Controlador de acceso con reconocimiento facial

Manual del usuario

Versión 1.0.2

Prefacio

General

Este manual presenta las funciones y el funcionamiento del Controlador de Acceso con Reconocimiento Facial (en adelante, el "Controlador de Acceso"). Lea atentamente antes de usar el dispositivo y conserve este manual para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

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

Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
Versión 1.0.2	Se agregó la gestión de usuarios en la página web.	Febrero de 2023
Versión 1.0.1	Se agregó la gestión de usuarios en la página web.	Diciembre de 2022
Versión 1.0.0	Primer lanzamiento.	Noviembre de 2022

Aviso de protección de la privacidad

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

Acerca del manual

- Este manual es solo de referencia. Podrían existir ligeras diferencias entre el manual y el producto.
- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas que no cumplan con el manual.
- El manual se actualizará según las últimas leyes y regulaciones de las jurisdicciones pertinentes. Para obtener información detallada, consulte el manual de usuario impreso, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. Este manual es solo de referencia. Podrían existir ligeras diferencias.

la versión electrónica y la versión en papel.

- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto podrían generar diferencias entre el producto real y el manual. Para obtener el programa más reciente y la documentación complementaria, póngase en contacto con el servicio de atención al cliente.
- Podría haber errores de impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. En caso de duda o controversia, nos reservamos el derecho de ofrecer una explicación definitiva.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de empresas en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta información sobre el manejo adecuado del 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 siga las instrucciones al usarlo.

Requisito de transporte

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

Requisito de almacenamiento

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

Requisitos de instalación

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

- El personal que trabaja en altura debe tomar todas las medidas necesarias para garantizar su seguridad personal, incluido el uso de casco y cinturones de seguridad.
- No coloque el controlador de acceso en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el controlador de acceso 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 que cumplan con las especificaciones de potencia nominal.
- La fuente de alimentación debe cumplir con los requisitos de ES1 de la norma IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de la fuente de alimentación dependen de 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.

Requisitos de operación

- Compruebe si la fuente de alimentación es correcta antes de usarlo.
- No desconecte el cable de alimentación del costado del controlador de acceso mientras el adaptador esté encendido.
- Opere el controlador de acceso dentro del rango nominal de entrada y salida de energía.

- Utilice el controlador de acceso en las condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquidos 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 instrucciones profesionales.
- Este producto es un equipo profesional.
- Este equipo no es adecuado para su uso en lugares donde es probable que haya niños.

Tabla de contenido

Prefacio.....I **Medidas de seguridad y advertencias importantes**..... III **1 Descripción general**.....1

1.1 Introducción.....1

1.2 Características.....1

1.3 Aplicación.....1

2 Operaciones locales.....3

2.1 Procedimiento de configuración básica..... 3

2.2 Iconos comunes..... 3

2.3 Pantalla de espera..... 3

2.4 Inicialización.....5

2.5 Iniciar sesión.....5

2.6 Gestión de usuarios.....5

2.6.1 Agregar nuevos usuarios.....5

2.6.2 Visualización de la información del usuario.....7

2.6.3 Configuración de la contraseña del administrador.....8

2.7 Comunicación en red.....8

2.7.1 Configuración de IP..... 8

2.7.2 Registro activo.....9

2.7.3 Configuración de Wi-Fi.....10

2.7.4 Configuración del puerto serie.....11

2.7.5 Configuración de Wiegand.....11

2.8 Gestión de acceso.....12

2.8.1 Configuración de combinaciones de desbloqueo.....12

2.8.2 Configuración de la alarma.....13

2.8.3 Configuración del estado de la puerta.....15

2.8.4 Configuración del tiempo de retención del bloqueo.....15

2.9 Gestión de asistencia.....15

2.9.1 Configuración de turnos.....15

2.9.2 Configuración de planes de vacaciones.....16

2.9.3 Configuración de departamentos.....17

2.9.4 Configuración de horarios de trabajo.....17

2.9.5 Configuración del tiempo del intervalo de verificación.....19

2.9.6 Configuración de modos de asistencia.....19

2.10 Sistema.....21

2.10.1 Configuración de la hora.....21

2.10.2 Configuración de parámetros faciales.....22

2.10.3 Ajuste del volumen.....24

2.10.4 (Opcional) Configuración de parámetros de huellas dactilares....24
2.10.5 Configuración de pantalla....25
2.10.6 Restauración de los valores predeterminados de fábrica....25
2.10.7 Reiniciar el dispositivo....25
2.10.8 Configuración del idioma....25
2.11 Administración USB....25
2.11.1 Exportación a USB....25
2.11.2 Importación desde USB....26
2.11.3 Actualización del sistema....26
2.12 Configuración de funciones....26
2.13 Desbloqueo de la puerta....28
2.13.1 Desbloqueo mediante tarjetas....28
2.13.2 Desbloqueo por rostro....28
2.13.3 Desbloqueo por contraseña de usuario....29
2.13.4 Desbloqueo mediante contraseña de administrador....29
2.13.5 Desbloqueo mediante código QR....29
2.13.6 Desbloqueo por huella dactilar....29
2.13.7 Desbloqueo mediante contraseña temporal....29
2.14 Información del sistema....30
2.14.1 Visualización de la capacidad de datos....30
2.14.2 Versión del dispositivo de visualización....30
3 Operaciones web....31
3.1 Inicialización....31
3.2 Inicio de sesión....31
3.3 Restablecimiento de la contraseña....32
3.4 Configuración de parámetros de la puerta....33
3.5 Configuración del intercomunicador....36
3.5.1 Configuración del servidor SIP....36
3.5.2 Configuración de parámetros básicos....39
3.5.3 Adición del VTO....41
3.5.4 Adición del VTH....42
3.5.5 Adición del VTS....44
3.5.6 Visualización del estado del dispositivo....45
3.5.7 Visualización de registros de llamadas....45
3.6 Configuración de horarios....45
3.6.1 Configuración de secciones de tiempo....45
3.6.2 Configuración de grupos de vacaciones....46
3.6.3 Configuración de planes de vacaciones....47
3.7 Capacidad de datos....48
3.8 Configuración de vídeo e imagen....48

3.8.1 Configuración de vídeo....48
3.8.1.1 Configuración del canal 1....48
3.8.1.2 Configuración del canal 2....52
3.8.2 Ajuste del volumen....55
3.9 Configuración de la detección de rostros....55
3.10 Configuración de la red....58
3.10.1 Configuración de TCP/IP....58
3.10.2 Configuración del puerto....59
3.10.3 Configuración del registro automático....60
3.10.4 Configuración del servicio en la nube....60
3.10.5 Configuración del puerto serie....61
3.10.6 Configuración de Wiegand....62
3.11 Gestión de la seguridad....63
3.11.1 Configuración de la autoridad IP....63
3.11.1.1 Acceso a la red....64
3.11.1.2 Prohibir PING....65
3.11.1.3 Conexión anti-media....66
3.11.2 Configuración del sistema....66
3.11.2.1 Creación de un certificado de servidor....68
3.11.2.2 Descarga del certificado raíz....69
3.12 Gestión de usuarios....73
3.12.1 Agregar cuenta de administrador....73
3.12.2 Agregar usuarios....74
3.12.3 Agregar usuarios ONVIF....76
3.12.4 Visualización de usuarios en línea....77
3.13 Configuración de indicaciones de voz....77
3.14 Mantenimiento....77
3.15 Gestión de la configuración....78
3.15.1 Exportación/importación de archivos de configuración....78
3.15.2 Restauración de los valores predeterminados de fábrica....79
3.15.3 Configuración de los accesos directos....79
3.15.4 Configuración de las funciones del puerto....80
3.16 Actualización del sistema....81
3.16.1 Actualización de archivos....81
3.16.2 Actualización en línea....81
3.17 Visualización de la información de la versión....81
3.18 Visualización de registros....81
3.18.1 Registros del sistema....81
3.18.2 Registros de administración....82
3.18.3 Desbloqueo de registros....82

4 Configuración inteligente de PSS Lite.....83
4.1 Instalación e inicio de sesión.....83
4.2 Agregar dispositivos.....83
4.2.1 Agregar individualmente.....83
4.2.2 Adición en lotes.....84
4.3 Gestión de usuarios.....85
4.3.1 Configuración del tipo de tarjeta.....85
4.3.2 Agregar usuarios.....86
4.3.2.1 Agregar uno por uno.....86
4.3.2.2 Adición en lotes.....87
4.3.3 Asignación de permisos de acceso.....88
4.3.4 Asignación de permisos de asistencia.....90
4.4 Gestión de acceso.....92
4.4.1 Apertura y cierre de puertas a distancia.....92
4.4.2 Configuración Siempre abierto y Siempre cerrado.....93
4.4.3 Monitoreo del estado de la puerta.....93
Apéndice 1 Puntos importantes del funcionamiento del intercomunicador.....95
Apéndice 2 Puntos importantes del escaneo de códigos QR.....96
Apéndice 3 Puntos importantes de las instrucciones de registro de huellas dactilares.....97
Apéndice 4 Puntos importantes del registro facial.....99
Apéndice 5 Recomendaciones de ciberseguridad.....102

1.1 Introducción

El controlador de acceso es un panel de control de acceso que permite el desbloqueo mediante reconocimiento facial, contraseñas, huella dactilar, tarjetas, códigos QR y sus combinaciones. Basado en un algoritmo de aprendizaje profundo, ofrece un reconocimiento más rápido y una mayor precisión. Es compatible con plataformas de gestión que satisfacen las diversas necesidades de los clientes.

1.2 Características

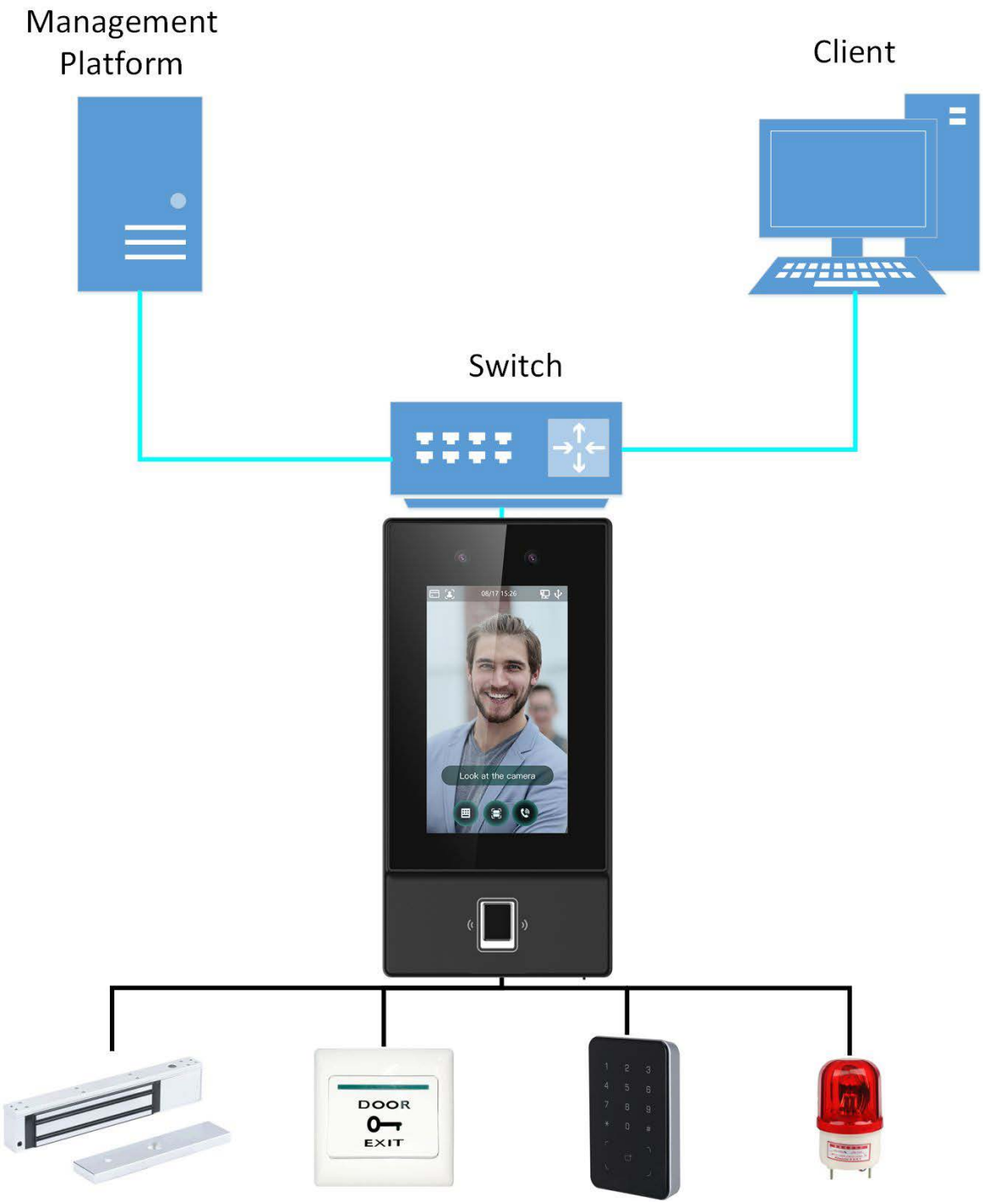
Las características principales pueden variar según los modelos del controlador de acceso.

- Pantalla táctil de cristal de 4,3 pulgadas con una resolución de 272 × 480.
- Cámara de doble lente gran angular de 2 MP con iluminación IR y DWDR.
- Múltiples métodos de desbloqueo, incluidos huella digital, rostro, tarjeta IC y contraseña.
- Admite 6.000 usuarios, 6.000 caras, 6.000 contraseñas, 6.000 huellas dactilares, 10.000 tarjetas, 50 administradores y 300.000 registros.
- Reconoce rostros a una distancia de 0,3 m a 1,5 m (0,98 ft - 4,92 ft); tasa de precisión de reconocimiento facial del 99,9 % y el tiempo de comparación 1: N es de 0,2 s por persona.
- Admite seguridad mejorada y, para proteger contra la apertura forzada del dispositivo, se admite la expansión del módulo de seguridad.
- Cuenta con detección de mascarilla y detección de casco de seguridad.
- Admite código QR de visitante y función de timbre.
- Admite realizar videollamadas y usar la aplicación para recibir notificaciones de alarma, desbloquear puertas de forma remota y realizar otras tareas.
- Conexión TCP/IP y Wi-Fi.
- Fuente de alimentación PoE.
- Clasificación IP65.

1.3 Aplicación

Es ampliamente utilizado en parques, comunidades, centros comerciales y fábricas, y es ideal para lugares como edificios de oficinas, edificios gubernamentales, escuelas y estadios.

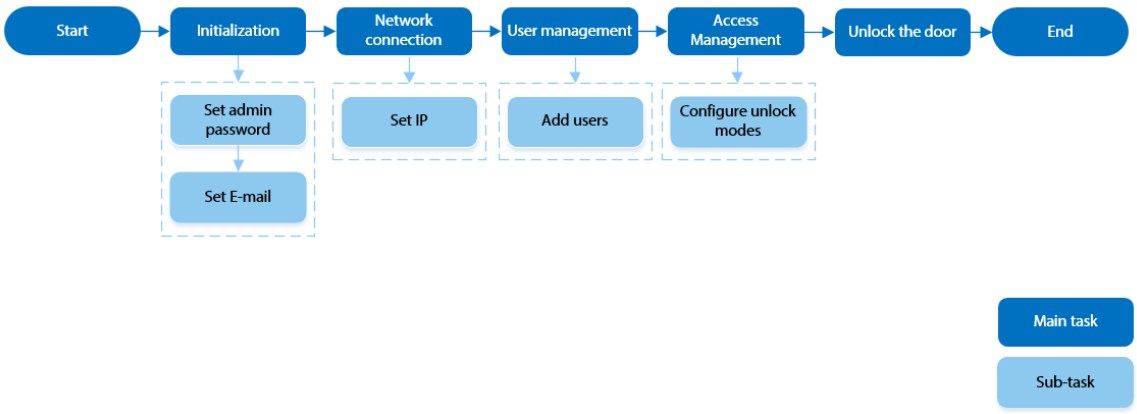
Figura 1-1 Redes



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 los 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.
	Regresar al menú anterior.
	Encendido.
	Apagado.
	Borrar
	Buscar

2.3 Pantalla de espera

Puedes desbloquear la puerta con reconocimiento facial, contraseñas y código QR. También puedes hacer llamadas a través del intercomunicador.

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

Figura 2-2 Pantalla de espera

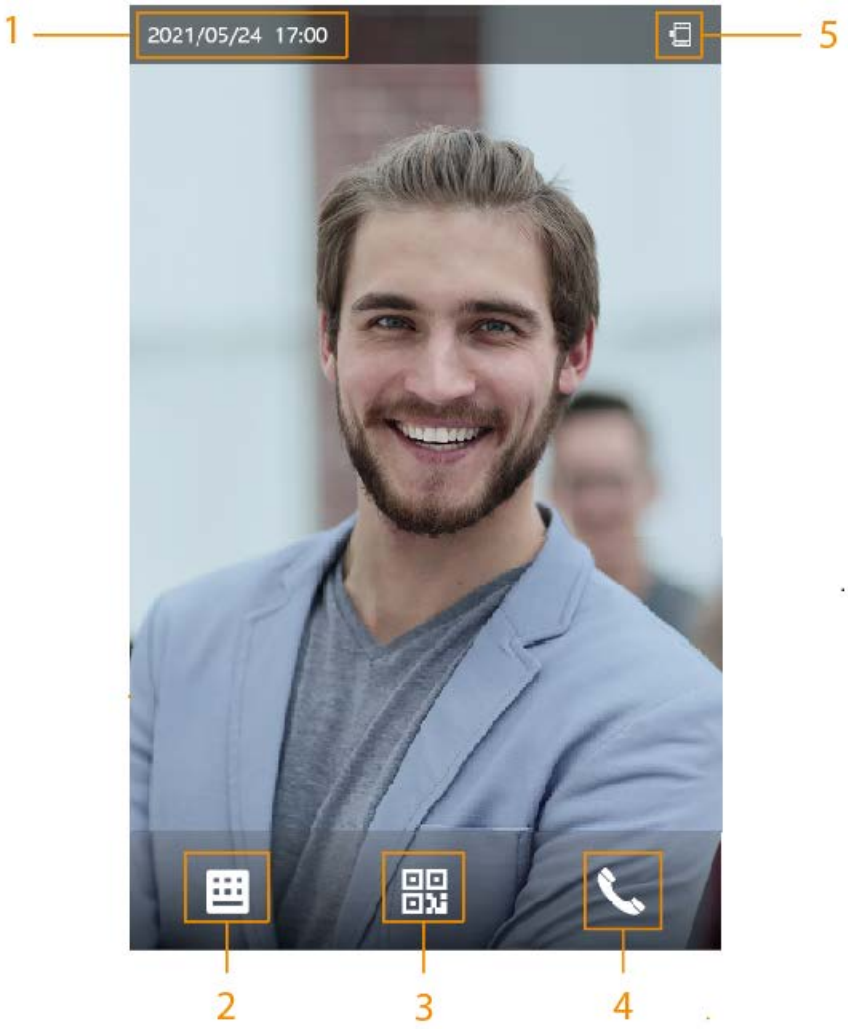


Tabla 2-2 Descripción de la pantalla de inicio

No.	Nombre	Descripción
1	Fecha y hora	Fecha y hora actual.
2	Contraseña	Introduzca la contraseña de usuario o la contraseña de administrador para desbloquear la puerta.
3	Código QR	Toque el ícono del código QR y escanee el código QR para desbloquear la puerta.
4	Intercomunicador	● Cuando el controlador de acceso funciona como servidor, puede llamar al VTO y al VTH. ● Cuando DSS funciona como servidor, el controlador de acceso puede llamar al VTO, VTS y DSS. Toque el ícono e ingrese el número de la habitación para llamar al propietario.
5	Visualización de estado	Muestra el estado de Wi-Fi, la red y el USB.

2.4 Inicialización

Para el primer uso o después de restaurar la configuración de fábrica, debe seleccionar un idioma en el Controlador de Acceso y luego configurar la contraseña y el correo electrónico de la cuenta de administrador. Puede usar la cuenta de administrador para acceder al menú principal del Controlador de Acceso y a 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 sean espacios 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 las cuentas de administrador pueden acceder al menú principal. La primera vez que lo use, use la cuenta de administrador para acceder al menú principal y luego podrá crear las demás cuentas de administrador.

Información de fondo

- 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.

Procedimiento

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

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

- Cara: Ingresa al menú principal mediante reconocimiento facial.
- Huella digital: Ingrese al menú principal mediante el uso de la huella digital.

  La función de huella dactilar solo está disponible para el modelo de huella dactilar del controlador de acceso.
- Perforación de tarjeta: ingrese al menú principal deslizando la tarjeta.
- 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 Gestión de usuarios

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

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

2.6.1 Agregar nuevos usuarios

Procedimiento

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

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

Figura 2-3 Agregar nuevo usuario

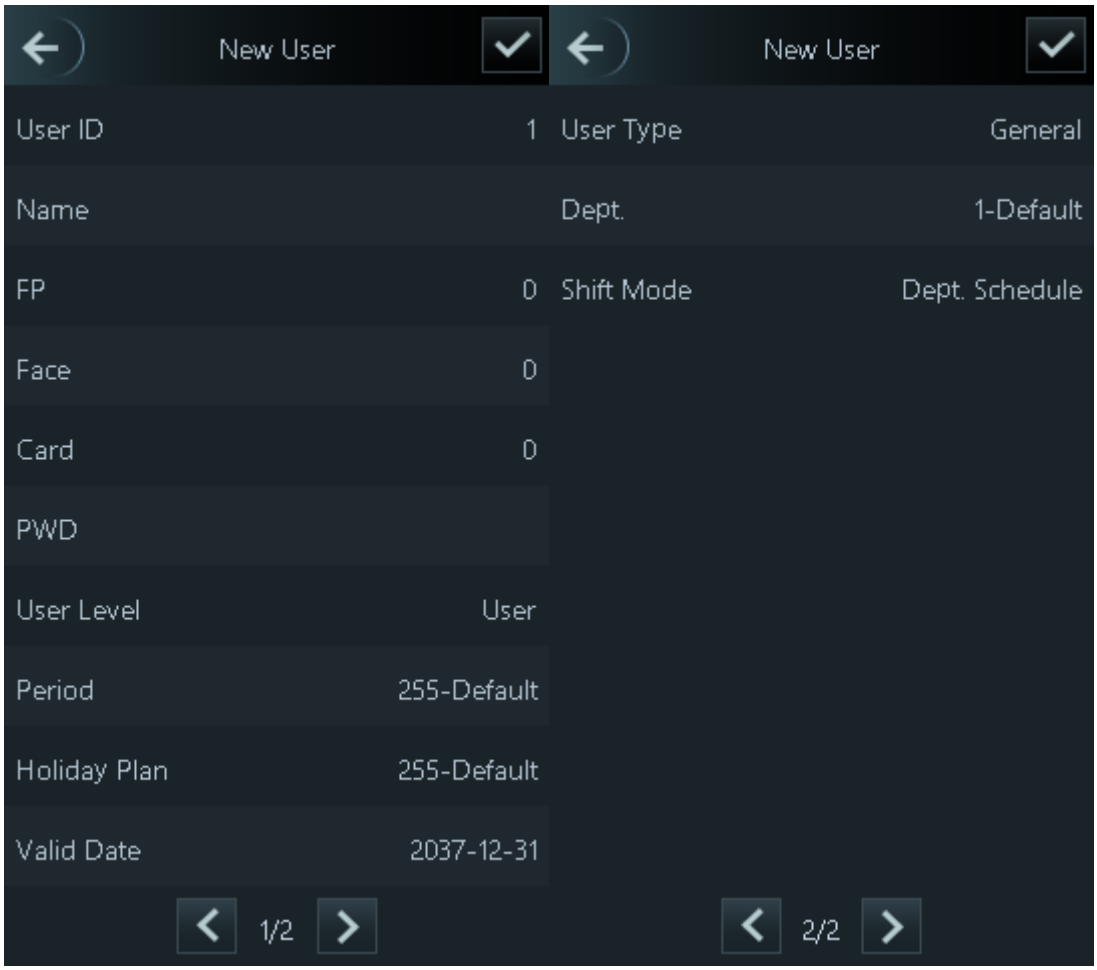


Tabla 2-3 Descripción de parámetros

Parámetro	Descripción
ID de usuario	Introduzca los ID de usuario. Pueden ser números, letras y combinaciones de estos, y su longitud máxima es de 32 caracteres. Cada ID es único.
Nombre	Ingrese un nombre con un máximo de 32 caracteres (incluidos números, símbolos y letras).
FP	Registrar huellas dactilares. Un usuario puede registrar hasta tres huellas dactilares, y se puede configurar una como huella de coacción. Se activará una alarma cuando se use la huella de coacción para abrir la puerta. Sólo ciertos modelos admiten el desbloqueo mediante huellas dactilares.
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 un máximo de cinco tarjetas. Ingrese su número de tarjeta o deslícela, y el controlador de acceso leerá la información. Puedes habilitar el**Tarjeta de coacción**Función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta.
Personas con discapacidad	Introduzca la contraseña de usuario. La longitud máxima de la contraseña es de 8 dígitos.

Parámetro	Descripción
Nivel de usuario	Puede seleccionar un nivel de usuario para los nuevos usuarios. ● **Usuario**:Los usuarios sólo 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 solo durante el período definido.
Plan de vacaciones	Las personas pueden desbloquear la puerta solo durante el plan de vacaciones definido.
Fecha válida	Establezca una fecha en la que caducarán los permisos de acceso de la persona.
Tipo de usuario	● **General**:Los usuarios generales pueden desbloquear la puerta. ● **Lista de bloqueo**: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 periodo definido o por un número determinado de veces. Una vez transcurrido el periodo definido o el tiempo de desbloqueo, no podrán desbloquear la puerta. ● **Patrulla**:Los usuarios de patrulla tendrán registrada su asistencia, pero no tendrán permisos de desbloqueo. ● **personaje**:Cuando el VIP desbloquee la puerta, el personal de servicio recibirá un aviso. ● **Otros**:Cuando desbloqueen la puerta, ésta permanecerá desbloqueada durante 5 segundos más. ● Usuario personalizado 1/Usuario personalizado 2: Lo mismo que los usuarios generales.
Dpto.	Establecer departamentos.
Modo Shift	Seleccionar modos de cambio.

Paso 3 Grifo **.**

2.6.2 Visualización de la información del usuario

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

Procedimiento

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

Paso 2 Ver todos los usuarios y cuentas de administrador agregados.

- :Desbloqueo mediante contraseña.
- :Desbloqueo mediante pase de tarjeta.
- :Desbloqueo mediante reconocimiento facial.
- :Desbloqueo mediante huella dactilar.

Operaciones relacionadas

En el**Usuario**Pantalla, puedes administrar los usuarios agregados.

- Buscar usuarios: Toque y luego ingrese el nombre de usuario.
- Editar usuarios: toque el usuario para editar su información.
- Eliminar usuarios
  - ◇ Eliminar individualmente: seleccione un usuario y luego toque

- ◇ Eliminar por lotes:
  - ◯ En el**Lista de usuarios**pantalla, toque para eliminar todos los usuarios.
  - ◯ En el**Lista de administradores**pantalla, toque para eliminar todos los usuarios administradores.

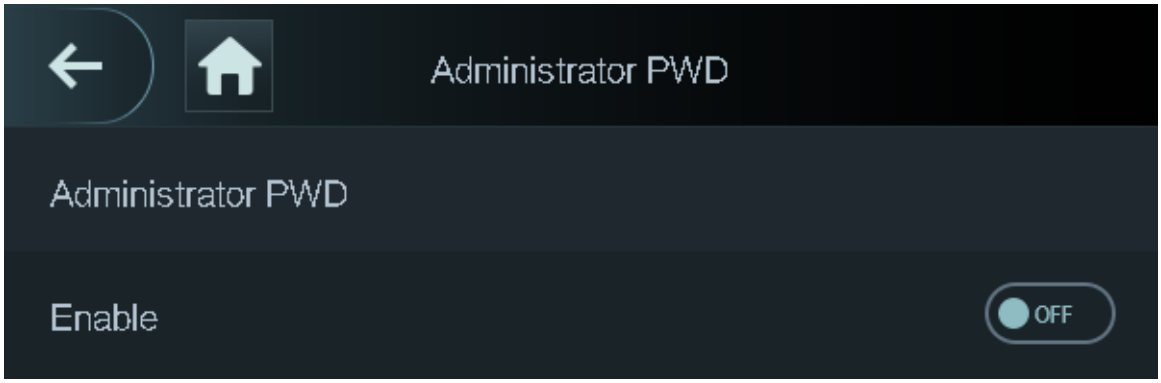
2.6.3 Configuración de la contraseña del administrador

Puede desbloquear la puerta ingresando únicamente la contraseña de administrador. Esta no está limitada por tipo de usuario. Solo se permite una contraseña de administrador por dispositivo.

Procedimiento

Paso 1 En el**Menú principal**pantalla, seleccionar**Usuario**>**Administrador PWD**.

Figura 2-4 Establecer contraseña de administrador



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

Paso 3 Toque

Paso 4 Activar la función de administrador.

2.7 Comunicación en 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 controlador de acceso.

2.7.1 Configuración de IP

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

Procedimiento

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

Paso 2 Configurar dirección IP.

Figura 2-5 Configuración de la dirección IP

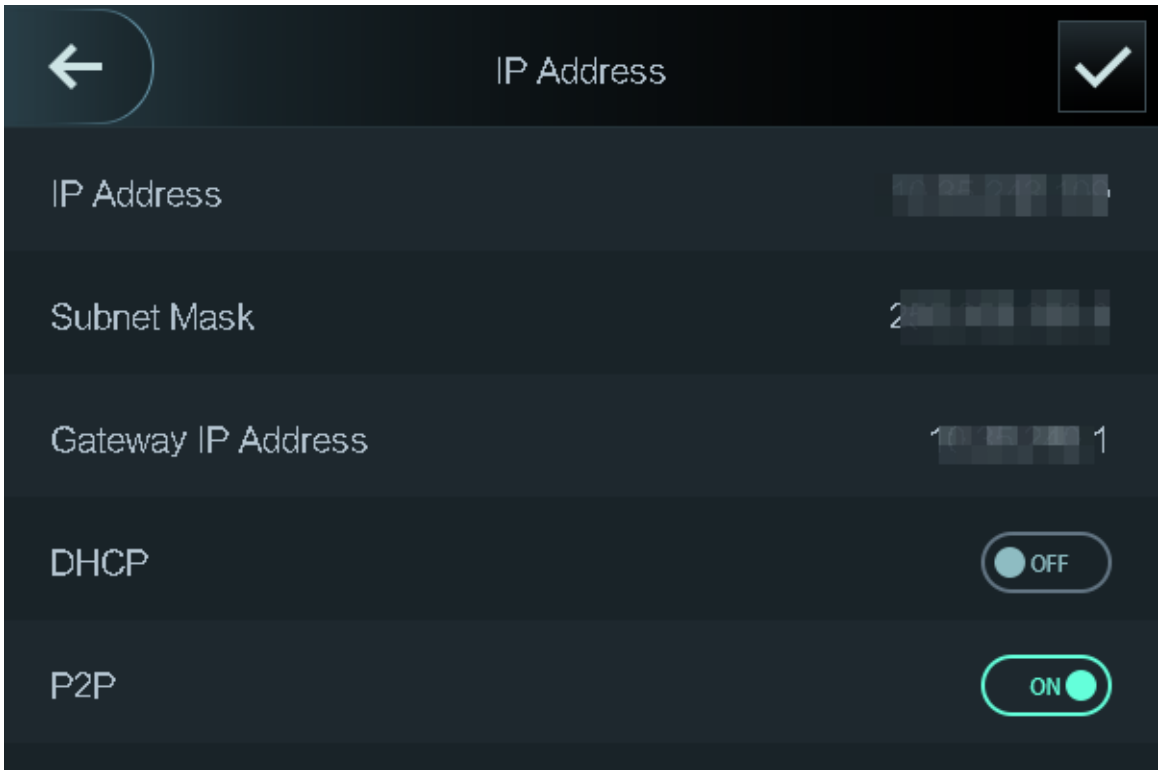


Tabla 2-4 Parámetros de configuración de IP

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 se activa DHCP, al controlador de acceso se le asignará automáticamente una dirección IP, una máscara de subred y una puerta de enlace.
P2P	La tecnología P2P (peer-to-peer) permite a los usuarios administrar dispositivos sin solicitar DDNS, configurar la asignación de puertos o implementar un servidor de tránsito.

2.7.2 Registro activo

Puede activar la función de registro automático para acceder al Controlador de Acceso a través de la plataforma de administración.

