● SSH: Secure Shell (SSH) es un protocolo de red criptográfico para operar servicios de red de forma segura a través de una red no segura. ● Capturar fotos: las imágenes de rostros se capturarán automáticamente cuando las personas abran la puerta. La función está activada por defecto. ● Borrar fotos capturadas: elimine todas las fotos capturadas automáticamente.

Parámetro	Descripción
Tarjeta No. Reverso	Cuando el Access Terminal se conecta a un dispositivo de terceros a través de la entrada Wiegand y el número de tarjeta leído por el Access Terminal está en el orden de reserva del número de tarjeta real, debe encender el**Tarjeta No. Reverso**función.
Sensor de puerta	NC: Cuando se abre la puerta, el circuito del sensor de puerta se cierra. NO: Cuando se abre la puerta, el circuito del sensor de la puerta está abierto. Las alarmas de intrusión y horas extras se activan solo después de que se enciende el detector de puerta.
Comentarios sobre los resultados	● Éxito/Fallo: solo muestra el éxito o el fracaso en la pantalla de espera. ● Sólo nombre: muestra la identificación del usuario, el nombre y la hora de autorización después de otorgar el acceso; muestra el mensaje no autorizado y el tiempo de autorización después del acceso denegado. ● Foto y nombre: muestra la imagen de la cara registrada del usuario, la identificación del usuario, el nombre y la hora de autorización después de otorgar el acceso; muestra el mensaje no autorizado y el tiempo de autorización después del acceso denegado. ● Fotos y nombre: muestra la imagen del rostro capturada y una imagen del rostro registrada de un usuario, ID de usuario, nombre y hora de autorización después de otorgar el acceso; muestra el mensaje no autorizado y el tiempo de autorización después del acceso denegado.
Atajo de reconocimiento	Seleccione métodos de verificación de identidad en la pantalla de espera. ● Contraseña: el icono del método de desbloqueo de contraseña se muestra en la pantalla de espera. ● Código QR: el icono del método de desbloqueo del código QR se muestra en la pantalla de espera. ● Llamada: el icono de la función de llamada se muestra en la pantalla de espera. ● Tipo de llamada: ◇ Sala de llamadas: toque el ícono de llamada en el modo de espera e ingrese el número de la habitación para realizar llamadas. ◇ Centro de administración de llamadas: toque el ícono de llamada en el modo de espera y luego llame al centro de administración. ◇ Sala de llamadas personalizada: toque el ícono de llamada para llamar al número de sala definido. Primero debe definir el número de habitaciones en el**Atajo de reconocimiento**pantalla.

2.13 Desbloqueo de la puerta

Puede desbloquear la puerta mediante rostros, contraseñas, huellas dactilares, tarjetas y más.

2.13.1 Desbloqueo por Tarjetas

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

2.13.2 Desbloqueo facial

Verificar la identidad de un individuo detectando sus rostros. Asegúrese de que el rostro esté centrado en el marco de detección de rostros.

2.13.3 Desbloqueo por Contraseña de Usuario

Ingrese el ID de usuario y la contraseña para desbloquear la puerta.

Paso 1 Grifo en la pantalla de espera.

Paso 2 grifo**Desbloqueo de personas con discapacidad**y luego ingrese el ID de usuario y la contraseña.

Paso 3 Grifo**Sí**.

2.13.4 Desbloqueo mediante contraseña de administrador

Ingrese solo la contraseña del administrador para desbloquear la puerta. El controlador de acceso sólo permite una contraseña de administrador. Usar la contraseña de administrador para desbloquear la puerta sin estar sujeto a niveles de usuario, modos de desbloqueo, períodos, planes de vacaciones y anti-passback, excepto para puertas normalmente cerradas. Un dispositivo permite solo una contraseña de administrador.

Requisitos previos

Se configuró la contraseña de administrador. Para obtener más información, consulte "2.7.3 Configuración de la contraseña del administrador".

La contraseña de administrador no se puede utilizar para desbloquear el estado de la puerta establecido en NC.

Procedimiento

Paso 1 Grifo en la pantalla de espera.

Paso 2 Grifo**Administrador PCD**y luego ingrese la contraseña de

Paso 3 admin ador. Grifo .

2.13.5 Desbloqueo mediante código QR

Paso 1 En la pantalla de espera, toque .

Paso 2 Coloque su código QR frente a la lente.

2.13.6 Desbloqueo por huella digital

Coloque su dedo en el escáner de huellas digitales. Esta función solo está disponible en el controlador de acceso.

que admite desbloqueo de huellas dactilares.

2.14 Ver registros de desbloqueo

Ver o buscar registros de desbloqueo de puertas. En el menú principal, toque**Registro**.

2.15 Información del sistema

Puede ver la capacidad de datos y la versión del dispositivo.

2.15.1 Visualización de la capacidad de datos

Sobre el**Menú principal**, seleccionar**Información del sistema**>**Capacidad de datos**, puede ver la capacidad de almacenamiento de cada tipo de datos.

2.15.2 Visualización de la versión del dispositivo

Sobre el**Menú principal**, seleccionar**Información del sistema**>**Capacidad de datos**, puede ver la versión del dispositivo, como el número de serie, la versión del software y más.

3 operaciones web

En la página web, también puede configurar y actualizar el controlador de acceso.

Las configuraciones web difieren según los modelos de Access Controller.

3.1 Inicialización

Inicialice el Controlador de acceso cuando inicie sesión en la página web por primera vez o después de que el Controlador de acceso se restablezca a los valores predeterminados de fábrica.

Requisitos previos

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

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

Paso 1 Abra un navegador, vaya a la dirección IP (la dirección predeterminada es 192.168.1.108) del Controlador de acceso.

Le recomendamos utilizar la última versión de Chrome o Firefox.

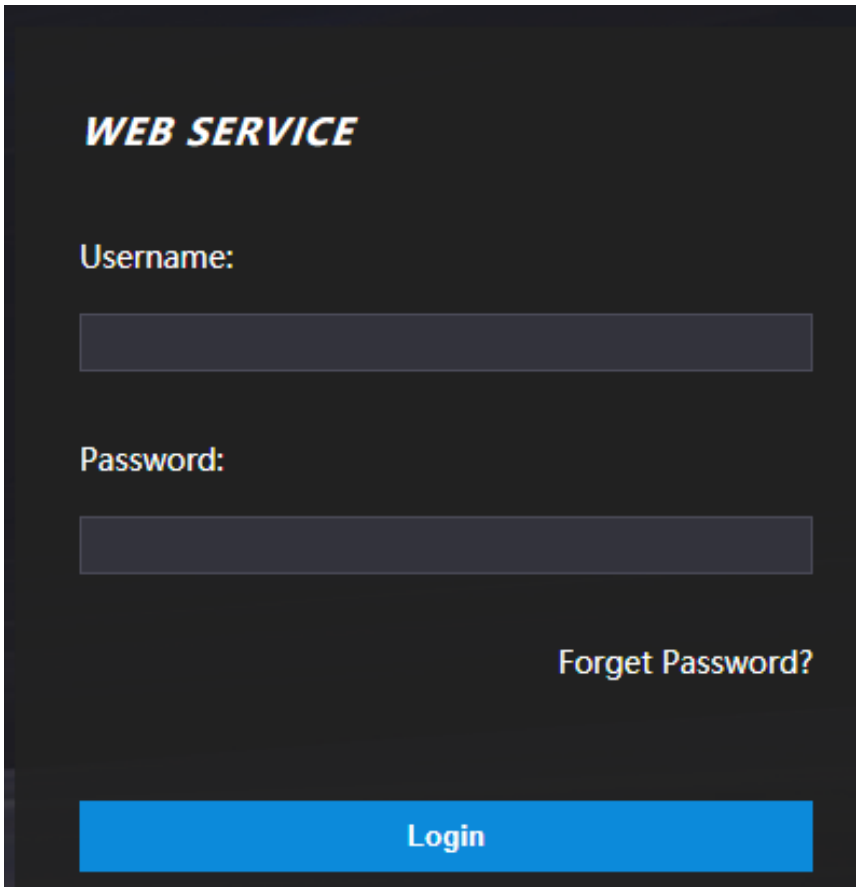
Paso 2 Configure la contraseña y la dirección de correo electrónico de acuerdo con las instrucciones en pantalla.

- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y especiales caracteres (excepto ' " ; : &). Establezca una contraseña de alta seguridad siguiendo la contraseña indicación de fuerza.
- Mantenga la contraseña segura después de la inicialización y cámbiela periódicamente para mejorar la seguridad.

3.2 Iniciar sesión

Paso 1 Abra un navegador, ingrese la dirección IP del controlador de acceso en la barra de direcciones y presione la tecla Enter.

Figura 3-1 Iniciar sesión



Paso 2 Ingrese el nombre de usuario y la contraseña.

- El nombre del administrador predeterminado es admin y la contraseña es la que usted configuró durante la inicialización. Le recomendamos cambiar la contraseña de administrador periódicamente para aumentar la seguridad.
- Si olvida la contraseña de inicio de sesión del administrador, puede hacer clic en**¿Contraseña olvidada?**Para Para obtener más información, consulte "3.3 Restablecimiento de la contraseña".

Paso 3 Hacer clic**Acceso**.

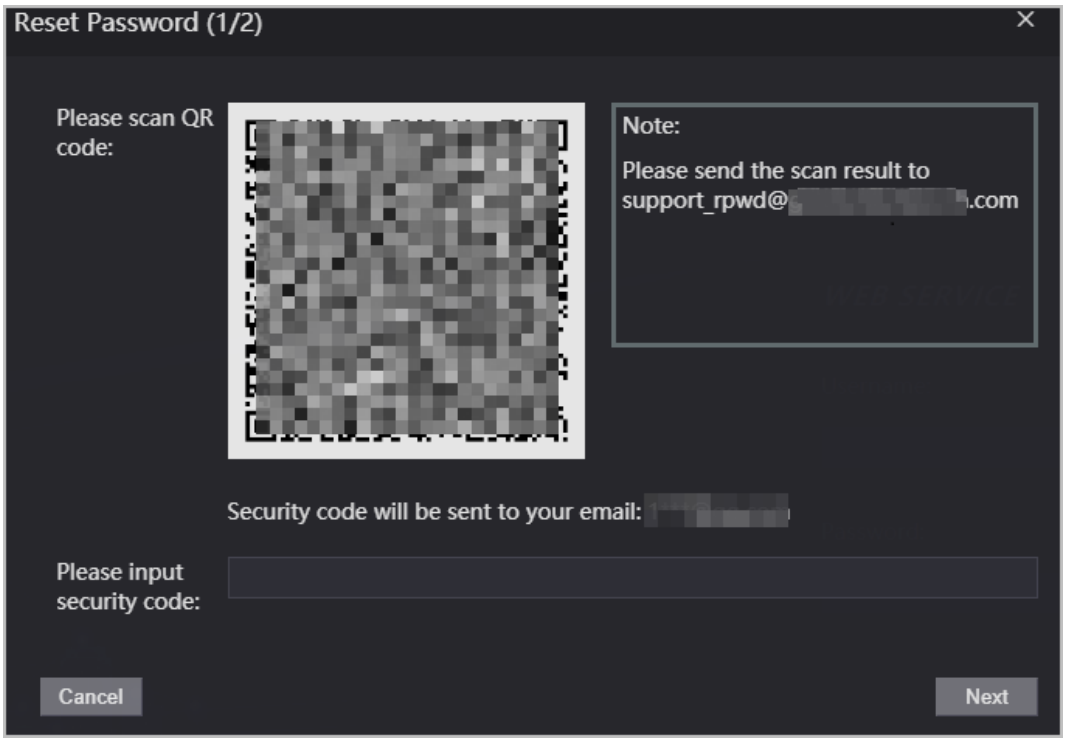
3.3 Restablecer la contraseña

Restablezca la contraseña a través del correo electrónico vinculado cuando olvide la contraseña de administrador. Paso 1 En la página de inicio de sesión, haga clic en**Has olvidado tu contraseña**.

Paso 2 Lea atentamente el mensaje que aparece en pantalla y luego haga clic en**DE**

Paso 3 **ACUERDO**. Escanea el código QR y obtendrás el código de seguridad.

Figura 3-2 Restablecer contraseña



- Se generarán hasta dos códigos de seguridad cuando se escanee el mismo código QR. Si el El código de seguridad deja de ser válido, actualice el código QR y escanéelo nuevamente.
- Después de escanear el código QR, recibirá un código de seguridad en su correo electrónico vinculado DIRECCIÓN. Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, será quedar inválido.
- Si se ingresa un código de seguridad incorrecto en una fila, la cuenta de administrador se congelará durante 5 minutos.

Etapa 4 Ingrese el código de seguridad.

Paso 5 Hacer clic**Próximo**.

Paso 6 Restablezca y confirme la nueva contraseña.

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

Paso 7 Hacer clic**DE ACUERDO**.

3.4 Configuración del parámetro de puerta

Configure los parámetros de control de acceso.

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Parámetro de la puerta**.

Figura 3-3 Parámetro de puerta

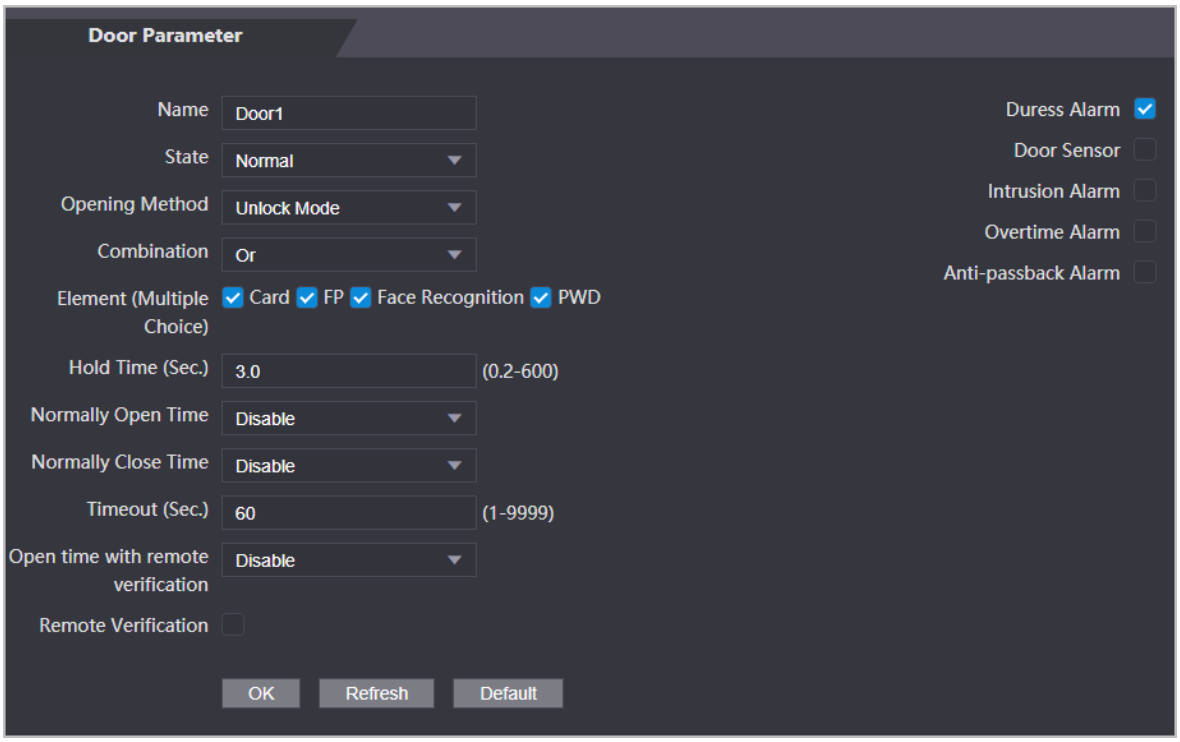


Tabla 3-1 Descripción de los parámetros de la puerta

Parámetro	Descripción
Nombre	Introduzca un nombre de la puerta.
Estado	Establecer el estado de la puerta. ● **NO**: La puerta permanece desbloqueada todo el tiempo. ● **CAROLINA DEL NORTE**: La puerta permanece cerrada todo el tiempo. ● **Normal**: Si**Normal**Si selecciona , la puerta se desbloqueará y bloqueará según su configuración.
Método de apertura	● Desbloqueo por período: establezca diferentes métodos de desbloqueo para diferentes períodos. ● Combinación de grupo: el usuario puede desbloquear la puerta solo después de que usuarios o grupos de usuarios definidos otorguen acceso. ● Modo de desbloqueo: establece combinaciones de desbloqueo.
Tiempo de espera (seg.)	Después de que se le conceda acceso a una persona, la puerta permanecerá desbloqueada durante un tiempo definido para que pueda pasar. Varía de 0,2 sa 600 s.
Horario normalmente abierto	La puerta permanece abierta o cerrada durante el periodo definido.
Hora normalmente cerrada	
Tiempo de espera (seg.)	Se activará una alarma de tiempo de espera si la puerta permanece desbloqueada durante un tiempo superior a este valor.
Abrir con verificación remota	Establezca el período de apertura de la puerta de verificación remota. Después de que los usuarios obtengan acceso en el controlador de acceso, también se les debe otorgar acceso desde la plataforma de administración antes de que se desbloquee la puerta.

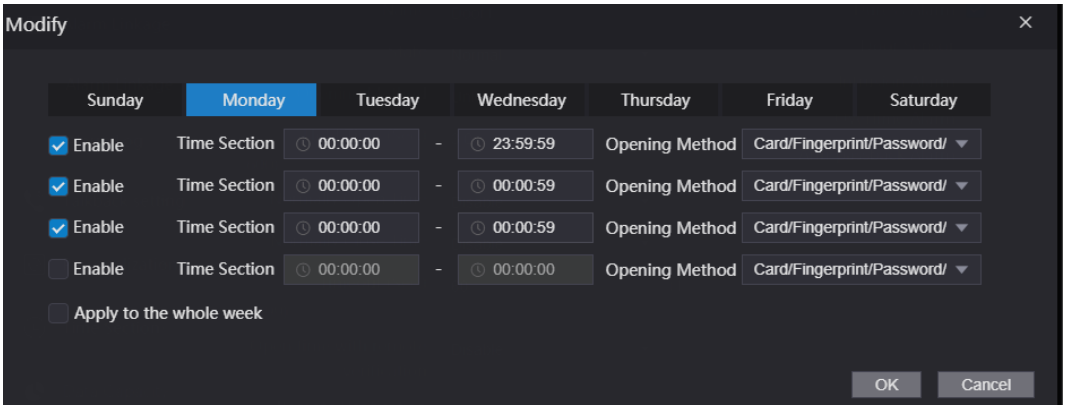
Parámetro	Descripción
Alarma de coacción	Se activará una alarma cuando se utilice una tarjeta de coacción o una contraseña de coacción para desbloquear la puerta.
Sensor de puerta	Las alarmas de intrusión y de horas extras sólo se pueden activar después de **Sensor de puerta**está habilitado.
Alarma de intrusión	Cuando**Sensor de puerta**está habilitado, se activará una alarma de intrusión si la puerta se abre de manera anormal.
Alarma de horas extras	Se activará una alarma de tiempo de espera si la puerta permanece desbloqueada durante más tiempo que el**Tiempo de espera (segundos)**.
Alarma anti-passback	Los usuarios deben verificar sus identidades tanto para entrar como para salir; de lo contrario se activará una alarma. Ayuda a evitar que el titular de una tarjeta le pase una tarjeta de acceso a otra persona para que pueda entrar. Cuando el anti-passback está habilitado, el titular de la tarjeta debe abandonar el área segura a través de un lector de salida antes de que el sistema le permita otra entrada. ● Si una persona entra sin autorización y sale sin autorización, se activará una alarma cuando intente volver a entrar y al mismo tiempo se le negará el acceso. ● Si una persona entra sin autorización y sale sin autorización, se activará una alarma cuando intente volver a entrar y al mismo tiempo se le negará el acceso.

Paso 3 Configurar el método de apertura.

- Desbloquear por período

  1. En el**Método de apertura**lista, seleccione**Desbloquear por período**y luego haga clic en .

Figura 3-4 Parámetro de la sección de tiempo



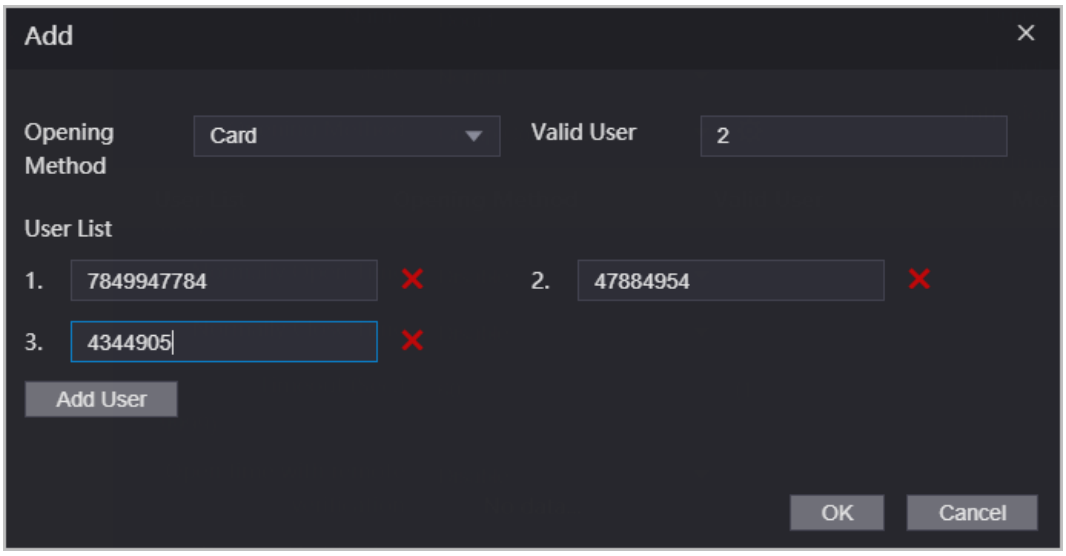
  2. Configure la hora y el método de apertura de una sección horaria. Puedes configurar hasta cuatro tramos horarios para un solo día.
  3. Seleccione**Aplica para toda la semana**para copiar el tiempo definido al resto de días.

- Combinación de grupo

  1. En el**Método de apertura**lista, seleccione**Combinación de grupo**y luego haga clic en
  2. Haga clic**Agregar**.
  3. Seleccione un método de desbloqueo en el**Método de apertura**list., e ingrese el número de usuarios válidos.

     Si el número de usuarios válidos es 2 y hay 3 usuarios en la lista de usuarios definida. Se requieren dos usuarios en la lista para otorgar acceso.

Figura 3-5 Combinación de grupos



4. En el**Lista de usuarios**área, haga clic**Agregar usuario**, ingrese el ID de usuario de los usuarios existentes.

   - ◇ No se pueden agregar usuarios VIP, de patrulla y de listas de bloqueo.
   - ◇ Los usuarios válidos en todos los grupos deben verificar sus identidades para otorgar acceso en el grupo. orden.

5. Haga clic**DE ACUERDO**.

- Modo de desbloqueo

  1. En el**Método de apertura**lista, seleccione**Combinación de grupo**y luego haga clic en .
  2. En el**Combinación**lista, seleccione**O**o**Y**.
     - ◇ **Y**significa que debes usar todos los métodos seleccionados para abrir la puerta.
     - ◇ **O**significa que puede abrir la puerta con cualquiera de los métodos seleccionados.
  3. En el**Elemento**lista, seleccione el método de desbloqueo.

Etapa 4 Configure otros parámetros. Hacer clic**DE**

Paso 5 **ACUERDO**.

3.5 Configuración del intercomunicador

El controlador de acceso puede funcionar como una estación de puerta para realizar la función de videoportero.

3.5.1 Configurar el servidor SIP

Cuando están conectados al mismo servidor SIP, todos los VTO y VTH pueden llamarse entre sí. Puede utilizar el controlador de acceso u otros VTO o la plataforma de gestión como servidor SIP.