Información de fondo

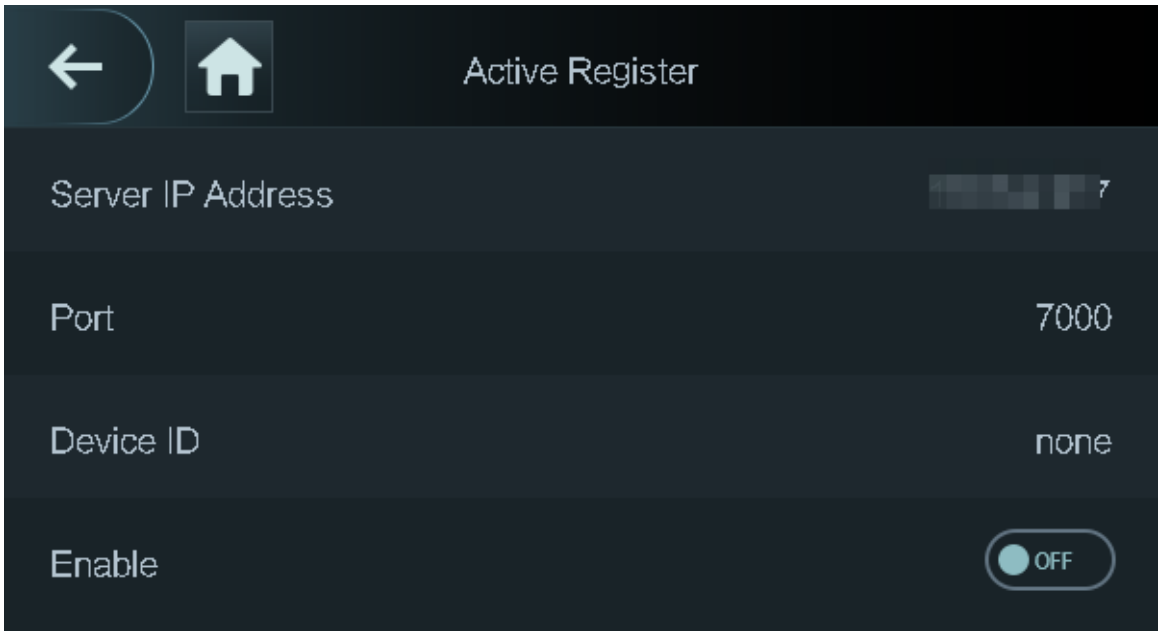
La plataforma de gestión puede borrar todas las configuraciones de personal e inicializar el controlador de acceso.

Para evitar la pérdida de datos, mantenga adecuadamente los permisos de la plataforma de administración.

Procedimiento

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

Figura 2-6 Registro automático



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

Tabla 2-5 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	Introduzca el ID del dispositivo (definido por el usuario). Cuando agrega el controlador de acceso a la administración plataforma, el ID del dispositivo en la plataforma de administración debe cumplir con el ID del dispositivo definido en el controlador de acceso.

Paso 3 Habilitar la función de registro activo.

2.7.3 Configuración de Wi-Fi

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

Procedimiento

Paso 1 En el**Menú principal**, seleccionar**Conexión**>**Red**>**Wi-Fi**

Paso 2 Encienda el Wi-Fi.

La función Wi-Fi solo está disponible en modelos seleccionados.

Paso 3 Grifo para buscar redes inalámbricas disponibles.

Paso 4 Seleccione una red inalámbrica e ingrese la contraseña.

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

Paso 5 toque .

2.7.4 Configuración del puerto serie

Procedimiento

Paso 1 En el**Menú principal**, seleccionar**Conexión**>**Puerto serie**

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: emite datos basados en el número de tarjeta cuando los usuarios pasan la tarjeta para desbloquear la puerta; emite datos basados en el primer número de tarjeta del usuario cuando utilizan otros métodos de desbloqueo.
  - ◇ No.: Genera datos basados en el ID 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.

2.7.5 Configuración de Wiegand

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

Procedimiento

Paso 1 En 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 otra terminal de acceso.

Figura 2-7 Salida Wiegand

Tabla 2-6 Descripción de la salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	Seleccione un formato Wiegand para leer números de tarjeta 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	Introduzca el ancho de 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. ● **ID de usuario**: Genera datos basados en el ID del usuario. ● **N° de tarjeta**:Emite datos basados en el primer número de tarjeta del usuario y el formato de los datos es hexadecimal o decimal.

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 Configuración de combinaciones de desbloqueo

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

Información de fondo

Los modos de desbloqueo pueden variar según el producto real.

Procedimiento

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

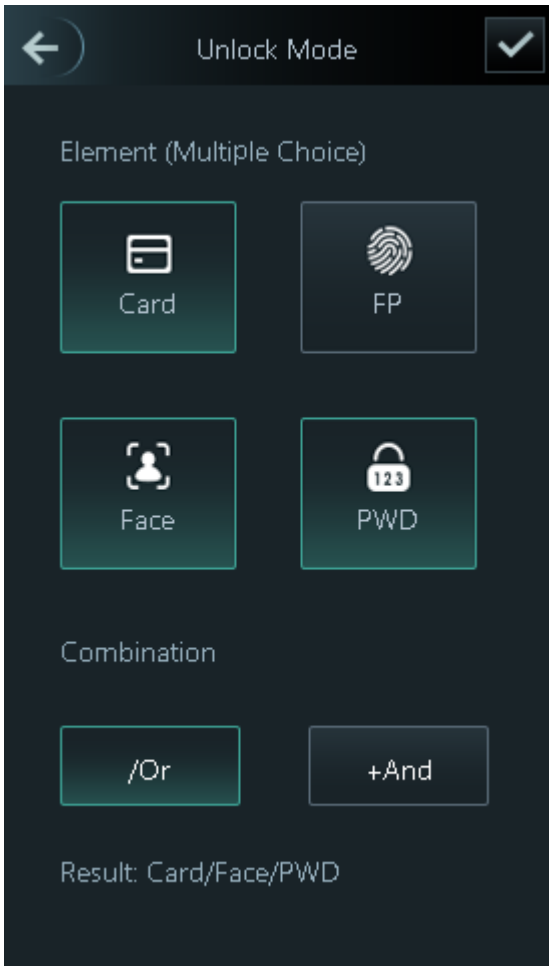
Paso 2 Seleccione métodos de desbloqueo.

Para cancelar su selección, toque nuevamente el método seleccionado.

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 2-8 Elemento (opción múltiple)



Paso 4 Grifo para guardar los cambios.

2.8.2 Configuración de la alarma

Se activará una alarma cuando ocurran eventos de acceso anormales.

Procedimiento

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

Paso 2 Habilitar el tipo de alarma.

Figura 2-9 Alarma

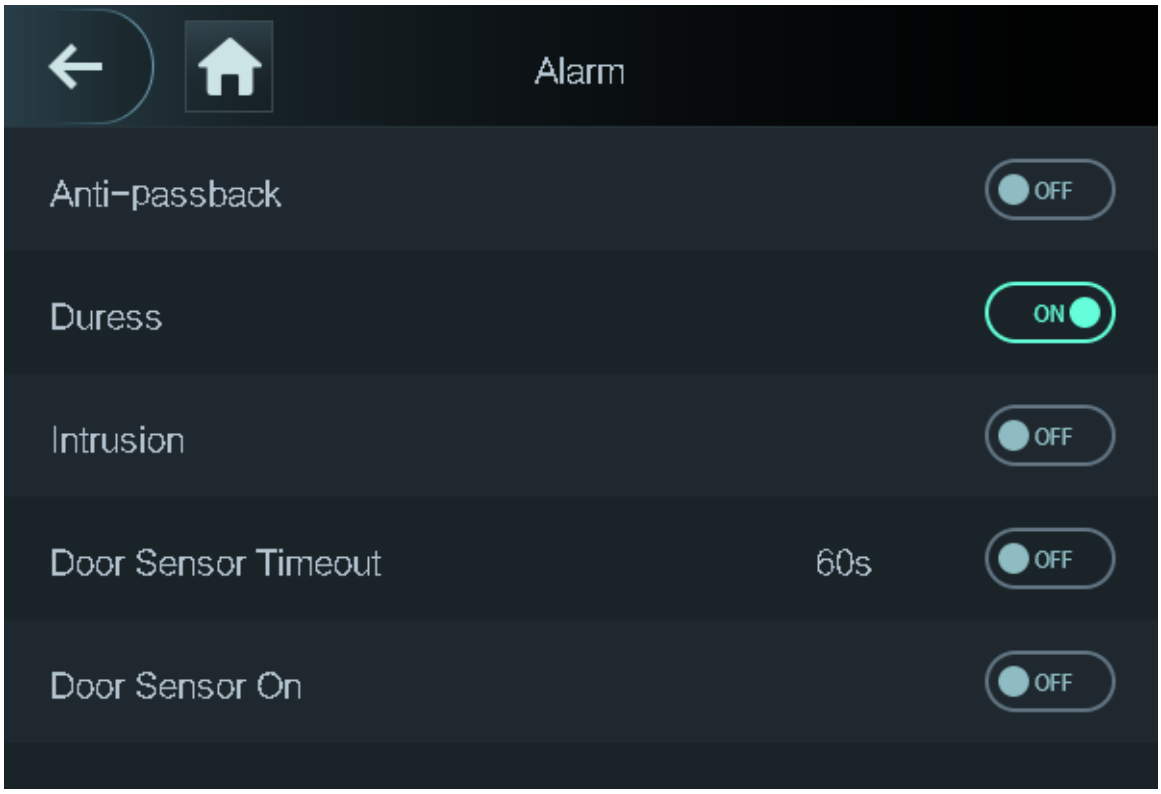


Tabla 2-7 Descripción de los parámetros de alarma

Parámetro	Descripción
Anti-passback	Los usuarios deben verificar su identidad tanto al entrar como al salir; de lo contrario, se activará una alarma. Esto ayuda a evitar que el titular de la tarjeta la entregue a otra persona para que pueda entrar. Cuando la función antirretorno está activada, el titular de la tarjeta debe salir del área protegida a través de un lector de salida para que el sistema le permita entrar de nuevo. ● Si una persona ingresa después de una autorización y sale sin autorización, se activará una alarma cuando intente ingresar nuevamente y se le negará el acceso al mismo tiempo. ● Si una persona ingresa sin autorización y sale después de la autorización, se activará una alarma cuando intente ingresar nuevamente y se le negará el acceso al mismo tiempo.
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 durante más tiempo que el tiempo de espera definido por el sensor de puerta, que varía de 1 a 9999 segundos.
Sensor de puerta activado	Las alarmas de intrusión y tiempo de espera se pueden activar solo después de habilitar el sensor de puerta.

2.8.3 Configuración del estado de la puerta

Procedimiento

Paso 1 En el**Menú principal**pantalla, seleccionar**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 se selecciona, la puerta se desbloqueará y bloqueará según su configuración.

2.8.4 Configuración del tiempo de retención del bloqueo

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

Procedimiento

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

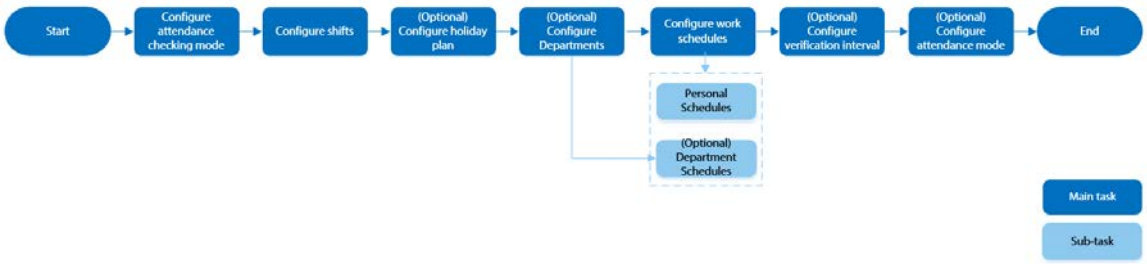
Paso 2 Introduce la duración del desbloqueo. Pulsa para guardar los cambios.

Paso 3

2.9 Gestión de asistencia

El sistema de control de asistencia permite la gestión de asistencia tanto en el dispositivo local como en el Smart PSS Lite. Esta sección solo muestra la configuración de la asistencia en el dispositivo local como ejemplo.

Figura 2-10 Diagrama de flujo de configuración del control de asistencia



2.9.1 Configuración de turnos

Configure turnos para definir las reglas de asistencia. Los empleados deben presentarse a trabajar a la hora de inicio del turno y salir a la hora de fin del mismo, excepto cuando trabajen horas extras.

Procedimiento

Paso 1 Seleccionar**Asistencia**>**Ajuste de cambio**>**Ajuste de cambio**.

Paso 2 Seleccione el número del turno.

Toca para ver más turnos. Puedes configurar hasta 24 turnos.

Paso 3 Configura los parámetros del turno.

Figura 2-11 Elemento (opción múltiple)

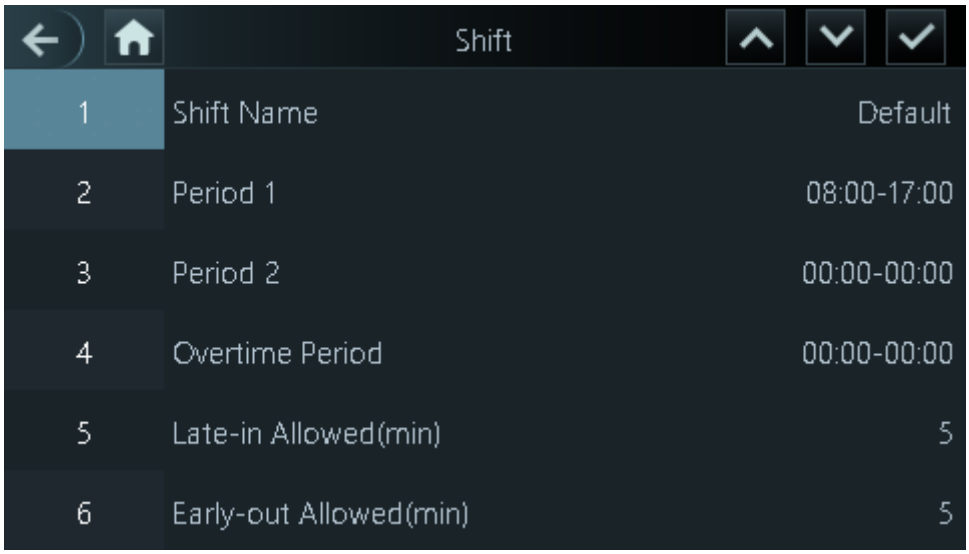


Tabla 2-8 Descripción de los parámetros de turno

Parámetro	Descripción
Nombre del turno	Introduzca el nombre del turno.
Periodo 1	Establezca los períodos de asistencia. Si configura de 08:00 a 17:00, deberá fichar la entrada antes de las 08:00 y la salida a las 17:00 o después; de lo contrario, la asistencia anormal se considerará anormal. Se pueden configurar dos periodos simultáneamente, sin que se superpongan. Los empleados deben registrar su entrada y salida en ambos periodos definidos y asegurarse de que la asistencia sea normal.
Periodo 2	
Período de horas extras	Las personas que fichan su entrada o salida dentro del período de horas extras definido trabajan más allá de las horas normales de trabajo.
Entrada tardía permitida (mín.)	El tiempo permitido para entrar tarde y salir temprano se utiliza principalmente para dar al empleado cierta flexibilidad para llegar un poco tarde o salir un poco antes del trabajo. Por ejemplo, si la hora habitual de entrada es a las 8:00 y el tiempo permitido para entrar tarde es de 5 minutos, al empleado que llegue a las 8:06 a. m. se le contabilizará un minuto de retraso.
Salida anticipada permitida (mín.)	

Todos los horarios de asistencia son precisos hasta el segundo nivel. Por ejemplo, si la hora de fichar...
está configurado a las 8:05 AM, el empleado que registre su entrada a las 8:05:59 AM será marcado como normal
Asistencia. Si el empleado llega a las 8:06 a. m., se le contabilizará un minuto de retraso.

Paso 4 Grifo .

2.9.2 Configuración de planes de vacaciones

Configurar planes de vacaciones durante los cuales no se realizará un seguimiento del tiempo de asistencia.

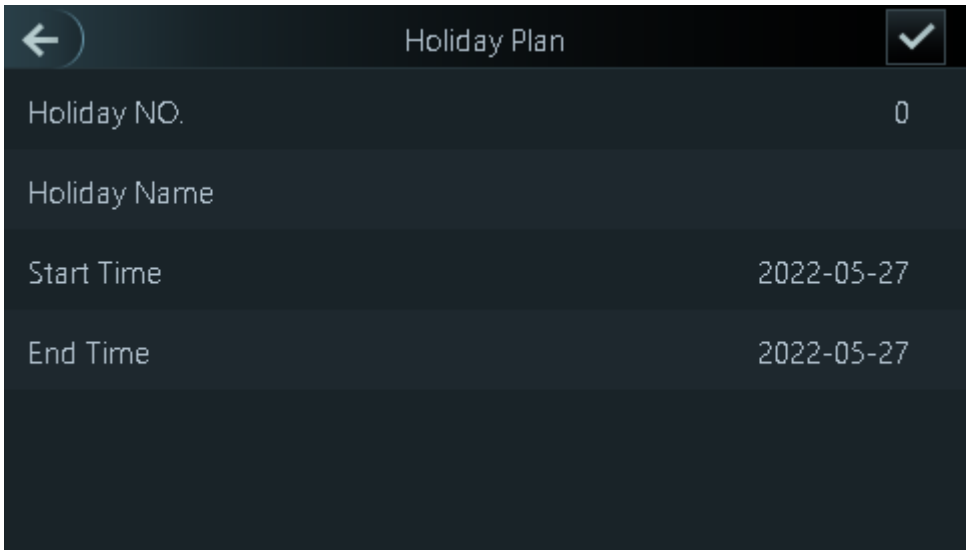
Procedimiento

Paso 1 Seleccionar**Asistencia**>**Ajuste de cambio**>**Día festivo**. Haga

Paso 2 clic para agregar planes de vacaciones.

Paso 3 Configurar los parámetros.

Figura 2-12 Plan de vacaciones



Paso 4 Grifo .

2.9.3 Configuración de departamentos

Definir departamentos.

Procedimiento

Paso 1 Seleccionar**Asistencia**>**Conjunto de dependencias**Seleccione

Paso 2 un departamento y luego cámbiele el nombre.

Existen 20 departamentos predeterminados. Recomendamos cambiarles el nombre.

Figura 2-13 Elemento (opción múltiple)

Paso 3 Grifo .

2.9.4 Configuración de horarios de trabajo

Un horario de trabajo generalmente se refiere a los días al mes y las horas diarias que se espera que un empleado esté en su trabajo. Puedes crear diferentes tipos de horarios de trabajo según diferentes...

individuos o departamentos, y luego los empleados deben seguir los horarios de trabajo establecidos.

Procedimiento

Paso 1 Seleccionar**Asistencia**>**Cronograma**.

Paso 2 Establecer horarios de trabajo para personas. 1. Toque**Horario personal**

2. Ingrese el ID de usuario y luego toque

3. En el calendario, seleccione la fecha y luego configure los turnos.

Sólo puedes establecer horarios de trabajo para el mes actual y el mes siguiente.

- 0 indica ruptura.
- Del 1 al 24 indica el número de turnos predefinidos. Para configurar los turnos, consulte "2.9.1 Configuración de turnos".
- 25 indica el viaje de negocios.
- 26 indica la licencia de ausencia.

4. Toque

Paso 3 Establecer horarios de trabajo para el departamento. 1. Toque **Horario del departamento**.

2. Toque un departamento y establezca turnos para una semana.

- 0 indica ruptura.
- Del 1 al 24 indica el número de turnos predefinidos. Para configurar los turnos, consulte "2.9.1 Configuración de turnos".
- 25 indica el viaje de negocios.
- 26 indica la licencia de ausencia.

Figura 2-14 Turnos departamentales

El horario de trabajo definido es en ciclos de una semana y se aplicará a todos los empleados de la departamento.

Paso 4 Grifo .

2.9.5 Configuración del tiempo del intervalo de verificación

el empleado repite el registro de entrada/salida dentro de un tiempo establecido, se registrará el registro de entrada/salida más temprano.

Procedimiento

Paso 1 Seleccionar**Asistencia**>**Cronograma**>**Tiempo(s) de intervalo de verificación**.

Paso 2 Ingrese el intervalo de tiempo y luego toque .

2.9.6 Configuración de modos de asistencia

Al fichar su entrada o salida, puede configurar los modos de asistencia para definir el estado del tiempo de asistencia.

Procedimiento

Paso 1 En el menú principal, toque**Asistencia**y luego toque para pasar a la página siguiente y luego encienda **Local/Remoto**.

Puede configurar el modo de asistencia solo después de la**Local/Remoto**La función está activada y los registros de asistencia local se cargarán en Smart PSS Lite.

Paso 2 En la pantalla del menú principal, seleccione**Asistencia**>**Conjunto de modos**.

Figura 2-15 Modo de asistencia

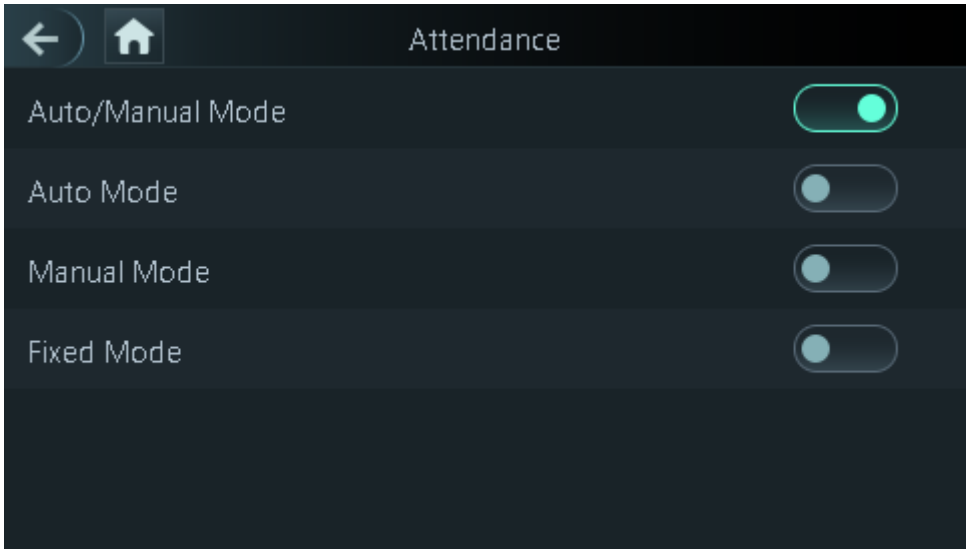


Tabla 2-9 Modo de asistencia

Parámetro	Descripción
Modo automático/manual	Después de registrar su entrada o salida, puede seleccionar fácilmente el estado de asistencia o la pantalla mostrará automáticamente el estado del tiempo de asistencia.
Modo automático	La pantalla muestra el estado de asistencia automáticamente después de registrar su entrada o salida.
Modo manual	Marcar entrada/salida y luego tocar**Estado de asistencia**Seleccionar con valentía el estado de asistencia.
Modo fijo	Al registrar su entrada o salida, la pantalla mostrará el estado de asistencia preconfigurado todo el tiempo.

Paso 3 Seleccione un modo de asistencia.

Paso 4 Configure los parámetros para el modo de asistencia.

Figura 2-16 Modo automático/modo manual

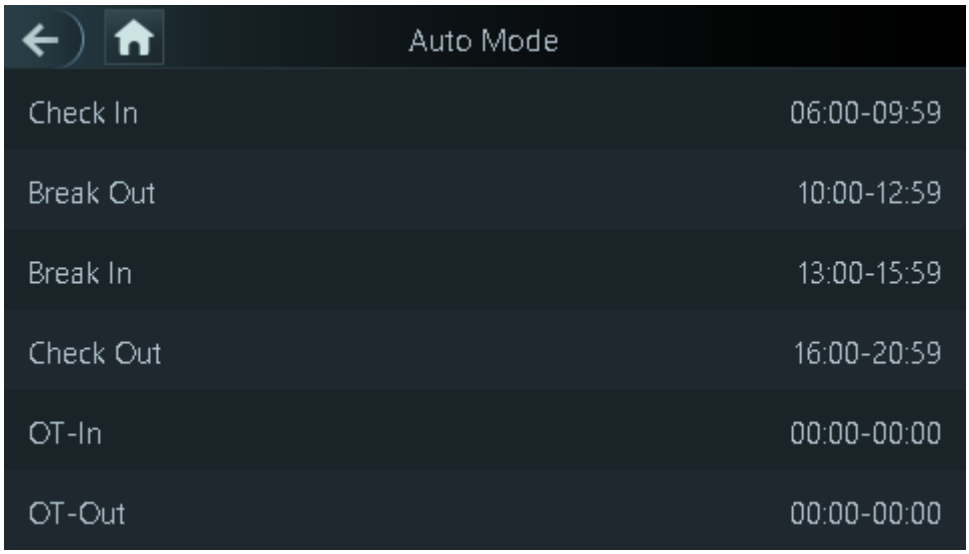


Figura 2-17 Modo fijo

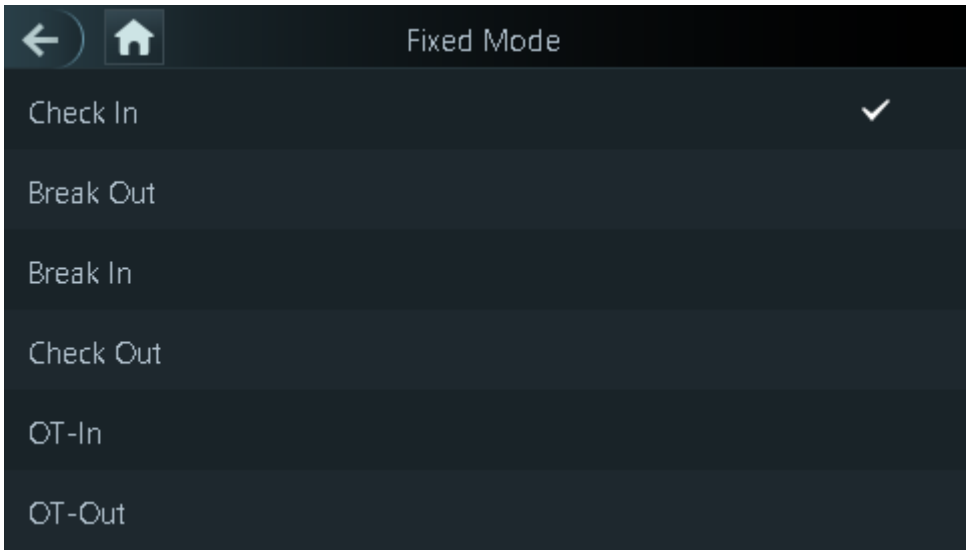


Tabla 2-10 Parámetros del modo de asistencia

Parámetros	Descripción
Registrarse	Marque su entrada cuando comience su jornada laboral habitual.
Fugarse	Marque su salida cuando finalice su licencia.
Interrumpir	Fiche cuando comience su licencia.
Verificar	Marque su salida cuando comience su jornada laboral normal.
Entrada OT	Ficha tu horario cuando empiezan tus horas extras de trabajo.
OT-Fuera	Marque su salida cuando finalice su jornada laboral de horas extras.

2.10 Sistema

2.10.1 Configuración de la hora

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

Procedimiento

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

Paso 2 Configurar la hora del sistema.

Figura 2-18 Tiempo

Tabla 2-11 Descripción de los parámetros de tiempo

Parámetro	Descripción
Sistema de 24 horas	La hora se muestra en formato de 24 horas.
Ajuste de fecha	Establecer la fecha.
Tiempo	Establezca la hora.
Formato de fecha	Seleccione un formato de fecha.

Parámetro	Descripción
Configuración del horario de verano	1. Toque**Configuración del horario de verano** 2. Habilitar el horario de verano. 3. Seleccionar**Fecha**o**Semana**desde**Horario de verano**Lista de tipos. 4. Ingrese la hora de inicio y la hora de finalización. 5. toque
Comprobación NTP	Un servidor de protocolo de tiempo de red (NTP) es una máquina dedicada a sincronizar la hora de todos los equipos cliente. Si su equipo está configurado para sincronizarse con un servidor horario de la red, su reloj mostrará la misma hora que el servidor. Cuando el administrador cambie la hora (para el horario de verano), todos los equipos cliente de la red también se actualizarán. 1. Toque**Comprobación NTP**. 2. Active la función de verificación NTP y configure los parámetros. ● **Dirección IP del servidor**:Ingrese la dirección IP del servidor NTP y el controlador de acceso sincronizará automáticamente la hora con el servidor NTP. ● **Puerto**:Ingrese el puerto del servidor NTP. ● **Intervalo (min)**: Introduzca el intervalo de sincronización horaria.
Huso horario	Seleccione la zona horaria.

2.10.2 Configuración de parámetros faciales

Procedimiento

Paso 1 En el menú principal, seleccione**Sistema**>**Parámetros faciales**

Paso 2 . Configure los parámetros del rostro y luego toque .

Figura 2-19 Parámetro de rostro (01)

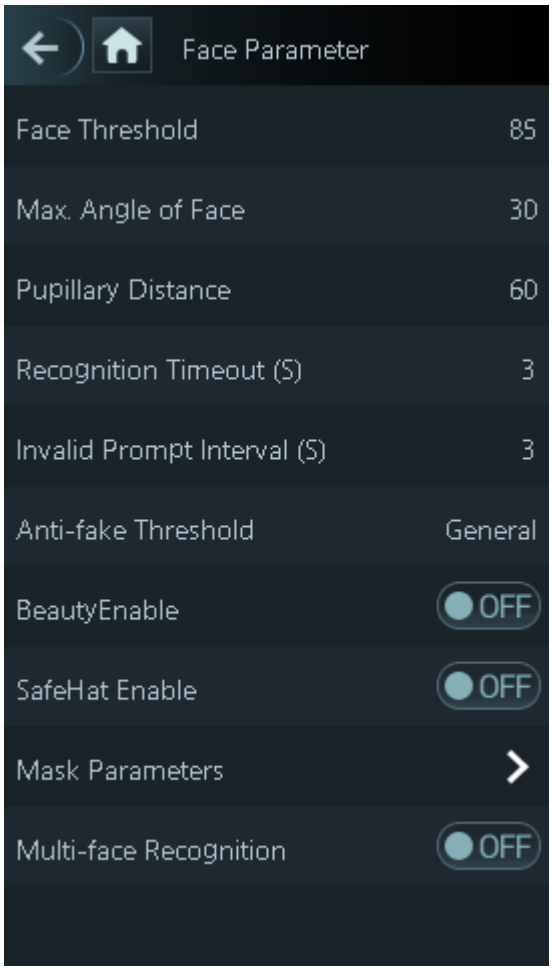


Tabla 2-12 Descripción de los parámetros faciales

Nombre	Descripción
Umbral facial	Ajuste la precisión del reconocimiento facial. Un umbral más alto significa mayor precisión.
Ángulo máximo de la cara	Establezca el ángulo máximo de pose facial para la detección facial. Un valor mayor implica un rango de ángulo facial mayor. Si el ángulo de pose facial está fuera del rango definido, el cuadro de detección facial no aparecerá.
Distancia pupilar	Las imágenes faciales requieren la distancia pupilar (píxeles) deseada entre los ojos para un reconocimiento correcto. El valor predeterminado es 45 píxeles. Este valor varía según el tamaño del rostro y la distancia entre los rostros y la lente. Si un adulto se encuentra a 1,5 metros de la lente, la distancia pupilar puede ser de 50 a 70 píxeles.
Tiempo de espera de reconocimiento (S)	Si se reconoce correctamente el rostro de una persona con permiso de acceso, el controlador de acceso indicará que el reconocimiento facial se ha realizado correctamente. Puede introducir el intervalo de tiempo para la indicación.
Intervalo de aviso de rostro 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 de reconocimiento facial. Puede introducir el intervalo de tiempo para la indicación.

Nombre	Descripción
Umbral anti-falsificación	Evite el reconocimiento facial falso utilizando una foto, un vídeo, una 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 la puerta para personas con mascarillas. ● Alto: un mayor nivel de detección anti-spoofing significa mayor precisión y seguridad. ● Extremadamente alto: un nivel extremadamente alto de detección anti-spoofing significa una precisión y seguridad extremadamente altas.
Belleza habilitada	Embellecer imágenes de rostros capturados.
Habilitar SafeHat	Detecta sombreros seguros.
Parámetros de la máscara	● Modo máscara: ◇ **Sin detección**:La máscara no se detecta durante el reconocimiento facial. ◇ **Recordatorio de mascarilla**Se detecta mascarilla durante el reconocimiento facial. Si la persona no la lleva, el sistema le recordará que la use y se le permitirá el acceso. ◇ **Intercepción de máscara**: Se detecta una mascarilla durante el reconocimiento facial. Si una persona no la lleva, el sistema le recordará que la use y se le denegará el acceso. ● Umbral de reconocimiento de máscara: un umbral más alto significa una mayor precisión en la detección de máscara.
Reconocimiento de múltiples caras	Permite detectar 4 imágenes faciales simultáneamente, y el modo de combinación de desbloqueo se invalida. La puerta se desbloquea cuando cualquiera de ellos accede.

2.10.3 Ajuste del volumen

Puede ajustar el volumen del altavoz y del micrófono.

Procedimiento

Paso 1 En 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 dactilares

Configure la precisión de la detección de huellas dactilares. Un valor más alto significa un umbral de similitud más alto y una mayor precisión. Esta función solo está disponible en controladores de acceso compatibles con desbloqueo por huella dactilar.

Procedimiento

Paso 1 En el**Menú principal**, seleccionar**Sistema**>**Parámetro**

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

2.10.5 Configuración de pantalla

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

Procedimiento

Paso 1 En el**Menú principal**, seleccionar**Sistema**>**Configuración de pantalla**. Grifo**Hora de**

Paso 2 **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

Procedimiento

Paso 1 En el**Menú principal**, seleccionar**Sistema**>**Restaurar fábrica**. Restaurar los valores

Paso 2 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 los registros.

2.10.7 Reiniciar el dispositivo

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

2.10.8 Configuración del idioma

Cambiar el idioma en el controlador de acceso. En el**Menú principal**, seleccionar**Sistema**>**Idioma**, seleccione el idioma para el controlador de acceso.

2.11 Administración 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 desconecte el USB ni realice ninguna operación del Acceso Controlador durante el proceso.
- Debes usar un USB para exportar la información de un controlador de acceso a otros dispositivos. Cara No se permite importar imágenes a través de USB.

2.11.1 Exportación a USB

Puede exportar datos del controlador de acceso a una memoria USB. Los datos exportados están cifrados y no se pueden editar.

Procedimiento

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

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

2.11.2 Importación desde USB

Puede importar datos desde USB al controlador de acceso.

Procedimiento

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

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

2.11.3 Actualización del sistema

Utilice un USB para actualizar el sistema del controlador de acceso.

Procedimiento

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 controlador de acceso.

Paso 2 En 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

En el**Menú principal**pantalla, seleccionar**Características**.

Figura 2-20 Características

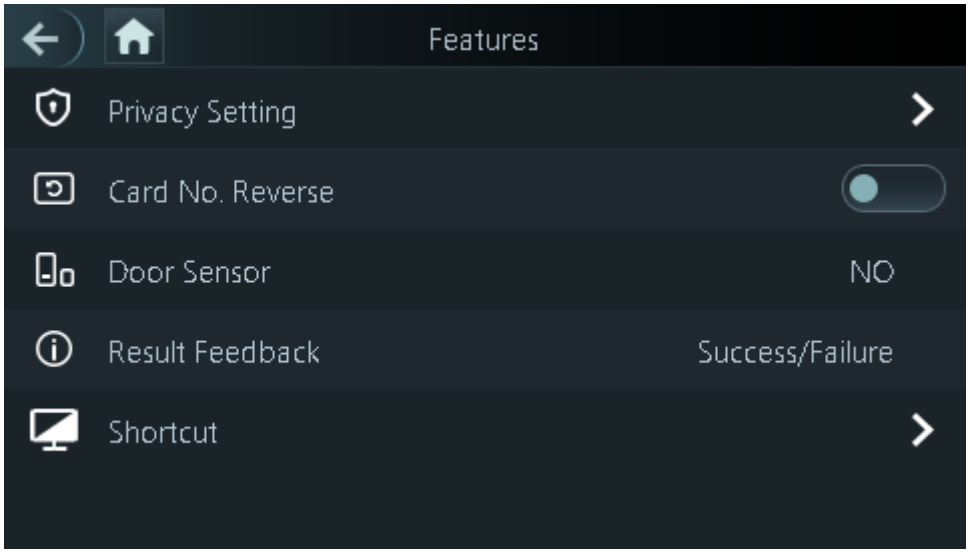


Tabla 2-13 Descripción de características

Parámetro	Descripción
Entorno privado	● Habilitar restablecimiento de contraseña: Puede habilitar esta función para restablecer la contraseña. La función Restablecer contraseña está habilitada por defecto. ● HTTPS: Protocolo seguro de transferencia de hipertexto (HTTPS) es un protocolo para la comunicación segura a través de una red informática. Cuando HTTPS está habilitado, se utilizará HTTPS 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: Se capturarán imágenes faciales automáticamente al abrir la puerta. Esta función está activada por defecto. ● Borrar fotos capturadas: elimina todas las fotos capturadas automáticamente.
Tarjeta N.º Reverso	Cuando el controlador de acceso se conecta a un dispositivo de terceros a través de la entrada Wiegand, y el número de tarjeta leído por el terminal de acceso está en el orden de reserva del número de tarjeta real, debe activar la función**Tarjeta N.º Reverso**función.
Sensor de puerta	NC: Cuando la puerta se abre, el circuito del sensor de la puerta se cierra. NO: Cuando la puerta se abre, el circuito del sensor de la puerta está abierto. Las alarmas de intrusión y de horas extras se activan solo después de que se enciende el detector de puerta.
Comentarios sobre los resultados	● Éxito/Fracaso: solo muestra el éxito o el fracaso en la pantalla de espera. ● Solo nombre: muestra el ID del usuario, el nombre y el tiempo de autorización después de conceder el acceso; muestra el mensaje de no autorizado y el tiempo de autorización después de denegar el acceso. ● Foto y nombre: muestra la imagen del rostro registrado del usuario, el ID del usuario, el nombre y el tiempo de autorización después de conceder el acceso; muestra el mensaje de no autorizado y el tiempo de autorización después de denegar el acceso. ● Fotos y nombre: muestra la imagen del rostro capturada y una imagen del rostro registrada de un usuario, el ID del usuario, el nombre y el tiempo de autorización después de conceder el acceso; muestra un mensaje de no autorizado y el tiempo de autorización después de denegar el acceso.

Parámetro	Descripción
Atajo	Seleccione los 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. ● Timbre: después de activar la función de timbre, el ícono del timbre se muestra en la pantalla de espera. ◇ RingBell: toque el ícono de timbre en la pantalla de espera y el controlador de acceso sonará. ◇ Vinculación de alarma: active la función de vinculación de alarma y luego sonará el timbre.  Esta función sólo está disponible en modelos seleccionados. ◇ Configuración de RingBell: seleccione el timbre de llamada 1 o el timbre de llamada 2. ◇ Duración del timbre: Establezca la duración del timbre (1-30 s). El valor predeterminado es 3. ● 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 sala 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: ingrese el número de sala y luego puede tocar el ícono de llamada en la pantalla de espera para llamar al número de sala definido.  Asegúrese de que el controlador de acceso se haya agregado a DMSS.

2.13 Desbloqueo de la puerta

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

2.13.1 Desbloqueo mediante tarjetas

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

2.13.2 Desbloqueo por rostro

Verifica la identidad de una persona detectando su rostro. Asegúrate de que el rostro esté centrado en el marco de detección.

2.13.3 Desbloqueo por contraseña de usuario

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

Procedimiento

Paso 1 Grifo en la pantalla de espera.

Paso 2 grifo**Desbloqueo de PWD**, y luego ingrese el ID de usuario y la contraseña.

Paso 3 Toque**Sí**.

2.13.4 Desbloqueo mediante contraseña de administrador

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

Prerrequisitos

Se configuró la contraseña de administrador. Para más detalles, consulte "2.6.3 Configuración de la contraseña de administrador".

Procedimiento

Paso 1 Grifo en la pantalla de espera.

Paso 2 Grifo**Contraseña de administrador**, y luego ingrese la contraseña de

Paso 3 administrador. Toque .

La contraseña de administrador no se puede utilizar para desbloquear la puerta si el estado está configurado como NC.

2.13.5 Desbloqueo mediante código QR

Procedimiento

Paso 1 En la pantalla de espera, toque .

Paso 2 Coloque su código QR delante de la lente.

2.13.6 Desbloqueo por huella dactilar

Coloque el dedo sobre el lector de huellas dactilares. Esta función solo está disponible en el controlador de acceso compatible con el desbloqueo por huella dactilar.

2.13.7 Desbloqueo mediante contraseña temporal

Desbloquee la puerta con la contraseña temporal.

Procedimiento

Paso 1 Agregue el controlador de acceso a DMSS.

DMSS generará una contraseña temporal para desbloquear la puerta. En la

Paso 2 pantalla de inicio, toque y luego toque**Personal temporal**. Introduzca la

Paso 3 contraseña temporal.

2.14 Información del sistema

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

2.14.1 Visualización de la capacidad de datos

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

2.14.2 Versión del dispositivo de visualización

En 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 del controlador de acceso.

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 restaure a los valores predeterminados de fábrica.

Prerrequisitos

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

Procedimiento

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

Le recomendamos que utilice la última versión de Chrome o Firefox.

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

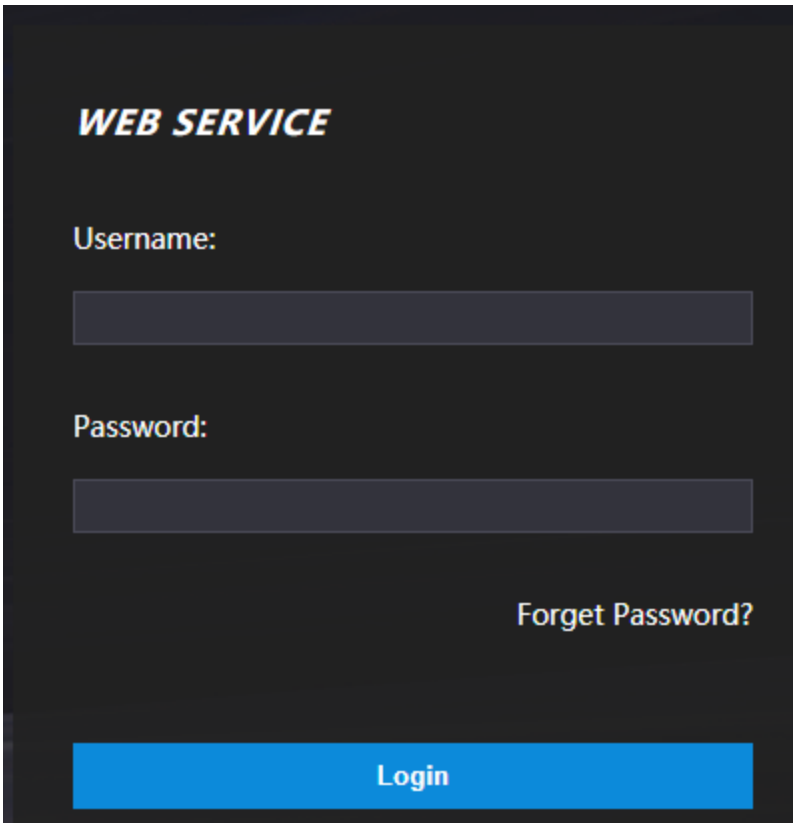
- La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y especiales caracteres (excluyendo ' " ; : &). Establezca una contraseña de alta seguridad siguiendo la contraseña Indicación de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

3.2 Inicio de sesión

Procedimiento

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

Figura 3-1 Inicio de sesión



Paso 2 Introduzca el nombre de usuario y la contraseña.

- El nombre de administrador predeterminado es admin y la contraseña es la que usted configure. Durante la inicialización, 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**¿Olvidaste tu contraseña?**Para Para más detalles, consulte "3.3 Restablecer la contraseña".

Paso 3 Hacer clic**Acceso**.

3.3 Restablecimiento de la contraseña

Restablezca la contraseña a través del correo electrónico vinculado cuando olvide la contraseña de administrador.

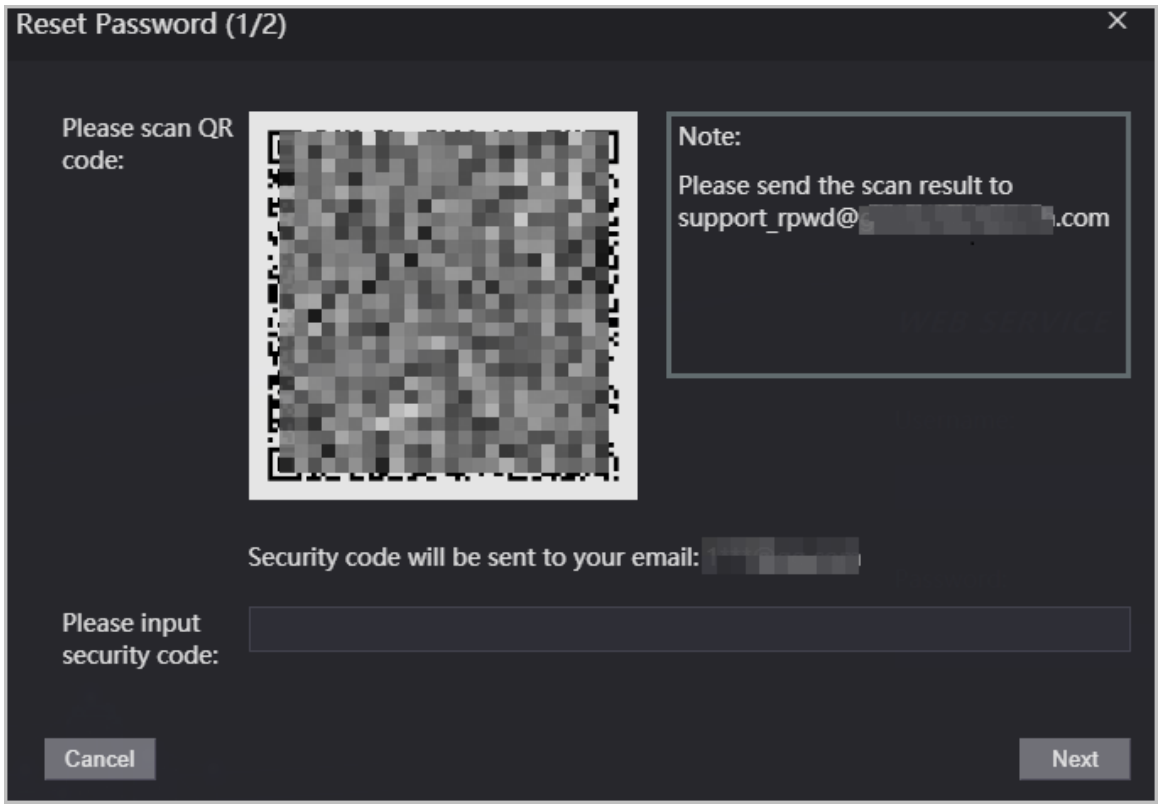
Procedimiento

Paso 1 En la página de inicio de sesión, haga clic en**Has olvidado tu contraseña**.

Paso 2 Lea atentamente las instrucciones en pantalla y luego haga clic**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 al escanear 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, recibirás un código de seguridad en tu correo electrónico vinculado. Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, se... se vuelven inválidos.
- Si se ingresa un código de seguridad incorrecto en una fila, la cuenta de administrador se congelará durante 5 minutos.

Paso 4 Introduzca el código de seguridad.

Paso 5 Haga clic.**Próximo**.

Paso 6 Restablecer y confirmar la nueva contraseña.

La contraseña debe constar de 8 a 32 caracteres que no sean espacios 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 de parámetros de la puerta

Configurar los parámetros de control de acceso.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccione**Parámetros de la puerta**.

Figura 3-3 Parámetro de puerta

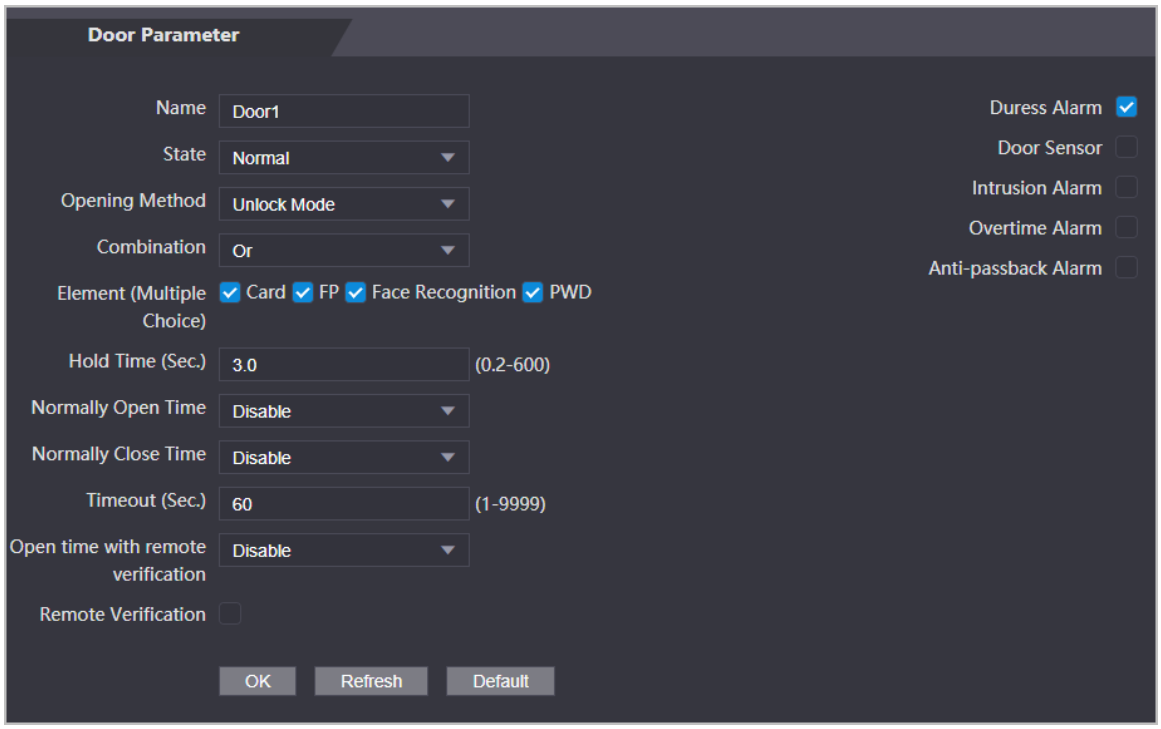


Tabla 3-1 Descripción de los parámetros de la puerta

Parámetro	Descripción
Nombre	Introduzca un nombre para 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 se selecciona, la puerta se desbloqueará y bloqueará según su configuración.
Método de apertura	● Desbloquear por período: configure 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 retención (seg.)	Tras conceder el acceso a una persona, la puerta permanecerá desbloqueada durante un tiempo definido para que pueda pasar. Este tiempo varía entre 0,2 s y 600 s.
Tiempo normalmente abierto	La puerta permanece abierta o cerrada durante el período definido.
Hora de cierre normal	
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 periodo de apertura de la puerta para la verificación remota. Una vez que los usuarios accedan al controlador de acceso, también deben obtener acceso desde la plataforma de administración antes de que se desbloquee la puerta.
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 se pueden activar solo después **Sensor de puerta**está habilitado.

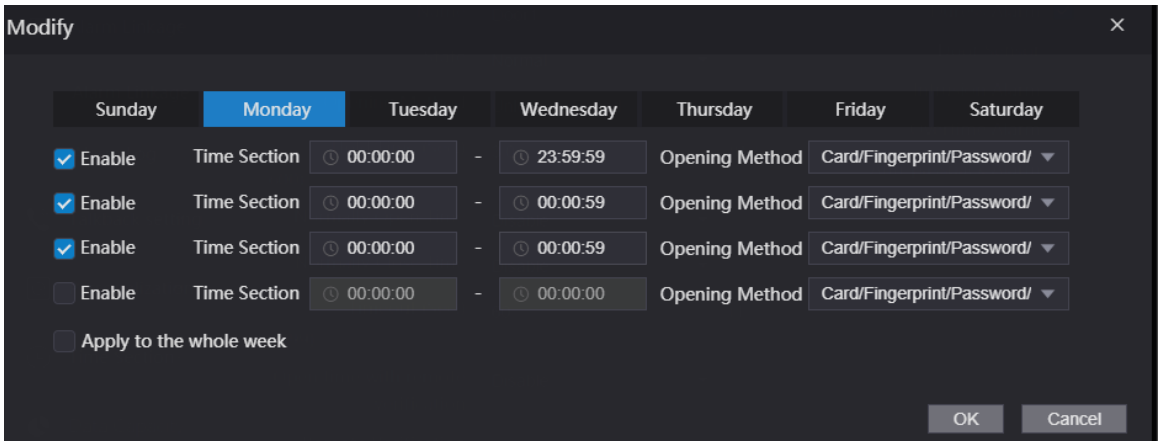
Parámetro	Descripción
Alarma de intrusión	Cuando**Sensor de puerta**está habilitado, se activará una alarma de intrusión si la puerta se abre de forma anormal.
Alarma de horas extras	Se activará una alarma de tiempo de espera si la puerta permanece desbloqueada durante más tiempo del indicado.**Tiempo de espera (seg.)**.
Alarma anti-passback	Los usuarios deben verificar su identidad tanto al entrar como al salir; de lo contrario, se activará una alarma. Esto ayuda a evitar que el titular de la tarjeta la entregue a otra persona para que pueda entrar. Cuando la función antirretorno está activada, el titular de la tarjeta debe salir del área protegida a través de un lector de salida para que el sistema le permita entrar de nuevo. ● Si una persona ingresa después de una autorización y sale sin autorización, se activará una alarma cuando intente ingresar nuevamente y se le negará el acceso al mismo tiempo. ● Si una persona ingresa sin autorización y sale después de la autorización, se activará una alarma cuando intente ingresar nuevamente y se le negará el acceso al mismo tiempo.

Paso 3 Configurar el método de apertura.

- Desbloqueo por período

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

Figura 3-4 Parámetro de la sección de tiempo



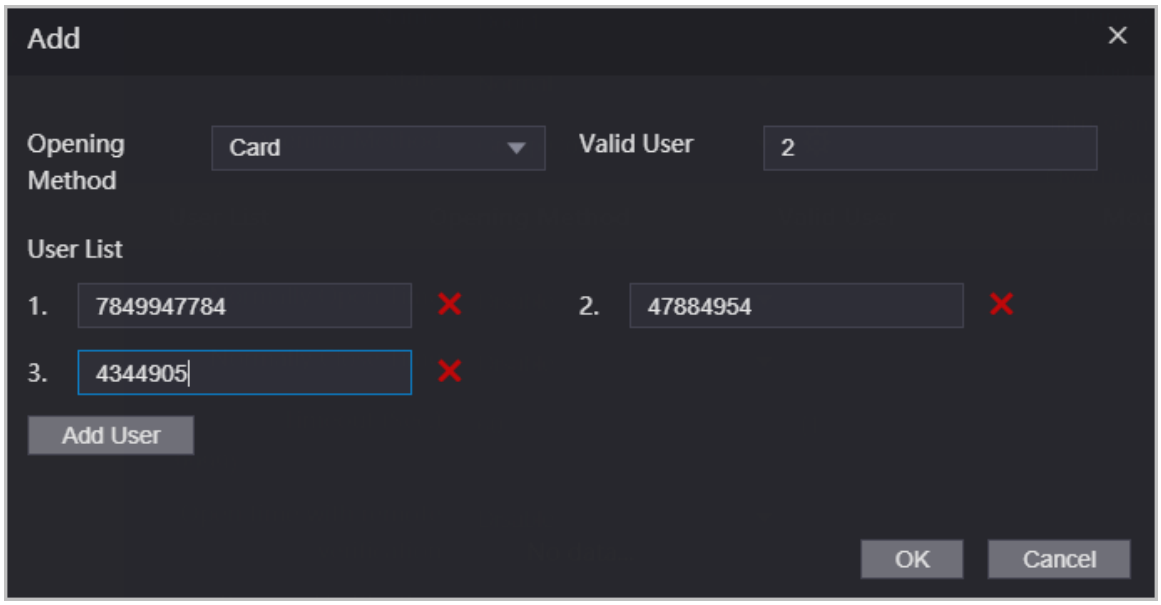
2. Configure la hora y el método de apertura de cada sección horaria. Puede configurar hasta cuatro secciones horarias para un mismo día.
3. Seleccionar**Aplicar a toda la semana.**para copiar la hora definida al resto de días.

- Combinación de grupos

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

Si el número de usuarios válidos es 2 y hay 3 usuarios en la lista definida, se requieren dos usuarios para conceder 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 lista de bloqueo.
- ◇ Los usuarios válidos en todos los grupos deben verificar sus identidades para otorgar acceso al grupo. orden.

5. Haga clic**DE ACUERDO**.

- Modo de desbloqueo

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

Paso 4 Configurar otros parámetros. Haga clic en

Paso 5 **DE ACUERDO**.

3.5 Configuración del intercomunicador

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

3.5.1 Configuración del servidor SIP

Al conectarse al mismo servidor SIP, todos los VTO y VTH pueden comunicarse entre sí. Puede usar el controlador de acceso, otros VTO o la plataforma de gestión como servidor SIP.

Información de fondo

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

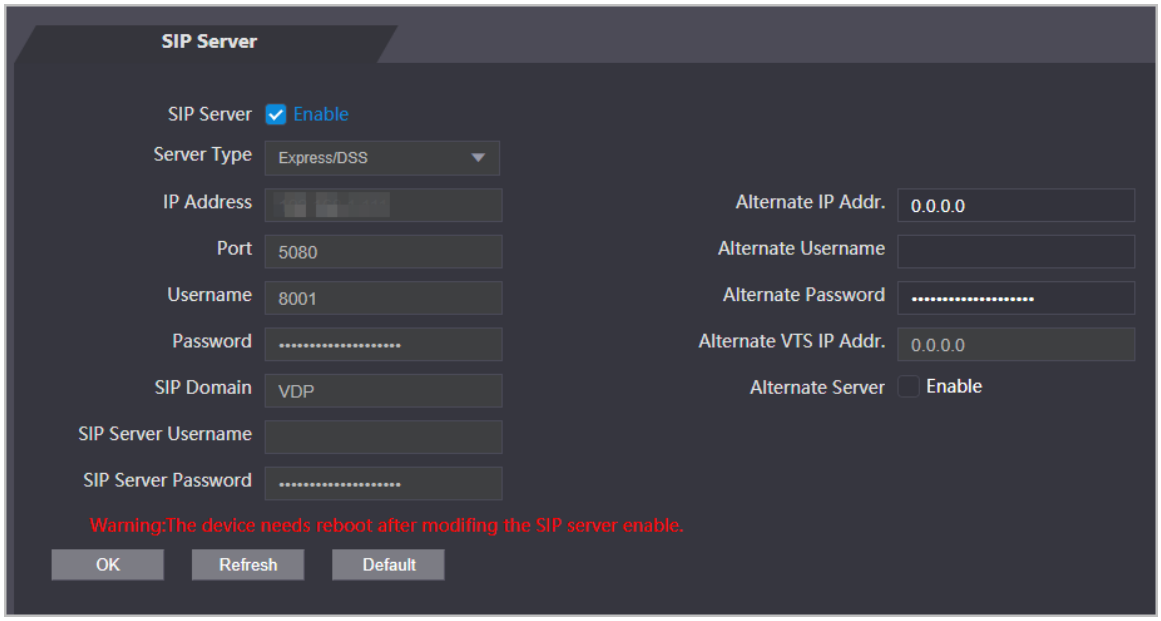
Procedimiento

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

Paso 2 Seleccione un tipo de servidor.

- Utilice el controlador de acceso como servidor SIP. Active**Servidor SIP**y mantener los demás parámetros como predeterminados.

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**Tipo de servidor**.
  2. Configure los parámetros y luego haga clic en**Ahorrar**.

Figura 3-7 Utilice VTO como servidor SIP

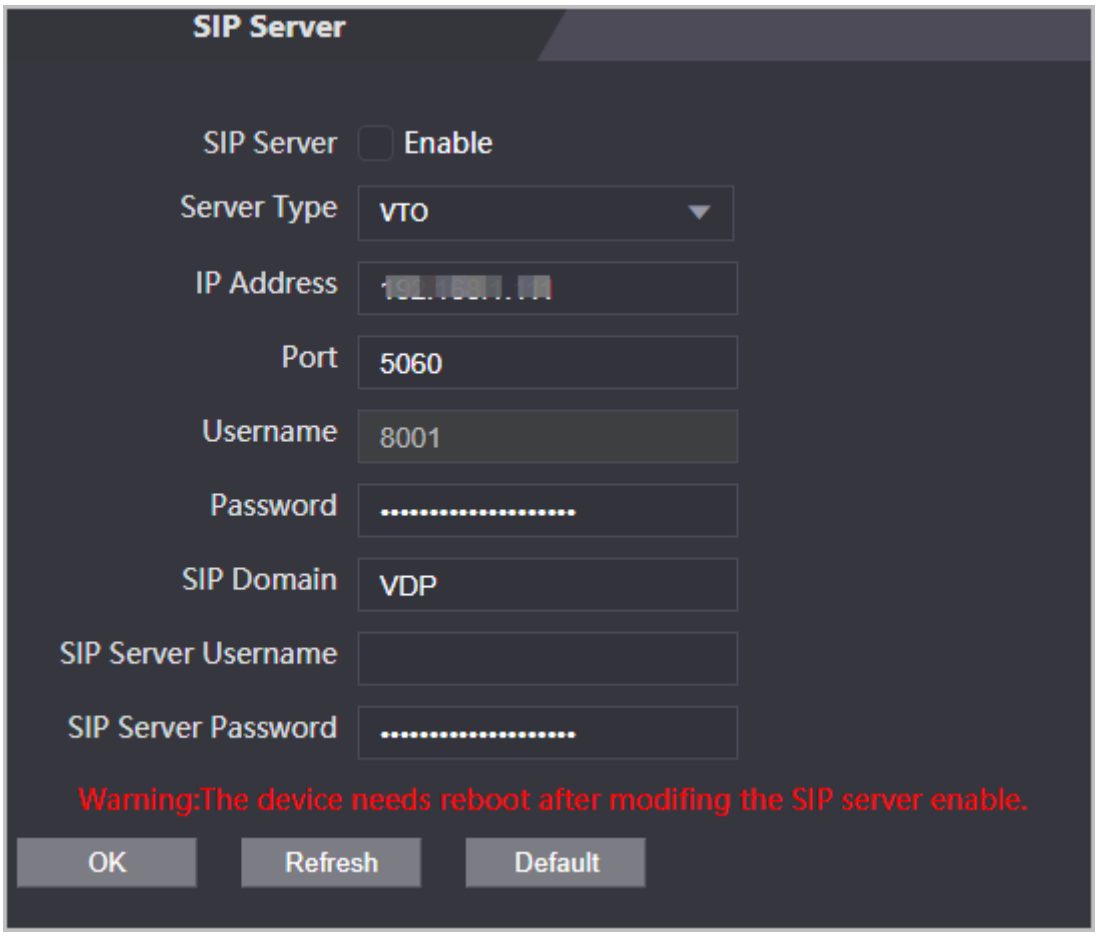


Tabla 3-2 Configuración del servidor SIP

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	Déjalo como predeterminado.
Contraseña	
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 habilitar**Servidor SIP**. Seleccionar**Express/DSS**desde**Tipo de servidor**.