Cuando el controlador de acceso funciona como servidor SIP, puede conectar hasta 500 dispositivos de control de acceso. dispositivos y VTH.

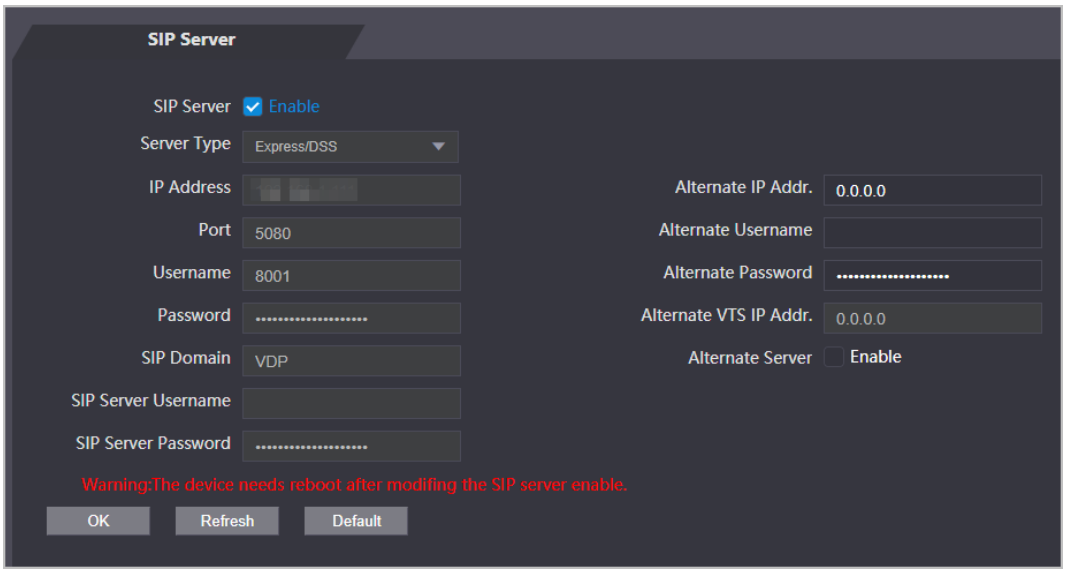
Paso 1 Seleccionar**Intercomunicador**>**Servidor SIP**.

Paso 2 Seleccione un tipo de servidor.

- Utilice el controlador de acceso como servidor SIP.

Encender**Servidor SIP**y mantener otros parámetros por defecto.

Figura 3-6 Utilice el controlador de acceso como servidor SIP



- Utilice otro VTO como servidor SIP:
  1. No habilitar**servidor SIP**. Seleccionar**VTO**desde el**Tipo de servidor**.
  2. Configure los parámetros y luego haga clic en**Ahorrar**.

Figura 3-7 Utilice VTO como servidor SIP

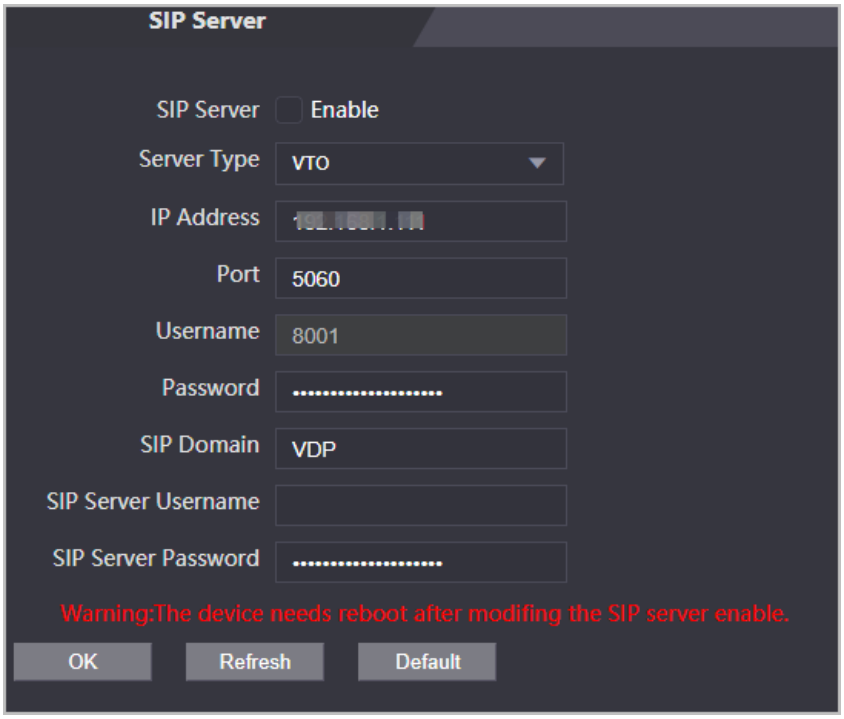


Tabla 3-2 Configuración del servidor SIP

Parámetro	Descripción
Dirección IP	Dirección IP de la plataforma.
Puerto	• 5060 de forma predeterminada cuando VTO funciona como servidor SIP. • 5080 por defecto cuando la plataforma funciona como servidor SIP.
Nombre de usuario	Déjalos como predeterminados.
Contraseña	

Parámetro	Descripción
Dominio SIP	VDP.
Nombre de usuario del servidor SIP	El nombre de usuario y la contraseña de inicio de sesión del servidor SIP.
Contraseña del servidor SIP	

- Utilice DSS Express o DSS pro como servidor SIP.

  No activesservidor SIP. SeleccionarExpreso/DSSdesde elTipo de servidor.

Figura 3-8 Utilice DSS Express o DSS pro como servidor SIP

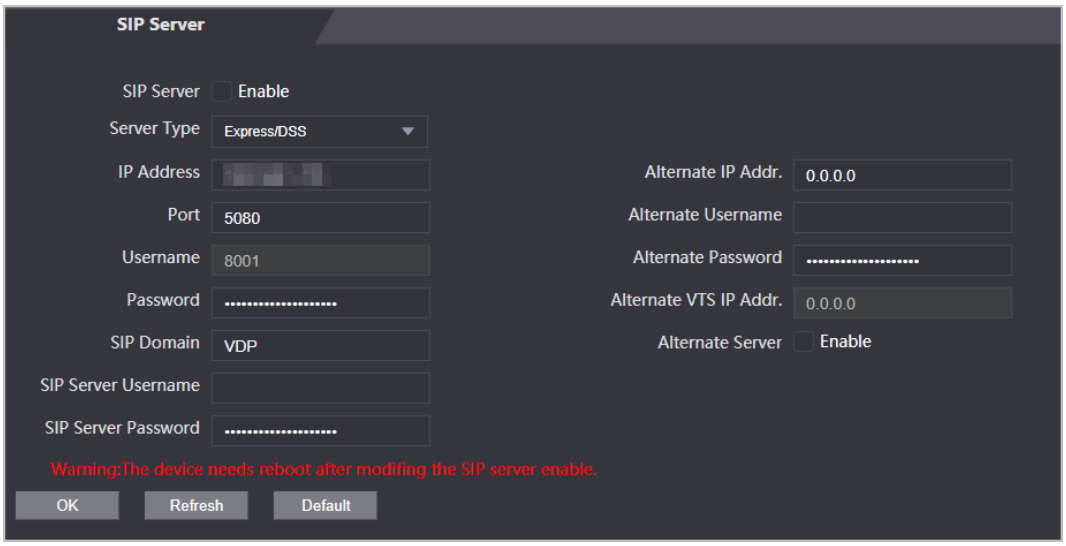


Tabla 3-3 Configuración del servidor SIP

Parámetro	Descripción
Dirección IP	Dirección IP de la plataforma.
Puerto	• 5060 de forma predeterminada cuando VTO funciona como servidor SIP. • 5080 por defecto cuando la plataforma funciona como servidor SIP.
Nombre de usuario	Déjalos como predeterminados.
Contraseña	
Dominio SIP	Déjalo por defecto.
Nombre de usuario del servidor SIP	El nombre de usuario y contraseña de inicio de sesión de la plataforma.
Contraseña del servidor SIP	
Dirección IP alternativa.	El servidor alternativo se utilizará como servidor SIP cuando DSS Express o DSS pro no responda. Le recomendamos configurar la dirección IP alternativa. • Si enciendes elServidor alternativofunción, configurará los controladores de acceso como servidor alternativo. • Si desea que otro VTO funcione como servidor alternativo, debe Debe ingresar la dirección IP, nombre de usuario y contraseña del VTO. Hacer no habilitarServidor alternativoen este caso. • Le recomendamos configurar el VTO principal como servidor alternativo.
Nombre de usuario alternativo	Se utiliza para iniciar sesión en el servidor alternativo.
Contraseña alternativa	

Parámetro	Descripción
Dirección IP VTS alternativa.	Ingrese la dirección IP del VTS alternativo. Cuando la plataforma de administración no responde, se activará el VTS alternativo para garantizar que VTO, VTH y VTS aún puedan realizar la función de videoportero.

Paso 3 Hacer clic**DE ACUERDO**.

3.5.2 Configuración de parámetros básicos

Configure la información básica de VTO, como el tipo de dispositivo y el número de dispositivo.

Paso 1 Seleccionar**Replicar**>**Local**.

Paso 2 Configure los parámetros.

- Utilice el controlador de acceso como servidor SIP.

Figura 3-9 Parámetro básico

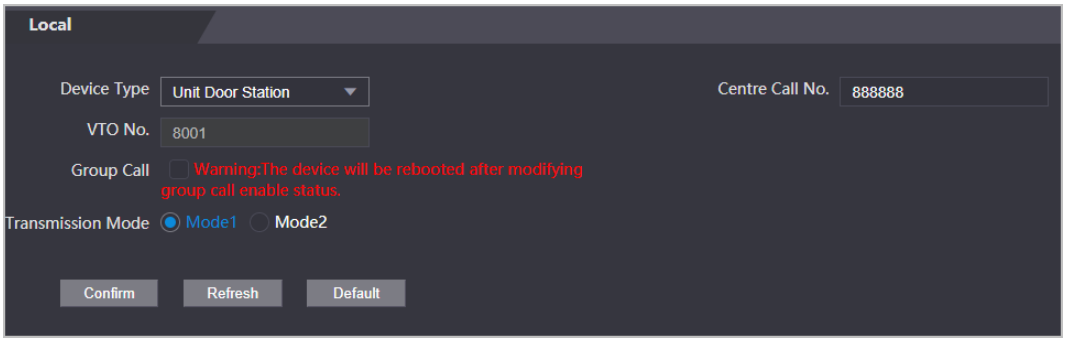


Tabla 3-4 Descripción de parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccionar**Estación de puerta de la unidad**.
VTO No.	El número del VTO, que no se puede configurar.
Llamada grupal	Cuando activa la función de llamada grupal, el VTO llama al VTH principal y a las extensiones al mismo tiempo.
Número de llamada del centro.	El número de teléfono predeterminado es 888888+VTS No. cuando el VTO llama al VTS. Puede comprobar el número del VTS desde el**Dispositivo**pantalla del VTS.
Modo de transmisión	El modo 1 está seleccionado de forma predeterminada.

- Utilice otro VTO como servidor SIP.

Figura 3-10 Parámetro básico

Tabla 3-5 Descripción de parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccionar**Estación de puerta de la unidad**.

Parámetro	Descripción
VTO No.	El número de la VTO. ● El número debe tener cuatro dígitos. Los dos primeros dígitos son 80 y los dos últimos dígitos comienzan desde 01. Tomemos como ejemplo 8001. ● Si existen varios VTO en una unidad, el número de VTO no se puede repetir.
Número de llamada del centro.	El número de teléfono predeterminado para el centro de gestión es 888888. Manténgalo como predeterminado.
Modo de transmisión	El modo 1 está seleccionado de forma predeterminada.

● Utilice la plataforma (DSS Express o DSS Pro) como servidor SIP.

Figura 3-11 Parámetro básico

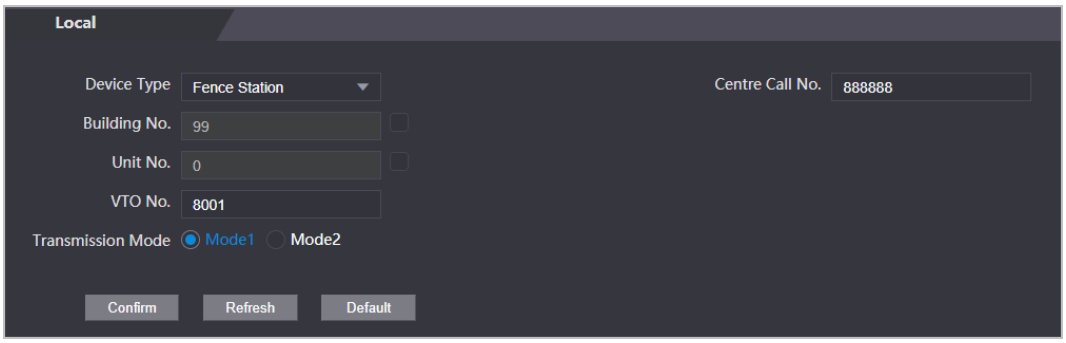


Tabla 3-6 Descripción de parámetros básicos

Parámetro	Descripción	
Tipo de dispositivo	Seleccione el tipo de dispositivo según la posición de instalación.	
Edificio número.	Seleccione la casilla de verificación y luego ingrese el número del edificio donde está instalada la estación de puerta de la unidad.	Si el edificio y la unidad están habilitados en DSS, ingrese el número del edificio y el número de la unidad en la página web. El número de edificio, el número de unidad y el número de VTO deben ajustarse a los parámetros configurados en DSS. Tome la habitación 1001, la unidad 2 y el edificio 1 como ejemplo. Si el número de edificio está habilitado en el DSS y la unidad no está habilitada, la habitación El número es "1#1001". Si el edificio y la unidad son ambos habilitados, el número de habitación es "1#2#1001". Si el edificio no está habilitado y la unidad no está habilitado tampoco, el número de habitación es "1001". Para Para obtener más información, consulte el manual de usuario de DSS.
Numero de unidad.	Seleccione la casilla de verificación y luego ingrese el número de la unidad donde está la estación de puerta de la unidad. instalado.	
VTO No.	El número de la estación de puerta de la unidad. Si existen múltiples VTO en la única unidad, el VTO No. No se puede repetir.	
Número de llamada del centro.	El número de teléfono predeterminado es 888888 cuando el VTO llama al VTS. Mantenlo como predeterminado.	
Transmisión Modo	El modo 1 está seleccionado de forma predeterminada.	

Paso 3 Hacer clic**Confirmar**.

3.5.3 Agregar el VTO

Cuando el controlador de acceso funciona como servidor SIP y tiene otros VTO, debe agregar otros VTO al servidor SIP para asegurarse de que puedan llamarse entre sí.

Paso 1 En la página web del controlador de acceso, seleccione**Configuración de conversación**>**VTO No. Gestión**.

Paso 2 Hacer clic**Agregar**y luego configure el VTO.

Figura 3-12 Agregar VTO

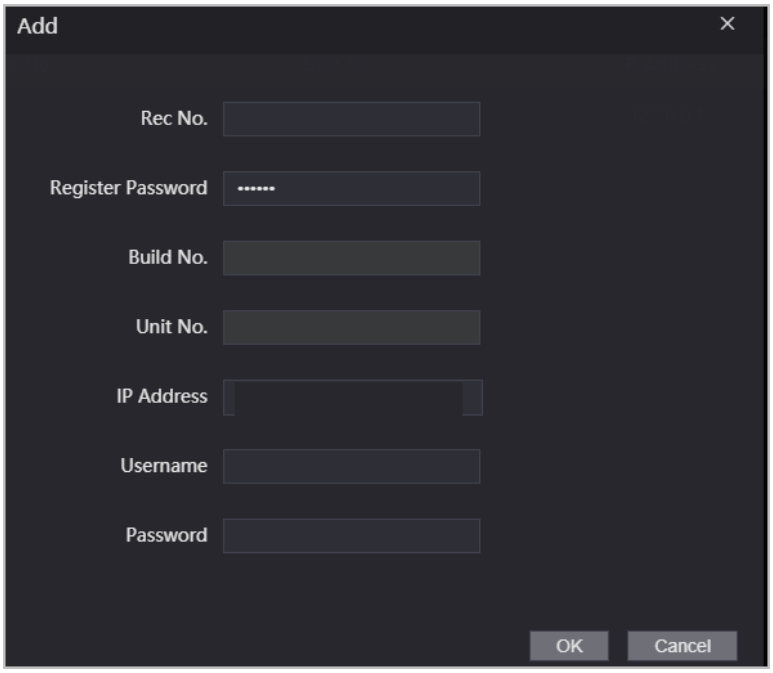


Tabla 3-7 Agregar configuración de VTO

Parámetro	Descripción
Rec no.	El número del VTO agregado. Puedes comprobar el número desde el **Dispositivo**página en la página web de la VTO.
Registro Contraseña	Manténgalo predeterminado.
Construir no.	No se puede configurar.
Numero de unidad.	
Dirección IP	La dirección IP del VTO agregado.
Nombre de usuario	El nombre de usuario y la contraseña utilizados para iniciar sesión en la página web del VTO agregado.
Contraseña	

Paso 3 Hacer clic**DE ACUERDO**.

3.5.4 Agregar el VTH

Cuando el controlador de acceso funciona como servidor SIP, puede agregar todos los VTH en la misma unidad al

Servidor SIP para asegurarse de que puedan llamarse entre sí.

Información de contexto

- Cuando hay VTH principal y una extensión, primero debe activar la función de llamada grupal y luego agregue VTH principal y extensión en el**Gestión VTH**página. Para saber cómo encender el grupo. función de llamada, consulte "3.5.2 Configuración de parámetros básicos".
- No se puede agregar extensión cuando no se agregan los VTH principales.

Paso 1 En la página de inicio, seleccione**Configuración de conversación**>**Gestión de nº de habitación**.

Paso 2 Agregue el VTH.

- Agregar individualmente

  1. Haga clic**Agregar**.
  2. Configure los parámetros y luego haga clic en**DE ACUERDO**.

Figura 3-13 Agregar individualmente

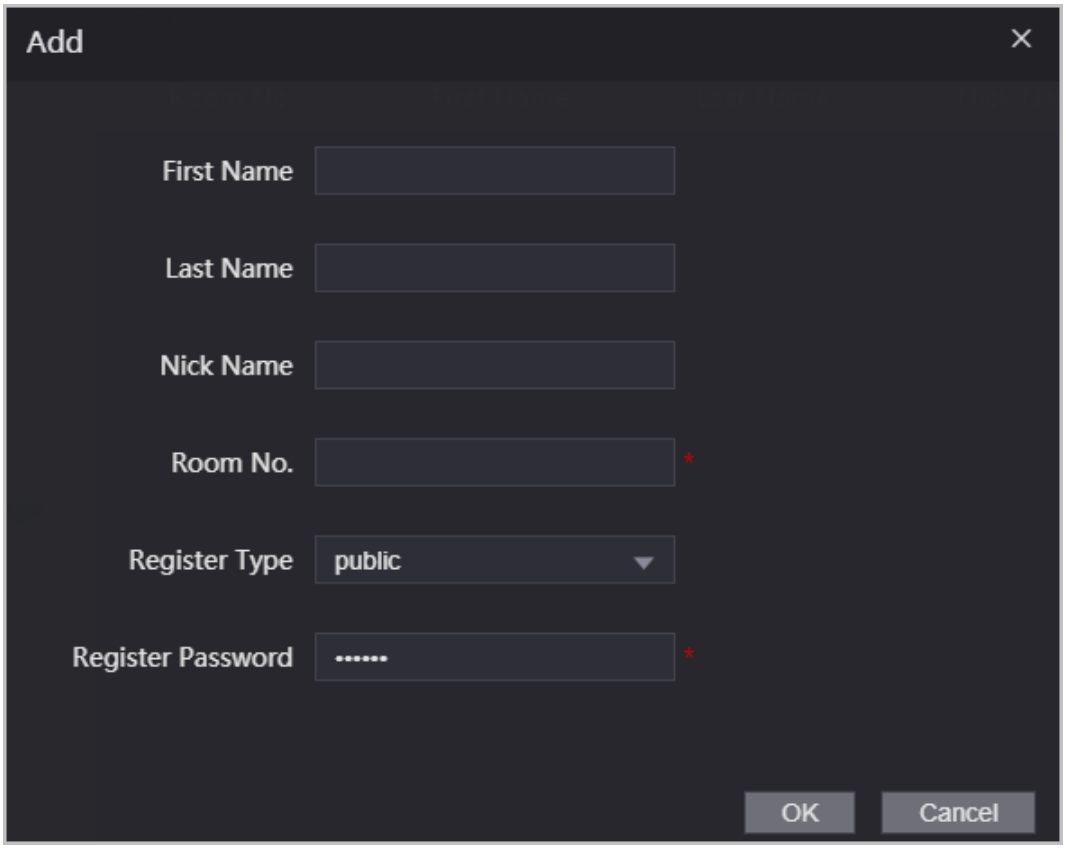


Tabla 3-8 Información de la habitación

Parámetro	Descripción
Habitación no.	Ingrese el número de habitación del VTH. ● El número de habitación consta de 1 a 5 dígitos y debe ajustarse al número de habitación configurado en el VTH. ● Cuando hay VTH principal y extensiones, el número de habitación del VTH principal termina en -0 y el número de habitación de la extensión termina en -1, -2 o -3. Por ejemplo, el VTH principal es 101-0 y el número de habitación de la extensión es 101-1, 101-2... ● Si la función de llamada grupal no está activada, no se puede configurar el número de habitación en el formato 9901-xx.
Nombre de pila Apellido Apodo	Ingrese el nombre del VTH para ayudarlo a diferenciar los VTH.
Tipo de registro Contraseña registrada	Mantenlos como predeterminados.

- Agregar en lotes

  1. Haga clic**Agregar lote**

  2. Configure los parámetros.

Figura 3-14 Agregar lote

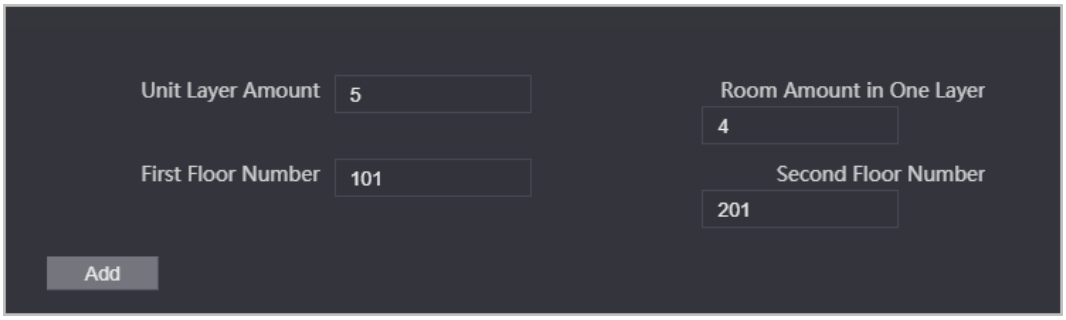


Tabla 3-9 Agregar lote

Parámetro	Descripción
Cantidad de capa unitaria	El número de pisos del edificio (entre 1 y 99).
Cantidad de espacio en una capa	El número de habitaciones en cada piso, que oscila entre 1 y 99.
Número del primer piso	La primera habitación en el primer piso.
Número del segundo piso	La primera habitación del segundo piso, que es igual a la primera habitación del primer piso más el número de habitaciones de cada piso.