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

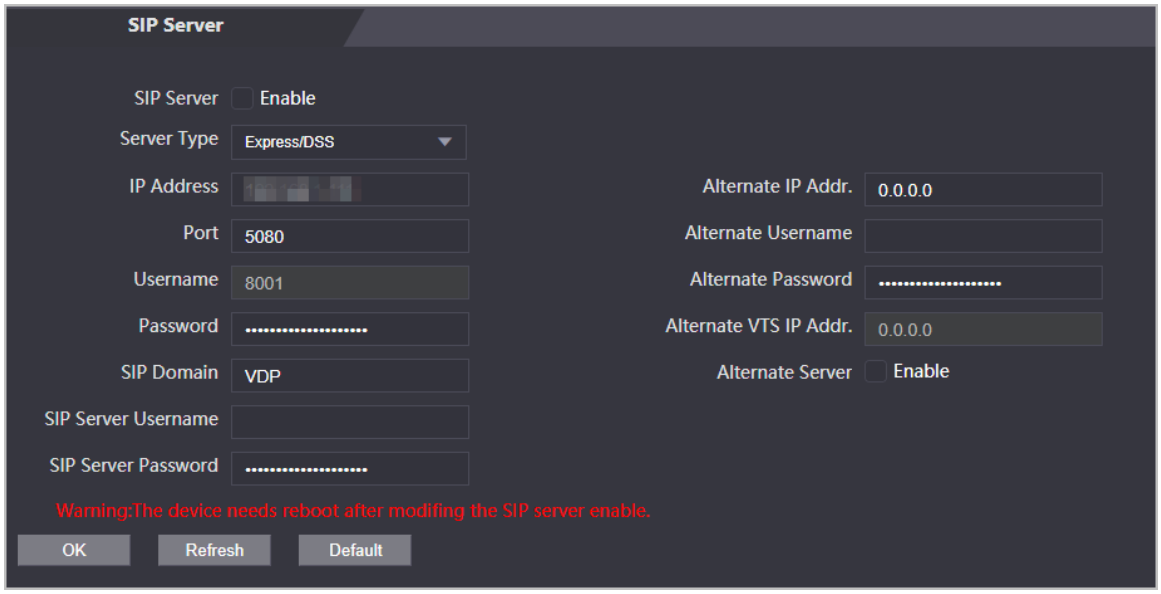


Tabla 3-3 Configuración del servidor SIP

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	Déjalo como predeterminado.
Contraseña	
Dominio SIP	Déjalos como predeterminados.
Nombre de usuario del servidor SIP	El nombre de usuario y la contraseña de inicio de sesión de la plataforma.
Contraseña del servidor SIP	

Parámetro	Descripción
Dirección IP alternativa.	El servidor alternativo se utilizará como servidor SIP cuando DSS Express o DSS Pro no respondan. Le recomendamos configurar la dirección IP alternativa. ● Si enciendes el**Servidor alternativo**Función, configurará los controladores de acceso en el servidor alternativo. ● Si desea que otro VTO funcione como servidor alternativo, debe Es necesario introducir la dirección IP, el nombre de usuario y la contraseña del VTO. No habilitar.**Servidor alternativo**en este caso. ● Le recomendamos que configure el VTO principal como servidor alternativo.
Nombre de usuario alternativo	Se utiliza para iniciar sesión en el servidor alternativo.
Contraseña alternativa	
Dirección IP alternativa de VTS.	Ingrese la dirección IP del VTS alternativo. Si la plataforma de administración no responde, se activará el VTS alternativo para garantizar que el VTO, el VTH y el VTS sigan funcionando con 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.

Procedimiento

Paso 1 Seleccionar**Talkback**>**Local**.

Paso 2 Configure los parámetros.

● Utilice el controlador de acceso como servidor SIP.

Figura 3-9 Parámetro básico

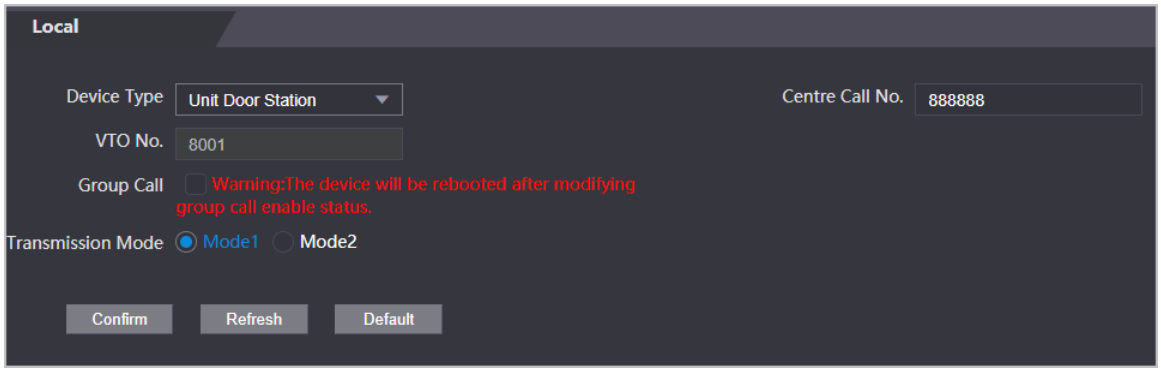


Tabla 3-4 Descripción de parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccionar**Estación de puerta de la unidad**.
VTO N°	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 + N.º de VTS cuando el VTO llama al VTS. Puede consultar el número del VTS en**Dispositivo**Pantalla de 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**.
VTO N°	El número del VTO. - El número debe tener cuatro dígitos. Los dos primeros dígitos son 80 y los dos últimos dígitos empiezan desde 01. Tomemos 8001 como ejemplo. - Si existen varios VTO en una unidad, no se puede indicar el número de VTO. repetido.
Número de llamada del centro	El número de teléfono predeterminado para el centro de administración 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

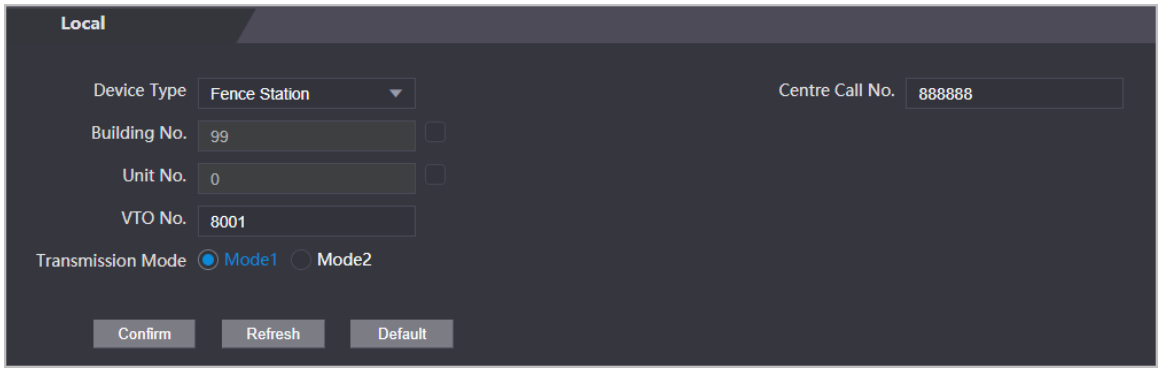


Tabla 3-6 Descripción de parámetros básicos

Parámetro	Descripción	
Tipo de dispositivo	Seleccione el tipo de dispositivo según la posición de instalación.	
Edificio No.	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, introduzca el número de edificio y el número de unidad en la página web. El número de edificio, el número de unidad y el número de VTO deben cumplir con los parámetros configurados en DSS.
Unidad N°	Seleccione la casilla de verificación y luego ingrese el número de la unidad donde se encuentra la estación de puerta de la unidad instalado.	

Parámetro	Descripción	
VTO N°	El número de la estación de puerta de la unidad. Si existen varios VTO en una unidad, el VTO No. No se puede repetir.	Tome la habitación 1001, 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... Si está habilitado, el número de habitación es "1001". Para más detalles, consulte el manual de usuario de DSS.
Número de llamada del centro	El número de teléfono predeterminado es 888888 cuando el VTO llama al VTS. Manténgalo como predeterminado.	
Transmisión Modo	El modo 1 está seleccionado de forma predeterminada.	

Paso 3 Hacer clic**Confirmar**.

3.5.3 Adición del 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.

Procedimiento

Paso 1 En la página web del Controlador de Acceso, seleccione**Configuración de Talkback**>**VTO No. Gestión**.

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

Figura 3-12 Agregar VTO

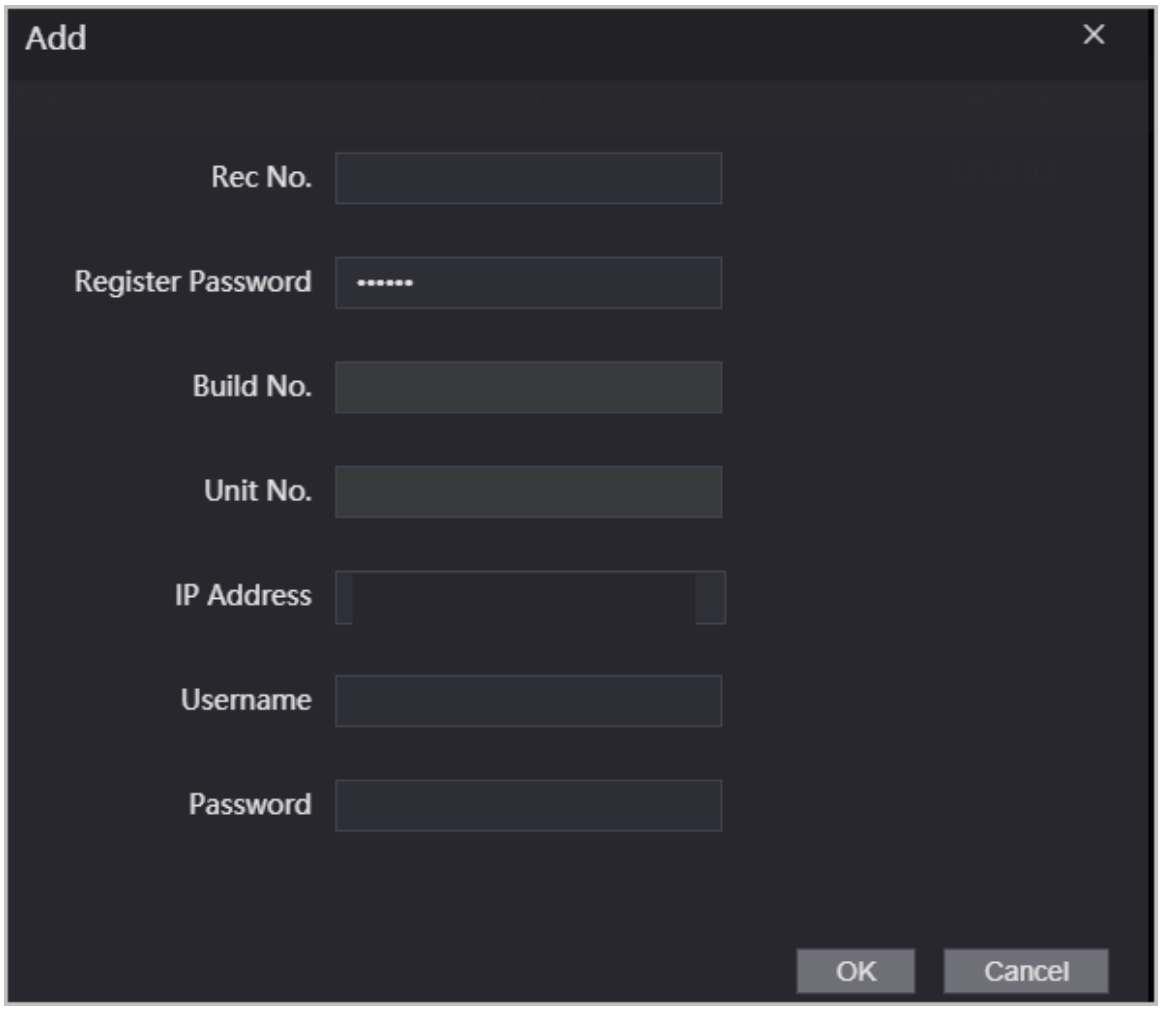


Tabla 3-7 Agregar configuración de VTO

Parámetro	Descripción
N.º de registro	El número del VTO añadido. Puede comprobarlo en el **Dispositivo** página en la página web de la VTO.
Registro Contraseña	Mantenlo predeterminado
Número de compilación	No se puede configurar.
Unidad N°	
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 Adición del 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 fondo

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

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración de Talkback**>**Sala No. Gerencia**

Paso 2 Añade el VTH.

- Añadir individualmente

  1. Haga clic**Agregar**.

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

Figura 3-13 Agregar individualmente

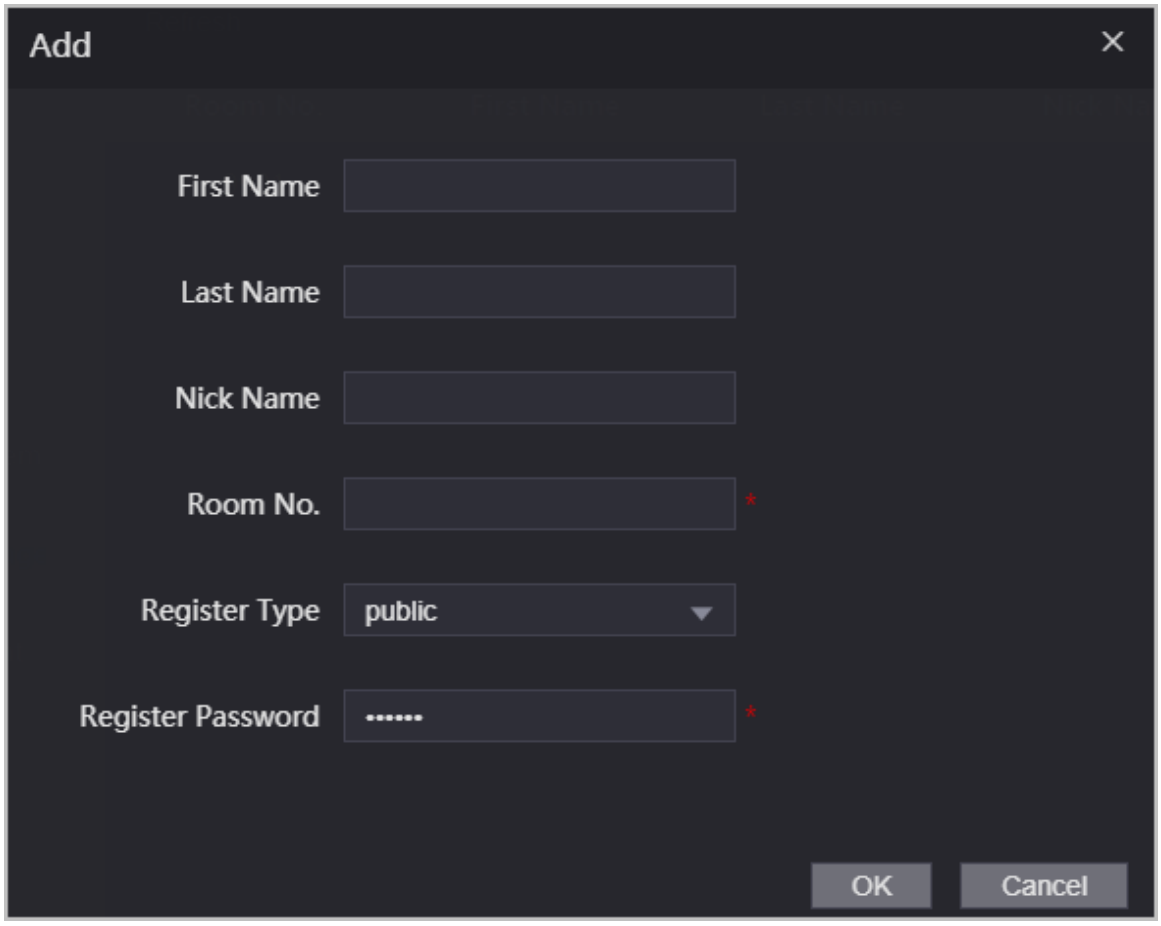


Tabla 3-8 Información de la habitación

Parámetro	Descripción
Habitación N°	Introduzca el número de habitación del VTH. ● El número de habitación consta de 1 a 5 dígitos y debe coincidir con el número de habitación configurado en el VTH. ● Cuando hay una VTH principal y extensiones, el número de habitación de la VTH principal termina en -0 y el de la extensión en -1, -2 o -3. Por ejemplo, la 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	Introduzca el nombre del VTH para ayudarle a diferenciarlos.
Apellido	
Apodo	
Tipo de registro	Mantenlos como predeterminados.
Contraseña registrada	

- Añadir en lotes

  1. Haga clic**Agregar por lotes**
  2. Configure los parámetros.

Figura 3-14 Adición por lotes

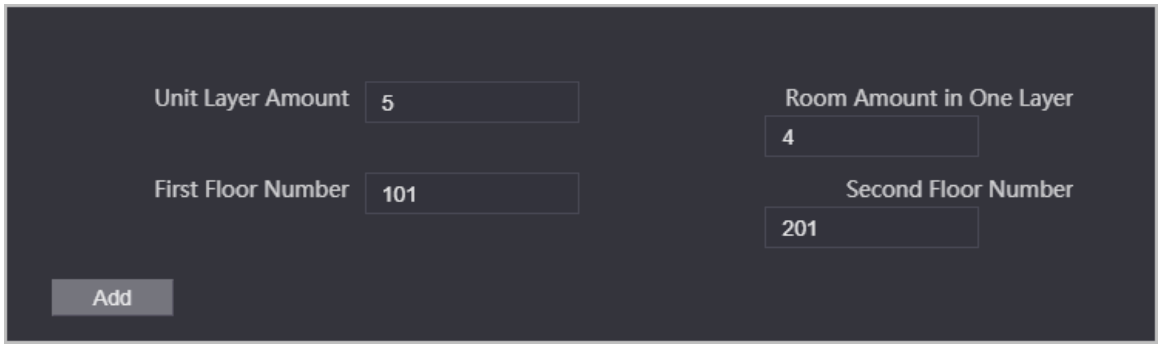


Tabla 3-9 Adición de lotes

Parámetro	Descripción
Cantidad de capa unitaria	El número de pisos del edificio (entre 1 y 99).
Cantidad de habitación en una capa	El número de habitaciones en cada piso, que varía entre 1 y 99.
Número del primer piso	La primera habitación del 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 Adición del VTS

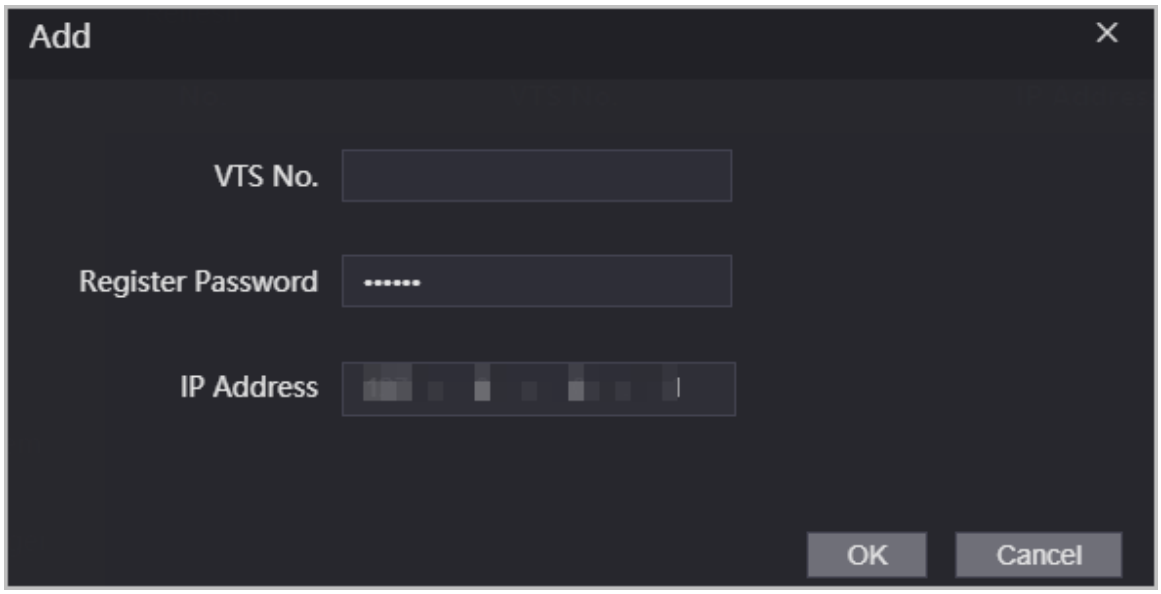
Cuando el controlador de acceso funciona como servidor SIP, puede agregar VTS al servidor SIP para asegurarse de que puedan llamarse entre sí.

Procedimiento

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

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

Figura 3-15 Gestión de VTS



Paso 3 Hacer clic**DE ACUERDO**.

3.5.6 Visualización del estado del dispositivo

Cuando el controlador de acceso funciona como servidor SIP, puede ver el estado de los dispositivos conectados al servidor SIP. En la página de inicio, seleccione**Configuración de Talkback**>**Estado**.

3.5.7 Visualización de registros de llamadas

Vea el registro completo de llamadas salientes y entrantes. En la página de inicio, seleccione**Configuración de Talkback**> **Llamar**.

3.6 Configuración de horarios

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

3.6.1 Configuración de secciones de tiempo

Puede configurar hasta 128 grupos (del 0 al 127) de secciones horarias. En cada grupo, debe configurar horarios de acceso para una semana completa. Un usuario solo puede desbloquear la puerta durante el horario programado.

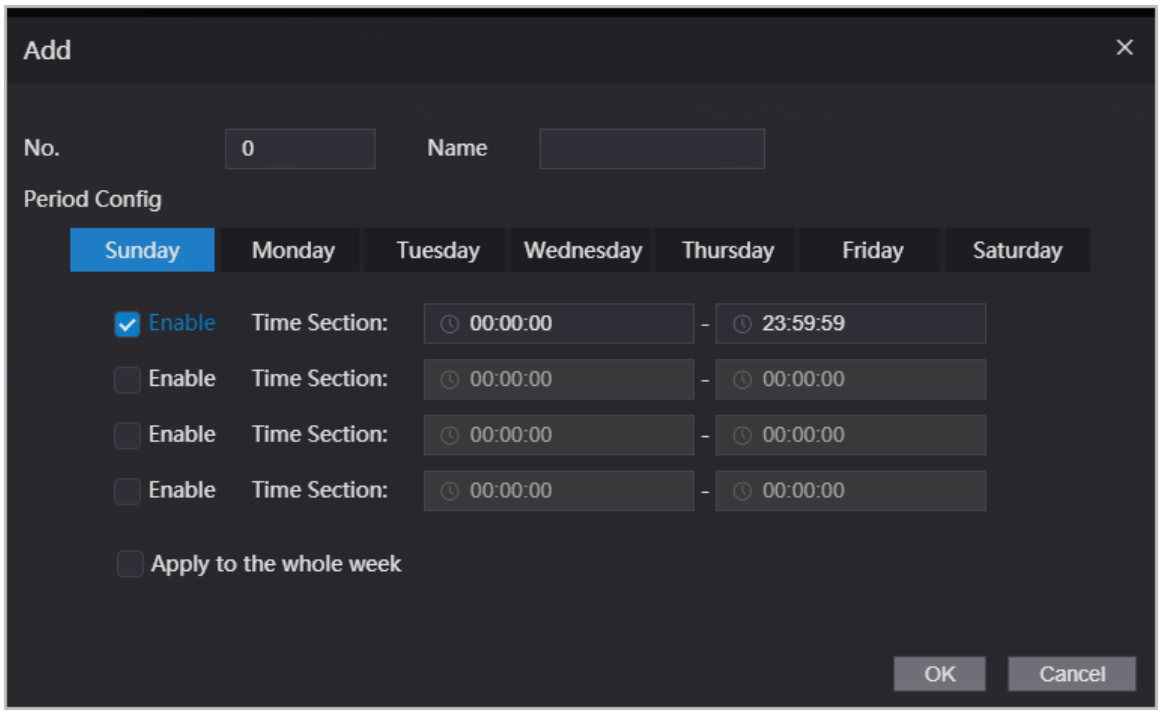
Procedimiento

Paso 1 Inicie sesión en la página web.

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

Paso 3 clic**Agregar**.

Figura 3-16 Parámetros de la sección de tiempo



Paso 4 Introduzca el número y el nombre de la sección de tiempo.

- **No.**:Ingrese un número de sección. Varía entre 0 y 127.
- **Nombre**: Ingrese un nombre para cada sección de tiempo. Puede ingresar un máximo de 32 caracteres (número, caracteres especiales y caracteres en inglés).

Paso 5 Configurar secciones de tiempo para cada día.

Paso 6 Puede configurar hasta cuatro secciones de tiempo para un solo día.

Paso 7 (Opcional) Haga clic en**Aplicar a toda la semana.**Para copiar la configuración al resto de días, haga clic en**DE**

Paso 8 **ACUERDO**.

3.6.2 Configuración de grupos de vacaciones

Configure franjas horarias para diferentes grupos de vacaciones. Puede configurar hasta 128 grupos de vacaciones (del 0 al 127) y hasta 16 franjas horarias para un solo grupo. Los usuarios pueden desbloquear puertas en las franjas horarias definidas.

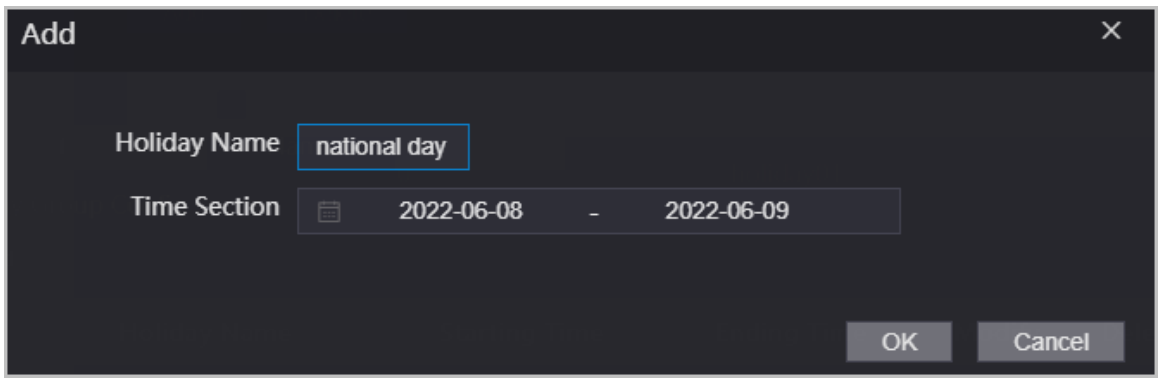
Procedimiento

Paso 1 Inicie sesión en la página web.

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

Paso 3 Haga clic**Agregar**.

Figura 3-17 Agregar un grupo de vacaciones



Paso 4 Establezca el nombre y la hora para el grupo de vacaciones.

- **Nombre de la festividad**: Ingrese el nombre del grupo de vacaciones. Ingrese un nombre para cada sección horaria. Puede ingresar un máximo de 32 caracteres (pueden incluir números, caracteres especiales y caracteres en inglés).
- **Sección de tiempo**Seleccione la hora de inicio y la hora de finalización de las vacaciones. Haga clic en**DE**

Paso 5 **ACUERDO**.

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

Paso 6 Hacer clic**DE ACUERDO**.

3.6.3 Configuración de planes de vacaciones

Asigne los grupos de vacaciones configurados al plan de vacaciones. Los usuarios solo pueden desbloquear la puerta durante el horario definido en el plan de vacaciones.

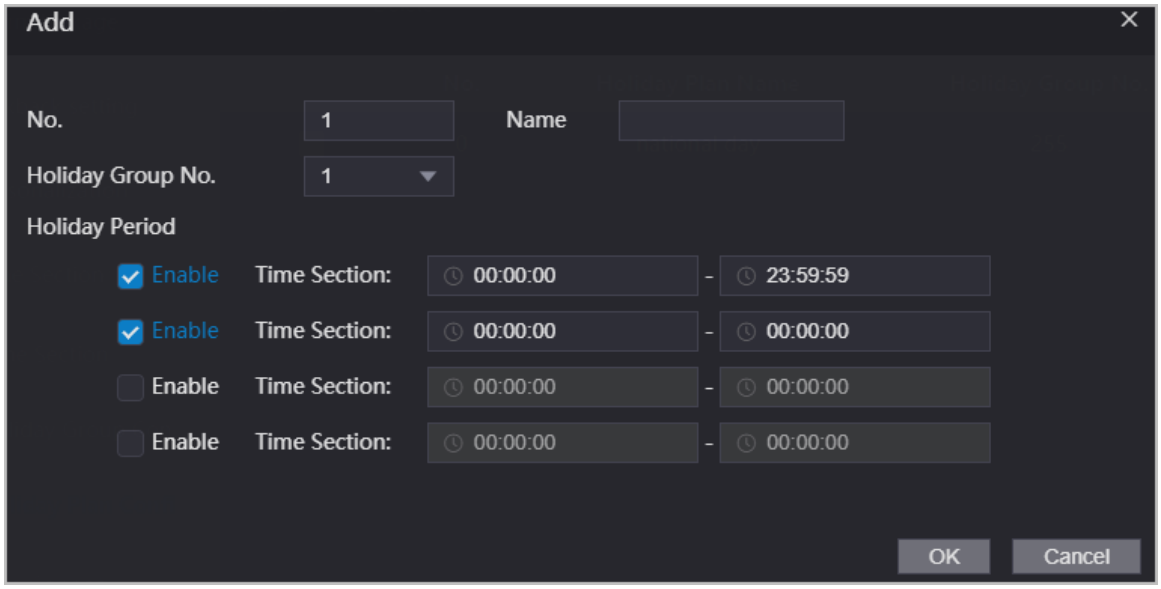
Procedimiento

Paso 1 Inicie sesión en la página web.

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

Paso 3 Haga clic**Agregar**.

Figura 3-18 Agregar plan de vacaciones



Paso 4 Introduzca un número y un nombre para el plan de vacaciones.

- **No.**Introduzca un número de sección. Varía entre 0 y 127.
- **Nombre**: Ingrese un nombre para cada sección de tiempo. Puede ingresar un máximo de 32 caracteres (pueden incluir 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**Período de vacaciones**Área, configure tramos horarios 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 faciales puede almacenar el controlador de acceso. Inicie sesión en la página web y seleccione**Capacidad de datos**.

3.8 Configuración de vídeo e imagen

Configure parámetros de vídeo e imagen, como la transmisión y el brillo. Le recomendamos usar 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.

Información de fondo

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

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

3.8.1.1 Configuración del canal 1

Procedimiento

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

Paso 2 **vídeo**. Seleccionar**1**desde**Canal Nro.**Lista. Configurar la

Paso 3 tarifa de fecha.

Figura 3-19 Tasa de fecha

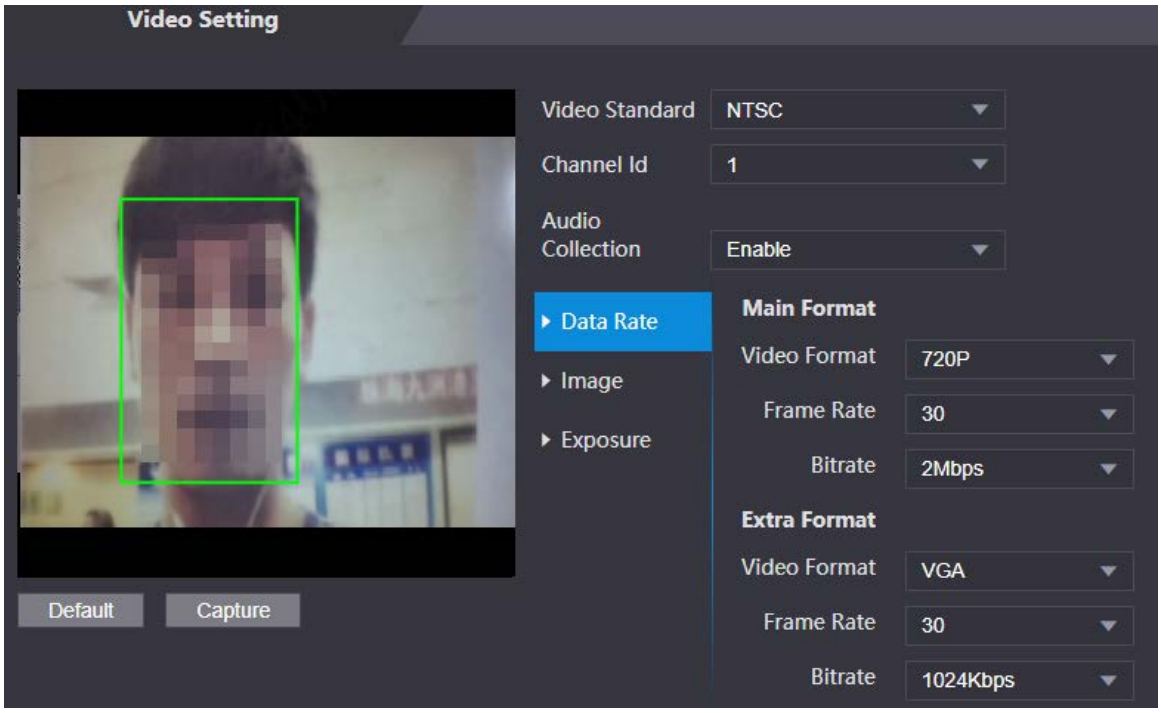


Tabla 3-11 Descripción de la tasa de fecha

Parámetro		Descripción
Formato principal	Formato de vídeo	Cuando el controlador de acceso funciona como El 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.
	Velocidad de cuadros	Número de fotogramas (o imágenes) por segundo. La velocidad de fotogramas oscila entre 1 y 25 fps.
	Tasa de bits	Indica la cantidad de datos transmitidos a través de una conexión a internet en un tiempo determinado. Seleccione el ancho de banda adecuado según la velocidad de su red.
Subtransmisión	Formato de vídeo	La subtransmisión admite D1, VGA y QVGA.
	Velocidad de cuadros	Número de fotogramas (o imágenes) por segundo. La velocidad de fotogramas oscila entre 1 y 25 fps.
	Tasa de bits	Indica la cantidad de datos transmitidos a través de una conexión a Internet en un período de tiempo determinado.

Paso 4 Configurar la imagen.

Figura 3-20 Imagen

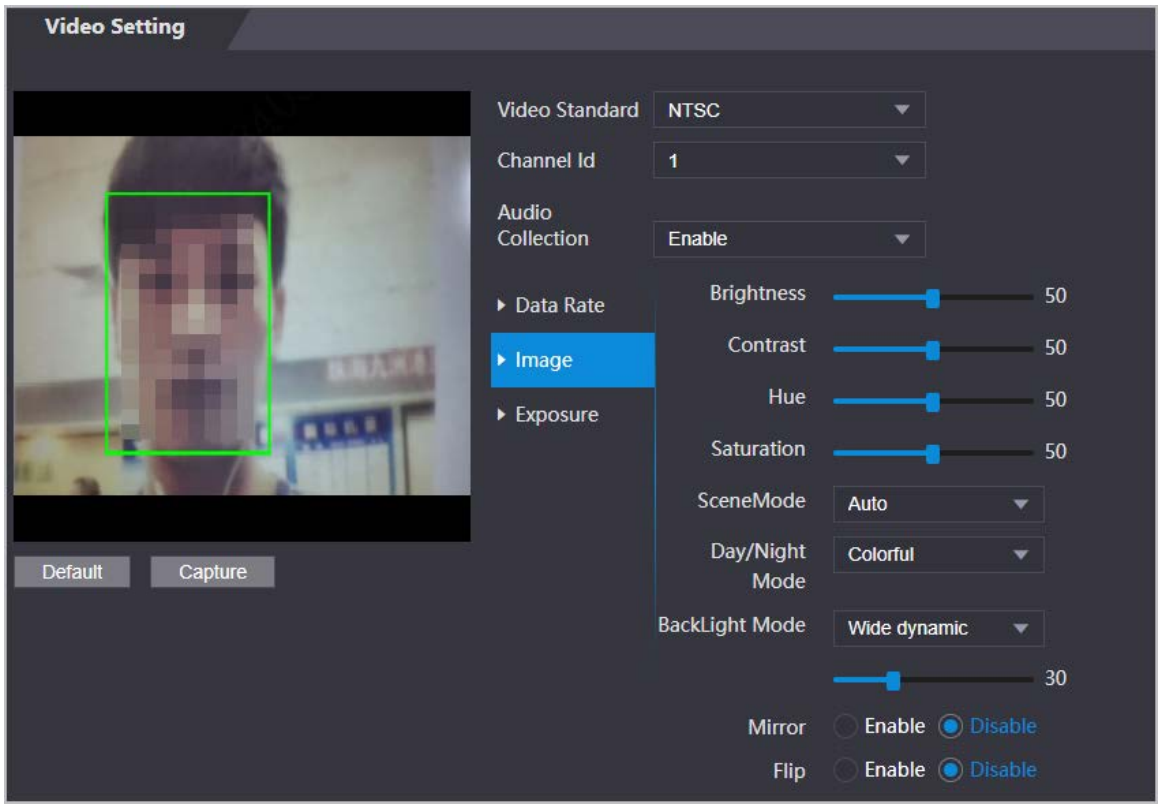


Tabla 3-12 Descripción de la imagen

Parámetro	Descripción
Contraste	El contraste es la diferencia de luminancia o color que distingue un objeto. Cuanto mayor sea el valor de contraste, mayor será el contraste de color.
Matiz	Se refiere a la intensidad o saturación de un color. Describe su intensidad o pureza.
Saturación	La saturación del color indica la intensidad del color en una imagen. A medida que aumenta la saturación, el color se vuelve más intenso, por ejemplo, más rojo o más azul. El valor de saturación no cambia el brillo de la imagen.
Modo de escena	El tono de la imagen es diferente en distintos modos de escena. ● **Cerca**:La función de 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 en función de la sensibilidad fotográfica. ● **Vistoso**:En este modo, las imágenes son coloridas. ● **En blanco y negro**:En este modo, las imágenes son en blanco y negro.

Parámetro	Descripción
Modo de luz de fondo	● **Cerca**:La compensación de luz de fondo está desactivada. ● **Iluminar desde el fondo**:La compensación de luz de fondo aporta automáticamente más luz a las áreas más oscuras de una imagen cuando la luz brillante que brilla detrás la 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 cámaras de seguridad CCTV/IP para procesar imágenes expuestas a luces como faros o focos. El sensor de imagen de la cámara detecta luces intensas en el video 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 el lado izquierdo y derecho invertidos.
Voltear	Cuando esta función está activada, las imágenes se pueden voltear.

Paso 5 Configurar los parámetros de exposición.

Figura 3-21 Exposición

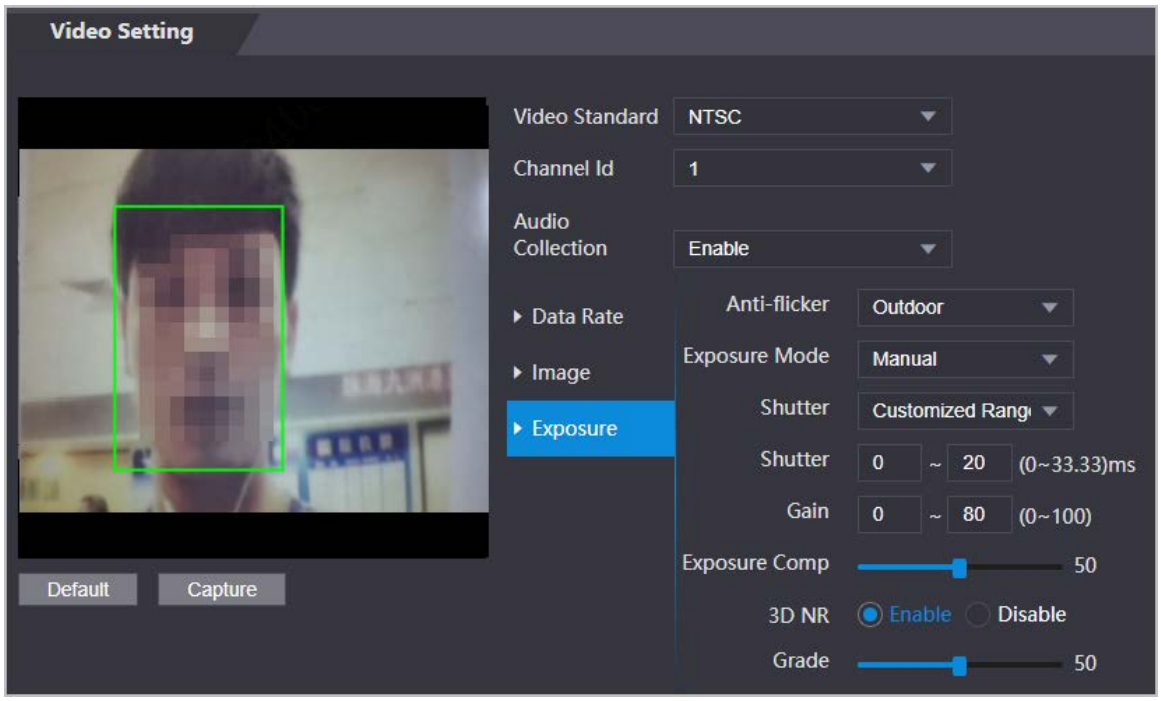


Tabla 3-13 Descripción de los parámetros de exposición

Parámetro	Descripción
Antiparpadeo	Configure el antiparpadeo para reducir el parpadeo y disminuir o reducir los colores desiguales o la exposición. ● **50 Hz**:Cuando la fuente de alimentación de red es de 50 Hz, la exposición se ajusta automáticamente para evitar la aparición de líneas horizontales. ● **60 Hz**:Cuando la fuente de alimentación de red es de 60 Hz, la exposición se ajusta automáticamente para reducir la aparición de líneas horizontales. ● **Exterior**: Cuando**Exterior**Está seleccionado, 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 controlador de acceso ajusta automáticamente el brillo de las imágenes. ● **Prioridad de obturador**El terminal de acceso ajustará el brillo de la imagen según el rango de exposición del obturador. Si el brillo de la imagen es insuficiente y el valor del obturador ha alcanzado su límite superior o inferior, el controlador de acceso ajustará automáticamente la ganancia 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**Antiparpadeo**lista, puedes seleccionar **Prioridad de obturador**como el modo de exposición. ◇ El modo de exposición puede variar según los distintos modelos de controlador de acceso.
Obturador	El obturador es un componente que permite el paso de la luz durante un periodo determinado. Cuanto mayor sea la velocidad de obturación, menor será el tiempo de exposición y más oscura la imagen.
Ganar	Cuando se establece el rango de valores de ganancia, se mejorará la calidad del video.
Exposición Compensación	Puede hacer que una fotografía 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, se puede reducir el ruido del video para garantizar videos de alta definición. Puedes configurar su calificación cuando esta función esté activada.
Calificación	

3.8.1.2 Configuración del canal 2

Procedimiento

Paso 1 Seleccionar**Configuración de vídeo**>

Paso 2 **Configuración de vídeo**Seleccione 2 de la**Canal**

Paso 3 **Nro.**. Configurar el estado del vídeo.

Le recomendamos activar la función WDR cuando el rostro esté a contraluz.

Figura 3-22 Imagen

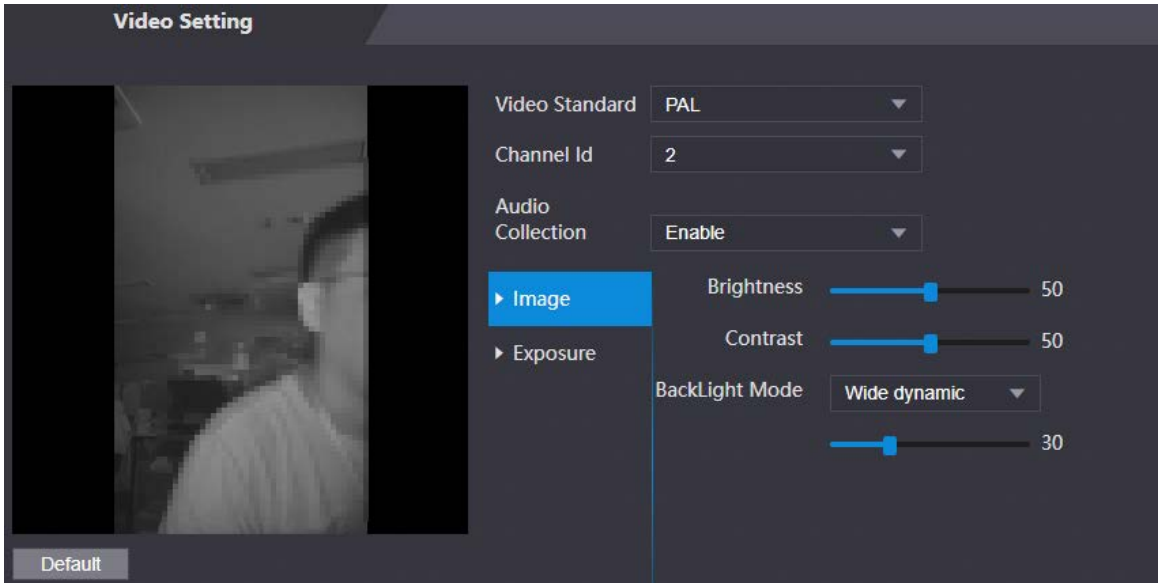


Tabla 3-14 Descripción de la imagen

Parámetro	Descripción
Brillo	El brillo es la claridad u oscuridad relativa 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 distingue un objeto. Cuanto mayor sea el valor de contraste, mayor será el contraste de color.
Modo de luz de fondo	● **Cerca**:La compensación de luz de fondo 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 detrás la 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 cámaras de seguridad CCTV/IP para procesar imágenes expuestas a luces como faros o focos. El sensor de imagen de la cámara detecta luces intensas en el video y reduce la exposición en estos puntos para mejorar la calidad general de la imagen.

Paso 4 Configurar los parámetros de exposición.

Figura 3-23 Parámetro de exposición

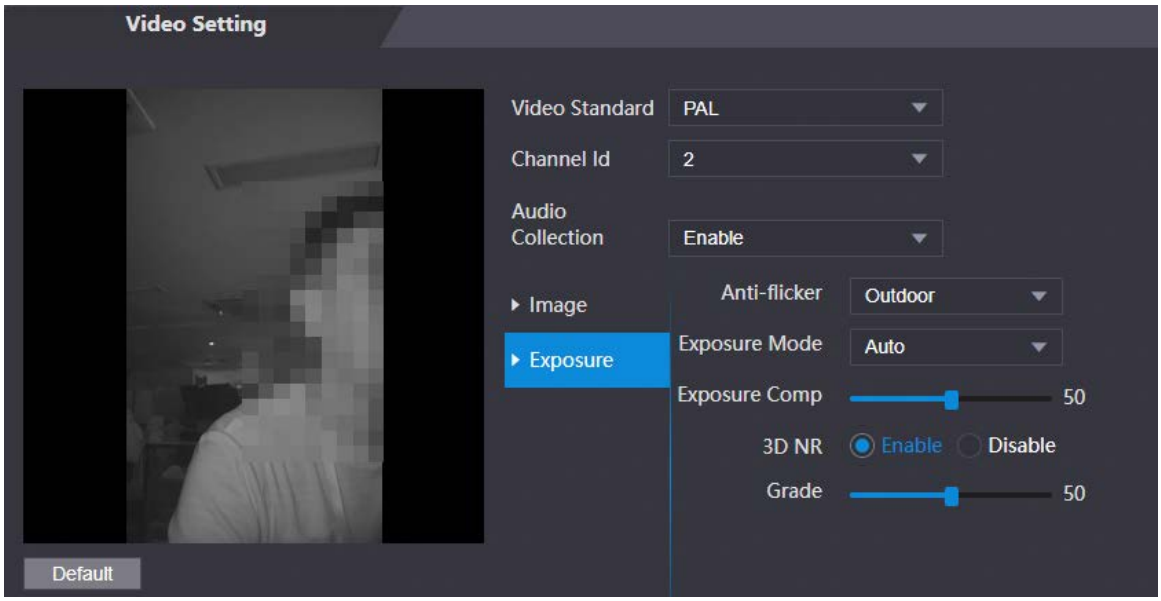


Tabla 3-15 Descripción de los parámetros de exposición

Parámetro	Descripción
Antiparpadeo	Configure el antiparpadeo para reducir el parpadeo y disminuir o eliminar los colores desiguales o la exposición. ● **50 Hz**:Cuando la fuente de alimentación de red es de 50 Hz, la exposición se ajusta automáticamente para evitar la aparición de líneas horizontales. ● **60 Hz**:Cuando la fuente de alimentación de red es de 60 Hz, la exposición se ajusta automáticamente para reducir la aparición de líneas horizontales. ● **Exterior**: Cuando**Exterior**Está seleccionado, se puede cambiar el modo de exposición.
Modo de exposición	Puede configurar la exposición para ajustar el brillo de la imagen. ● **Auto**:El controlador de acceso ajusta automáticamente el brillo de las imágenes. ● **Prioridad de obturador**El terminal de acceso ajustará el brillo de la imagen según el rango de exposición del obturador. Si el brillo de la imagen es insuficiente y el valor del obturador ha alcanzado su límite superior o inferior, el controlador de acceso ajustará automáticamente la ganancia 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**Antiparpadeo**lista, tu puede seleccionar**Prioridad de obturador**como el modo de exposición. ◇ El modelo de exposición puede variar según los diferentes Modelos de Controlador de Acceso.
Obturador	El obturador es un dispositivo que permite el paso de la luz durante un periodo determinado. Cuanto mayor sea la velocidad de obturación, menor será el tiempo de exposición y más oscura la imagen.
Ganar	Cuando se establece el rango de valores de ganancia, se mejorará la calidad del video.

Parámetro	Descripción
Compensación de exposición	Puede hacer que una fotografía 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, se puede reducir el ruido del video para garantizar videos de alta definición. Puedes configurar su calificación cuando esta función esté activada.
Calificación	

3.8.2 Ajuste del volumen

Puede ajustar el volumen del altavoz.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Configuración de vídeo**>**Ajuste del volumen**Arrastre el

Paso 3 control deslizante para ajustar el volumen. Haga clic.**DE ACUERDO**.

Paso 4

3.9 Configuración de la detección de rostros

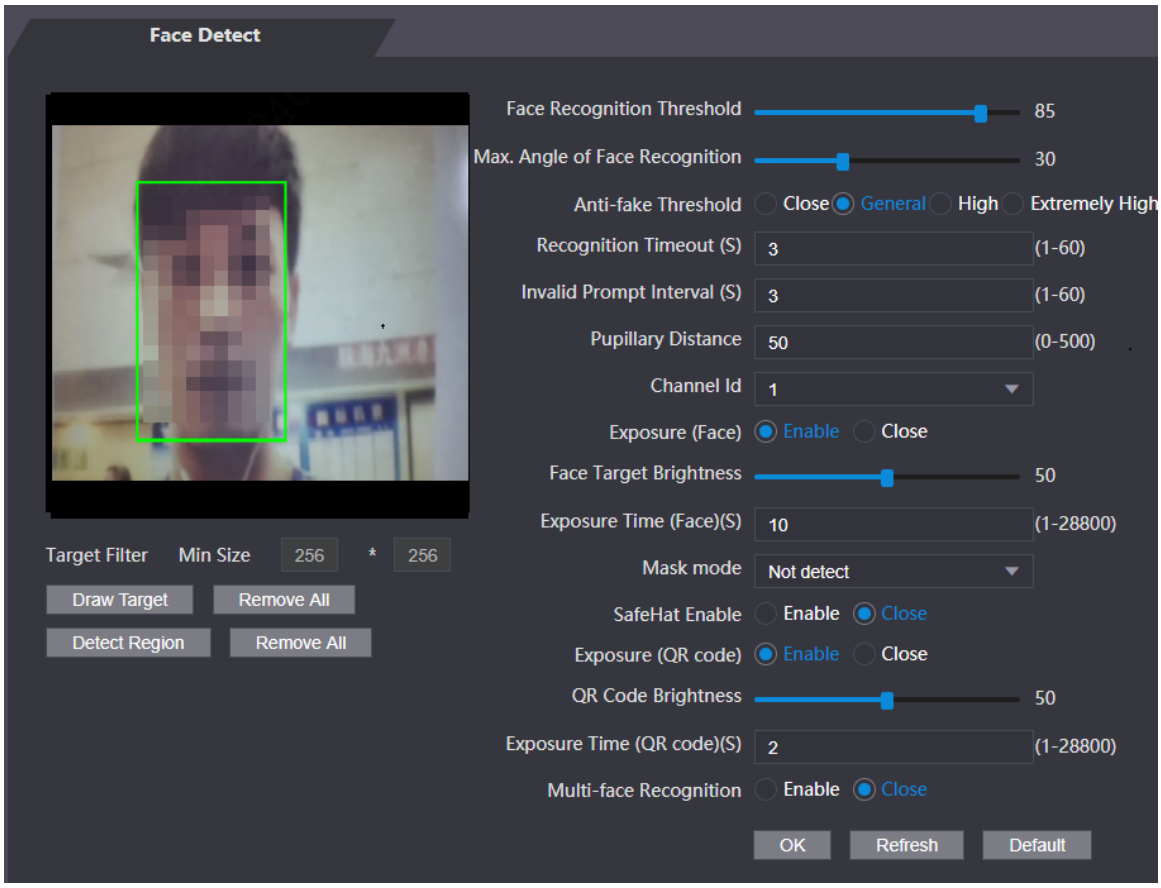
Puede configurar parámetros relacionados con el rostro humano en esta interfaz para aumentar la precisión del reconocimiento facial.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccione**Detección de rostros**.

Figura 3-24 Detección de rostro



Paso 3 Configurar 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 mayor precisión.
Ángulo máximo de la cara	Establezca el ángulo máximo de pose facial para la detección facial. Un valor mayor implica un rango de ángulo facial mayor. Si el ángulo de pose facial está fuera del rango definido, el cuadro de detección facial no aparecerá.
Umbral anti-falsificación	Evite el reconocimiento facial falso utilizando una foto, un vídeo, una 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 la puerta para personas con mascarillas. ● Alto: un mayor nivel de detección anti-spoofing significa mayor precisión y seguridad. ● Extremadamente alto: un nivel extremadamente alto de detección anti-spoofing 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 indicará que el reconocimiento facial se ha realizado correctamente. Puede introducir el intervalo de tiempo para la indicación.
Intervalo de aviso de rostro 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 de reconocimiento facial. Puede introducir el intervalo de tiempo para la indicación.

Parámetro	Descripción
Distancia pupilar	Las imágenes faciales requieren la distancia pupilar (píxeles) deseada entre los ojos para un reconocimiento correcto. El valor predeterminado es 45 píxeles. Este valor varía según el tamaño del rostro y la distancia entre los rostros y la lente. Si un adulto se encuentra a 1,5 metros de la lente, la distancia pupilar puede ser de 50 a 70 píxeles.
Identificación del canal	1 es para la cámara de luz blanca y 2 es para la cámara de luz infrarroja.
Exposición (cara)	Una vez habilitada la exposición facial, los rostros humanos se verán más claros cuando el controlador de acceso se instale en exteriores.
Brillo del objetivo facial	El valor predeterminado es 50. Ajuste el brillo según sea necesario.
Tiempo de exposición	Después de detectar un rostro, el controlador de acceso emitirá luz para iluminar el rostro y no volverá a emitir luz hasta que transcurra el intervalo establecido.
Modo máscara	● **Sin detección**:La máscara no se detecta durante el reconocimiento facial. ● **Recordatorio de mascarilla**: Se detecta mascarilla durante el reconocimiento facial. Si la persona no la usa, el sistema le recordará que la use y se le permitirá el acceso. ● **Intercepción de máscara**Se detecta una mascarilla durante el reconocimiento facial. Si una persona no la lleva, el sistema le recordará que la use y le denegará el acceso.
Exposición (código QR)	Cuando el controlador de acceso se instala en exteriores, el código QR será más claro según el brillo del código QR definido cuando lo escanee.
Brillo del código QR	
Tiempo de exposición (código QR) (S)	Después de escanear un código QR, el controlador de acceso emitirá luz para iluminar el código QR y no volverá a emitir luz hasta que haya transcurrido el tiempo de exposición definido.
Reconocimiento de múltiples caras	Permite detectar 4 imágenes faciales simultáneamente, y el modo de combinación de desbloqueo se invalida. La puerta se desbloquea cuando cualquiera de ellos accede.

Paso 4 Dibuje 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 la cara en el área definida.

Paso 5 Dibuje el 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.

Solo cuando el tamaño de la cara sea mayor que el tamaño definido, el controlador de acceso podrá 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.

Procedimiento

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

Paso 2 Configurar parámetros.

Figura 3-25 TCP/IP

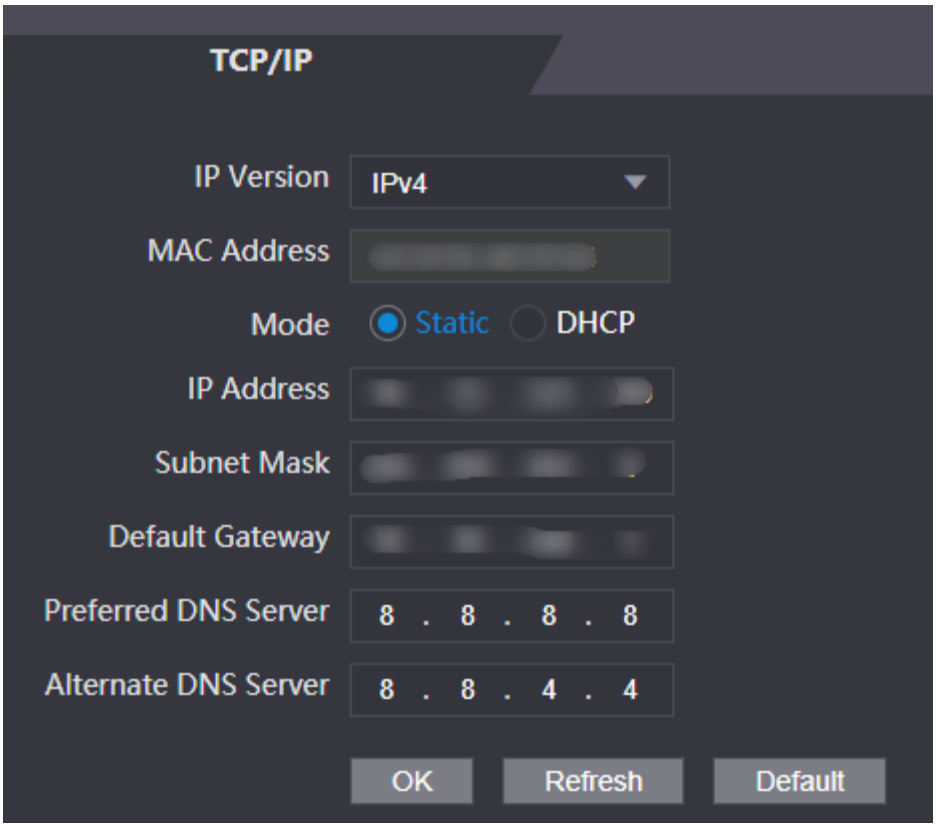


Tabla 3-17 Descripción de TCP/IP

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. Al activar DHCP, se le asignará automáticamente al controlador de acceso una dirección IP, una máscara de subred y una puerta de enlace.
Dirección IP Máscara de subred Puerta de enlace predeterminada	Si selecciona el modo estático, configure la dirección IP, la máscara de subred y la puerta de enlace. La dirección IP y la puerta de enlace deben estar en el mismo segmento de red.

Parámetro	Descripción
DNS preferido	Establecer la dirección IP del servidor DNS preferido.
DNS alternativo	Establecer la dirección IP del servidor DNS alternativo.

Paso 3 Hacer clic**DE ACUERDO**.

3.10.2 Configuración del puerto

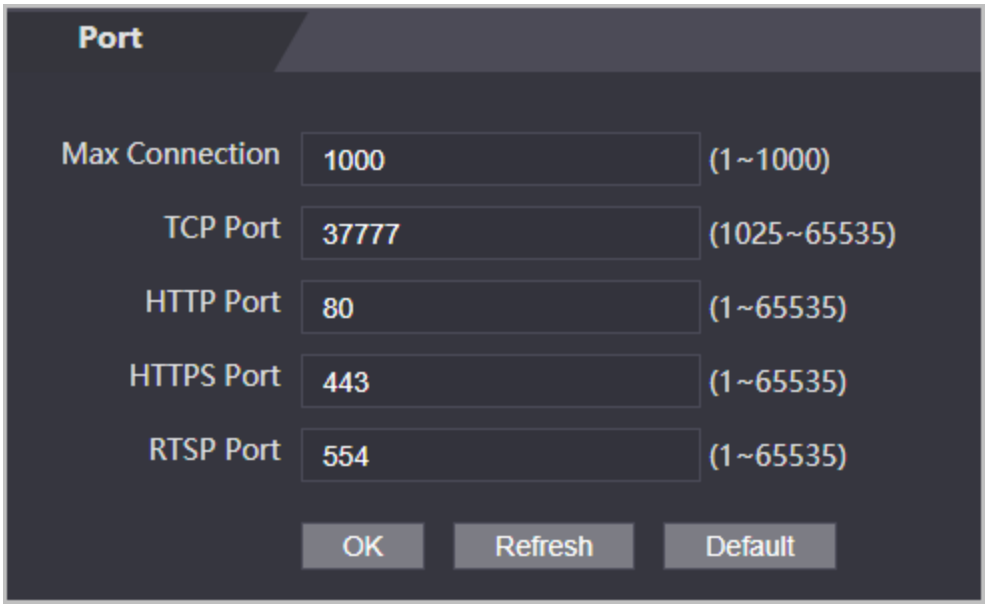
Puede limitar el acceso al controlador de acceso al mismo tiempo a través de la web, el cliente de escritorio y el teléfono.

Procedimiento

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

Paso 2 Configurar números de puerto.

Figura 3-26 Configurar puertos



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

Tabla 3-18 Descripción de los 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 clic**DE ACUERDO**.

3.10.3 Configuración del 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.

Procedimiento

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

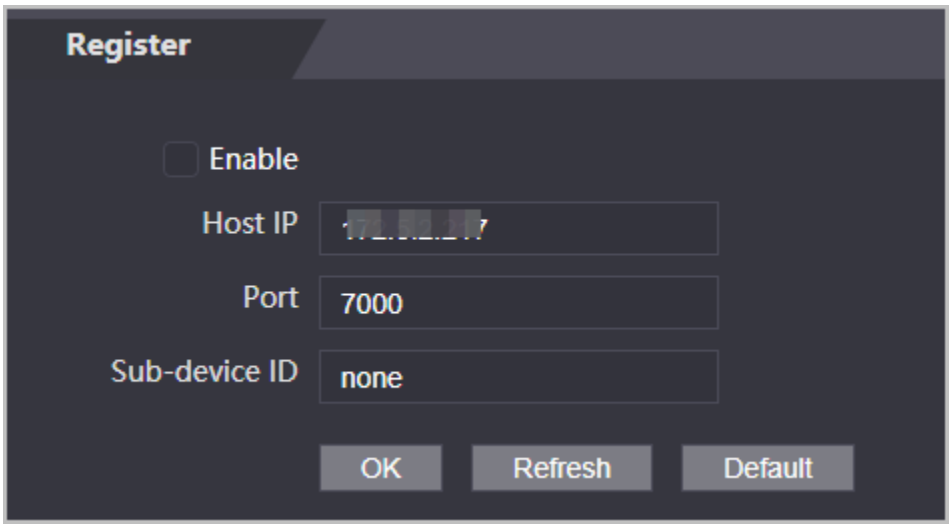


Tabla 3-19 Descripción del registro automático

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	Introduzca el ID del subdispositivo (definido por el usuario). Cuando agrega el controlador de acceso a la plataforma de administración, El ID del subdispositivo en la plataforma de administración 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

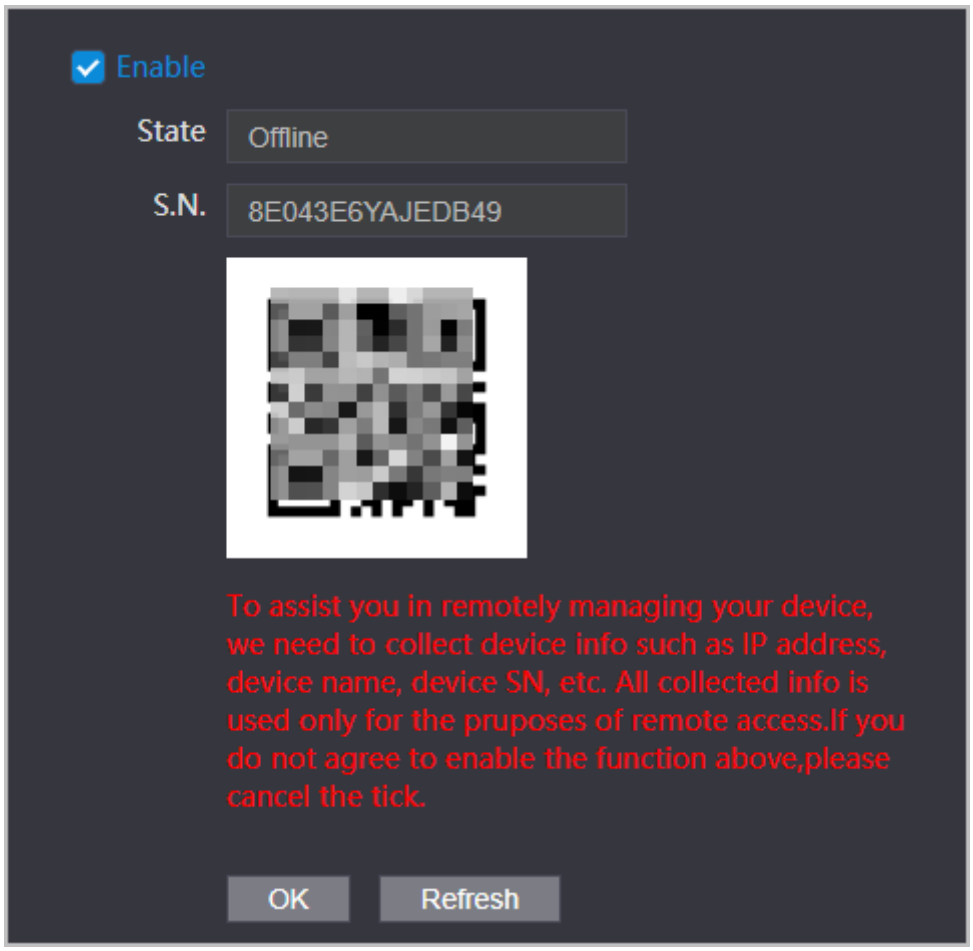
El servicio en la nube ofrece un servicio de penetración NAT. Los usuarios pueden administrar múltiples dispositivos mediante DMSS. No es necesario solicitar un nombre de dominio dinámico, configurar la asignación de puertos ni implementar un servidor.