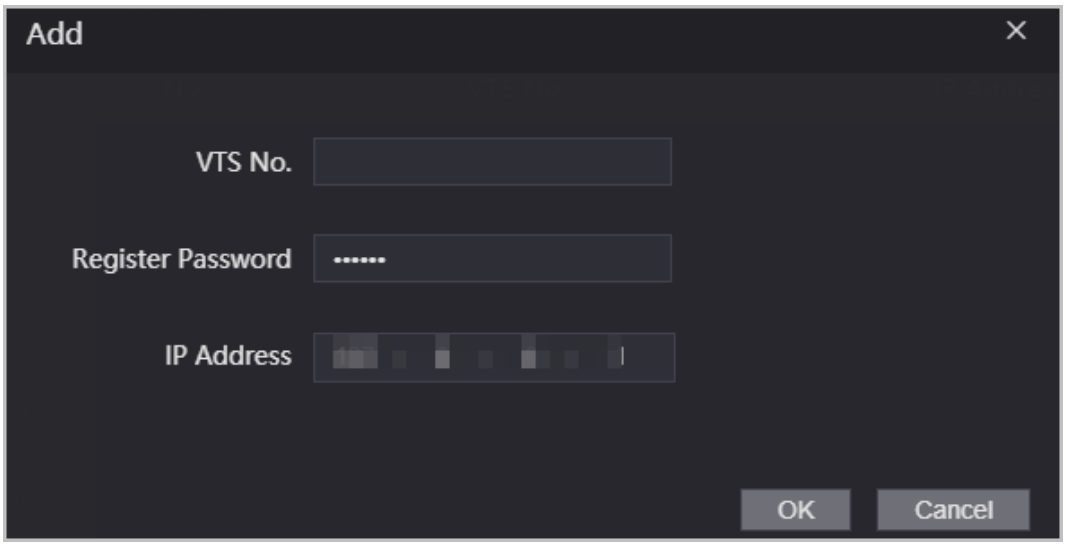
3.5.5 Agregar el VTS

Cuando el controlador de acceso funciona como servidor SIP, puede agregar VTS al servidor SIP para asegurarse de que puedan llamarse entre sí.

Paso 1 En la página de inicio, seleccione**Configuración de conversación**>**Gestión VTS**.

Paso 2 Hacer clic**Agregar**y establecer parámetros.

Figura 3-15 Gestión de VTS



Paso 3 Hacer clic**DE ACUERDO**.

3.5.6 Ver el estado del dispositivo

Cuando el controlador de acceso funciona como servidor SIP, puede ver el estado de los dispositivos que están conectados al servidor SIP.

En la página de inicio, seleccione**Configuración de conversación**>**Estado**.

3.5.7 Ver registros de llamadas

Ver todo el registro de llamadas salientes y llamadas entrantes. En la página de inicio, seleccione**Configuración de conversación**>**Llamar**.

3.6 Configurar secciones de tiempo

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

3.6.1 Configurar secciones de tiempo

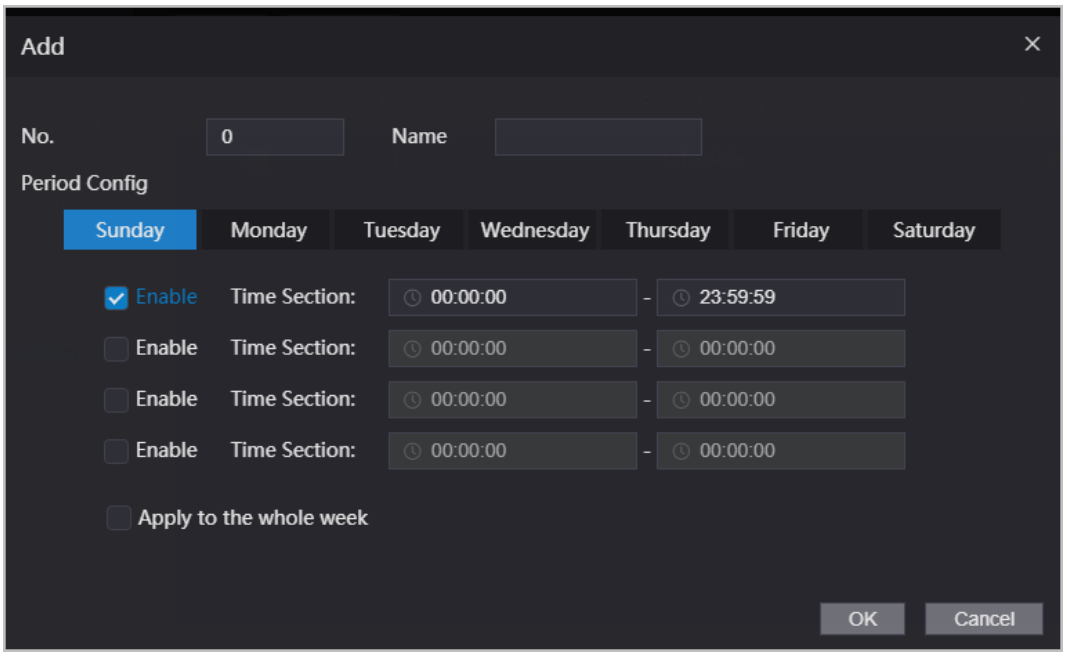
Puede configurar hasta 128 grupos (del No.0 al No.127) de sección de tiempo. En cada grupo, es necesario configurar horarios de acceso a las puertas durante toda una semana. Un usuario solo puede desbloquear la puerta durante el tiempo programado.

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Sección de tiempo**>**Sección de tiempo**.

Paso 3 Hacer clic**Agregar**.

Figura 3-16 Parámetros de la sección de tiempo



Etapa 4 Ingrese el número y el nombre de la sección de tiempo.

- **No.**: Ingrese un número de sección. Va desde 0 hasta 127.
- **Nombre**: Introduzca un nombre para cada sección de tiempo. Puede ingresar un máximo de 32 caracteres (contiene números, caracteres especiales y caracteres en inglés).

Paso 5 Configura secciones horarias para cada día.

Paso 6 Puedes configurar hasta cuatro tramos horarios para un solo día.

Paso 7 (Opcional) Haga clic**Aplica para toda la semana**para copiar la configuración al resto de días. Hacer clic**DE**

Paso 8 **ACUERDO**.

3.6.2 Configurar grupos de vacaciones

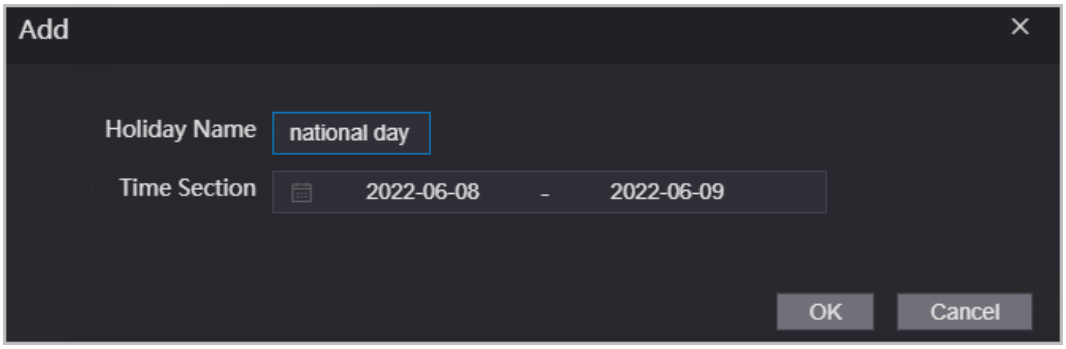
Establece secciones horarias para diferentes grupos de vacaciones. Puede configurar hasta 128 grupos de vacaciones (del 0 al 127). y hasta 16 tramos horarios para un único grupo de vacaciones. Los usuarios pueden desbloquear puertas en las secciones de tiempo definidas.

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Sección de tiempo**>**Grupo de vacaciones**>**configuración**.

Paso 3 Hacer clic**Agregar**.

Figura 3-17 Agregar un grupo de vacaciones



Etapa 4 Establezca el nombre y la hora del grupo de vacaciones.

- **Nombre de vacaciones**: Introduzca el nombre del grupo de vacaciones. Introduce un nombre para cada vez

sección. Puede ingresar un máximo de 32 caracteres (contiene números, caracteres especiales y caracteres en inglés).

- **Sección de tiempo**: Seleccione la hora de inicio y finalización de las vacaciones. Hacer clic**DE**

Paso 5 **ACUERDO**.

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

Paso 6 Hacer clic**DE ACUERDO**.

3.6.3 Configurar planes de vacaciones

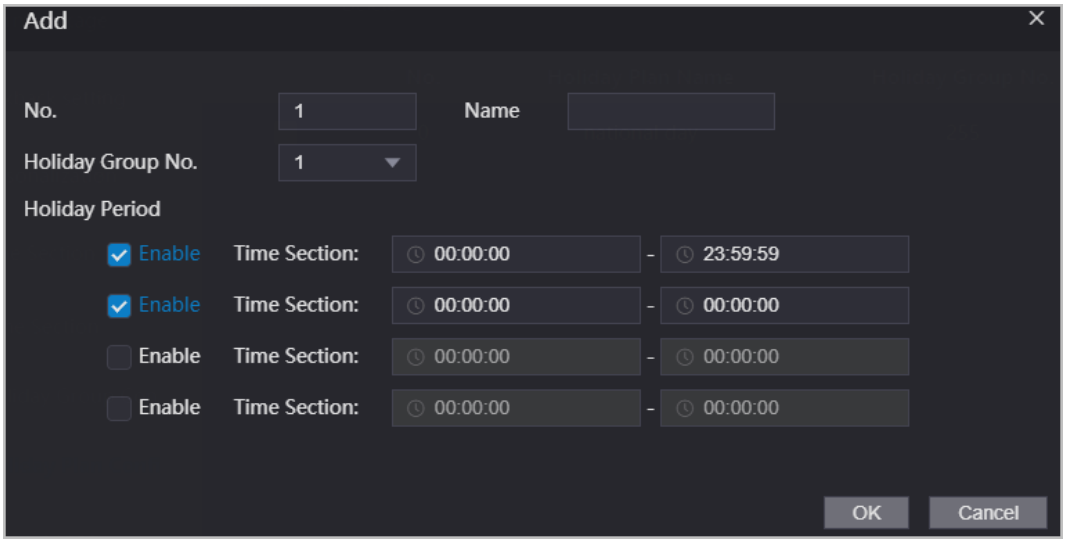
Asigne los grupos de vacaciones configurados al plan de vacaciones. Los usuarios sólo pueden desbloquear la puerta en el tiempo definido en el plan de vacaciones.

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Sección de tiempo**>**Configuración del plan de vacaciones**.

Paso 3 Hacer clic**Agregar**.

Figura 3-18 Agregar plan de vacaciones



Etapa 4 Ingrese un número y nombre para el plan de vacaciones.

- **No.**: Introduzca un número de sección. Va de 0 a 127.
- **Nombre**: Introduzca un nombre para cada sección de tiempo. Puede ingresar un máximo de 32 caracteres (contiene números, caracteres especiales y caracteres en inglés).

Paso 5 En el**Grupo de vacaciones No.**lista, seleccione el número del grupo de vacaciones definido.

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

Paso 6 En el**Periodo de festivos**área, configure las secciones horarias en el grupo de vacaciones. Puede configurar hasta cuatro tramos horarios.

Paso 7 Hacer clic**DE ACUERDO**.

3.7 Capacidad de datos

Puede ver cuántos usuarios, tarjetas e imágenes de rostros puede almacenar el Access Controller.

Inicie sesión en la página web y seleccione**Capacidad de datos**.

3.8 Configurar vídeo e imagen

Configure los parámetros de video e imagen, como la transmisión y el brillo.

Le recomendamos utilizar los parámetros predeterminados en esta sección.

3.8.1 Configuración de vídeo

En la página de inicio, seleccione**Configuración de vídeo**y luego configure la transmisión de video, el estado, la imagen y la exposición.

- Estándar de vídeo: Seleccionar**NTSC**.
- ID de canal: el canal 1 es para configuraciones de imagen de luz visible. El canal 2 es para configuraciones de imagen de luz infrarroja.
- Predeterminado: restaurar la configuración predeterminada.
- Capturar: tome una instantánea de la imagen actual.

El estándar de vídeo PAL es de 25 fps y el estándar de vídeo NTSC es de 30 fps.

3.8.1.1 Configuración del canal 1

Paso 1 Seleccionar**Configuración de vídeo**>**Configuración de**

Paso 2 **vídeo**. Seleccionar**1**desde el**Canal No.**lista. Configura la

Paso 3 tarifa de la fecha.

Figura 3-19 Tarifa de fecha

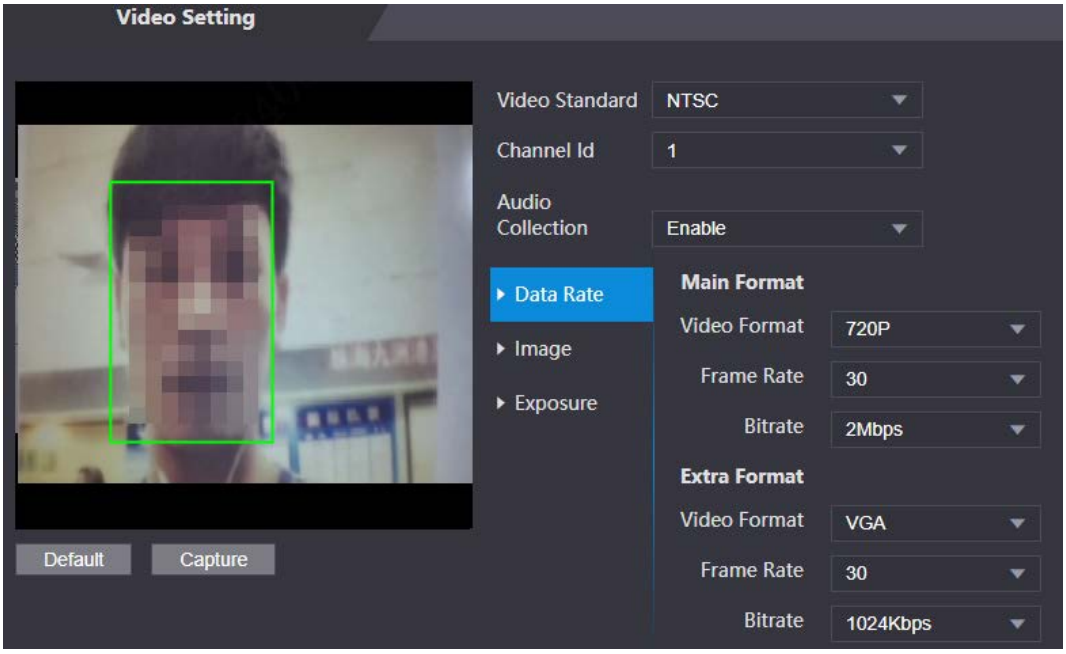


Tabla 3-11 Descripción de la tarifa por fecha

Parámetro		Descripción
Formato principal	Formato de video	Cuando el controlador de acceso funciona como VTO y conecta el VTH, el El límite de transmisión adquirido de VTH es 720p. Cuando la resolución se cambia a 1080p, la llamada y la función del monitor podría verse afectada.
	Cuadros por segundo	El número de fotogramas (o imágenes) por segundo. El rango de velocidad de fotogramas es de 1 a 25 fps.
	tasa de bits	Indica la cantidad de datos transmitidos a través de una conexión a Internet en un período de tiempo determinado. Seleccione un ancho de banda adecuado según la velocidad de su red.
Sub corriente	Formato de video	La subtransmisión admite D1, VGA y QVGA.
	Cuadros por segundo	El número de fotogramas (o imágenes) por segundo. El rango de velocidad de fotogramas es de 1 a 25 fps.
	tasa de bits	Indica la cantidad de datos transmitidos a través de una conexión a Internet en un período de tiempo determinado.

Etapa 4 Configura la imagen.

Figura 3-20 Imagen

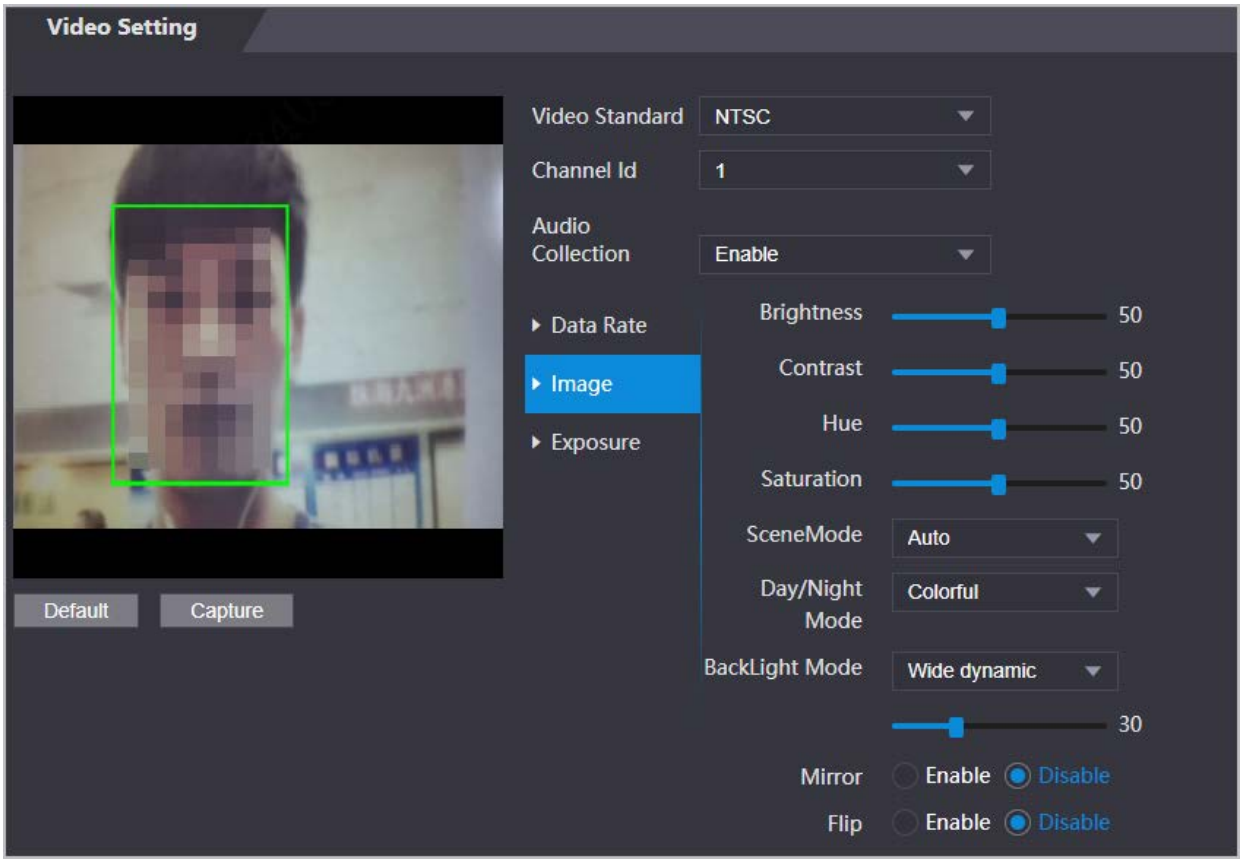


Tabla 3-12 Descripción de la imagen

Parámetro	Descripción
Contraste	El contraste es la diferencia de luminancia o color que hace que un objeto sea distinguible. Cuanto mayor sea el valor de contraste, mayor será el contraste de color.
Matiz	Se refiere a la fuerza o saturación de un color. Describe la intensidad del color o su pureza.
Saturación	La saturación de color indica la intensidad del color en una imagen. A medida que aumenta la saturación, aparecen más fuertes, por ejemplo más rojos o más azules. El valor de saturación no cambia el brillo de la imagen.
Modo escena	El tono de la imagen es diferente en diferentes modos de escena. ● **Cerca**: La función del modo de escena está desactivada. ● **Auto**: El sistema ajusta automáticamente el modo de escena según la sensibilidad fotográfica. ● **Soleado**: En este modo, se reducirá el tono de la imagen. ● **Noche**: En este modo, se aumentará el tono de la imagen.
Día/Noche	El modo Día/Noche afecta la compensación de luz en diferentes situaciones. ● **Auto**: El sistema ajusta automáticamente el modo día/noche según la sensibilidad fotográfica. ● **Vistoso**: En este modo, las imágenes son coloridas. ● **En blanco y negro**: En este modo, las imágenes están en blanco y negro.
Modo de retroiluminación	● **Cerca**: La compensación de luz de fondo está desactivada. ● **Iluminar desde el fondo**: La compensación de contraluz aporta automáticamente más luz a las áreas más oscuras de una imagen cuando la luz brillante que brilla desde atrás las oscurece. ● **Amplia dinámica**: El sistema atenúa las áreas brillantes y compensa las áreas oscuras para crear un equilibrio que mejore la calidad general de la imagen. ● **Inhibición**: La compensación de altas luces (HLC) es una tecnología utilizada en las cámaras de seguridad CCTV/IP para tratar imágenes expuestas a luces como faros o focos. El sensor de imagen de la cámara detecta luces intensas en el vídeo y reduce la exposición en estos puntos para mejorar la calidad general de la imagen.
Espejo	Cuando la función está activada, las imágenes se mostrarán con los lados izquierdo y derecho invertidos.
Voltear	Cuando esta función está activada, las imágenes se pueden voltear.

Paso 5 Configure los parámetros de exposición.

Figura 3-21 Exposición

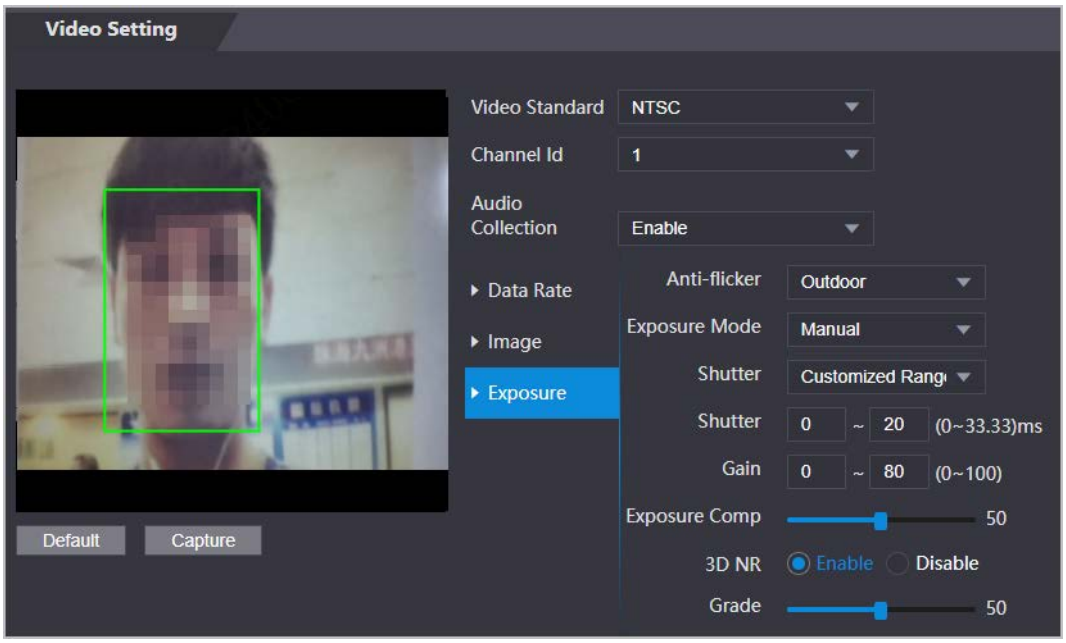


Tabla 3-13 Descripción del parámetro de exposición

Parámetro	Descripción
Contra parpadeo	Configure el antiparpadeo para reducir el parpadeo y disminuir o reducir los colores o la exposición desiguales. ● **50Hz**: Cuando la fuente de alimentación es de 50 Hz, la exposición se ajusta automáticamente para evitar la aparición de líneas horizontales. ● **60Hz**: Cuando la fuente de alimentación es de 60 Hz, la exposición se ajusta automáticamente para reducir la aparición de líneas horizontales. ● **Exterior**: Cuando**Exterior**Cuando se selecciona, se puede cambiar el modo de exposición.
Modo de exposición	Puede configurar la exposición para ajustar el brillo de la imagen. ● **Auto**: El Access Controller ajusta automáticamente el brillo de las imágenes. ● **Prioridad de obturador**: El Access Terminal ajustará el brillo de la imagen según el rango de exposición del obturador. Si el brillo de la imagen no es suficiente y el valor del obturador ha alcanzado su límite superior o inferior, el controlador de acceso ajustará el valor de ganancia automáticamente para obtener el nivel de brillo ideal. ● **Manual**: Puede configurar la ganancia y el valor del obturador manualmente para ajustar el brillo de la imagen. ◇ Cuando seleccionas**Exterior**desde el**Contra parpadeo**lista, puedes seleccionar**Prioridad de obturador**como modo de exposición. ◇ El modo de exposición puede diferir dependiendo de los diferentes modelos de Controlador de acceso.