Procedimiento

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

Paso 2 . Activa la función de 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.

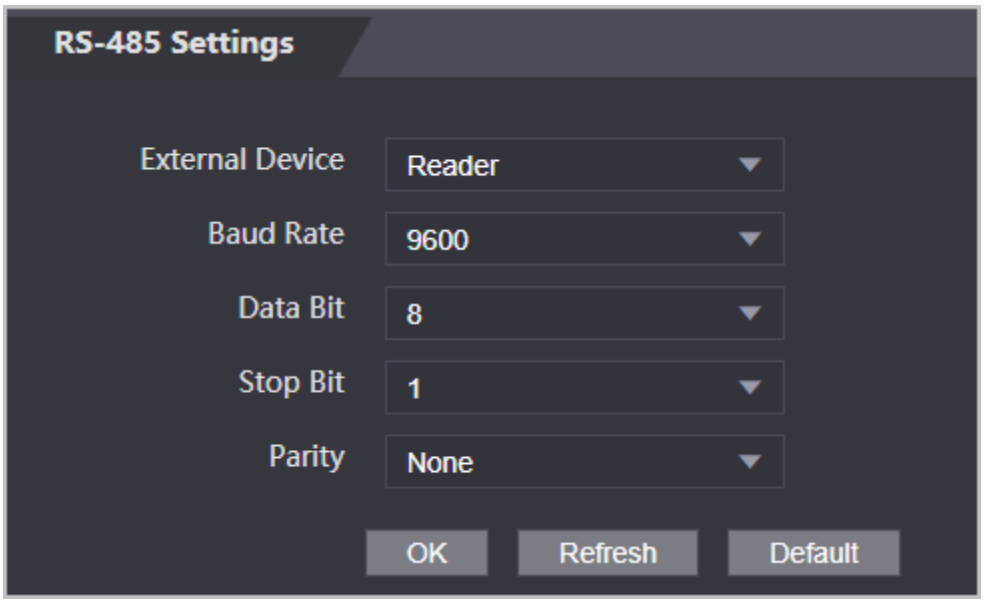
3.10.5 Configuración del puerto serie

Procedimiento

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 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: emite datos basados en el número de tarjeta cuando los usuarios pasan la tarjeta para desbloquear la puerta; emite datos basados en el primer número de tarjeta del usuario cuando utilizan otros métodos de desbloqueo.
  - ◇ No.: Genera datos basados en el ID 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

Información de fondo

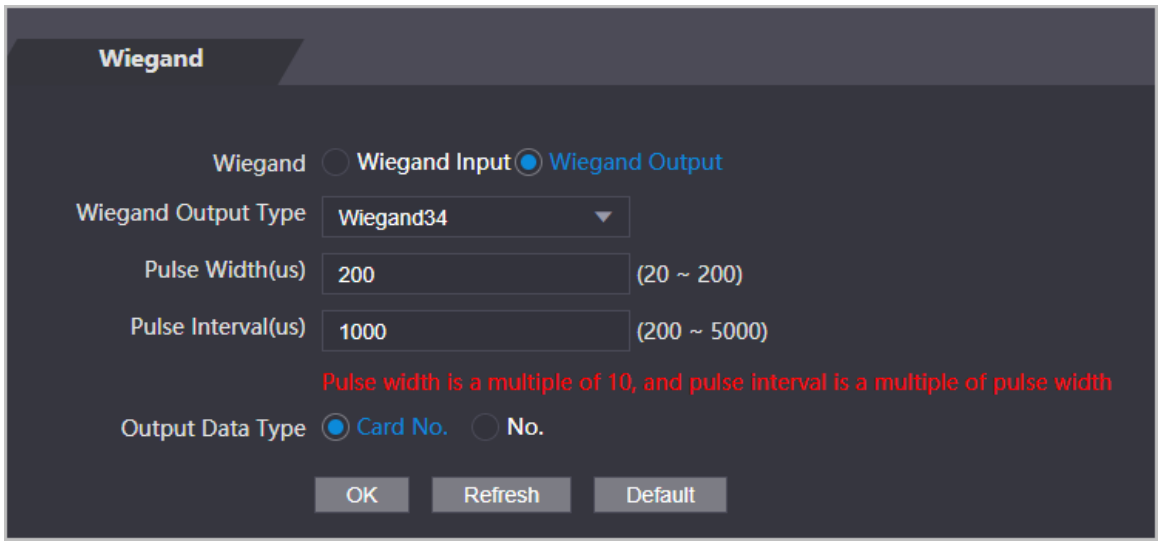
El controlador de acceso permite el modo de entrada y salida Wiegand.

Procedimiento

Paso 1 En 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 otra 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 tarjeta 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	Introduzca el ancho de 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 del usuario. ● **Nº de tarjeta**:Emite datos basados en el primer número de tarjeta del usuario.

3.11 Gestión de la seguridad

3.11.1 Configuración de la autoridad IP

Procedimiento

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 de la**Tipo**lista.

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

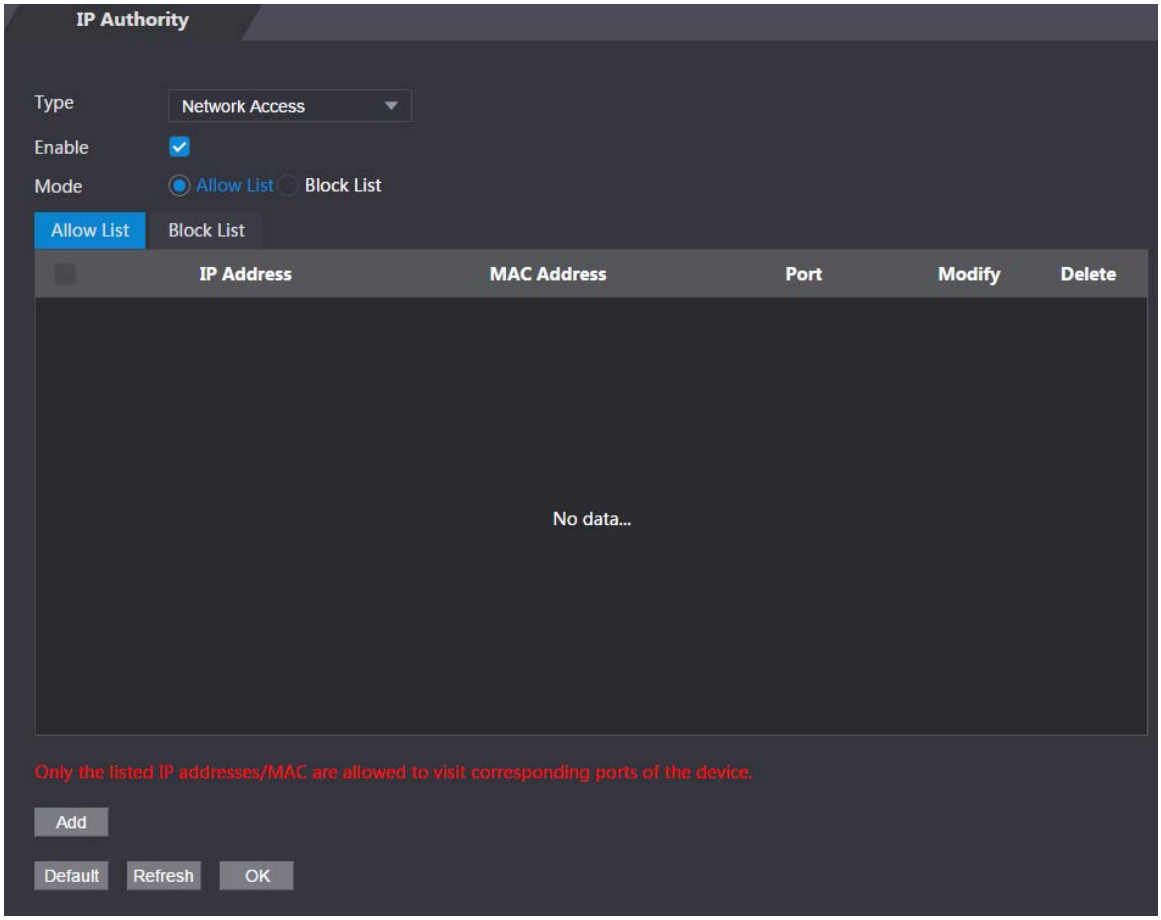
3.11.1.1 Acceso a la red

Procedimiento

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

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

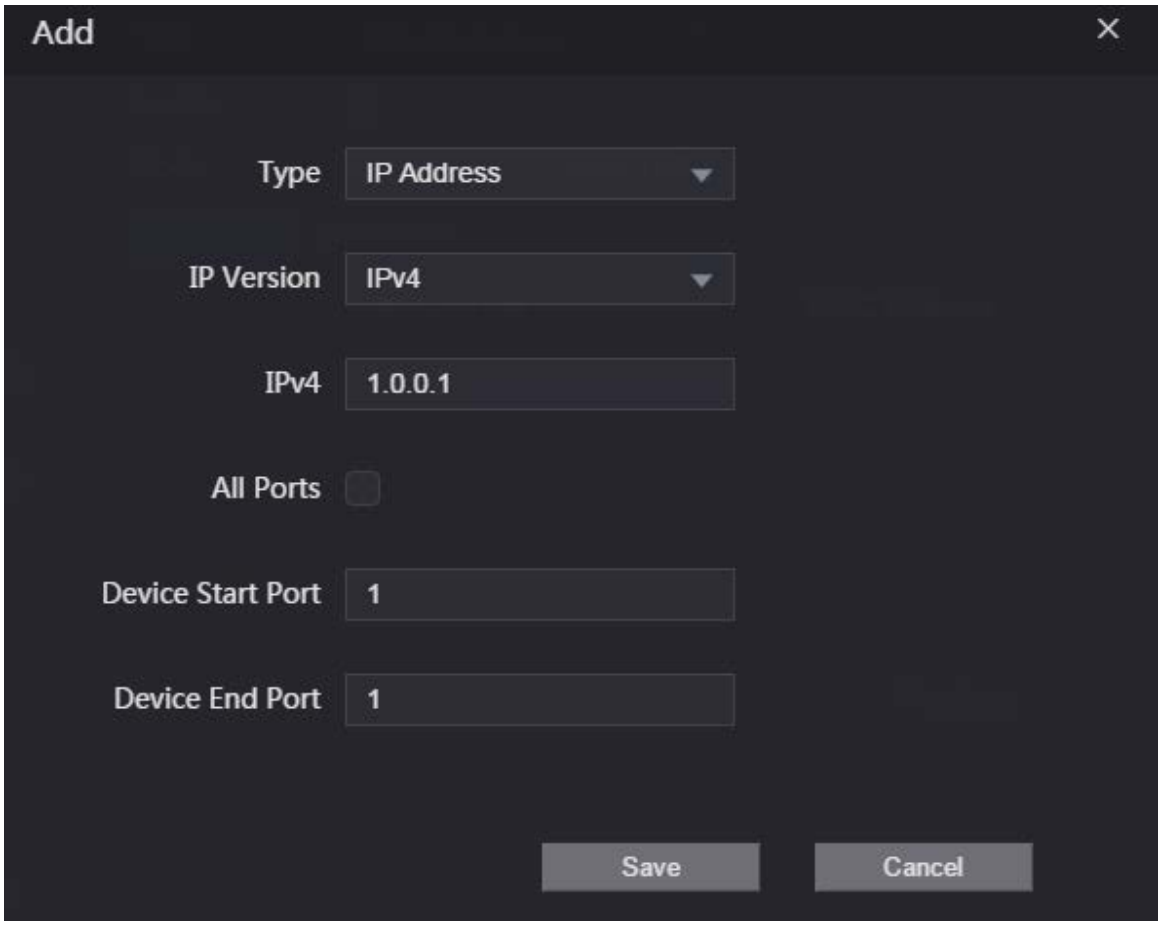
Figura 3-31 Acceso a la red



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

Paso 4 Haga clic**Agregar**.

Figura 3-32 Agregar IP



Paso 5 Configurar parámetros.

Tabla 3-21 Descripción de cómo agregar parámetros de 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 lo despejas**Todos los puertos**Casilla de verificación, configure el puerto de inicio del dispositivo 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. Haga clic en**DE**

Paso 7 **ACUERDO**.

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

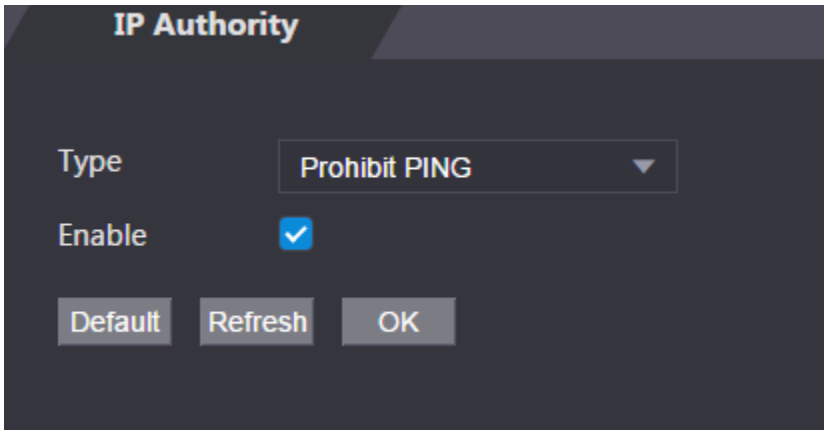
3.11.1.2 Prohibir PING

Procedimiento

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

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

Figura 3-33 Prohibir PING



Paso 3 Hacer clic**DE ACUERDO**.

3.11.1.3 Conexión anti-media

Procedimiento

Paso 1 Seleccione el**Anti-Media Conexión**desde**Tipo**lista. Seleccione el**Permitir**

Paso 2 casilla de verificación. Haga clic en**DE ACUERDO**.

Paso 3

3.11.2 Configuración del sistema

Procedimiento

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

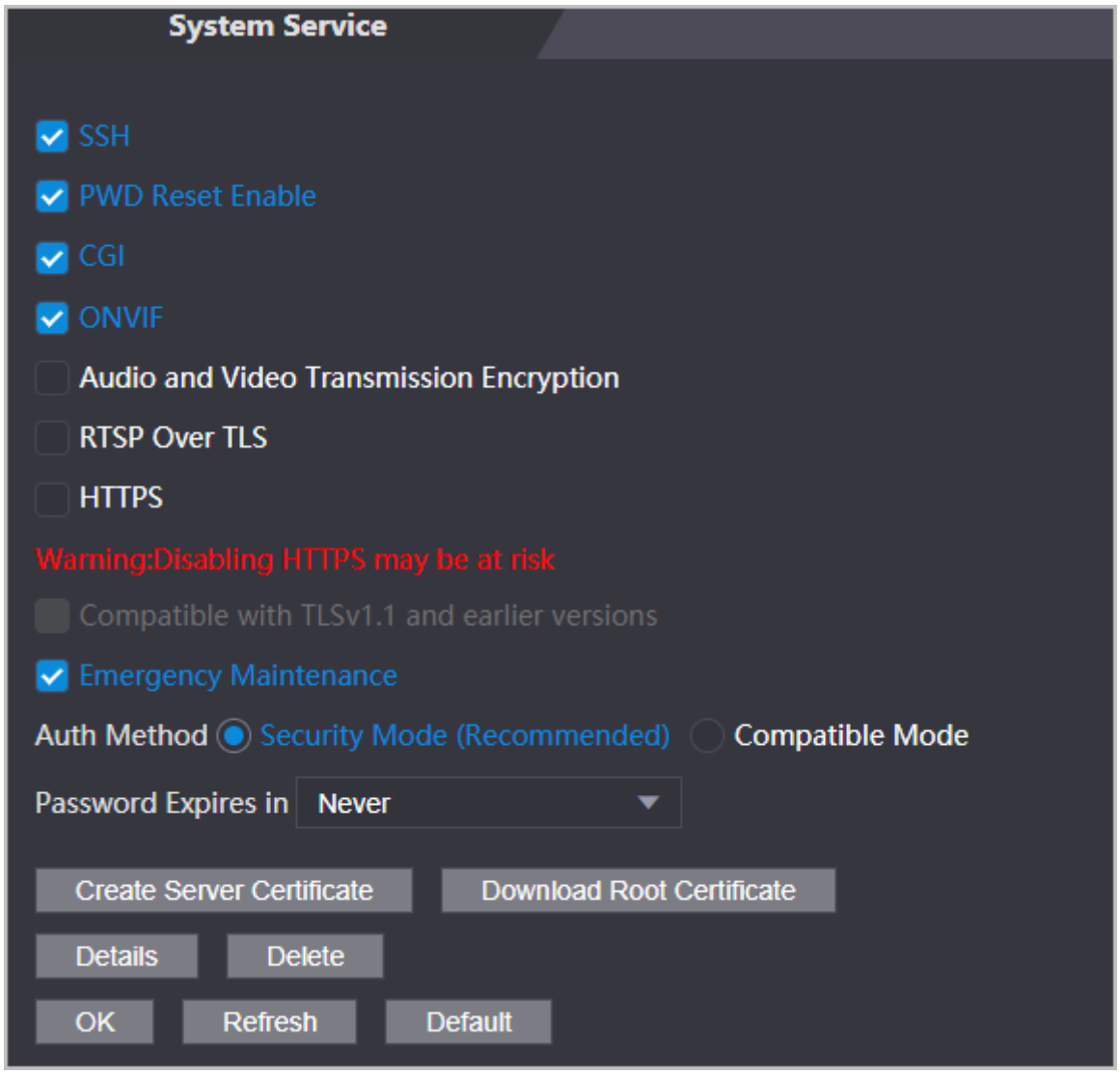


Tabla 3-22 Descripción del servicio del sistema

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 restablecimiento de PWD	Si está habilitada, puede restablecer la contraseña. Esta función está habilitada por defecto.
CGI	La interfaz de puerta de enlace común (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 usar comandos CGI. CGI está habilitado por defecto.
ONVIF	Permita que otros dispositivos extraigan la transmisión de video del VTO a través del protocolo ONVIF.
Audio y vídeo Transmisión Cifrado	Si esta función está habilitada, la transmisión de audio y video se cifra automáticamente.

Parámetro	Descripción
RTSP sobre TLS	Si esta función está habilitada, la transmisión de audio y vídeo se cifra a través del 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, se utilizará HTTPS 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	Le recomendamos que seleccione el modo de seguridad .

Paso 4 Hacer clic**DE ACUERDO**.

3.11.2.1 Creación de un certificado de servidor

Información de fondo

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

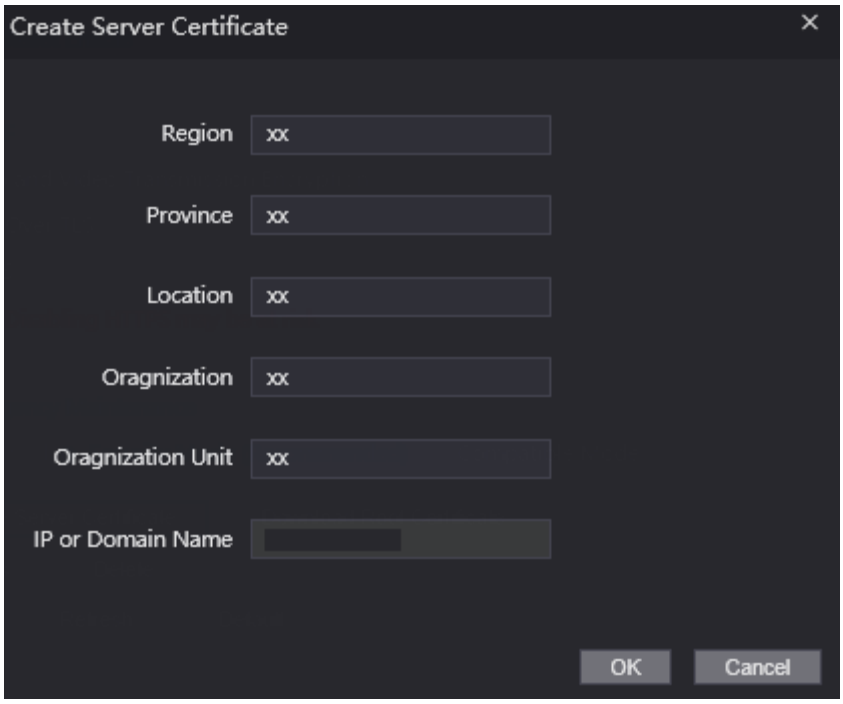
- Si utiliza HTTPS por primera vez o se cambia la dirección IP del controlador de acceso, cree un Certificado de servidor e instalar un certificado raíz.
- Si utiliza otra computadora para iniciar sesión en la página web del Controlador de acceso, deberá Descargue e instale nuevamente el certificado raíz en la nueva computadora o copie el certificado raíz A ello.

Procedimiento

Paso 1 En el**Servicio del sistema**página, haga clic**Crear certificado de servidor**Ingrese

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

Figura 3-35 Crear certificado de servidor



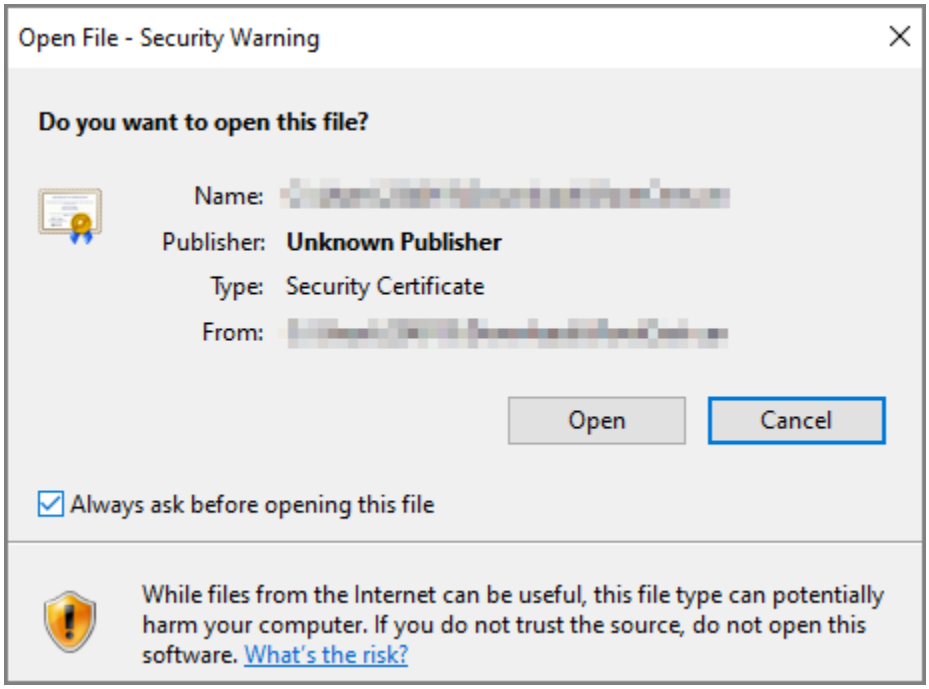
3.11.2.2 Descarga del certificado raíz

Procedimiento

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

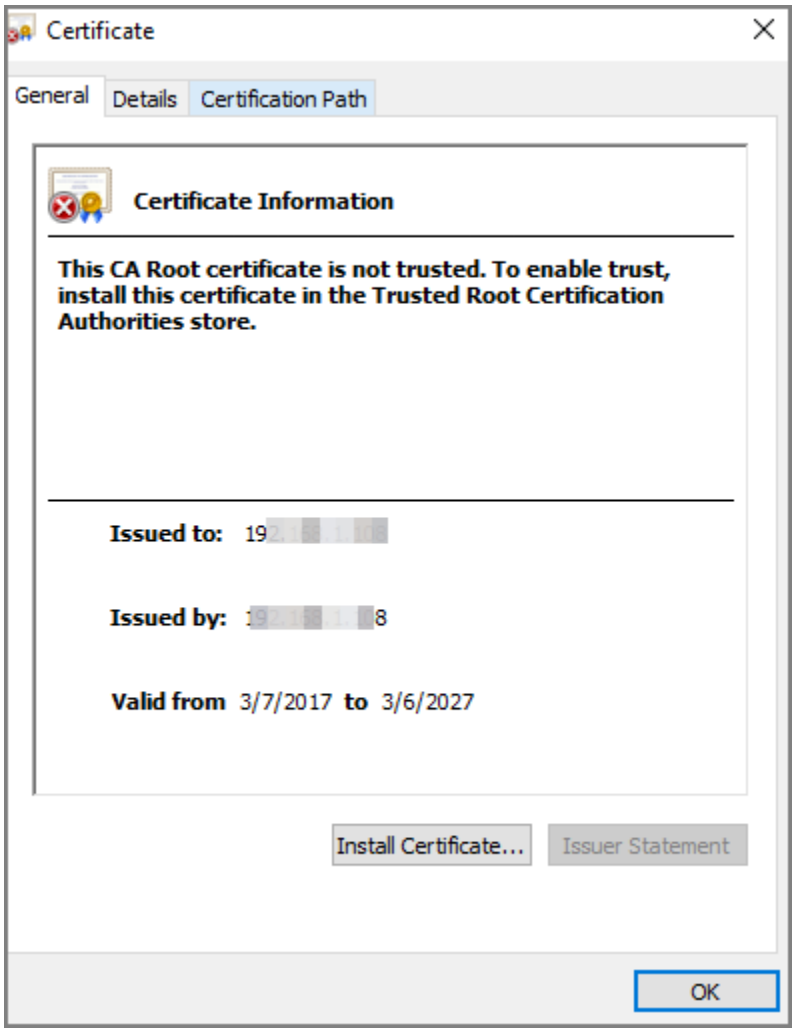
Paso 2 doble clic en el archivo que ha descargado y luego haga clic en**Abierto**.

Figura 3-36 Descarga de archivos



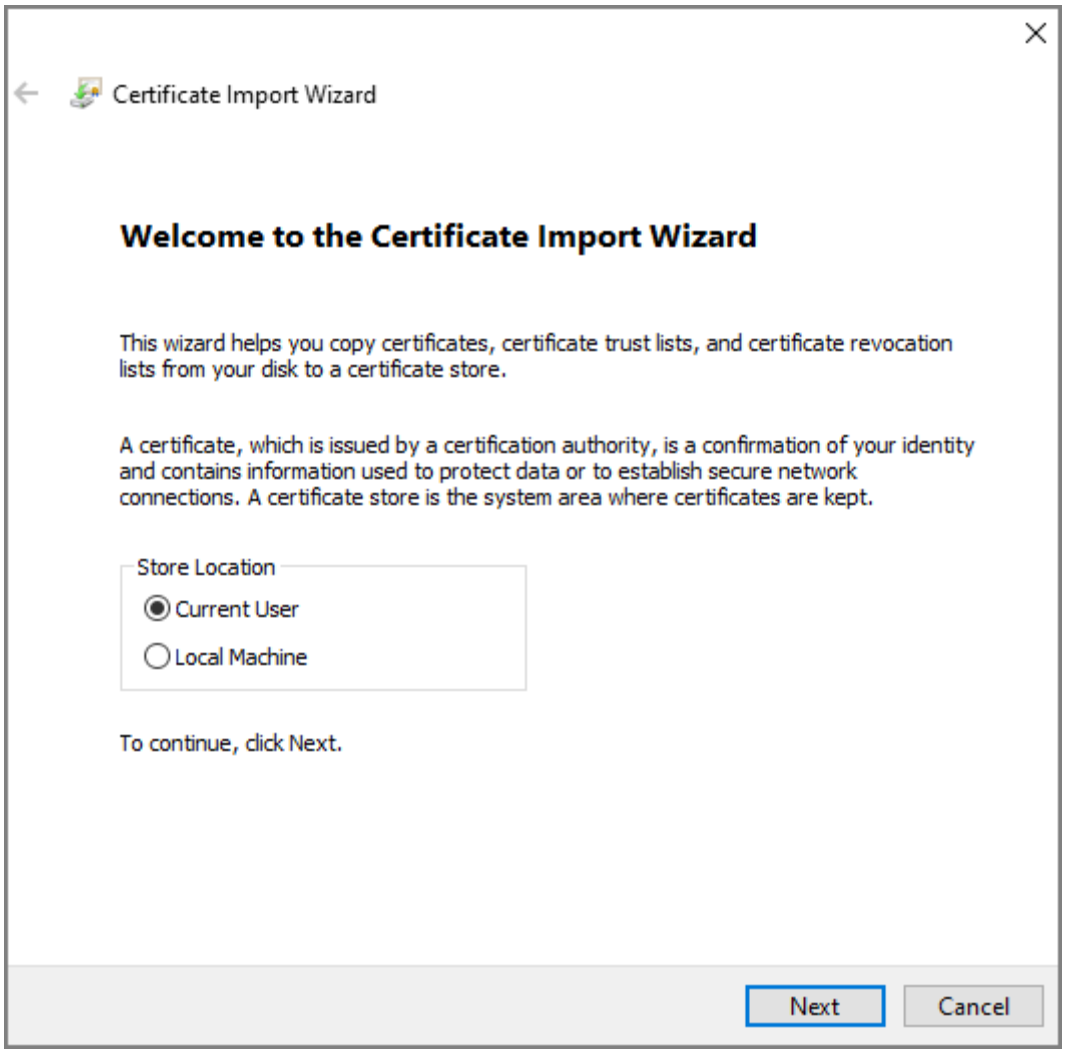
Paso 3 Hacer clic**Instalar certificado**.

Figura 3-37 Información del certificado



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

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

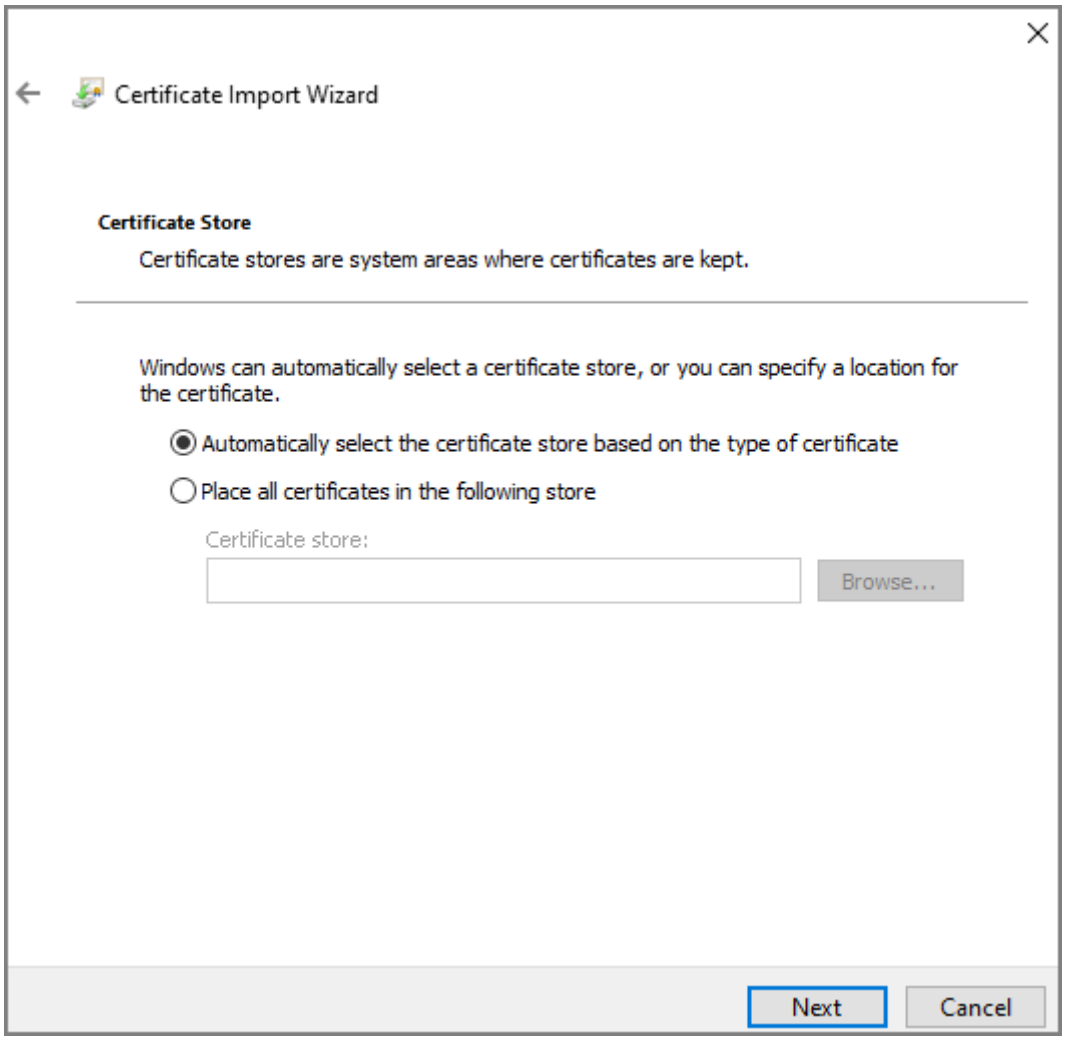


Paso 5 Seleccione la ubicación de almacenamiento adecuada.

1) Seleccionar**Coloque todos los certificados en el siguiente almacén**.

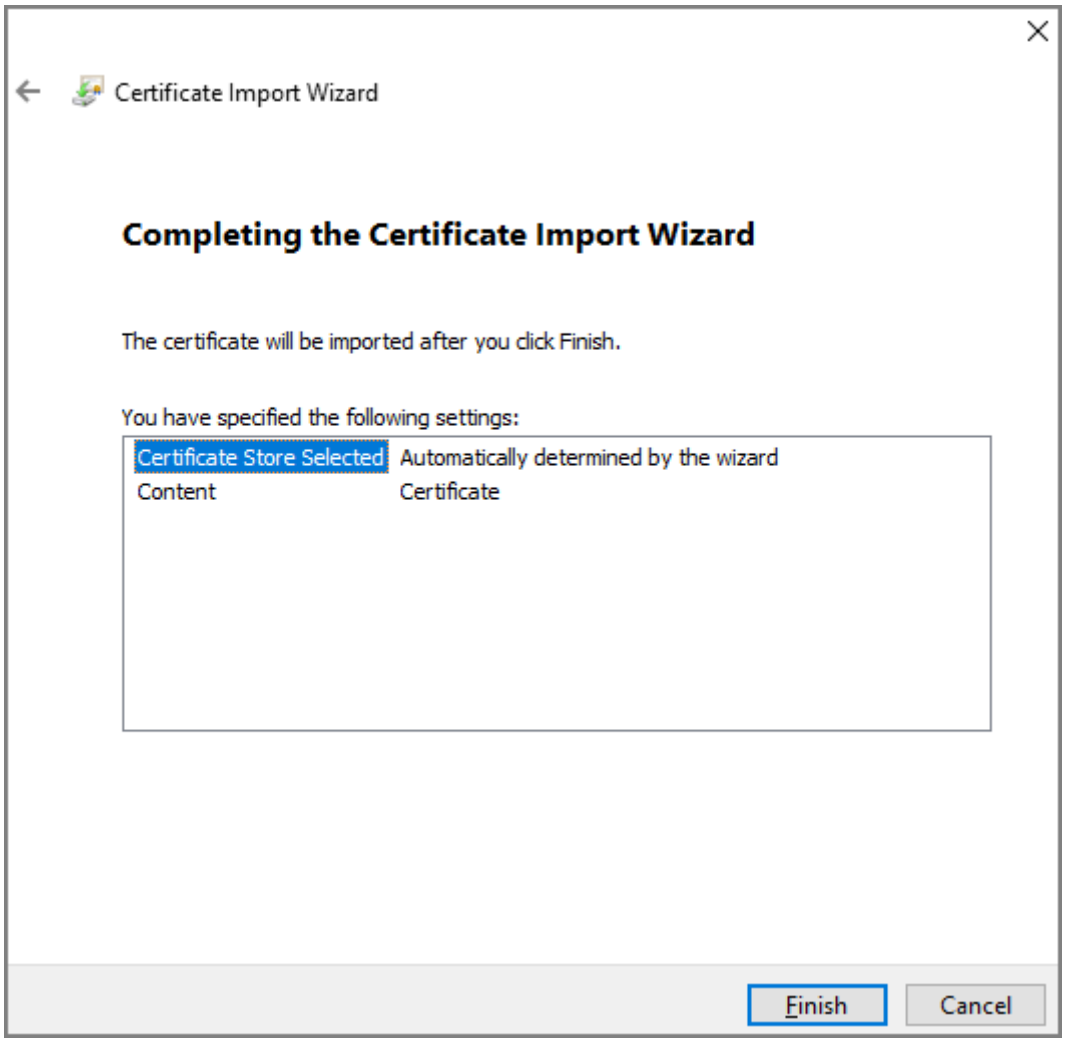
2) Haga clic**Navegar**para importar el certificado a la**Autoridades de certificación raíz de confianza** tienda y luego haga clic en**Próximo**.

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 sus contraseñas e ingresar una dirección de correo electrónico para restablecer la contraseña cuando la olvide.

3.12.1 Agregar cuenta de administrador

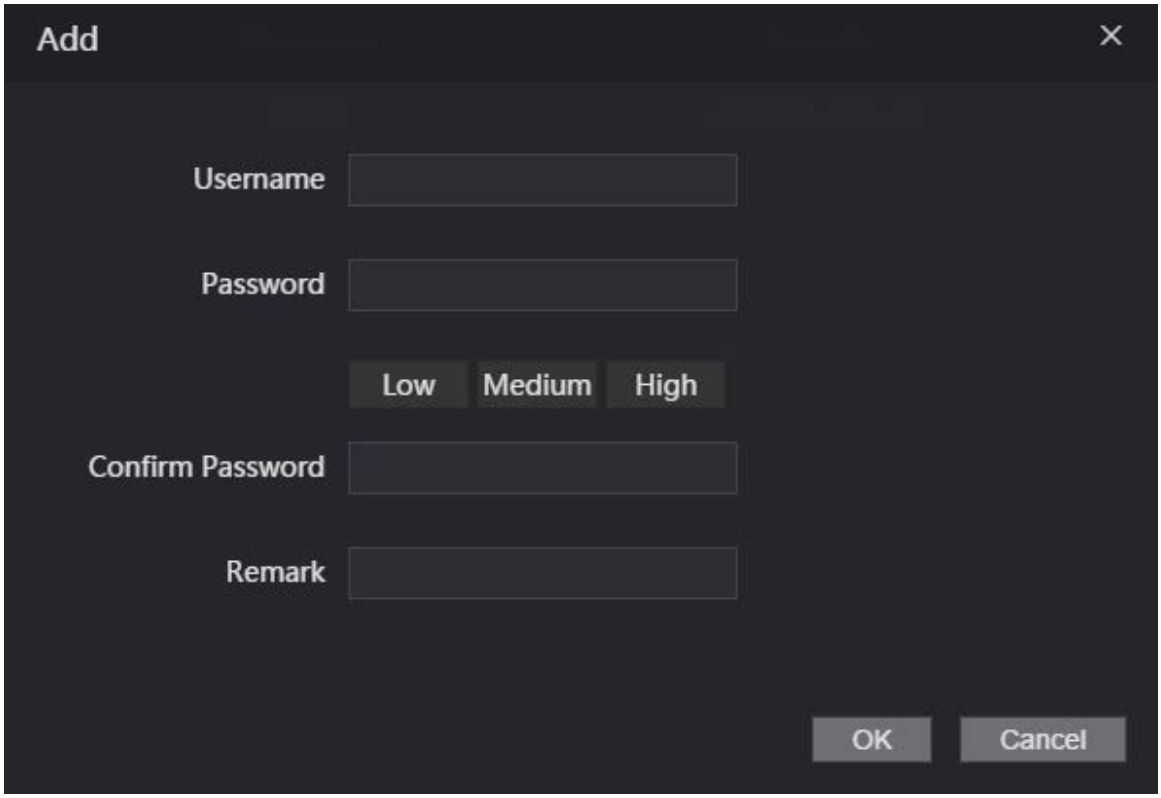
Procedimiento

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

Paso 2 . Haga 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 hasta 31 caracteres y solo permite números, letras, guiones bajos, líneas intermedias, puntos o @.
- La contraseña debe constar de 8 a 32 caracteres que no sean espacios 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 contraseña Indicación de fuerza.

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

Agregue usuarios al Controlador de Acceso para que puedan desbloquear la puerta una vez verificada su identidad. El Controlador de Acceso permite el desbloqueo mediante tarjeta, huella dactilar, contraseña, reconocimiento facial o combinaciones de ambos. Se debe configurar al menos un método de verificación.

Procedimiento

Paso 1 En el**Menú principal**, seleccionar**Gestión de usuarios.**>

Paso 2 **Usuario**. Configure los parámetros.

Figura 3-42 Agregar nuevo usuario

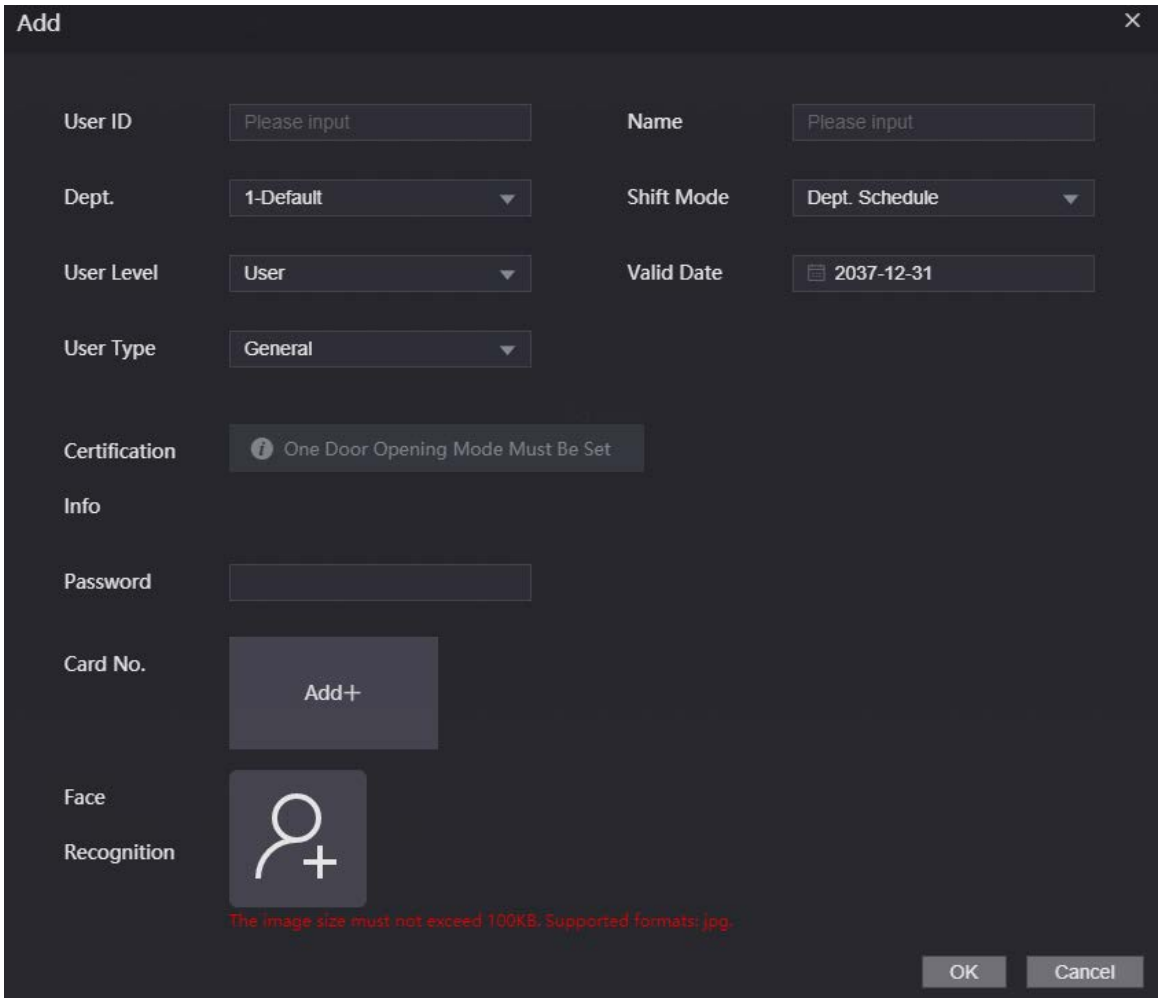


Tabla 3-23 Descripción de parámetros

Parámetro	Descripción
ID de usuario	Introduzca los ID de usuario. Pueden ser números, letras y combinaciones de estos, y su longitud máxima es de 32 caracteres. Cada ID es único.
Nombre	Ingrese un nombre con un máximo de 32 caracteres (incluidos números, símbolos y letras).
Dpto.	Establecer departamentos.
Modo Shift	Seleccionar modos de cambio.
Nivel de usuario	Puede seleccionar un nivel de usuario para los nuevos usuarios. ● **Usuario**:Los usuarios sólo tienen permiso de acceso a la puerta. ● **Administración**:Los administradores pueden desbloquear la puerta y configurar el controlador de acceso.
Fecha válida	Establezca una fecha en la que caducarán los permisos de acceso de la persona.

Parámetro	Descripción
Tipo de usuario	● **General**:Los usuarios generales pueden desbloquear la puerta. ● **Lista de bloqueo**: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 periodo definido o por un número determinado de veces. Una vez transcurrido el periodo definido o el tiempo de desbloqueo, no podrán desbloquear la puerta. ● **Patrulla**:Los usuarios de patrulla tendrán registrada su asistencia, pero no tendrán permisos de desbloqueo. ● **personaje**:Cuando el VIP desbloquee la puerta, el personal de servicio recibirá un aviso. ● **Otros**:Cuando desbloqueen la puerta, ésta permanecerá desbloqueada durante 5 segundos más. ● Usuario personalizado 1/Usuario personalizado 2: Lo mismo que los usuarios generales.
Contraseña	Introduzca la contraseña de usuario. La longitud máxima de la contraseña es de 8 dígitos.
N° de tarjeta	Un usuario puede registrar hasta 5 tarjetas. Ingrese el número de su tarjeta manualmente o deslícela por el lector para que se registre automáticamente. Puedes habilitar el**Tarjeta de coacción**Función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta. Asegúrese de que haya un lector de tarjetas externo conectado al Controlador de acceso si desea registrar el número de tarjeta a través del lector de tarjetas.
Reconocimiento facial	Importe imágenes de rostros a la página web. El formato de imagen debe ser JPG y su tamaño debe ser inferior a 100 KB. Se pueden registrar hasta dos imágenes de rostros por persona.

Paso 3 Hacer clic**DE ACUERDO**.

Operaciones relacionadas

- Importar usuarios: Haga clic en**Plantilla de exportación**, complete la plantilla y luego haga clic en**Importar información del usuario**para importar el archivo a la página web.
- Borrar registro: borra toda la información del usuario.
- Eliminación por lotes: elimina los usuarios seleccionados.

3.12.3 Agregar usuarios ONVIF

Información de fondo

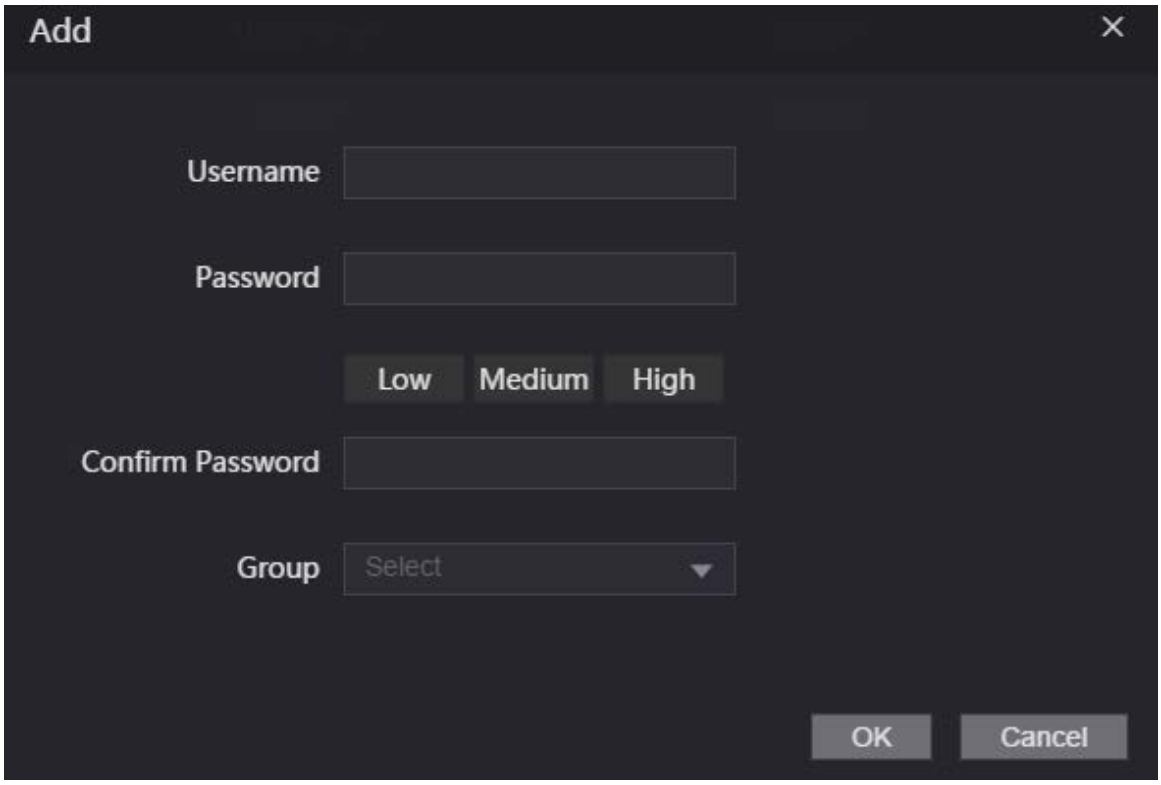
El Foro Abierto de Interfaz de Video en Red (ONVIF) es un foro global y abierto de la industria, creado para desarrollar un estándar abierto global para la interfaz de productos de seguridad basados en IP física, lo que permite la compatibilidad entre diferentes fabricantes. La identidad de los usuarios de ONVIF se verifica mediante el protocolo ONVIF. El usuario predeterminado de ONVIF es admin.

Procedimiento

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

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

Figura 3-43 Agregar usuario ONVIF



Paso 3 Hacer clic**DE ACUERDO**.

3.12.4 Visualización de usuarios en línea

Puedes ver los usuarios conectados que actualmente están conectados a la página web. En la página de inicio, selecciona**Usuario en línea**.

3.13 Configuración de indicaciones de voz

Establecer indicaciones de voz durante la verificación de identidad.

Procedimiento

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

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

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

3.14 Mantenimiento

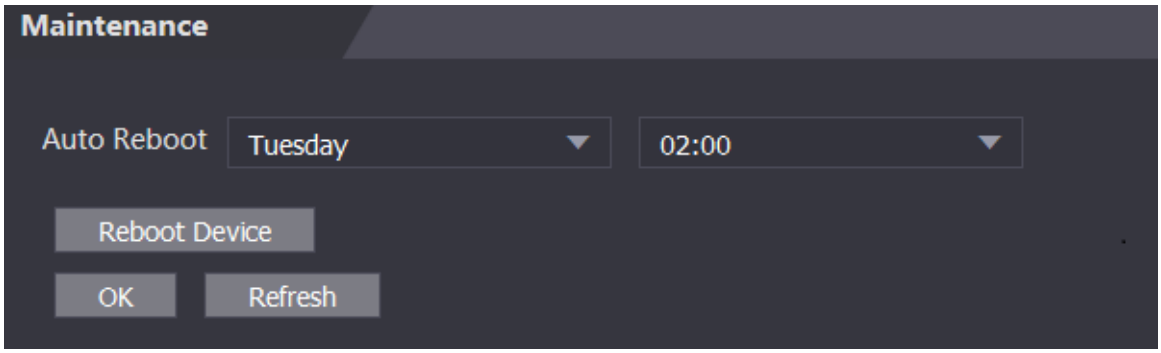
Puede reiniciar periódicamente el controlador de acceso durante el tiempo de inactividad para mejorar su rendimiento.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccione**Mantenimiento**.

Figura 3-44 Mantenimiento



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

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

3.15 Gestión de la configuración

Cuando más de un controlador de acceso necesitan las mismas configuraciones, puede configurar parámetros para ellos importando o exportando archivos de configuración.

3.15.1 Exportación/importación de archivos de configuración

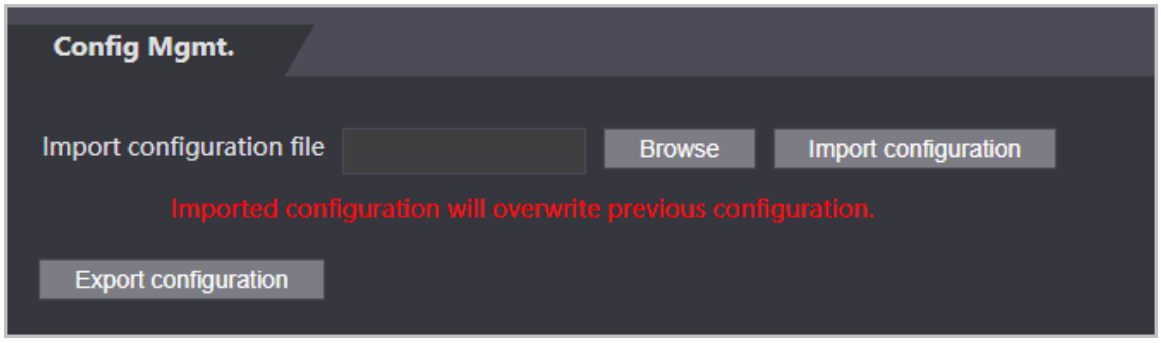
Puede importar o exportar el archivo de configuración del controlador de acceso. Si desea aplicar la misma configuración a varios dispositivos, puede importar el archivo de configuración.

Procedimiento

Paso 1 Inicie sesión en la página web.

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

Figura 3-45 Gestión de la 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 IP 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

Información de fondo

Restaurando el**Controlador de acceso**El uso de las configuraciones predeterminadas provocará pérdida de datos. Tenga en cuenta lo siguiente.

Procedimiento

Paso 1 Seleccionar**Gestión de configuración.**>**Por defecto**. Restaurar 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 del usuario y los registros.

3.15.3 Configuración de los accesos directos

Procedimiento

Paso 1 En la página web del Controlador de Acceso, seleccione**Gestión de cofig.**>**Conjunto de atajos**.

Paso 2 Configure los parámetros de acceso directo.

Figura 3-46 Conjunto de accesos directos

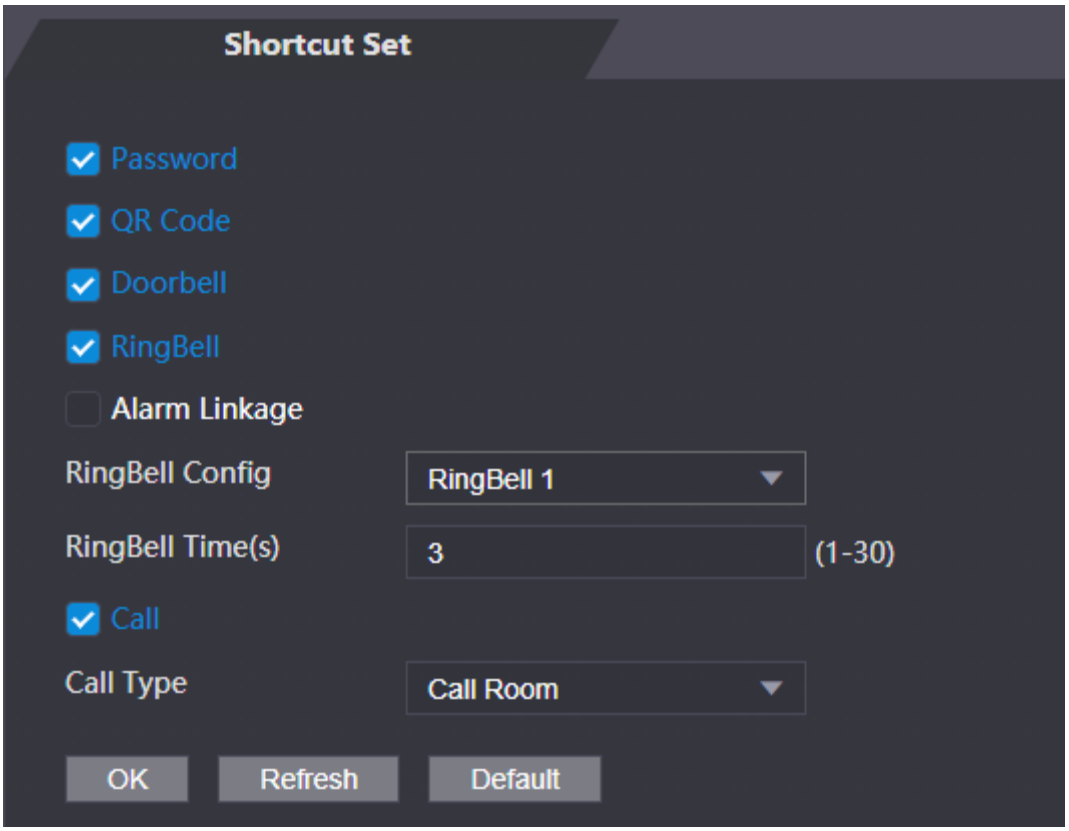


Tabla 3-25 1

Parámetro	Descripción
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.

Parámetro	Descripción
Timbre de la puerta	Después de activar la función de timbre, el icono del timbre se muestra en la pantalla de espera. ● RingBell: toque el ícono de timbre en la pantalla de espera y el controlador de acceso sonará. ● Vinculación de alarma: active la función de vinculación de alarma y luego sonará el timbre. Esta función sólo está disponible en modelos seleccionados. ● Configuración de RingBell: seleccione el timbre de llamada 1 o el timbre de llamada 2. ● Duración del timbre: Establezca la duración del timbre (1-30 s). El valor predeterminado es 3.
Llamar	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 sala 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: ingrese el número de sala y luego puede tocar el ícono de llamada en la pantalla de espera para llamar al número de sala definido. Asegúrese de que el controlador de acceso se haya agregado a DMSS.

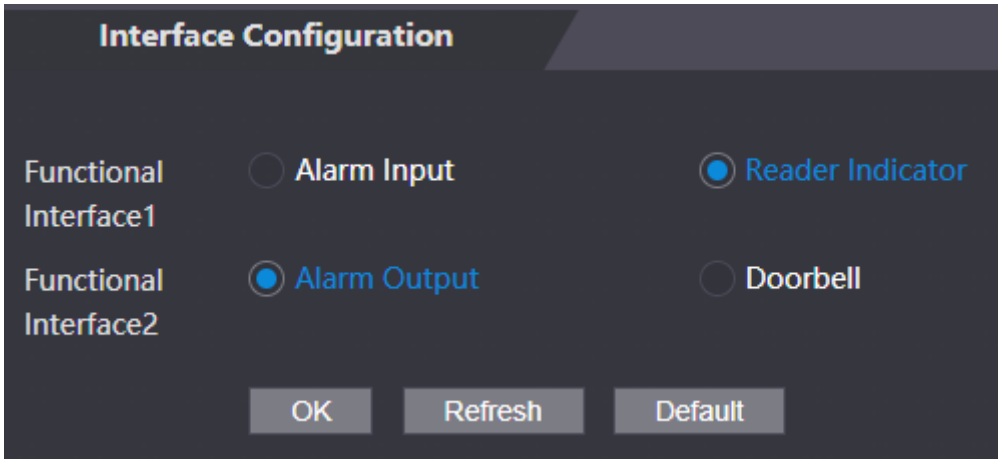
3.15.4 Configuración de las funciones del puerto

Algunos cables pueden usarse para diferentes propósitos. Conecte los cables según sus necesidades.

Procedimiento

Paso 1 En la página web del Controlador de Acceso, seleccione**Gestión de configuración.**>**Configuración de interfaz**.

Figura 3-47 Configurar funciones del puerto



Paso 2 Seleccione la función del puerto. Haga clic.**DE**

Paso 3 **ACUERDO**.

3.16 Actualización del sistema

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

Durante la actualización.

3.16.1 Actualización de archivos

Procedimiento

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

Procedimiento

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

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

- Seleccionar**Comprobación automática**El controlador de acceso comprobará automáticamente si su última versión está disponible.
- Seleccionar**Comprobación manual**y podrás comprobar inmediatamente si la última versión está disponible.

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

3.17 Visualización de la información de la versión

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

3.18 Visualización de registros

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

3.18.1 Registros del sistema

Ver y buscar registros del sistema.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccione**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**. Haga clic**Respaldo**para descargar el registro del sistema.

3.18.2 Registros de administración

Busque registros de administración utilizando el ID de administrador.

Procedimiento

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

Paso 2 **Registro de administración**Ingrese el ID de administrador y luego

Paso 3 haga clic en**Consulta**.

3.18.3 Desbloqueo de registros

Busque registros de desbloqueo y expórtelos.

Procedimiento

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.

4 Configuración inteligente de PSS Lite

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

Procedimiento

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 la contraseña y las preguntas de seguridad.

Establezca la contraseña para el primer uso y luego configure las preguntas de seguridad para restablecerla. Contraseña cuando la olvidaste.

Paso 3 Introduzca 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. Puede agregarlos por lotes o individualmente.

4.2.1 Agregar individualmente

Puede agregar un controlador de acceso individualmente ingresando sus direcciones IP o nombres de dominio.

Procedimiento

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

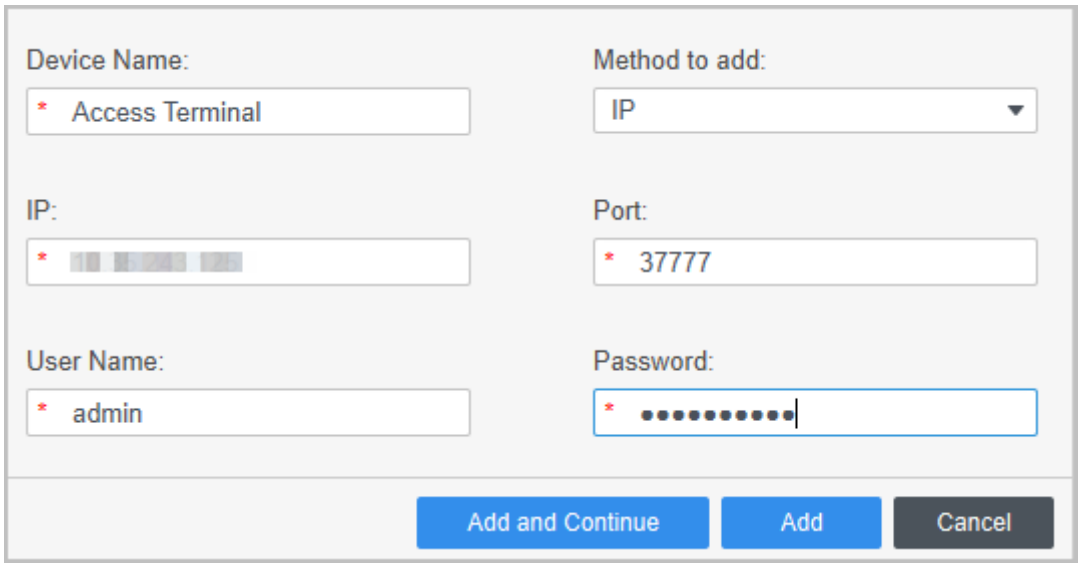


Tabla 4-1 Parámetros del dispositivo Descripción

Parámetro	Descripción
Nombre del dispositivo	Introduzca un nombre para el controlador de acceso. Le recomendamos que lo nombre según su área de instalación.
Método para agregar	Seleccionar**Propiedad intelectual**para agregar el Terminal de Acceso ingresando su Dirección IP.
Propiedad intelectual	Introduzca la dirección IP del controlador de acceso.
Puerto	El número de puerto es 37777 por defecto.
Nombre de usuario/Contraseña	Introduzca el nombre de usuario y la contraseña del Terminal de Acceso.

Paso 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 Adición en lotes

Le recomendamos usar la función de búsqueda automática al agregar controladores de acceso por lotes. Asegúrese de que los controladores de acceso que agregue estén en el mismo segmento de red.