Parámetro	Descripción
Obturador	La persiana es un componente que deja pasar la luz durante un período determinado. Cuanto mayor sea la velocidad de obturación, más corto será el tiempo de exposición y más oscura será la imagen.
Ganar	Cuando se establece el rango del valor de ganancia, se mejorará la calidad del video.
Exposición Compensación	Puede hacer que una foto sea más brillante o más oscura ajustando el valor de compensación de exposición.
Reducción de ruido 3D	Cuando la Reducción de ruido 3D (RD) está activada, el ruido del vídeo se puede reducir para garantizar vídeos de alta definición.
Calificación	Puede establecer su calificación cuando esta función está activada.

3.8.1.2 Configuración del canal 2

Paso 1 Seleccionar**Configuración de vídeo**>

Paso 2 **Configuración de vídeo**. Seleccione 2 del**Canal No.**

Paso 3 . Configura el estado del vídeo.

Le recomendamos que active la función WDR cuando la cara esté a contraluz.

Figura 3-22 Imagen

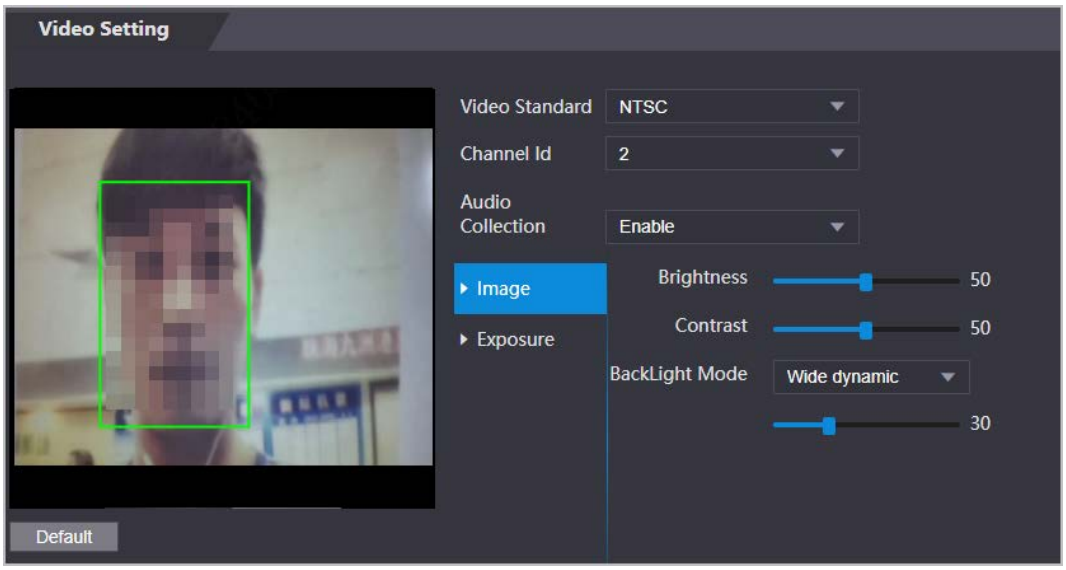


Tabla 3-14 Descripción de la imagen

Parámetro	Descripción
Brillo	El brillo es la relativa claridad u oscuridad de un color en particular. Cuanto mayor sea el valor, más brillante será la imagen.
Contraste	El contraste es la diferencia de luminancia o color que hace que un objeto sea distinguible. Cuanto mayor sea el valor de contraste, mayor será el contraste de color.

Parámetro	Descripción
Modo de retroiluminación	● **Cerca**: La compensación de contraluz está desactivada. ● **Iluminar desde el fondo**: La compensación de luz negra aporta automáticamente más luz a las áreas más oscuras de una imagen cuando la luz brillante que brilla desde atrás las oscurece. ● **Amplia dinámica**: El sistema atenúa las áreas brillantes y compensa las áreas oscuras para garantizar la creación de un equilibrio que mejore la calidad general de la imagen. ● **Inhibición**: La compensación de altas luces (HLC) es una tecnología utilizada en las cámaras de seguridad CCTV/IP para tratar imágenes expuestas a luces como faros o focos. El sensor de imagen de la cámara detecta luces fuertes en el vídeo y reduce la exposición en estos puntos para mejorar la calidad general de la imagen.

Etapa 4 Configure los parámetros de exposición.

Figura 3-23 Parámetro de exposición

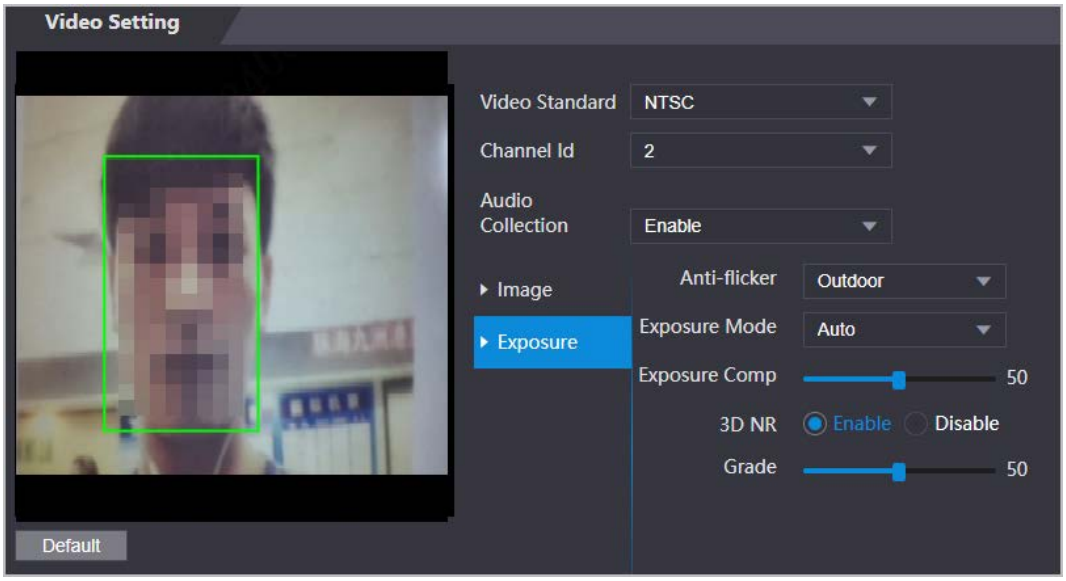


Tabla 3-15 Descripción del parámetro de exposición

Parámetro	Descripción
Contra parpadeo	Configure el antiparpadeo para reducir el parpadeo y disminuir o eliminar los colores o la exposición desiguales. ● **50Hz**: Cuando la fuente de alimentación es de 50 Hz, la exposición se ajusta automáticamente para evitar la aparición de líneas horizontales. ● **60Hz**: Cuando la fuente de alimentación es de 60 Hz, la exposición se ajusta automáticamente para reducir la aparición de líneas horizontales. ● **Exterior**: Cuando**Exterior**Cuando se selecciona, se puede cambiar el modo de exposición.

Parámetro	Descripción
Modo de exposición	Puede configurar la exposición para ajustar el brillo de la imagen. ● **Auto**: El Access Controller ajusta automáticamente el brillo de las imágenes. ● **Prioridad de obturador**: El Access Terminal ajustará el brillo de la imagen según el rango de exposición del obturador. Si el brillo de la imagen no es suficiente y el valor del obturador ha alcanzado su límite superior o inferior, el controlador de acceso ajustará el valor de ganancia automáticamente para obtener el nivel de brillo ideal. ● **Manual**: Puede configurar la ganancia y el valor del obturador manualmente para ajustar el brillo de la imagen.  ◇ Cuando seleccionas**Exterior**desde el**Contra parpadeo**lista, puede seleccionar**Prioridad de obturador**como modo de exposición. ◇ El modelo de exposición puede diferir según los diferentes modelos de Access Controller.
Obturador	La persiana es un dispositivo que deja pasar la luz durante un período determinado. Cuanto mayor sea la velocidad de obturación, más corto será el tiempo de exposición y más oscura será la imagen.
Ganar	Cuando se establece el rango del valor de ganancia, se mejorará la calidad del video.
Compensación de exposición	Puede hacer que una foto sea más brillante o más oscura ajustando el valor de compensación de exposición.
Reducción de ruido 3D	Cuando la Reducción de ruido 3D (RD) está activada, el ruido del vídeo se puede reducir para garantizar vídeos de alta definición. Puede establecer su calificación cuando esta función está activada.
Calificación	

3.8.2 Configuración del volumen

Puede ajustar el volumen del altavoz.

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Configuración de vídeo**>**Configuración de volumen**.

Paso 3 Arrastre el control deslizante para ajustar el volumen. Hacer clic**DE**

Etapa 4 **ACUERDO**.

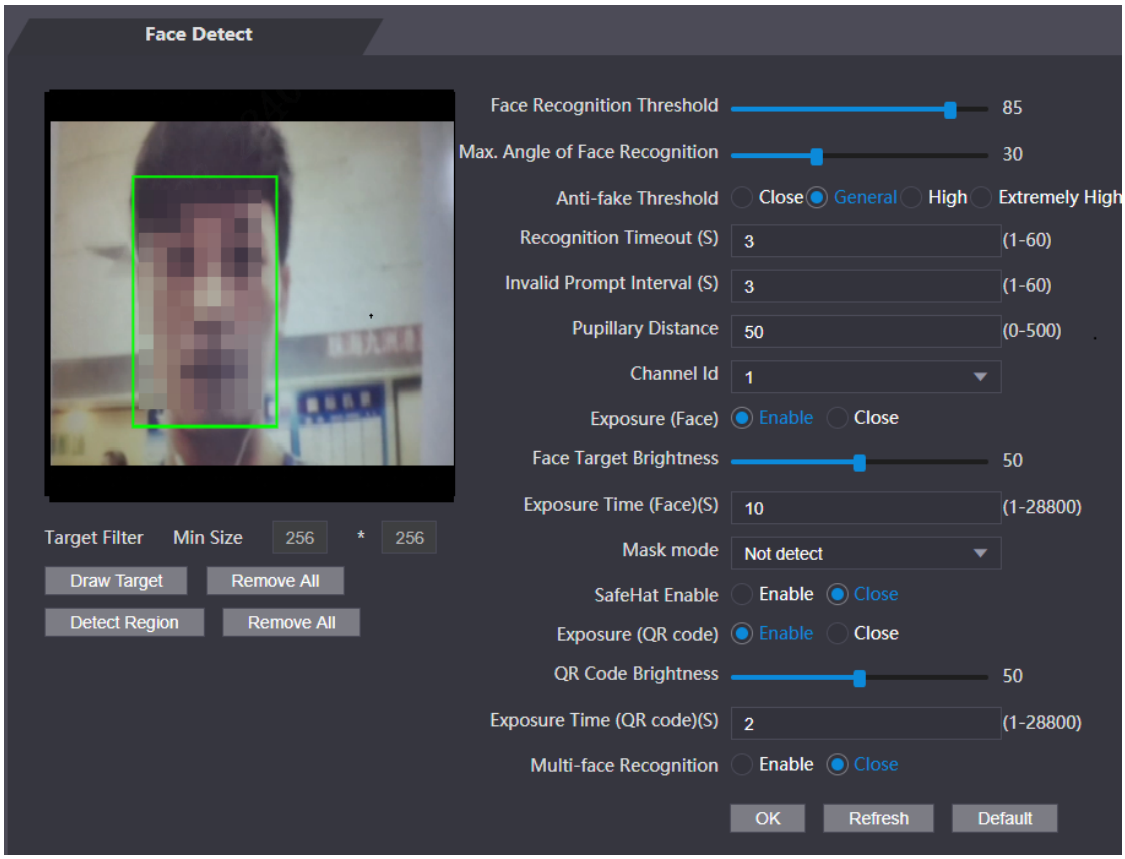
3.9 Configurar la detección de rostros

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

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Detección de rostros**.

Figura 3-24 Detección de rostro



Paso 3 Configure los parámetros.

Tabla 3-16 Descripción de los parámetros de detección de rostros

Parámetro	Descripción
Umbral facial	Ajuste la precisión del reconocimiento facial. Un umbral más alto significa una mayor precisión.
Máx. Ángulo de la cara	Establezca el ángulo máximo de pose del rostro para la detección de rostros. Un valor mayor significa un rango de ángulo de cara mayor. Si el ángulo de pose de la cara está fuera del rango definido, el cuadro de detección de caras no aparecerá.
Umbral antifalsificación	Evite el reconocimiento facial falso mediante el uso de una foto, video, máscara o un sustituto diferente del rostro de una persona autorizada. ● Cerrar: Desactiva esta función. ● General: un nivel normal de detección anti-spoofing significa una mayor tasa de acceso a las puertas para personas con máscaras faciales. ● Alto: Un nivel más alto de detección anti-spoofing significa mayor precisión y seguridad. ● Extremadamente alto: un nivel extremadamente alto de detección anti-suplantación de identidad significa una precisión y seguridad extremadamente altas.
Tiempo de espera de reconocimiento (S)	Si se reconoce correctamente el rostro de una persona con permiso de acceso, el controlador de acceso le indicará que el reconocimiento facial se realizó correctamente. Puede ingresar el tiempo del intervalo de solicitud.

Parámetro	Descripción
Intervalo de aviso facial no válido (S)	Si una persona sin permiso de acceso intenta desbloquear la puerta varias veces en el intervalo definido, el controlador de acceso indicará un fallo en el reconocimiento facial. Puede ingresar el tiempo del intervalo de solicitud.
Distancia pupilar	Las imágenes de rostros requieren los píxeles deseados entre los ojos (llamado distancia pupilar) para un reconocimiento exitoso. El píxel predeterminado es 45. El píxel cambia según el tamaño de la cara y la distancia entre las caras y la lente. Si un adulto está a 1,5 metros de la lente, la distancia pupilar puede ser de 50 px a 70 px.
Canal ID	1 es para la cámara de luz blanca y 2 es para la cámara de luz IR.
Exposición (cara)	Una vez habilitada la exposición facial, los rostros humanos serán más claros cuando el controlador de acceso se instale en exteriores.
Brillo del objetivo de la cara	El valor predeterminado es 50. Ajuste el brillo según sea necesario.
Tiempo de exposición	Después de que se detecta una cara, el Controlador de acceso emitirá luz para iluminar la cara y no volverá a emitir luz hasta que haya transcurrido el intervalo que usted configuró.
Modo máscara	● **No detectar**: La máscara no se detecta durante el reconocimiento facial. ● **Recordatorio de mascarilla**: La máscara se detecta durante el reconocimiento facial. Si la persona no usa mascarilla, el sistema le recordará que debe usarla y se le permitirá el acceso. ● **Intercepción de máscara**: La máscara se detecta durante el reconocimiento facial. Si una persona no lleva mascarilla, el sistema le recordará que la use y se le negará el acceso.
Exposición (código QR)	Cuando el controlador de acceso se instala en exteriores, el código QR será más claro según el brillo definido del código QR cuando lo escanee.
Código QR Brillo	
Tiempo de exposición (código QR) (S)	Después de escanear un código QR, el Controlador de acceso emitirá una luz para iluminar el código QR y el Controlador de acceso no volverá a emitir luz hasta que haya transcurrido el tiempo de exposición definido.
Reconocimiento multicara	Admite la detección de 4 imágenes de rostros al mismo tiempo y el modo de combinaciones de desbloqueo deja de ser válido. La puerta se desbloquea después de que cualquiera de ellos obtenga acceso.

Etapa 4 Dibuja el área de detección de rostros.

1. Haga clic**Detectar región**,
2. Haga clic derecho para dibujar el área de detección y luego suelte el botón izquierdo del mouse para completar el dibujo.

   Se detectará el rostro en el área definida. Dibuja el

Paso 5 tamaño del objetivo.

1) Haga clic**Dibujar objetivo**

2) Haga clic derecho para dibujar el cuadro de reconocimiento facial para definir el tamaño mínimo del rostro detectado.

Sólo cuando el tamaño de la cara es mayor que el tamaño definido, el controlador de acceso puede detectar la cara.

Paso 6 Hacer clic**DE ACUERDO**.

3.10 Configuración de la red

3.10.1 Configuración de TCP/IP

Debe configurar la dirección IP del controlador de acceso para asegurarse de que pueda comunicarse con otros dispositivos.

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

Paso 2 Configurar parámetros.

Figura 3-25 TCP/IP

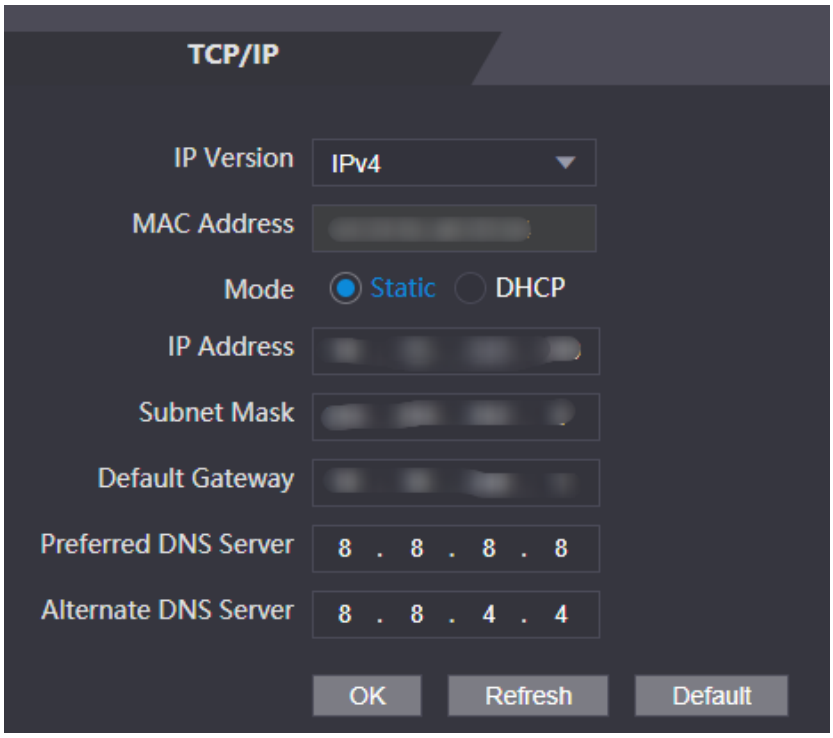


Tabla 3-17 Descripción de TCP/IP

Parámetro	Descripción
Versión IP	IPv4
Dirección MAC	Dirección MAC del controlador de acceso.
Modo	● **Estático**: ingrese manualmente la dirección IP, la máscara de subred y la puerta de enlace. ● **DHCP**: Significa Protocolo de configuración dinámica de host. Cuando DHCP está activado, al controlador de acceso se le asignará automáticamente la dirección IP, la máscara de subred y la puerta de enlace.
Dirección IP	Si selecciona el modo estático, configure la dirección IP, la máscara de subred y la puerta de enlace.
Máscara de subred	

Parámetro	Descripción
Puerta de enlace predeterminada	La dirección IP y la puerta de enlace deben estar en el mismo segmento de red.
DNS preferido	Establezca la dirección IP del servidor DNS preferido.
DNS alternativo	Establezca la dirección IP del servidor DNS alternativo.

Paso 3 Hacer clic**DE ACUERDO**.

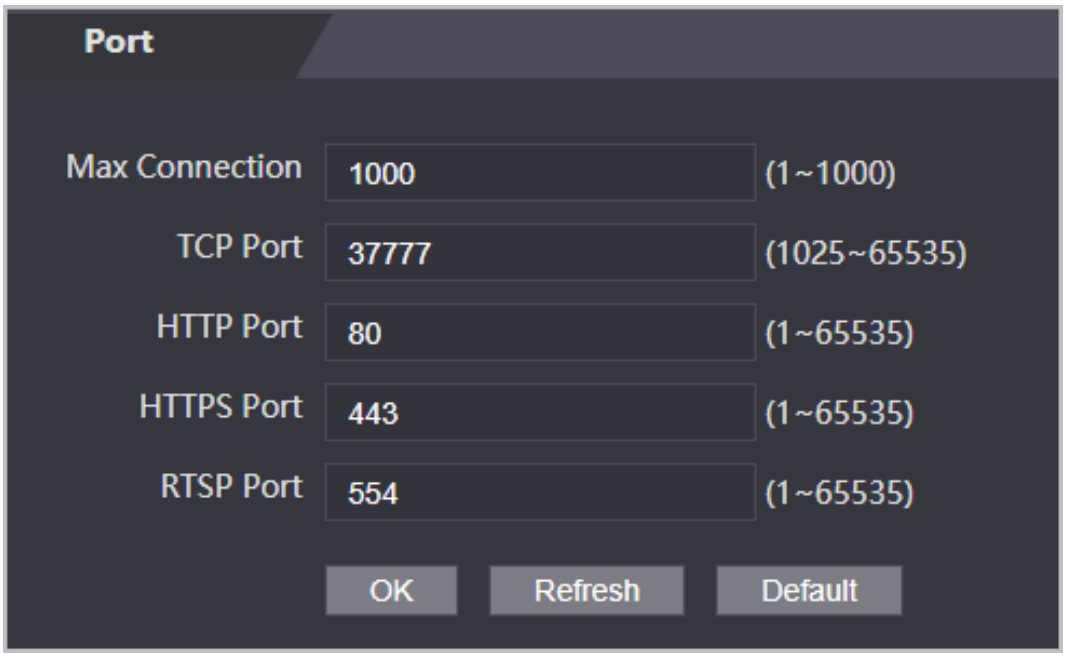
3.10.2 Configuración del puerto

Puede limitar el acceso al controlador de acceso al mismo tiempo a través de la web, el cliente de escritorio y el teléfono. Paso 1

Seleccionar**Configuración de red**>**Puerto**.

Paso 2 Configure los números de puerto.

Figura 3-26 Configurar puertos



Excepto**Conexión máxima**y**Puerto RTSP**, debe reiniciar el controlador de acceso para realizar las configuraciones serán efectivas después de cambiar otros parámetros.

Tabla 3-18 Descripción de puertos

Parámetro	Descripción
Conexión máxima	Puede establecer la cantidad máxima de clientes (como web, cliente de escritorio y teléfono) que pueden acceder al controlador de acceso al mismo tiempo.
Puerto TCP	El valor predeterminado es 37777.
Puerto HTTP	El valor predeterminado es 80. Si desea cambiar el número de puerto, agregue el nuevo número de puerto después de la dirección IP cuando inicie sesión en la página web.
Puerto HTTPS	El valor predeterminado es 443.
Puerto RTSP	El valor predeterminado es 554.

Paso 3 Hacer clicDE ACUERDO.

3.10.3 Configurar el registro automático

El Controlador de acceso informa su dirección al servidor designado para que usted pueda obtener acceso al Controlador de acceso a través de la plataforma de administración.

Paso 1 En la página de inicio, seleccione**Configuración de red**>**Registro**.

Paso 2 Habilite la función de registro automático y configure los parámetros.

Figura 3-27 Registro

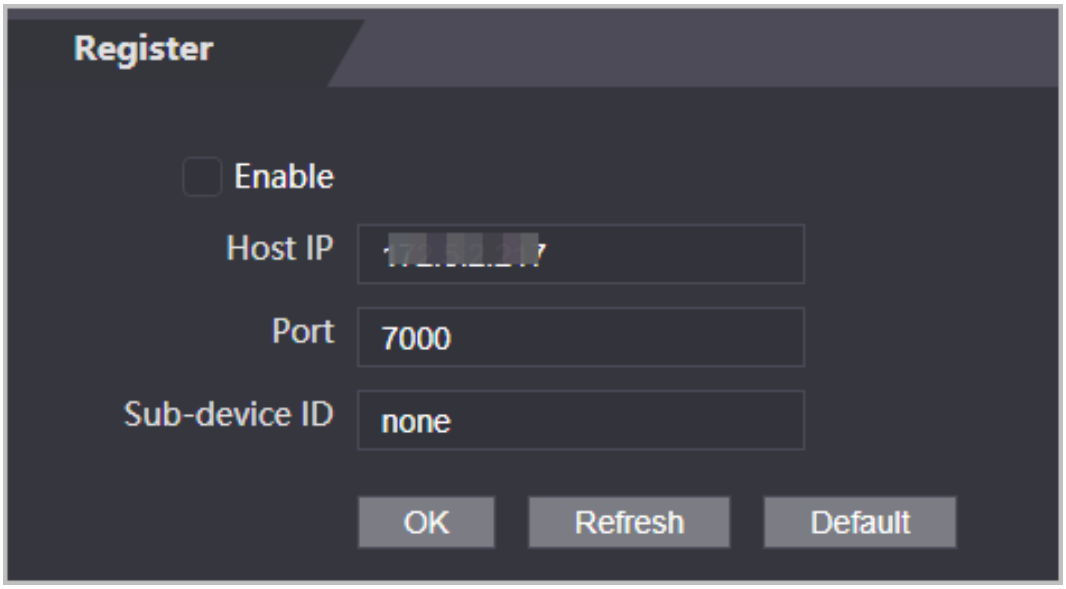


Tabla 3-19 Descripción del registro automático

Parámetro	Descripción
IP del host	La dirección IP o el nombre de dominio del servidor.
Puerto	El puerto del servidor utilizado para el registro automático.
ID de subdispositivo	Ingrese la ID del subdispositivo (definida por el usuario). Cuando agrega el controlador de acceso a la plataforma de administración, El ID del subdispositivo en la plataforma de gestión debe cumplir con el ID del subdispositivo definido en el controlador de acceso.

Paso 3 Hacer clic**Aplicar**.

3.10.4 Configuración del servicio en la nube

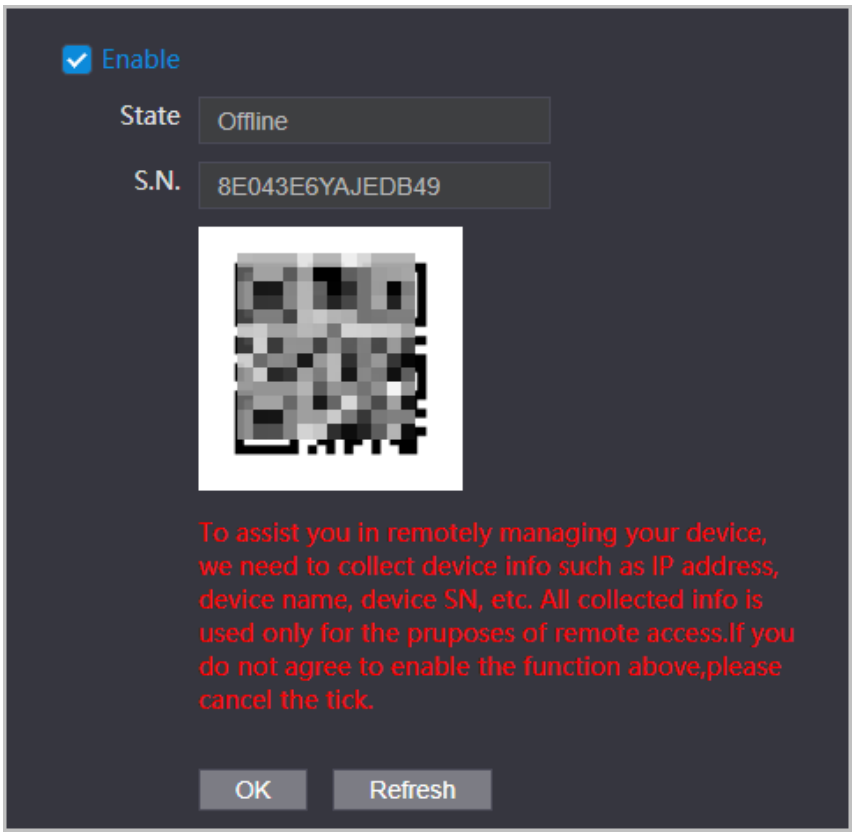
El servicio en la nube proporciona un servicio de penetración NAT. Los usuarios pueden administrar múltiples dispositivos a través de DMSS. No es necesario solicitar un nombre de dominio dinámico, configurar la asignación de puertos o implementar el servidor.

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración de red**>**Servicio de almacenamiento en la**

Paso 2 **nube**. Active la función del servicio en la nube.

Figura 3-28 Servicio en la nube



Paso 3 Hacer clic**DE ACUERDO**.

Operaciones relacionadas

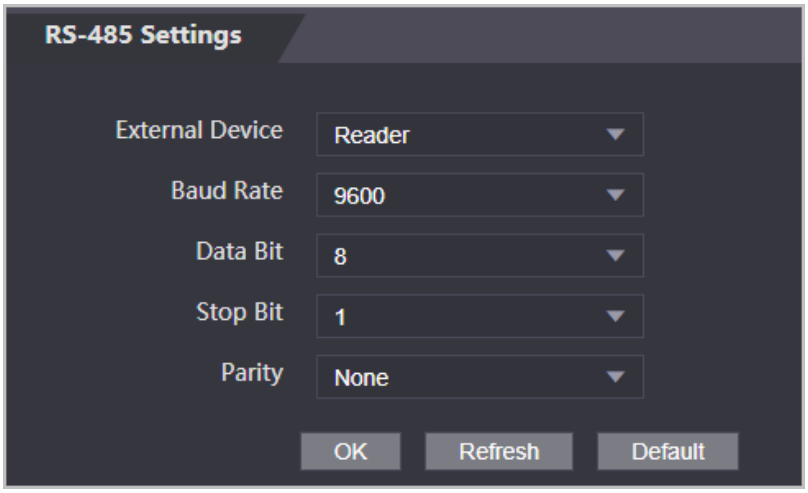
Descargue DMSS y regístrese, puede escanear el código QR a través de DMSS para agregarle el controlador de acceso.

3.10.5 Configuración del puerto serie

Paso 1 En la página de inicio, seleccione**Configuración de red**>**Configuración del puerto serie Wiegand**.

Paso 2 Seleccione un tipo de puerto.

Figura 3-29 Puerto serie



- Seleccionar**Lector**cuando el controlador de acceso se conecta a un lector de tarjetas.
- Seleccionar**Controlador**cuando el controlador de acceso funciona como lector de tarjetas y el controlador de acceso

El Controlador enviará datos al Controlador de Acceso para controlar el acceso. Tipo de datos de salida:

- ◇ Tarjeta: genera datos basados en el número de tarjeta cuando los usuarios deslizan la tarjeta para desbloquear la puerta; genera datos basados en el primer número de tarjeta del usuario cuando utiliza otros métodos de desbloqueo.
- ◇ No.: genera datos basados en la identificación del usuario.

- Seleccionar**Lector (OSDP)**cuando el controlador de acceso está conectado a un lector de tarjetas basado en el protocolo OSDP.
- Módulo de seguridad: cuando se conecta un módulo de seguridad, el botón de salida y el bloqueo no serán efectivos.

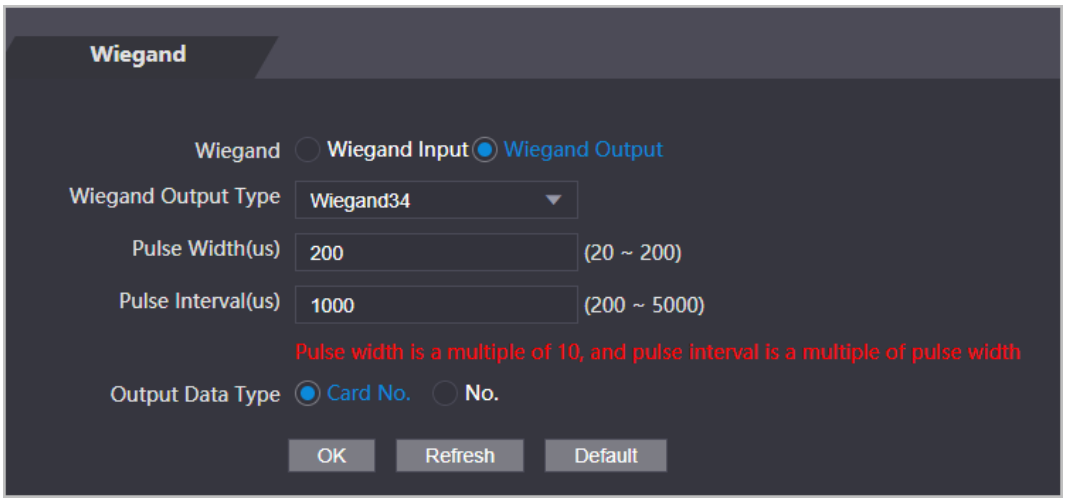
3.10.6 Configuración de Wiegand

El controlador de acceso permite el modo de entrada y salida Wiegand.

Paso 1 Sobre el**Menú principal**, seleccionar**Conexión**>**Wiegand**.

Paso 2 Seleccione un Wiegand.

Figura 3-30 Salida Wiegand



- Seleccionar**Entrada Wiegand**cuando conecta un lector de tarjetas externo al controlador de acceso.
- Seleccionar**Salida Wiegand**cuando el Controlador de Acceso funciona como un lector de tarjetas y necesita conectarlo a un controlador u otro terminal de acceso.

Tabla 3-20 Descripción de la salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	Seleccione un formato Wiegand para leer números de tarjetas o números de identificación. ● **Wiegand26**: Lee tres bytes o seis dígitos. ● **Wiegand34**: Lee cuatro bytes u ocho dígitos. ● **Wiegand66**: Lee ocho bytes o dieciséis dígitos.
Ancho de pulso	Ingrese el ancho del pulso y el intervalo de pulso de la salida Wiegand.
Intervalo de pulso	
Tipo de datos de salida	Seleccione el tipo de datos de salida. ● **No.**: genera datos basados en el ID de usuario. ● **Número de tarjeta**: Genera datos basados en el primer número de tarjeta del usuario.

3.11 Gestión de seguridad

3.11.1 Configurar la autoridad IP

Paso 1 Inicie sesión en la página web.

Paso 2 Hacer clic**Gestión de seguridad.**>**Autoridad de propiedad intelectual**.

Paso 3 Seleccione un modo de ciberseguridad del**Tipo**lista.

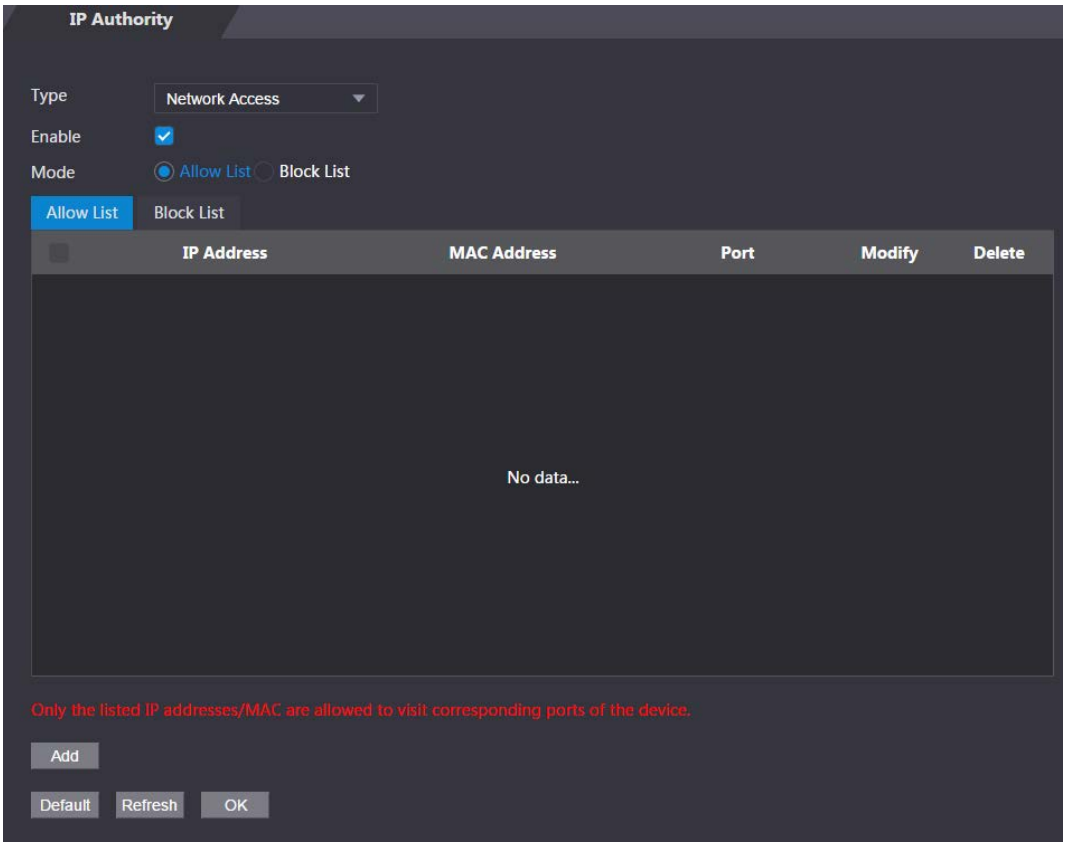
- **Acceso a la red**: establece la lista de permitidos y la lista de bloqueo para controlar el acceso al controlador de acceso.
- **Prohibir PING**: Permitir**ping prohibido**función, y el controlador de acceso no responderá a la solicitud de ping.
- **Anti media conexión**: Permitir**Anti media conexión**funciona, y el controlador de acceso aún puede funcionar correctamente bajo un ataque de media conexión.

3.11.1.1 Acceso a la red

Paso 1 Seleccionar**Acceso a la red**desde el**Tipo**lista. Selecciona

Paso 2 el**Permitir**casilla de verificación.

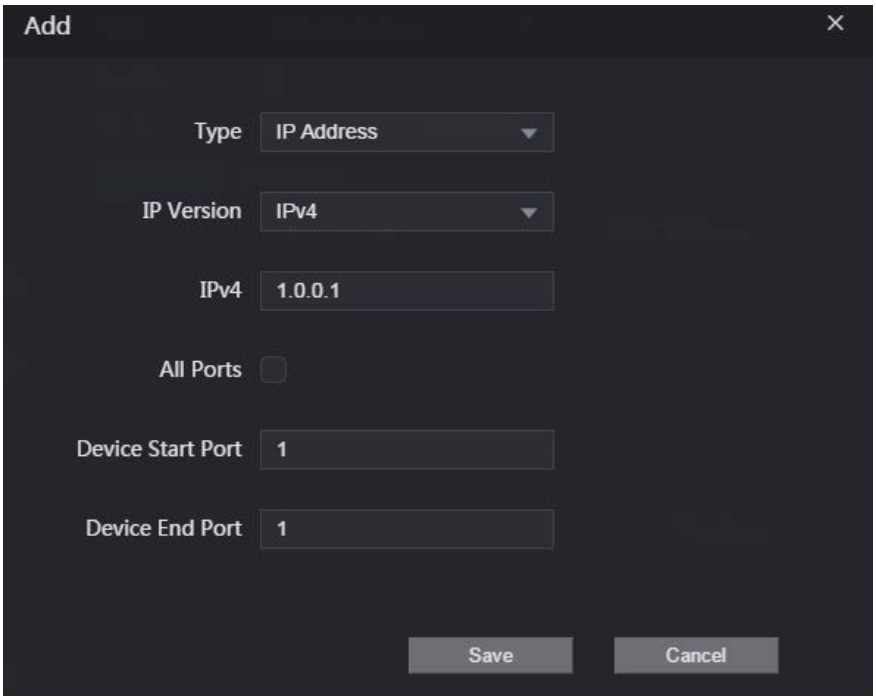
Figura 3-31 Acceso a la red



Paso 3 Seleccionar**Lista de permitidos**o**Lista de bloqueos**.

Etapa 4 Hacer clic**Agregar**.

Figura 3-32 Agregar IP



Paso 5 Configurar parámetros.

Tabla 3-21 Descripción de cómo agregar parámetros IP

Parámetro	Descripción
Tipo	Seleccione el tipo de dirección de la**Tipo**lista.
Versión IP	IPv4 por defecto.
Todos los puertos	Seleccionar**Todos los puertos**casilla de verificación y su configuración se aplicará a todos los puertos.
Puerto de inicio del dispositivo	si limpias**Todos los puertos**casilla de verificación, configure el puerto de inicio y el puerto final del dispositivo.
Puerto final del dispositivo	

Paso 6 Hacer clic**Ahorrar**, y el**Autoridad de propiedad intelectual**Se muestra la interfaz. Hacer clic

Paso 7 **DE ACUERDO**.

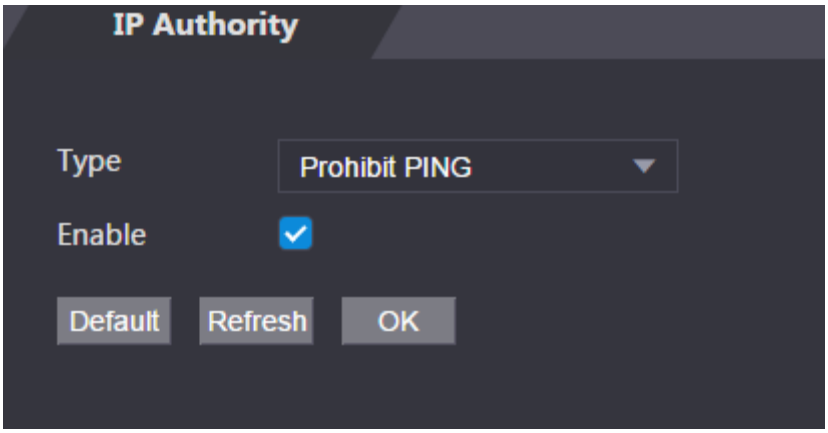
- Hacer clic para editar la lista de permitidos o bloqueados.
- Hacer clic para eliminar la lista de permitidos o bloqueados

3.11.1.2 Prohibir PING

Paso 1 Seleccionar**Prohibir PING**desde el**Tipo**lista.

Paso 2 Selecciona el**Permitir**casilla de verificación.

Figura 3-33 Prohibir PING



Paso 3 Hacer clic**DE ACUERDO**.

3.11.1.3 Anti-media conexión

Paso 1 Selecciona el**Anti media conexión**desde el**Tipo**lista. Selecciona el

Paso 2 **Permitir**casilla de verificación. Hacer clic**DE ACUERDO**.

Paso 3

3.11.2 Configuración del sistema

Paso 1 Inicie sesión en la interfaz web.

Paso 2 Seleccionar**Gestión de seguridad.**>**Servicio del sistema**. Habilite o

Paso 3 deshabilite los servicios del sistema según sea necesario.

Figura 3-34 Servicio del sistema

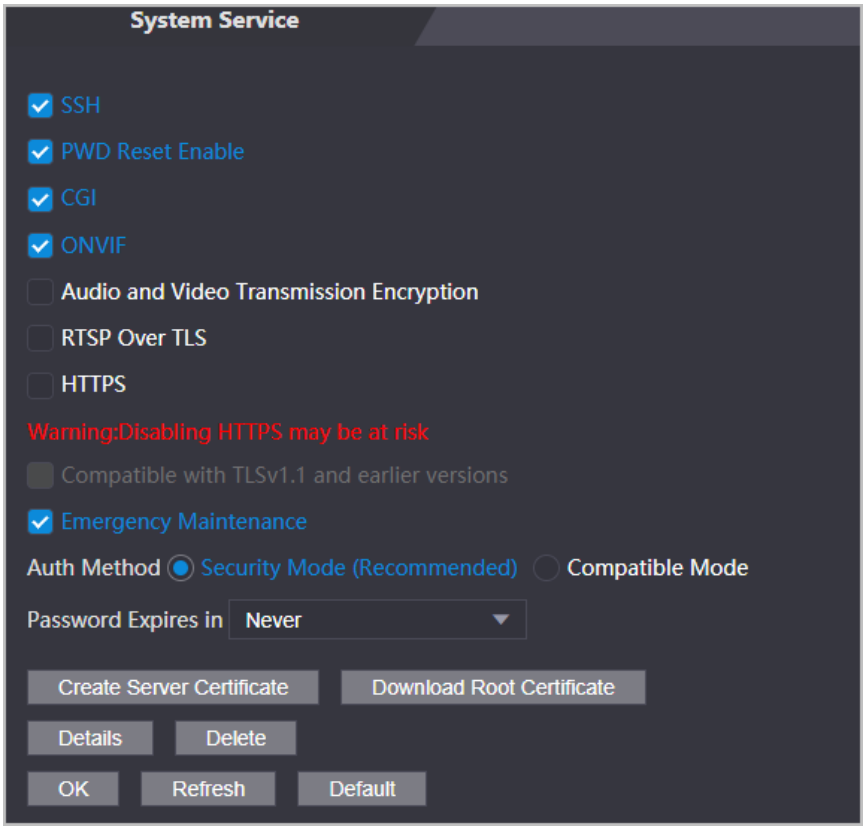


Tabla 3-22 Descripción del servicio del sistema

Parámetro	Descripción
SSH	Secure Shell (SSH) es un protocolo de red criptográfico para operar servicios de red de forma segura a través de una red no segura. Cuando SSH está habilitado, SSH proporciona un servicio criptográfico para la transmisión de datos.
Habilitar reinicio de PWD	Si está habilitado, puede restablecer la contraseña. Esta función está habilitada de forma predeterminada.
CGI	Common Gateway Interface (CGI) ofrece un protocolo estándar para que los servidores web ejecuten programas de manera similar a las aplicaciones de consola que se ejecutan en un servidor que genera páginas web dinámicamente. Cuando CGI está habilitado, se pueden utilizar comandos CGI. El CGI está habilitado de forma predeterminada.
ONVIF	Permita que otros dispositivos extraigan la transmisión de video del VTO a través del protocolo ONVIF.
Audio y video Transmisión Cifrado	Si esta función está habilitada, la transmisión de audio y video se cifra automáticamente.
RTSP sobre TLS	Si esta función está habilitada, la transmisión de audio y video se cifra mediante el protocolo RTSP.
HTTPS	El Protocolo seguro de transferencia de hipertexto (HTTPS) es un protocolo para la comunicación segura a través de una red informática. Cuando HTTPS está habilitado, HTTPS se utilizará para acceder a los comandos CGI; de lo contrario, se utilizará HTTP.
Compatible con TLSv1.1 y anteriores versiones	Habilite esta función si su navegador utiliza TLS V1.1 o versiones anteriores.
Emergencia Mantenimiento	Habilítelo para análisis de fallas y mantenimiento.
Método de autenticación	Te recomendamos seleccionar el modo de seguridad.

Etapa 4 Hacer clic**DE ACUERDO**.

3.11.2.1 Creación de certificado de servidor

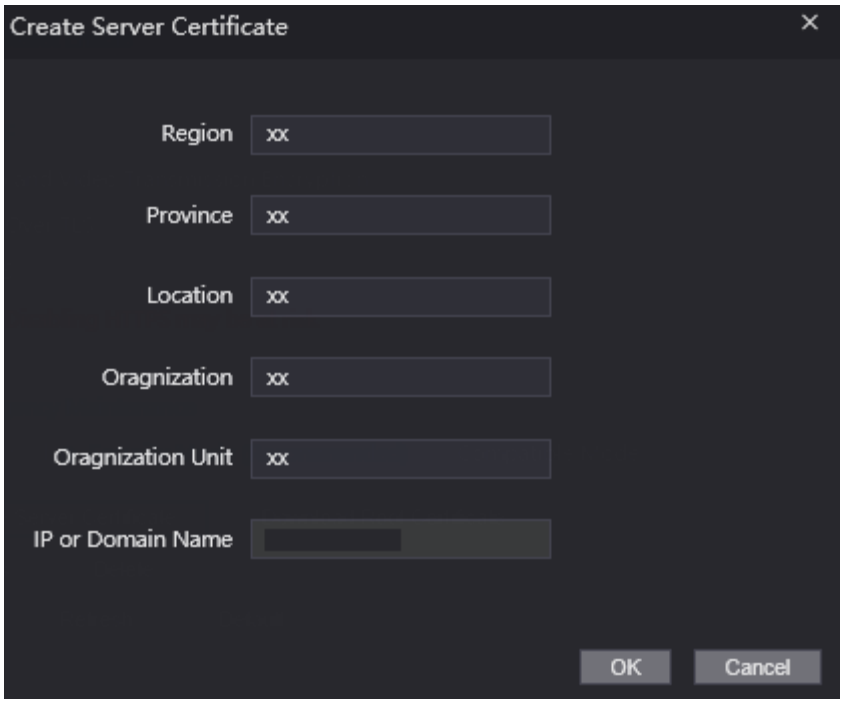
Configure el servidor HTTPS para mejorar la seguridad de su sitio web con un certificado de servidor.

- Si utiliza HTTPS por primera vez o se cambia la dirección IP del controlador de acceso, cree una certificado del servidor e instale un certificado raíz.
- Si utiliza otra computadora para iniciar sesión en la página web del Controlador de acceso, debe descargue e instale el certificado raíz nuevamente en la nueva computadora o copie el certificado raíz al eso.

Paso 1 Sobre el**Servicio del sistema**página, haga clic**Crear certificado de servidor**.

Paso 2 Ingrese la información y haga clic**DE ACUERDO**. El controlador de acceso se reiniciará.

Figura 3-35 Crear certificado de servidor

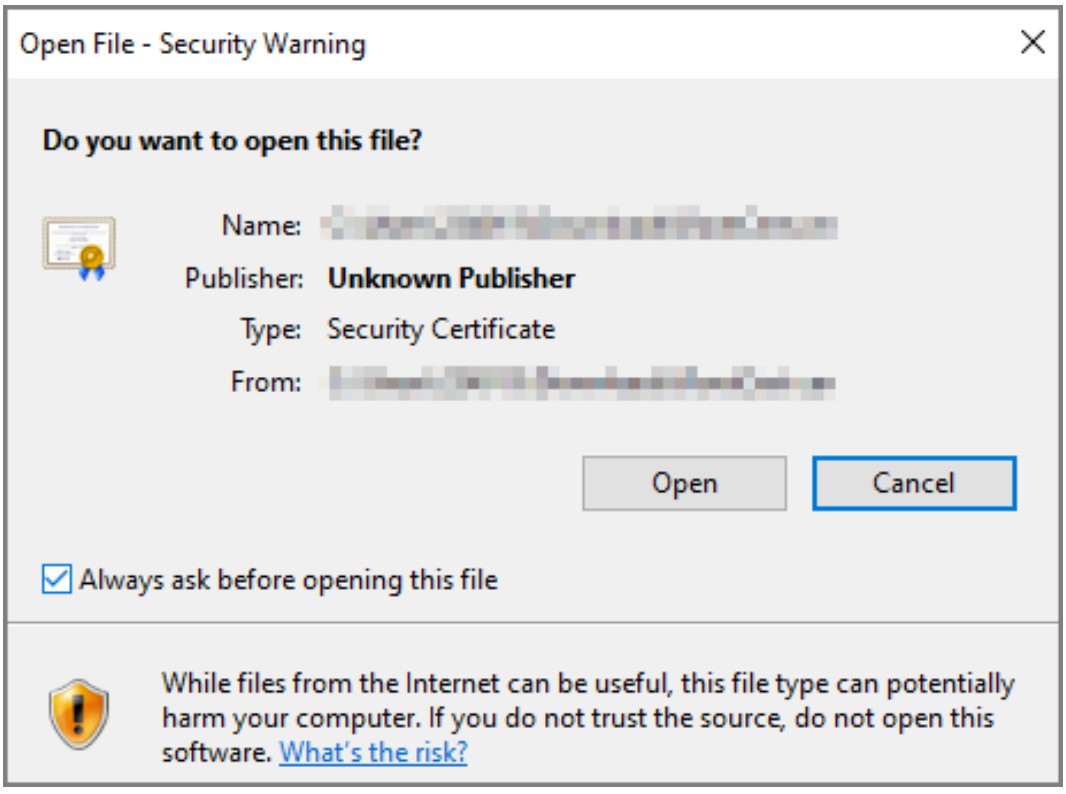


3.11.2.2 Descarga del certificado raíz

Paso 1 Sobre el**Servicio del sistema**página, haga clic**Descargar certificado raíz**. Haga

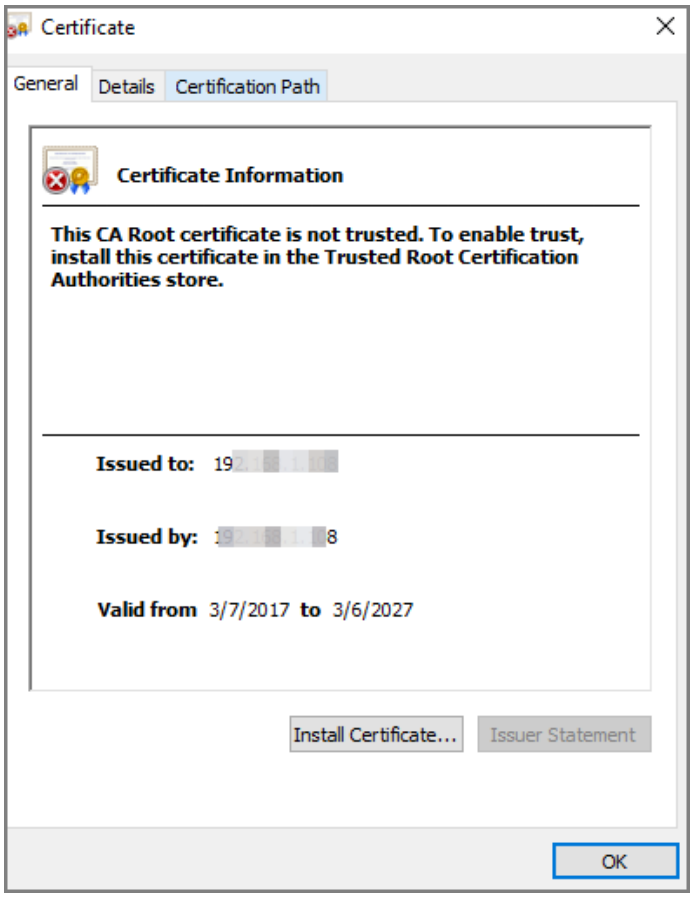
Paso 2 doble clic en el archivo que ha descargado y luego haga clic en**Abierto**.

Figura 3-36 Descarga de archivos



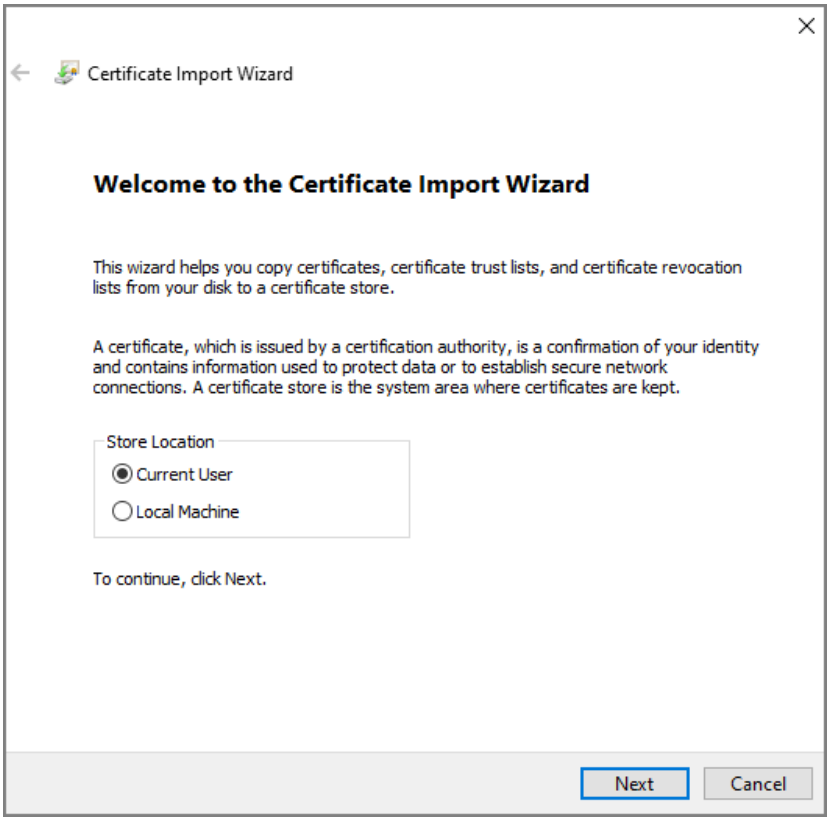
Paso 3 Hacer clic**Instalar certificado**.

Figura 3-37 Información del certificado



Etapa 4 Seleccionar**Usuario actual**o**Máquina local**y luego haga clic en**Próximo**.

Figura 3-38 Asistente de importación de certificados (1)

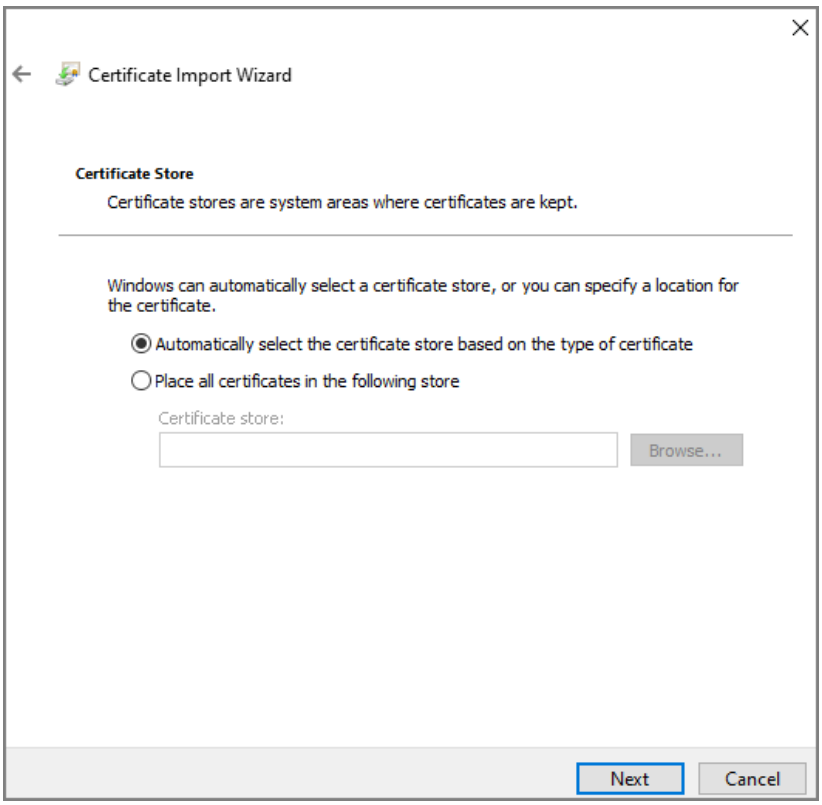


Paso 5 Seleccione la ubicación de almacenamiento adecuada.

1) Seleccionar**Coloque todos los certificados en la siguiente tienda.**.

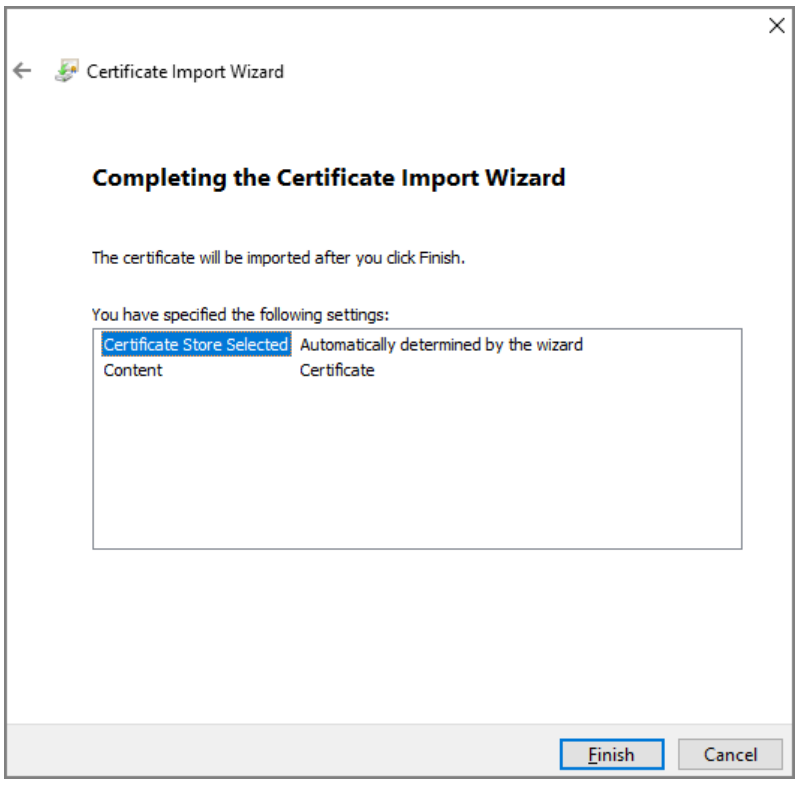
2) Haga clic**Navegar**para importar el certificado al**Autoridades de certificación raíz de confianza** almacenar y luego haga clic en**Próximo**.

Figura 3-39 Asistente de importación de certificados (2)



Paso 6 Hacer clic**Finalizar**.

Figura 3-40 Asistente de importación de certificados (3)



3.12 Gestión de usuarios

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

3.12.1 Agregar usuarios

Puede agregar nuevos usuarios y luego podrán iniciar sesión en la página web del Controlador de acceso.

Procedimiento

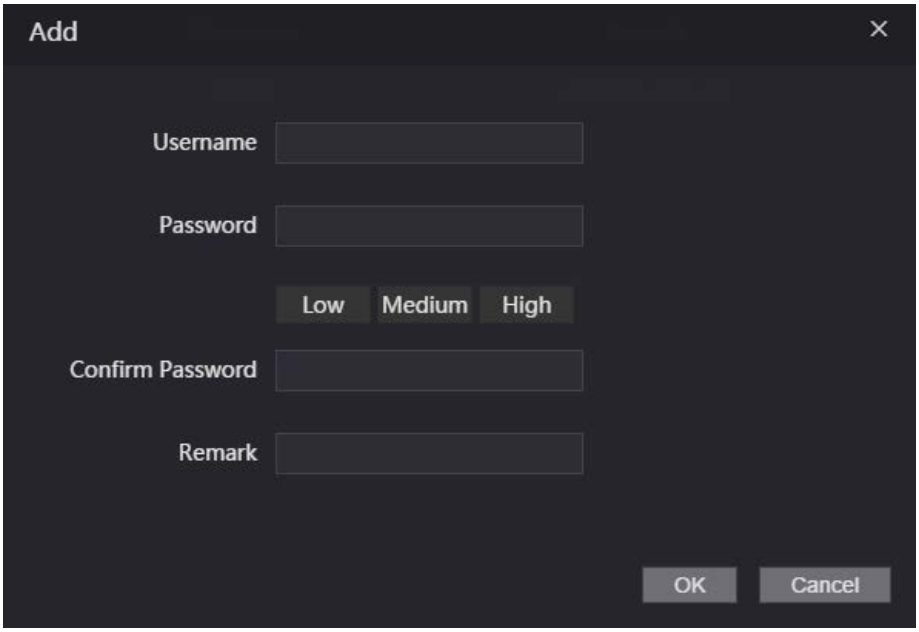
Paso 1 En la página de inicio, seleccione**Gestión de usuarios.**>**Gestión de usuarios.**

Paso 2 . Hacer clic**Agregar**e ingrese la información del usuario.

- El nombre de usuario no puede ser el mismo que el de la cuenta existente. El nombre de usuario consta de hasta a 31 caracteres y solo permite números, letras, guiones bajos, líneas medias, puntos o @.
- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y especiales caracteres (excluyendo ' " ; : &).

  Establezca una contraseña de alta seguridad siguiendo las instrucciones de seguridad de la contraseña.

Figura 3-41 Agregar usuario



Paso 3 Hacer clic**DE ACUERDO**.

Sólo la cuenta de administrador puede cambiar la contraseña y la cuenta de administrador no se puede eliminar.

3.12.2 Agregar usuarios ONVIF

Open Network Video Interface Forum (ONVIF), un foro industrial global y abierto que se establece para el desarrollo de un estándar abierto global para la interfaz de productos de seguridad físicos basados en IP, que permite la compatibilidad de diferentes fabricantes. Los usuarios de ONVIF tienen su

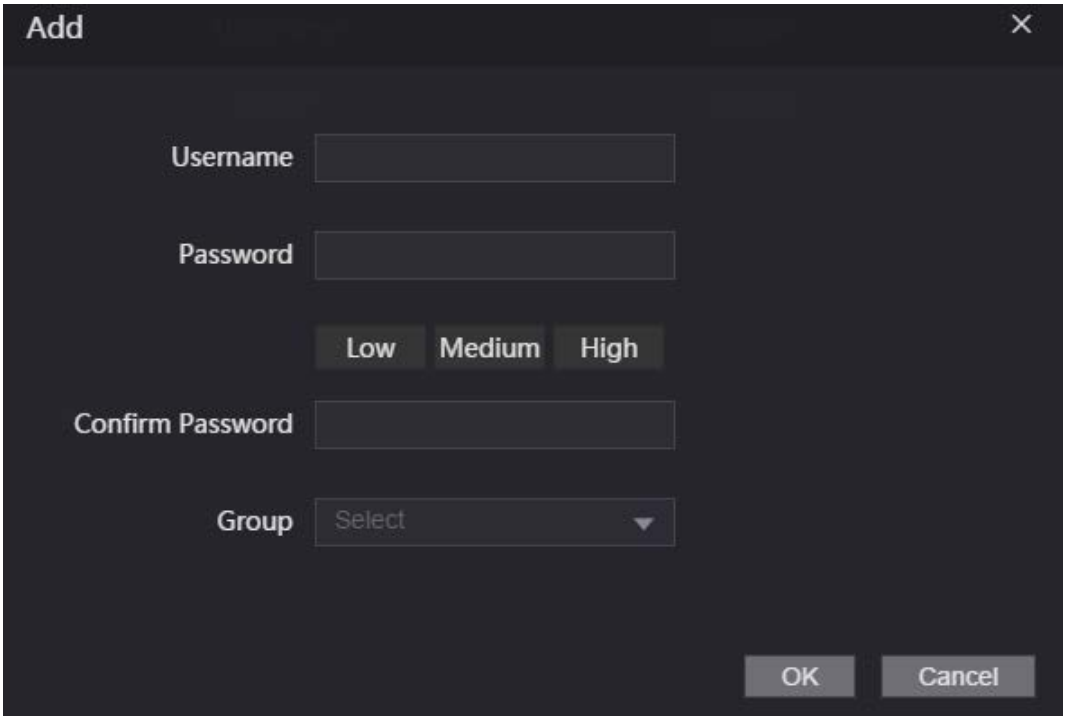
identidades verificadas a través del protocolo ONVIF. El usuario ONVIF predeterminado es administrador.

Procedimiento

Paso 1 En la página de inicio, seleccione**Gestión de usuarios**.>**Usuario Onvif**.

Paso 2 Hacer clic**Agregar**y luego configurar los parámetros.

Figura 3-42 Agregar usuario ONVIF



Paso 3 Hacer clic**DE ACUERDO**.

3.12.3 Visualización de usuarios en línea

Puede ver los usuarios en línea que actualmente inician sesión en la página web. En la página de inicio, seleccione**Usuario en línea**.

3.13 Configuración de indicaciones de voz

Configure mensajes de voz durante la verificación de identidad.

Paso 1 En la página de inicio, seleccione**Audio personalizado**

Paso 2 . Seleccione un mensaje rápido de la**Tipo**lista

Paso 3 Hacer clic**Navegar**para seleccionar un archivo de audio y luego haga clic en**Subir**.

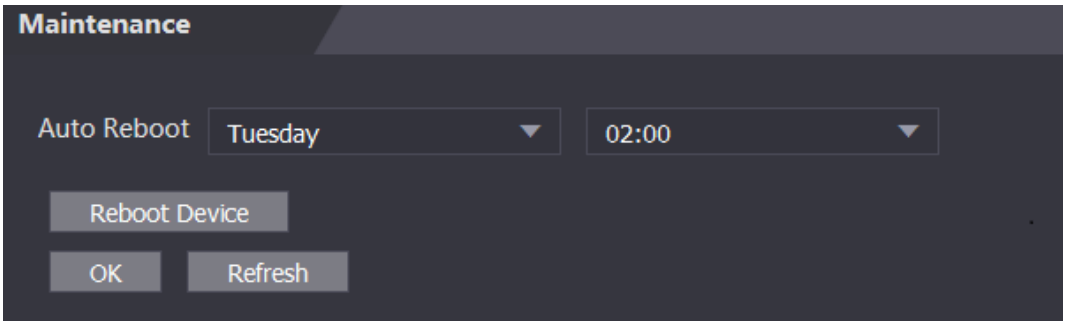
3.14 Mantenimiento

Puede reiniciar periódicamente el controlador de acceso durante el tiempo de inactividad para mejorar su rendimiento.

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Mantenimiento**.

Figura 3-43 Mantenimiento



Paso 3 Establezca la hora y luego haga clic**DE ACUERDO**.

Etapa 4 (Opcional) Haga clic**Reiniciar dispositivo**, el controlador de acceso se reiniciará inmediatamente.

3.15 Gestión de configuración

Cuando más de un controlador de acceso necesita las mismas configuraciones, puede configurar sus parámetros importando o exportando archivos de configuración.

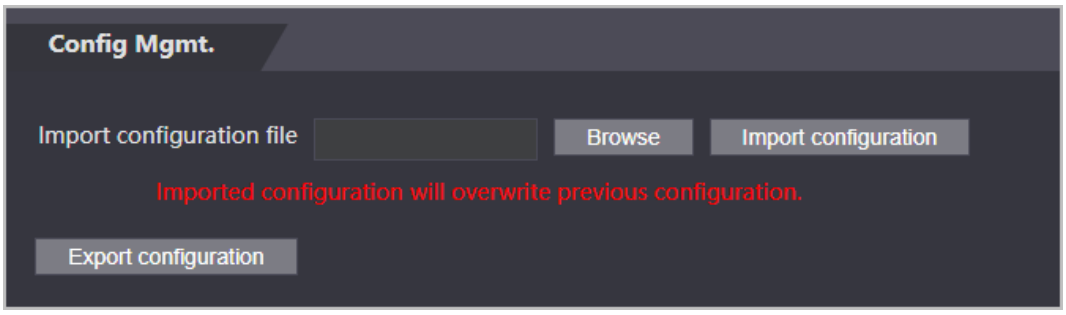
3.15.1 Exportar/Importar archivos de configuración

Puede importar o exportar el archivo de configuración del Access Controller. Cuando desee aplicar las mismas configuraciones a varios dispositivos, puede importarles el archivo de configuración.

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Gestión de configuración.**>**Gestión de configuración.**.

Figura 3-44 Gestión de configuración



Paso 3 Exportar o importar archivos de configuración.

- Exportar archivo de configuración.

  Hacer clic**Configuración de exportación**para descargar el archivo al local.

  La propiedad intelectual no se exportará.

- Importar archivo de configuración.

  1. Haga clic**Navegar**para seleccionar el archivo de configuración.
  2. Haga clic**Importar configuración**.

El archivo de configuración solo se puede importar al dispositivo con el mismo modelo.

3.15.2 Restauración de los valores predeterminados de fábrica

Restaurando el**Controlador de acceso**Las configuraciones predeterminadas provocarán la pérdida de datos. Por favor tenga en cuenta.

Paso 1 Seleccionar**Gestión de configuración.**>**Por defecto** Restaure los

Paso 2 valores predeterminados de fábrica si es necesario.

- **Restaurar fábrica**: Restablece las configuraciones del controlador de acceso y elimina todos los datos.
- **Restaurar fábrica (guardar usuario y registro)**: Restablece las configuraciones del Controlador de acceso y elimina todos los datos excepto la información y los registros del usuario.

3.16 Sistema de actualización

- Utilice el archivo de actualización correcto. Asegúrese de obtener el archivo de actualización correcto del soporte técnico.
- No desconecte la fuente de alimentación o la red, ni reinicie o apague el controlador de acceso. durante la actualización.

3.16.1 Actualización de archivos

Paso 1 En la página de inicio, seleccione**Mejora**.

Paso 2 En el**Actualización de archivos**área, haga clic**Navegar**y luego cargue el archivo de actualización.

El archivo de actualización debe ser un archivo .bin.

Paso 3 Hacer clic**Actualizar**.

El controlador de acceso se reiniciará una vez completada la actualización.

3.16.2 Actualización en línea

Paso 1 En la página de inicio, seleccione**Mejora**.

Paso 2 En el**Actualización en línea**área, seleccione un método de actualización.

- Seleccionar**Verificación automática**, el controlador de acceso comprobará automáticamente si la última versión está disponible.
- Seleccionar**Verificación manual**, y podrá comprobar inmediatamente si la última versión está disponible.

Paso 3 Actualice el controlador de acceso cuando esté disponible la última versión.

3.17 Ver información de la versión

En la página de inicio, seleccione**Información de la versión**y podrá ver información de la versión, como el modelo del dispositivo, el número de serie, la versión del hardware, información legal y más.

3.18 Ver registros

Vea registros como registros del sistema, registros de administración y registros de desbloqueo.

3.18.1 Registros del sistema

Ver y buscar registros del sistema.

Paso 1 Inicie sesión en la página web. Seleccionar**Registro**

Paso 2 **del sistema**>**Registro del sistema**.

Paso 3 Seleccione el rango de tiempo y el tipo de registro y luego haga clic en**Consulta**. Hacer clic**Respaldo**para descargar el registro del sistema.

3.18.2 Registros de administración

Busque registros de administrador utilizando el ID de administrador.

Paso 1 Inicie sesión en la página web. Seleccionar**Registro del sistema**>

Paso 2 **Registro de administrador**. Introduzca el ID de administrador y

Paso 3 luego haga clic en**Consulta**.

3.18.3 Desbloqueo de registros

Busque registros de desbloqueo y expórtelos.

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Registro del sistema**>**Buscar registros**.

Paso 3 Seleccione el rango de tiempo y el tipo de registro y luego haga clic en**Consulta**.

Puedes hacer clic**Exportar datos**para descargar el registro.

3.18.4 Registros de alarmas

Ver registros de alarmas.

En la página de inicio, seleccione**Registro del sistema**>**Registro de alarmas**.

4 Configuración inteligente de PSS Lite

Esta sección presenta cómo administrar y configurar el controlador de acceso a través de Smart PSS Lite. También puede configurar reglas de tiempo de asistencia en la plataforma, como turnos, modos, horarios y más. Para obtener más información, consulte el manual del usuario de Smart PSS Lite.

4.1 Instalación e inicio de sesión

Instale e inicie sesión en Smart PSS Lite. Para obtener más información, consulte el manual de usuario de Smart PSS Lite.

Paso 1 Obtenga el paquete de software del Smart PSS Lite del soporte técnico y luego instale y ejecute el software según las instrucciones.

Paso 2 Inicialice Smart PSS Lite cuando inicie sesión por primera vez, incluida la configuración de contraseña y preguntas de seguridad.

Configure la contraseña para el primer uso y luego configure preguntas de seguridad para restablecer su contraseña cuando la olvidaste.

Paso 3 Ingrese su nombre de usuario y contraseña para iniciar sesión en Smart PSS Lite.

4.2 Agregar dispositivos

Debe agregar el controlador de acceso a Smart PSS Lite. Puedes agregarlos en lotes o individualmente.

4.2.1 Agregar individualmente

Puede agregar Access Controller individualmente ingresando sus direcciones IP o nombres de dominio.

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Administrador de dispositivos**y haga clic

Paso 3 **Agregar**. Ingrese la información del dispositivo.

Figura 4-1 Información del dispositivo

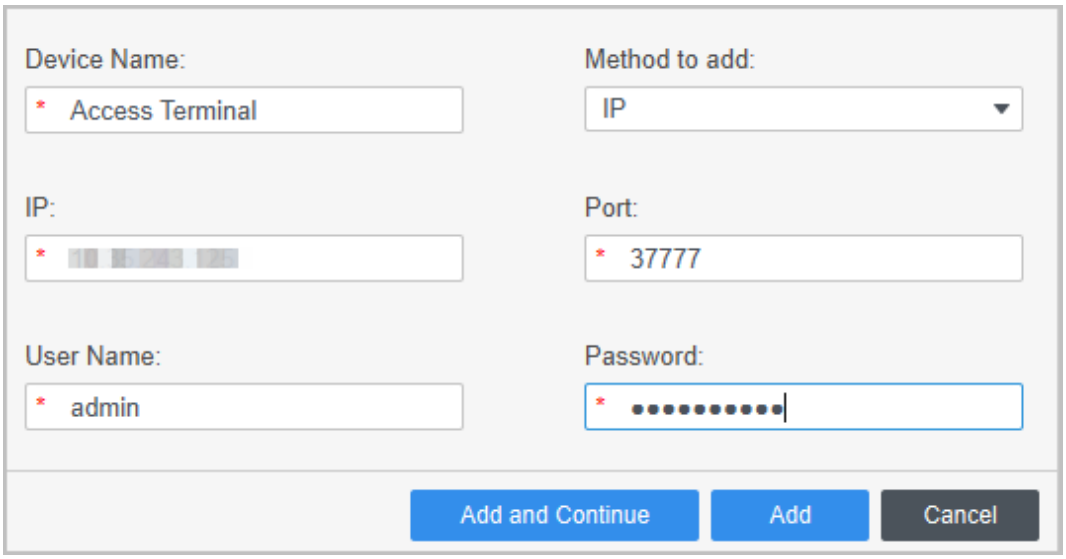


Tabla 4-1 Parámetros del dispositivo Descripción

Parámetro	Descripción
Nombre del dispositivo	Ingrese un nombre del controlador de acceso. Le recomendamos que le ponga el nombre de su área de instalación.
Método para agregar	Seleccionar**IP**para agregar el Terminal de acceso ingresando su dirección IP.
IP	Ingrese la dirección IP del controlador de acceso.
Puerto	El número de puerto es 37777 de forma predeterminada.
Usuario Contraseña	Ingrese el nombre de usuario y contraseña del Terminal de Acceso.

Etapa 4 Hacer clic**Agregar**.

El controlador de acceso agregado se muestra en la**Dispositivos**página. Puedes hacer clic**Agregar y continuar**para agregar más controladores de acceso.

4.2.2 Agregar en lotes

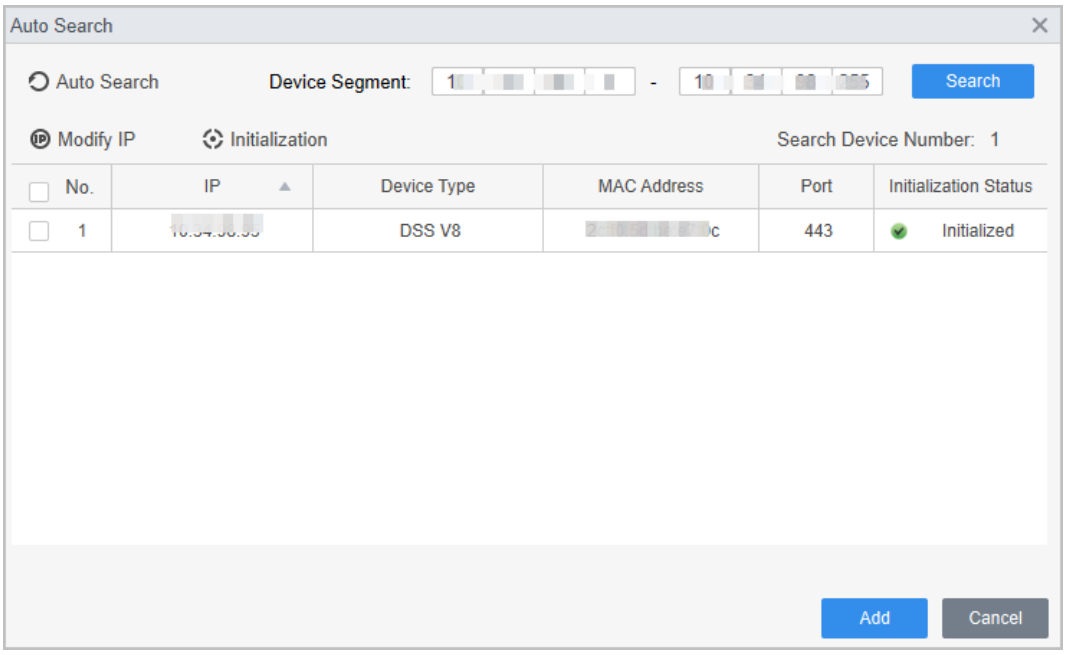
Le recomendamos que utilice la función de búsqueda automática cuando agregue controladores de acceso en lotes. Asegúrese de que los controladores de acceso que agregue estén en el mismo segmento de red. Paso 1

Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Administrador de dispositivos**y buscar dispositivos.

- Hacer clic**Auto búsqueda**, para buscar dispositivos en la misma LAN.
- Ingrese el rango del segmento de red y luego haga clic en**Buscar**.

Figura 4-2 Búsqueda automática



Se mostrará una lista de dispositivos.

Seleccione un dispositivo y luego haga clic en**Modificar IP**para modificar su dirección IP.

Paso 3 Seleccione el controlador de acceso que desea agregar a Smart PSS Lite y luego haga clic en**Agregar**.

Etapa 4 Ingrese el nombre de usuario y la contraseña del controlador de acceso.

Puede ver el controlador de acceso agregado en la página**Dispositivos**página.

El Access Controller inicia sesión automáticamente en Smart PSS Lite después de agregarlo.**En línea**es se muestra después de iniciar sesión correctamente.

4.3 Gestión de usuarios

Agregue usuarios, asígneles tarjetas y configure sus permisos de acceso.

4.3.1 Configurar el tipo de tarjeta

Configure el tipo de tarjeta antes de asignar tarjetas a los usuarios. Por ejemplo, si la tarjeta asignada es una tarjeta de identificación, configure el tipo de tarjeta en Tarjeta de identificación.

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Solución de acceso**>**Gerente de Personal**>**Usuario**. Sobre el

Paso 3 **Tipo de emisión de tarjeta**y luego seleccione un tipo de tarjeta.

Asegúrese de que el tipo de tarjeta sea el mismo que la tarjeta realmente asignada; de lo contrario, la tarjeta El número no se puede leer.

Etapa 4 Hacer clic**DE ACUERDO**.

4.3.2 Agregar usuarios

4.3.2.1 Agregar individualmente

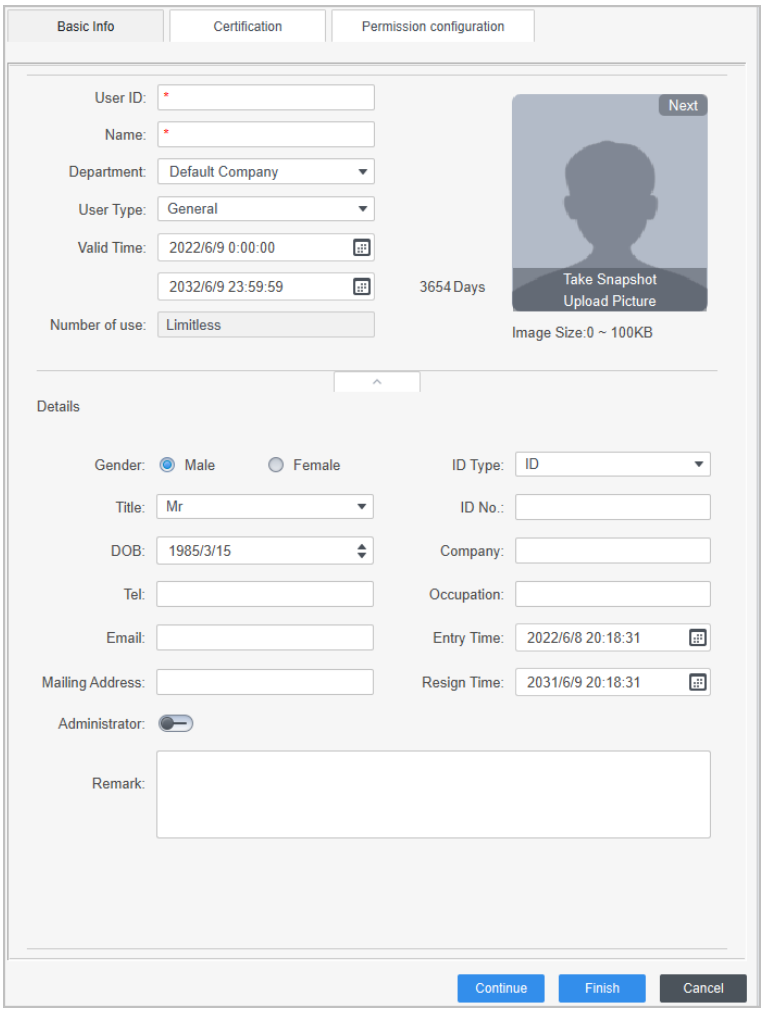
Puede agregar usuarios individualmente.

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Solución de acceso**>**Gerente de Personal**>**Usuario**>**Agregar**.

Paso 3 Hacer clic**Información básica**pestaña, e ingrese la información básica del usuario, y luego importe la imagen de la cara.

Figura 4-3 Agregar información básica



Etapa 4 Haga clic en el**Certificación**pestaña para agregar información de certificación del usuario.

- Configurar contraseña: la contraseña debe tener entre 6 y 8 dígitos.
- Configurar tarjeta: El número de tarjeta se puede leer automáticamente o ingresar manualmente. Para leer el número de tarjeta automáticamente, seleccione un lector de tarjetas y luego coloque la tarjeta en el lector de tarjetas.

  1. Sobre el**Tarjeta**área, haga clic y seleccione**Emisor de la tarjeta**y luego haga clic en**DE ACUERDO**.
  2. Haga clic**Agregar**, pase una tarjeta por el lector de tarjetas. Se muestra el número de tarjeta.
  3. Haga clic**DE ACUERDO**.

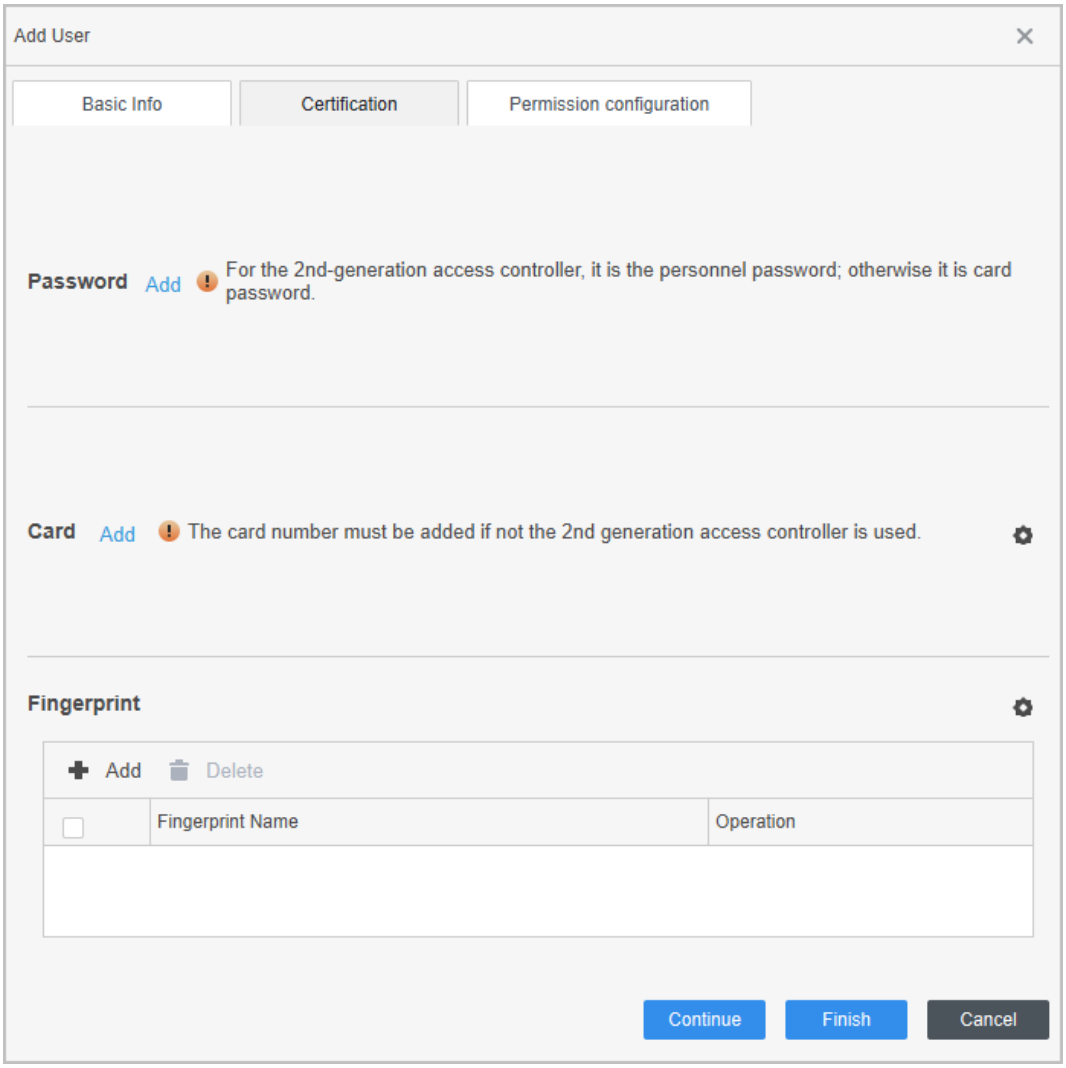
  Después de agregar una tarjeta, puede configurarla como tarjeta principal o tarjeta de coacción, reemplazar la tarjeta por una nueva o eliminarla.

- Configurar huella digital.

  1. Sobre el**Huella dactilar**área, haga clic **DE** y seleccione**Escáner de huellas dactilares**y luego haga clic en **ACUERDO**.

  2. Haga clic**Agregar huella digital**, presione con el dedo el escáner tres veces seguidas.

Figura 4-4 Agregar contraseña, tarjeta y huella digital



Paso 5 Configurar permisos para el usuario. Para obtener más información, consulte "4.3.3 Asignación de permiso de acceso".

Paso 6 Hacer clic**Finalizar**.

4.3.2.2 Agregar en lotes

Puede agregar usuarios en lotes.

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Gerente de Personal**>**Usuario**>**Agregar lote**.

Paso 3 Seleccionar**Emisor de la tarjeta**desde el**Dispositivo**lista y luego configure los parámetros.

Figura 4-5 Agregar usuarios en lotes

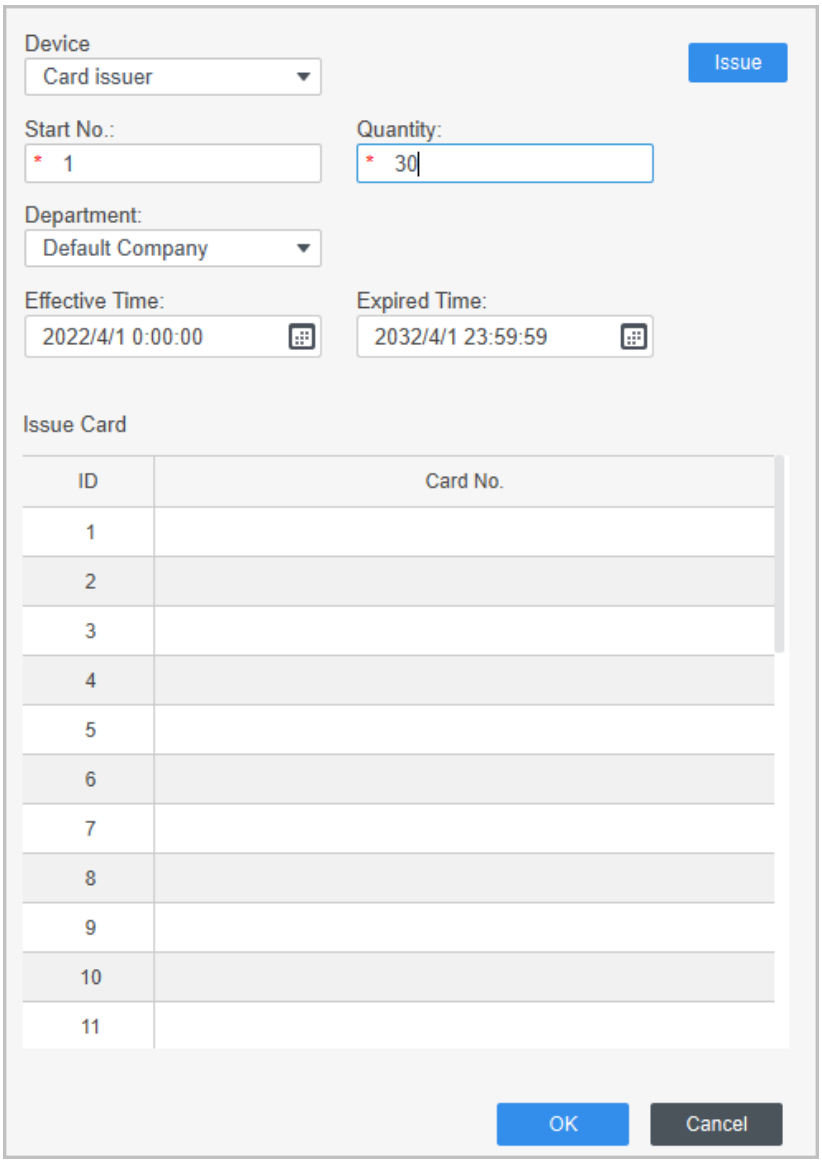


Tabla 4-2 Parámetros para agregar usuarios en lotes

Parámetro	Descripción
Empezar no.	La ID de usuario comienza con el número que usted definió.
Cantidad	La cantidad de usuarios que desea agregar.
Departamento	Seleccione el departamento al que pertenece el usuario.
Tiempo efectivo/tiempo vencido	Los usuarios pueden desbloquear la puerta dentro del período definido.

Etapa 4 Hacer clic**Asunto**.

El número de tarjeta se leerá automáticamente. Hacer clic**DE**

Paso 5 **ACUERDO**.

Paso 6 Sobre el**Usuario**página, haga clic para completar la información del usuario.

4.3.3 Asignación de permiso de acceso

Cree un grupo de permisos que sea una colección de permisos de acceso a puertas y luego asocie usuarios con el grupo para que puedan desbloquear las puertas correspondientes.

Paso 1 Inicie sesión en Smart PSS Lite.

Paso 2 Hacer clic**Solución de acceso**>**Gerente de Personal**>**Configuración de permisos**.

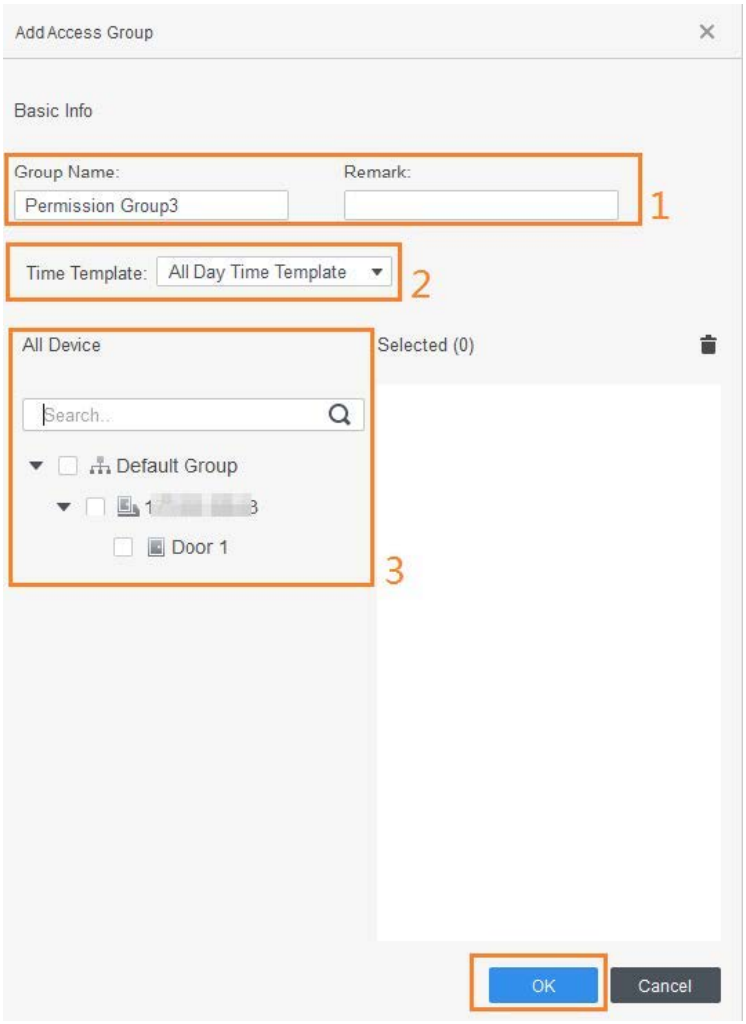
Paso 3 Haga clic.

Etapa 4 Ingrese el nombre del grupo, los comentarios (opcional) y seleccione una plantilla de tiempo.

Paso 5 Seleccione el dispositivo de control de acceso.

Paso 6 Hacer clic**DE ACUERDO**.

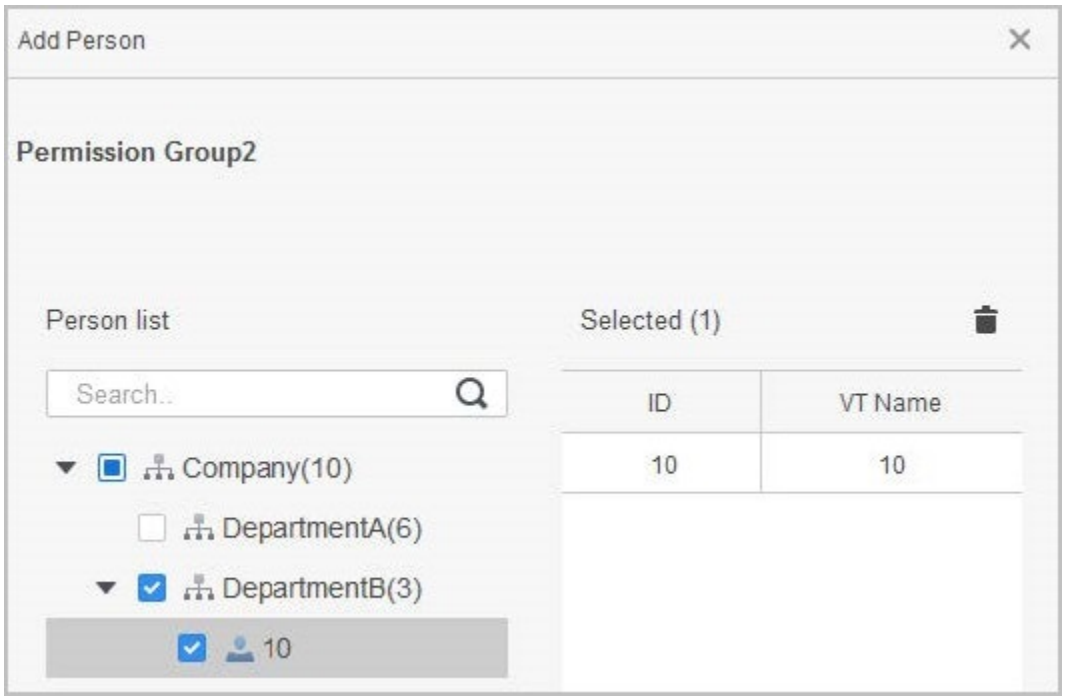
Figura 4-6 Crear un grupo de permisos



Paso 7 Hacer clic del grupo de permisos que agregó.

Paso 8 Seleccione usuarios para asociarlos con el grupo de permisos.

Figura 4-7 Agregar usuarios a un grupo de permisos



Paso 9 Hacer clic**DE ACUERDO**.

Los usuarios del grupo de permisos pueden desbloquear la puerta después de una verificación de identidad válida.

4.4 Gestión de acceso

4.4.1 Apertura y cierre de puertas de forma remota

Puede monitorear y controlar la puerta de forma remota a través de Smart PSS Lite. Por ejemplo, puede abrir o cerrar la puerta de forma remota.

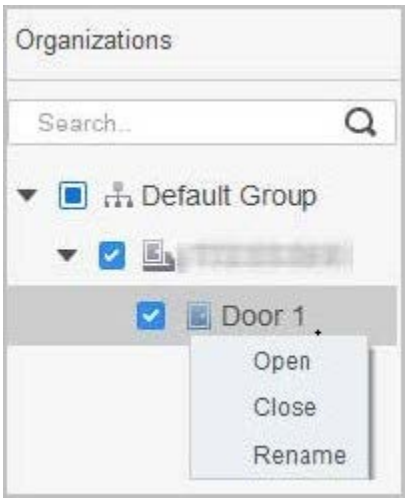
Procedimiento

Paso 1 Hacer clic**Solución de acceso**>**Administrador de acceso**en la página de inicio.

Paso 2 Controla remotamente la puerta.

- Seleccione la puerta, haga clic derecho y seleccione**Abierto**o**Cerca**.

Figura 4-8 Puerta abierta



- Haga clic en o para abrir o cerrar la puerta.

Operaciones relacionadas

- Filtrado de eventos: seleccione el tipo de evento en el**Información del evento**y la lista de eventos muestra el tipo de evento seleccionado, como eventos de alarma y eventos anormales.
- Bloqueo de actualización de eventos: haga clic para bloquear la lista de eventos y luego la lista de eventos dejará de actualizarse. Haga clic para desbloquear.
- Eliminación de eventos: haga clic para borrar todos los eventos en la lista de eventos.

4.4.2 Configuración de Siempre abierto y Siempre cerrado

Después de configurar siempre abierta o siempre cerrada, la puerta permanece abierta o cerrada todo el tiempo.

Paso 1 Hacer clic**Solución de acceso**>**Administrador de acceso**en la página de

Paso 2 inicio. Hacer clic**Siempre abierto**o**Siempre cerca**para abrir o cerrar la puerta.

Figura 4-9 Siempre abierto o cerrado

La puerta permanecerá abierta o cerrada todo el tiempo. Puedes hacer clic**Normal**para restaurar el control de acceso al estado normal, y luego la puerta se abrirá o cerrará según los métodos de verificación configurados.

4.4.3 Monitoreo del estado de la puerta

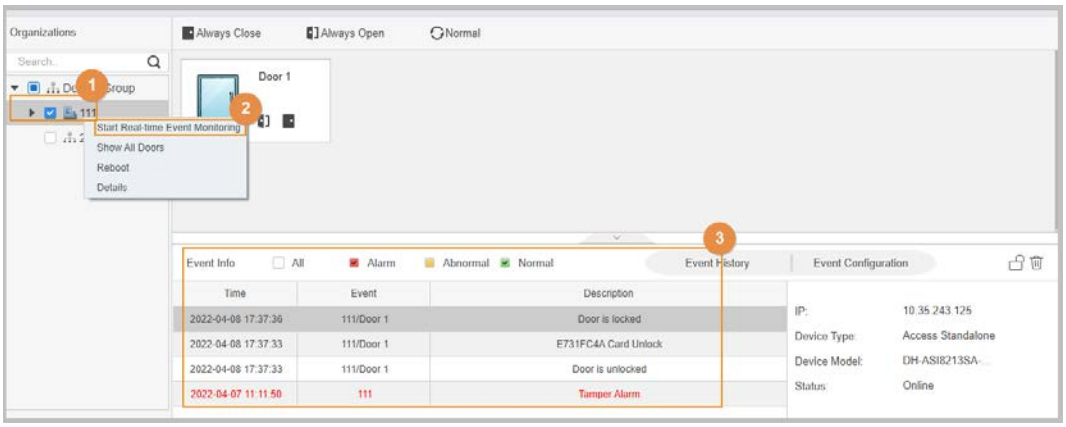
Paso 1 Hacer clic**Solución de acceso**>**Administrador de acceso**en la página de inicio.

Paso 2 Seleccione el Controlador de acceso en el árbol de dispositivos, haga clic con el botón derecho en el Terminal de acceso y luego seleccione **Iniciar el monitoreo de eventos en tiempo real**.

Los eventos de control de acceso en tiempo real se mostrarán en la lista de eventos.

Hacer clic**Detener monitor**, los eventos de control de acceso en tiempo real no se mostrarán.

Figura 4-10 Monitorear el estado de la puerta



- Mostrar todas las puertas: muestra todas las puertas controladas por el controlador de acceso.
- Reiniciar: reinicie el controlador de acceso.
- Detalles: vea los detalles del dispositivo, como la dirección IP, el modelo y el estado.

Apéndice 1 Puntos importantes del intercomunicador

Operación

El controlador de acceso puede funcionar como VTO para realizar la función de intercomunicación.

Requisitos previos

La función de intercomunicación se configura en el controlador de acceso y en el VTO.

Procedimiento

Paso 1 En la pantalla de espera, toque Ingresar  .

Paso 2 número de habitación y luego toque  .

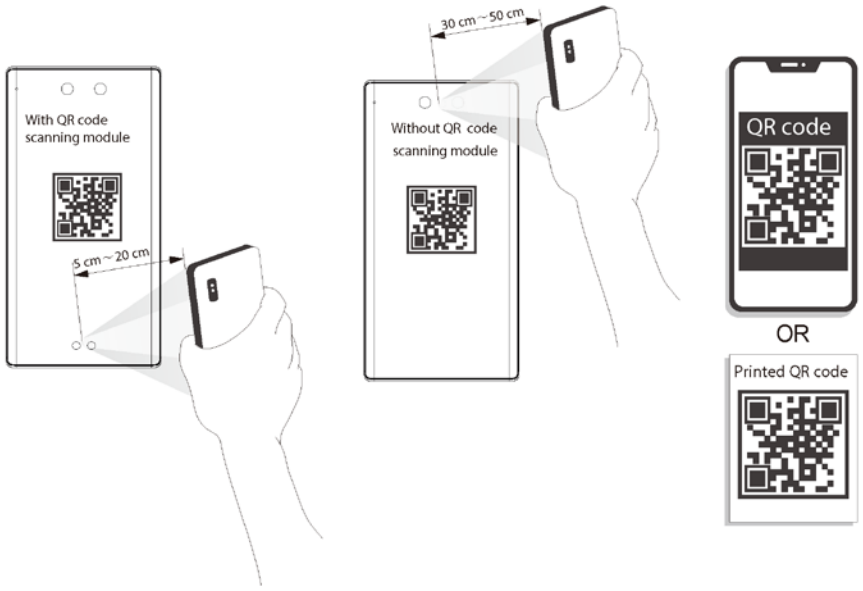
Apéndice 2 Puntos importantes del código QR

Exploración

- Controlador de acceso (con módulo de escaneo de códigos QR): coloque el código QR en su teléfono a una distancia de 3 cm a 5 cm de la lente de escaneo de códigos QR. Admite códigos QR de más de 30 mm × 30 mm - 5 cm × 5 cm y de menos de 100 bytes de tamaño.

La distancia de detección del código QR varía según los bytes y el tamaño del código QR.

Apéndice Figura 2-1 Escaneo de código QR



Apéndice 3 Puntos importantes de las huellas dactilares

Instrucciones de registro

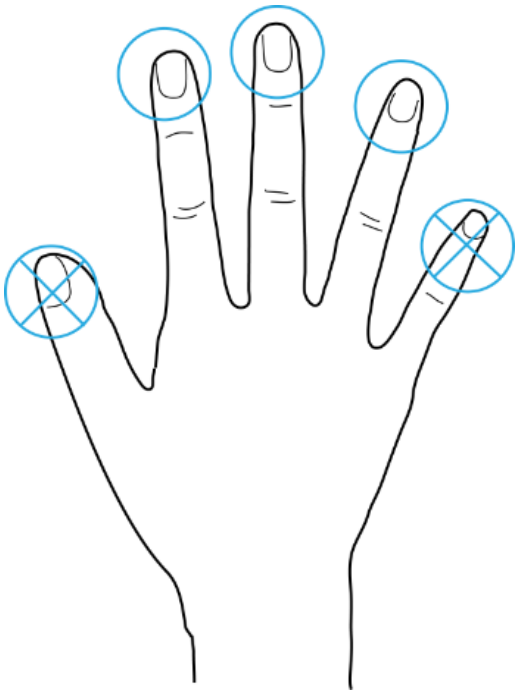
Al registrar la huella digital, preste atención a los siguientes puntos:

- Asegúrese de que sus dedos y la superficie del escáner estén limpios y secos.
- Presione su dedo en el centro del escáner de huellas digitales.
- No coloque el sensor de huellas dactilares en un lugar con luz intensa, alta temperatura y alta humedad.
- Si sus huellas digitales no están claras, utilice otros métodos de desbloqueo.

Dedos recomendados

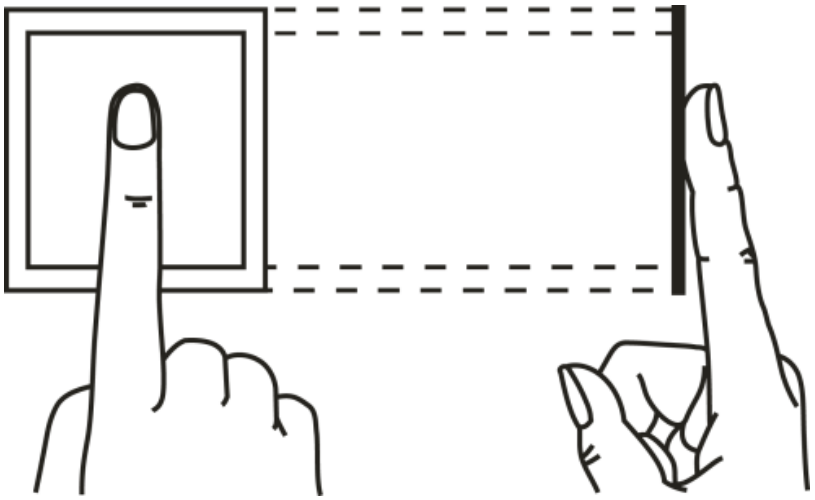
Se recomiendan los dedos índice, medio y anular. Los pulgares y los meñiques no se pueden colocar fácilmente en el centro de grabación.

Apéndice Figura 3-1 Dedos recomendados

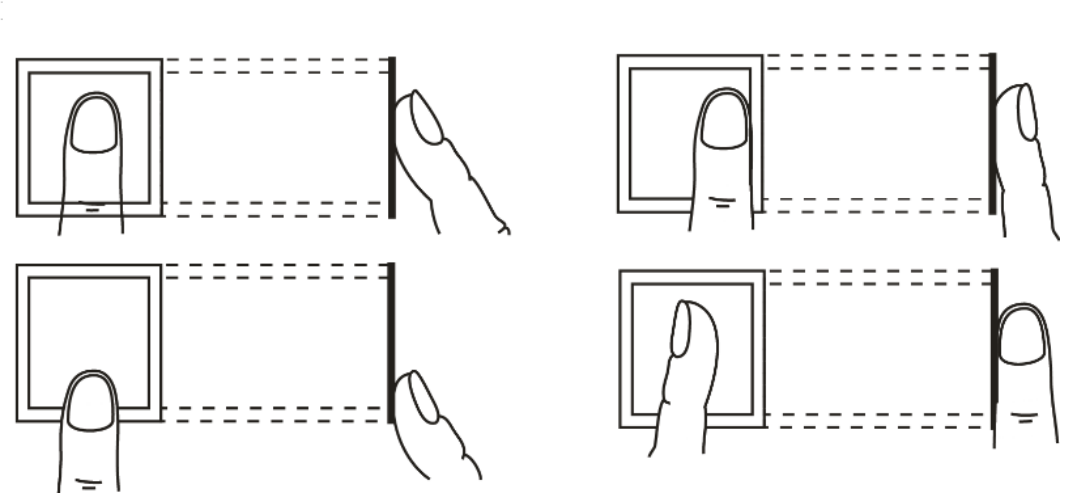


Cómo presionar su huella digital en el escáner

Apéndice Figura 3-2 Colocación correcta



Apéndice Figura 3-3 Ubicación incorrecta



Apéndice 4 Puntos importantes de cara Registro

Antes del registro

- Las gafas, los sombreros y la barba pueden influir en el rendimiento del reconocimiento facial.
- No te cubras las cejas cuando uses sombreros.
- No cambies mucho el estilo de tu barba si utilizas el controlador de acceso; de lo contrario, el reconocimiento facial podría fallar.
- Mantén tu cara limpia.
- Mantenga el controlador de acceso al menos a dos metros de distancia de fuentes de luz y al menos a tres metros de ventanas o puertas; de lo contrario, la luz de fondo y la luz solar directa podrían afectar el rendimiento del reconocimiento facial del controlador de acceso.

Durante el registro

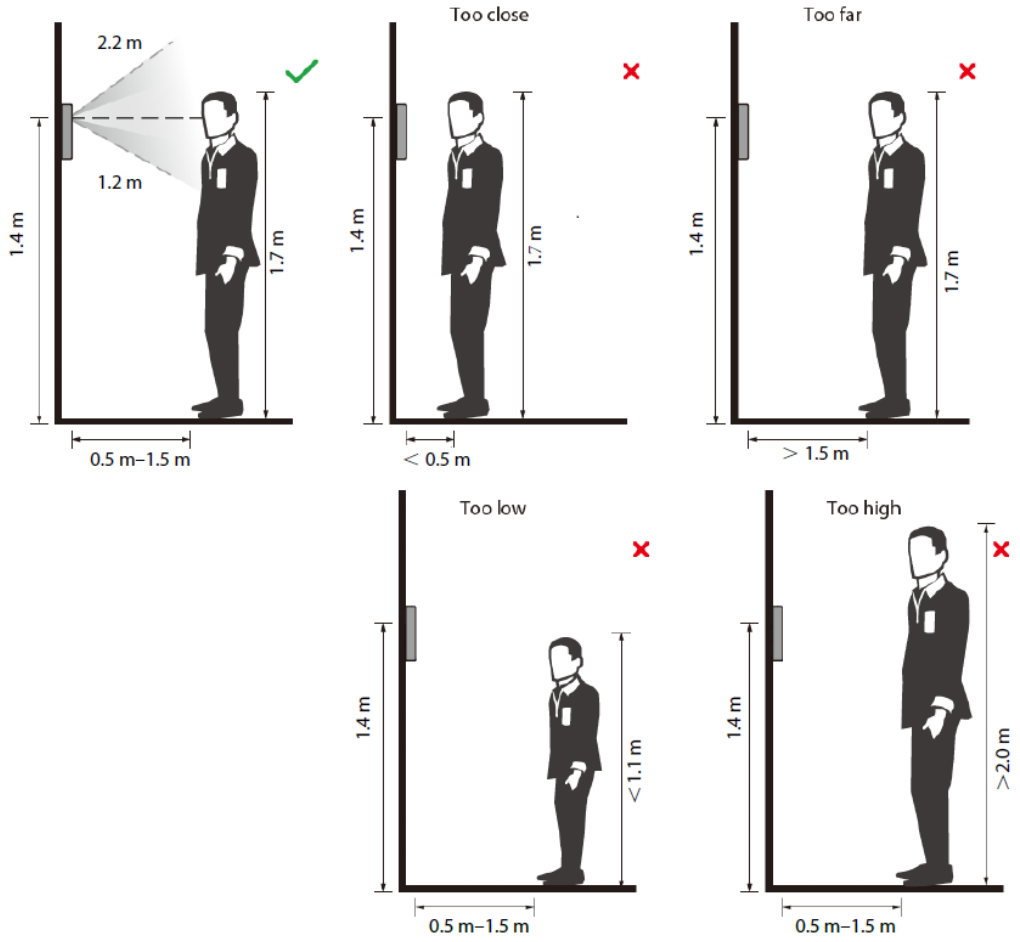
- Puedes registrar rostros a través del Controlador de Acceso o a través de la plataforma. Para el registro a través de la plataforma, consultar el manual de usuario de la plataforma.
- Coloque su cabeza en el centro del marco de captura de fotografías. La imagen de la cara se capturará automáticamente.

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

Posición de la cara

Si su rostro no está en la posición adecuada, la precisión del reconocimiento facial podría verse afectada.

Apéndice Figura 4-1 Posición facial adecuada



Requisitos de caras

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

Apéndice Figura 4-2 Posición de la cabeza

Apéndice Figura 4-3 Distancia de la cara

- Al importar imágenes de rostros a través de la plataforma de administración, asegúrese de que la imagen La resolución está dentro del rango de 150 × 300 píxeles a 600 × 1200 píxeles. Se recomienda que la resolución debe ser superior a 500 × 500 píxeles, el tamaño de la imagen debe ser inferior a 100 KB y el El nombre de la imagen y el ID de la persona deben ser los mismos.
- Asegúrese de que la cara ocupe más de 1/3 pero no más de 2/3 del área total de la imagen. y la relación de aspecto no supera 1:2.

Apéndice 5 Recomendaciones de ciberseguridad

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

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres.
- Incluya al menos dos tipos de personajes; Los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos.
- No incluya el nombre de la cuenta 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 cliente a tiempo

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

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

1. Protección física

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

2. Cambie las contraseñas con regularidad

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de que las adivinen o las descifren.

3. Establecer y actualizar contraseñas Restablecer información oportuna

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

4. Habilite el bloqueo de cuenta

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

5. Cambie HTTP predeterminado y otros puertos de servicio

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

6. Habilite HTTPS

Le sugerimos habilitar HTTPS, para que visite 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. Asigne cuentas y privilegios de manera razonable

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

9. Deshabilite los servicios innecesarios y elija modos seguros

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

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

- SNMP: elija SNMP v3 y configure contraseñas de cifrado y contraseñas de autenticación seguras.
- SMTP: elija TLS para acceder al servidor de buzones.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de 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 cifrada para reducir el riesgo de que los datos de audio y video sean robados durante la transmisión.

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

11. Auditoría segura

- Verifique los usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo inició sesión sin autorización.
- Verifique 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 período prolongado, se recomienda habilitar la función de registro de red para garantizar que los registros críticos estén sincronizados con el servidor de registro de red para su seguimiento.

13. Construya un entorno de red seguro

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

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