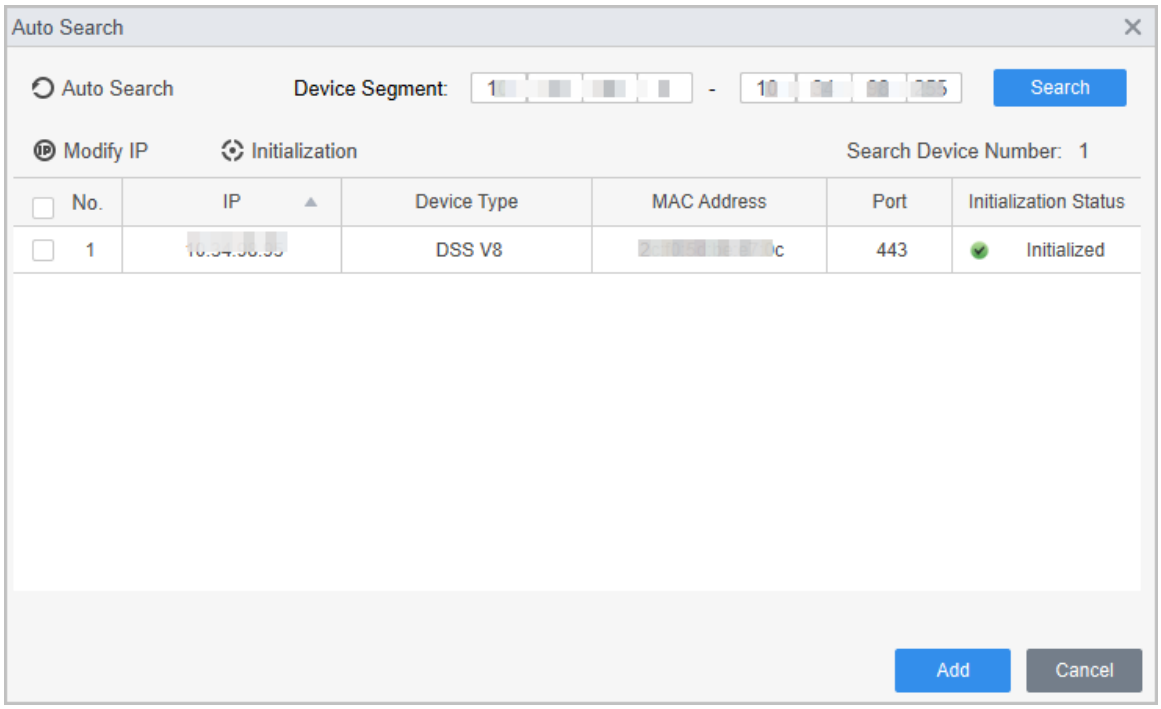
Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

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

Paso 4 Introduzca el nombre de usuario y la contraseña del Controlador de Acceso.

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

El controlador de acceso inicia sesión automáticamente en Smart PSS Lite después de agregarse.**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 Configuración del tipo de tarjeta

Configure el tipo de tarjeta antes de asignarlas a los usuarios. Por ejemplo, si la tarjeta asignada es una tarjeta de identificación, configure el tipo como tarjeta de identificación.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

Paso 3 **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.

Paso 4 Hacer clic**DE ACUERDO**.

4.3.2 Agregar usuarios

4.3.2.1 Agregar uno por uno

Puede agregar usuarios uno por uno.

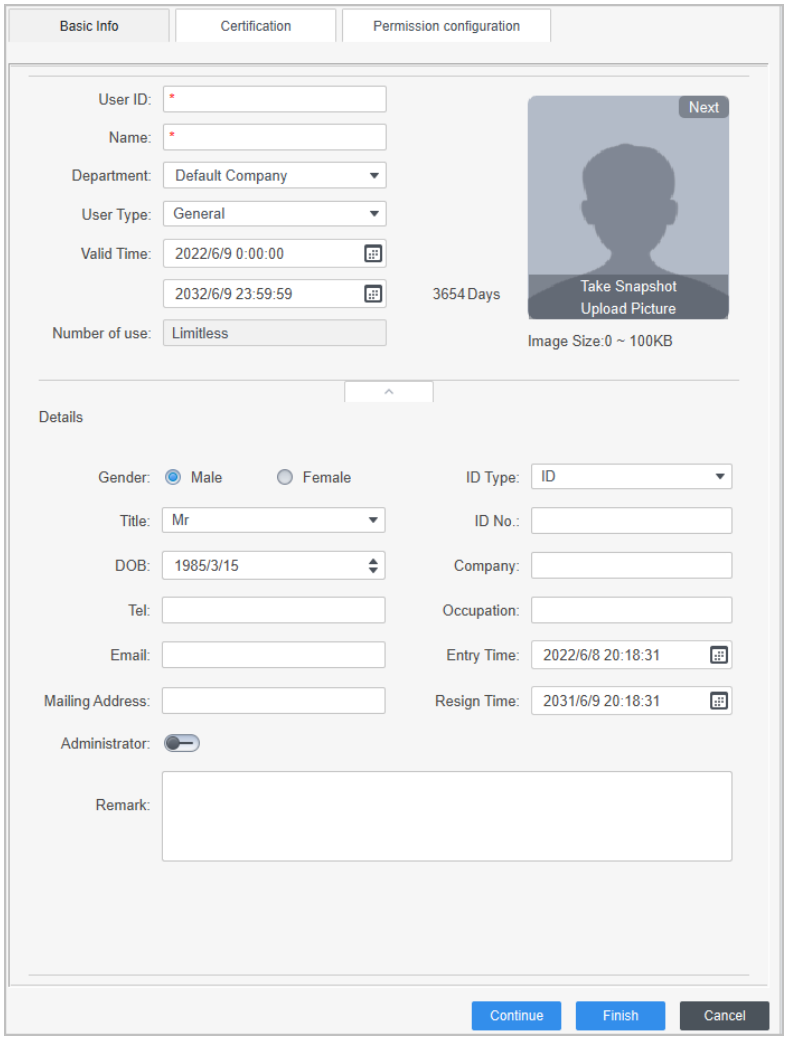
Procedimiento

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, ingrese la información básica del usuario y luego importe la imagen del rostro.

Figura 4-3 Agregar información básica



Paso 4 Haga clic en el**Proceso de dar un título**Pestaña para agregar información de certificación del usuario.

- Configurar contraseña: La contraseña debe constar de 6 a 8 dígitos.
- Configurar tarjeta: El número de tarjeta puede leerse automáticamente o introducirse manualmente. Para leerlo automáticamente, seleccione un lector de tarjetas y colóquelo en él.

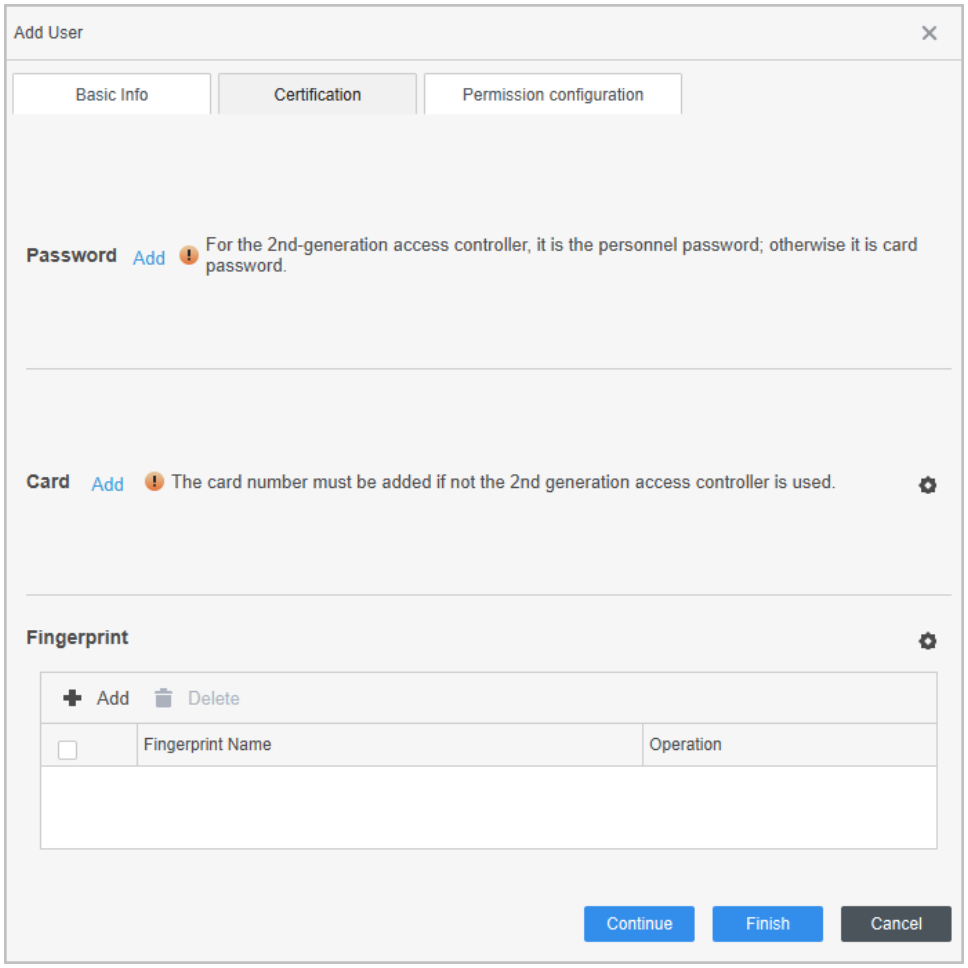
1. En el**Tarjeta**área, haga clic y seleccione**emisor de la tarjeta**, y luego haga clic en**DE ACUERDO**.
2. Haga clic**Agregar**Pase una tarjeta por el lector. Se mostrará el número de la tarjeta.
3. Haga clic**DE ACUERDO**.

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

- Configurar huella digital.

  1. En 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 su dedo sobre el escáner tres veces seguidas.

Figura 4-4 Agregar contraseña, tarjeta y huella digital



Paso 5 Configure los permisos del usuario. Para más detalles, consulte "4.3.3 Asignación de permisos de acceso". Haga clic

Paso 6 en**Finalizar**.

4.3.2.2 Adición en lotes

Puede agregar usuarios en lotes.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

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

Figura 4-5 Agregar usuarios en lotes

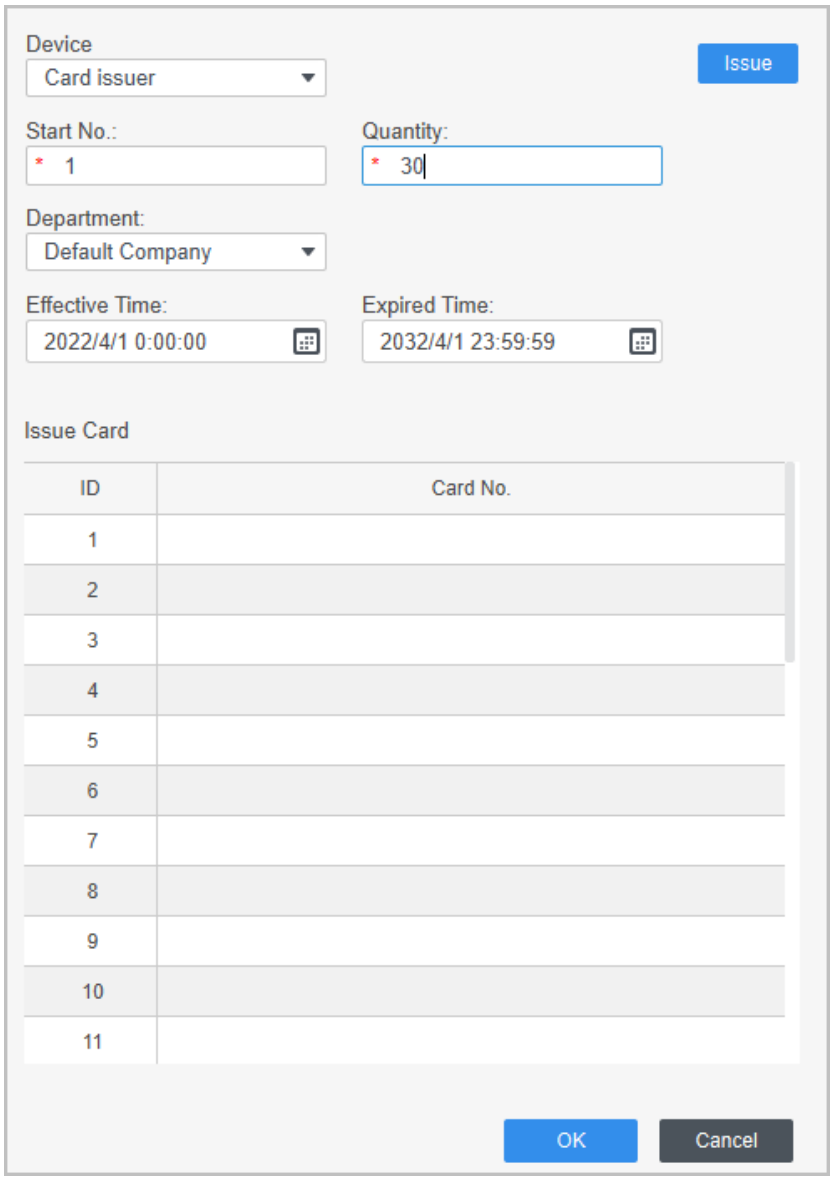


Tabla 4-2 Parámetros para agregar usuarios en lotes

Parámetro	Descripción
Número de inicio	El ID de usuario comienza con el número que usted definió.
Cantidad	El número 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.

Paso 4 Hacer clic**Asunto**.

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

Paso 5 **ACUERDO**.

Paso 6 En el**Usuario**página, haga clic Para completar la información del usuario.

4.3.3 Asignación de permisos 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 los usuarios puedan desbloquear las puertas correspondientes.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

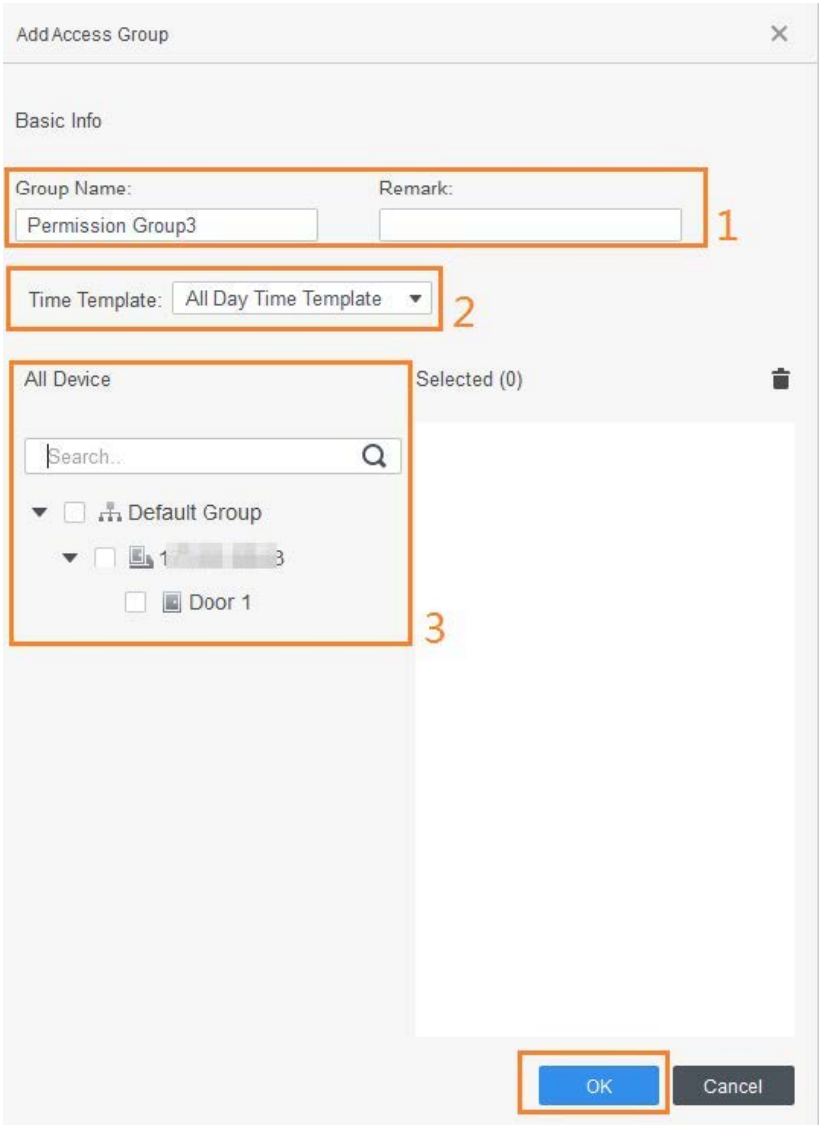
Paso 3 en .

Paso 4 Introduzca el nombre del grupo, las observaciones (opcionales) y seleccione una plantilla de tiempo.

Paso 5 Seleccione el dispositivo de control de acceso.

Paso 6 Hacer clic**DE ACUERDO**.

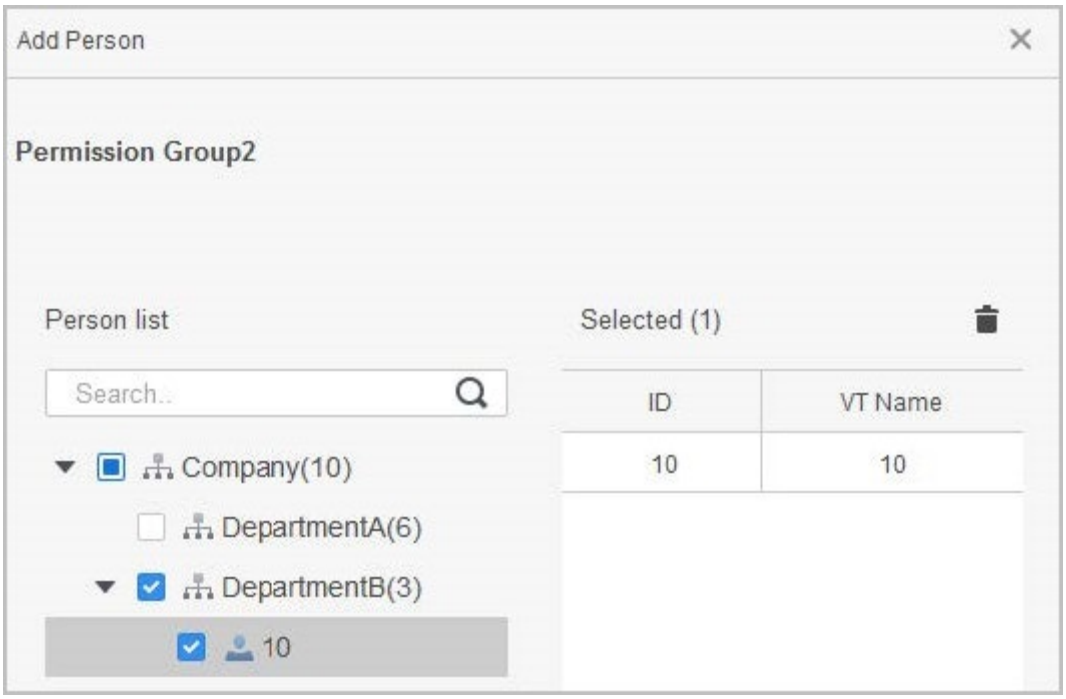
Figura 4-6 Crear un grupo de permisos



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.

4.3.4 Asignación de permisos de asistencia

Cree un grupo de permisos que sea una colección de permisos de control de asistencia y luego asocie empleados al grupo para que puedan registrar su entrada y salida a través de métodos de verificación definidos.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

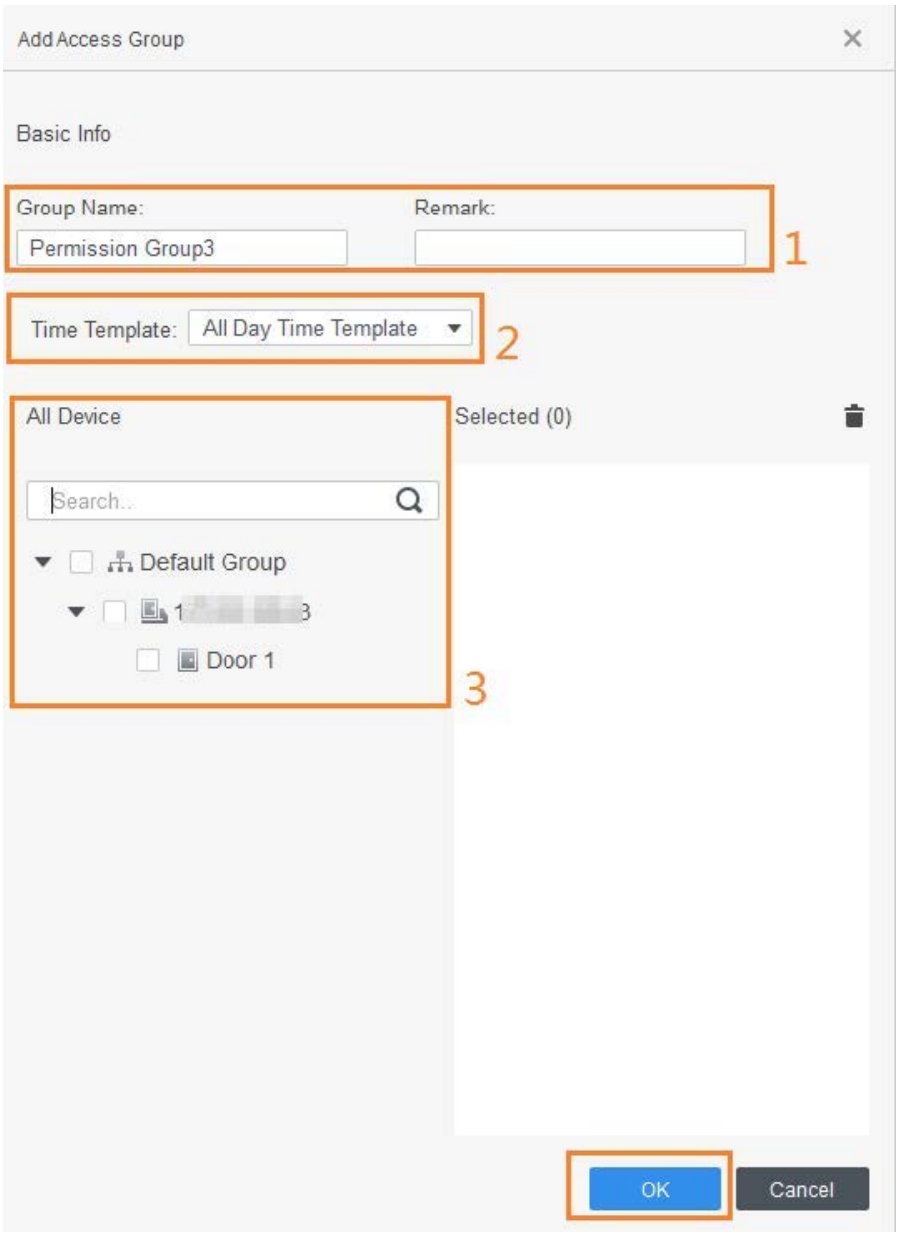
Paso 3 en .

Paso 4 Introduzca el nombre del grupo, las observaciones (opcionales) y seleccione una plantilla de tiempo.

Paso 5 Seleccione el dispositivo de control de acceso.

Paso 6 Hacer clic**DE ACUERDO**.

Figura 4-8 Crear un grupo de permisos



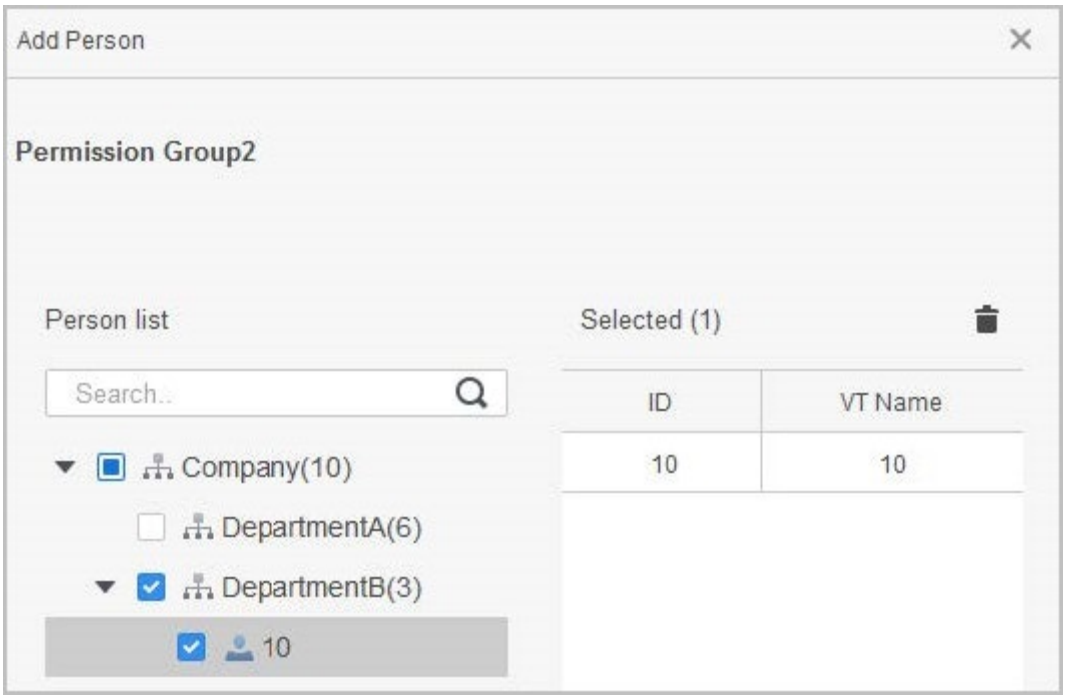
El control de tiempo y asistencia solo admite entrada y salida mediante contraseña y reconocimiento facial.

asistencia.

Paso 7 Hacer clic del grupo de permisos que agregó.

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

Figura 4-9 Agregar usuarios a un grupo de permisos



Paso 9 Hacer clic**DE ACUERDO**.

4.4 Gestión de acceso

4.4.1 Apertura y cierre de puertas a distancia

Puede supervisar y controlar la puerta a distancia a través de Smart PSS Lite. Por ejemplo, puede abrirla o cerrarla a distancia.

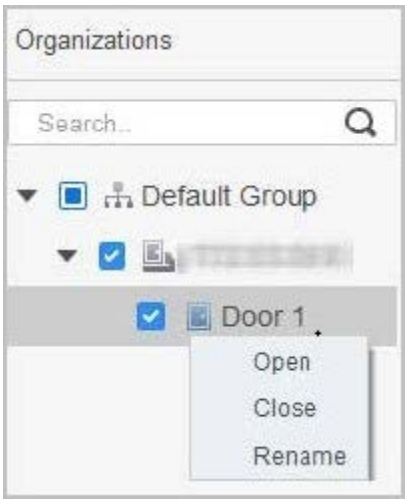
Procedimiento

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

Paso 2 Controla la puerta a distancia.

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

Figura 4-10 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; esta dejará de actualizarse. Haga clic para desbloquearla.
- Eliminar eventos: haga clic para borrar todos los eventos en la lista de eventos.

4.4.2 Configuración Siempre abierto y Siempre cerrado

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

Procedimiento

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

Paso 2 Haga clic en**Siempre abierto**o**Siempre cerca**para abrir o cerrar la puerta.

Figura 4-11 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

Procedimiento

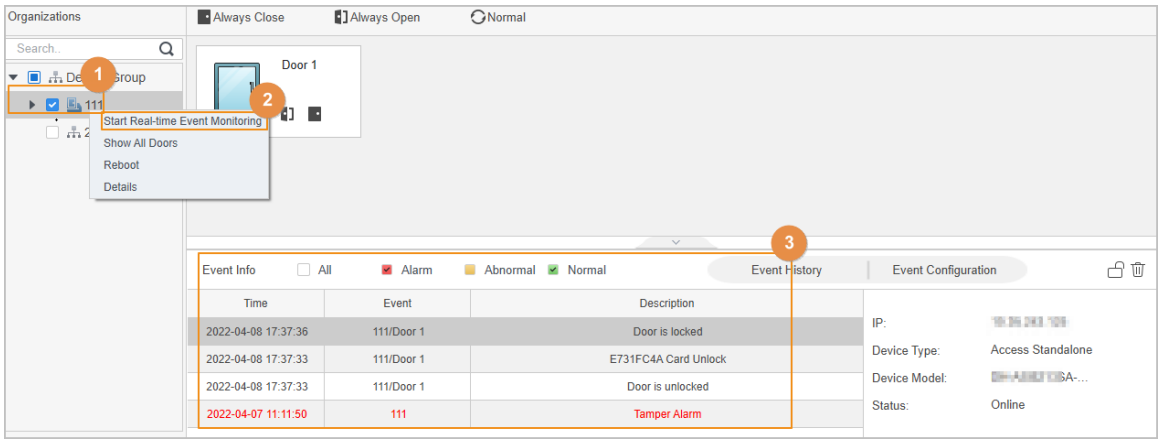
Paso 1 Hacer clic**Solución de acceso**>**Administrador de acceso**en la página de inicio.

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

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

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

Figura 4-12 Estado de la puerta del monitor



Operaciones relacionadas

- 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.

Prerrequisitos

La función de intercomunicador 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  .

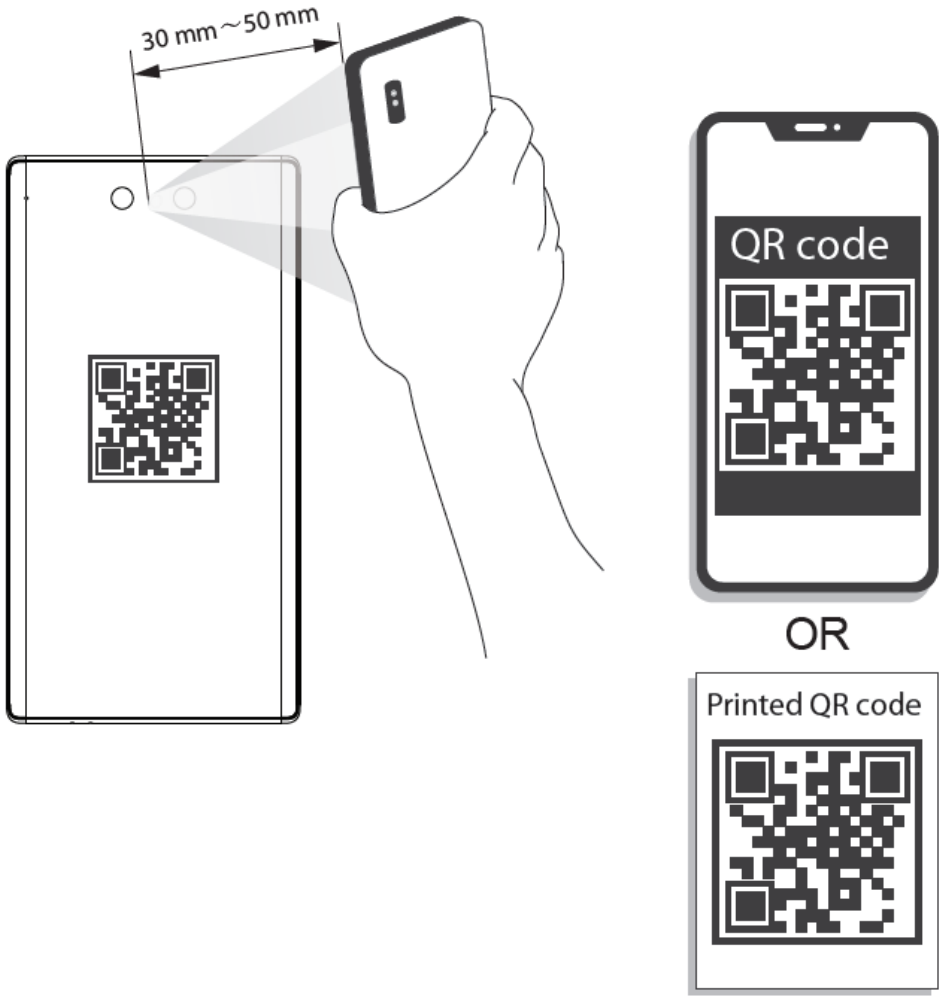
Apéndice 2 Puntos importantes del código QR

Exploración

Coloque el código QR en su teléfono a una distancia de 3 a 5 cm del lente del escáner. Admite códigos QR de más de 30 mm × 30 mm (5 a 5 cm × 5 cm) y menos de 128 bytes.

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 la toma de huellas dactilares

Instrucciones de registro

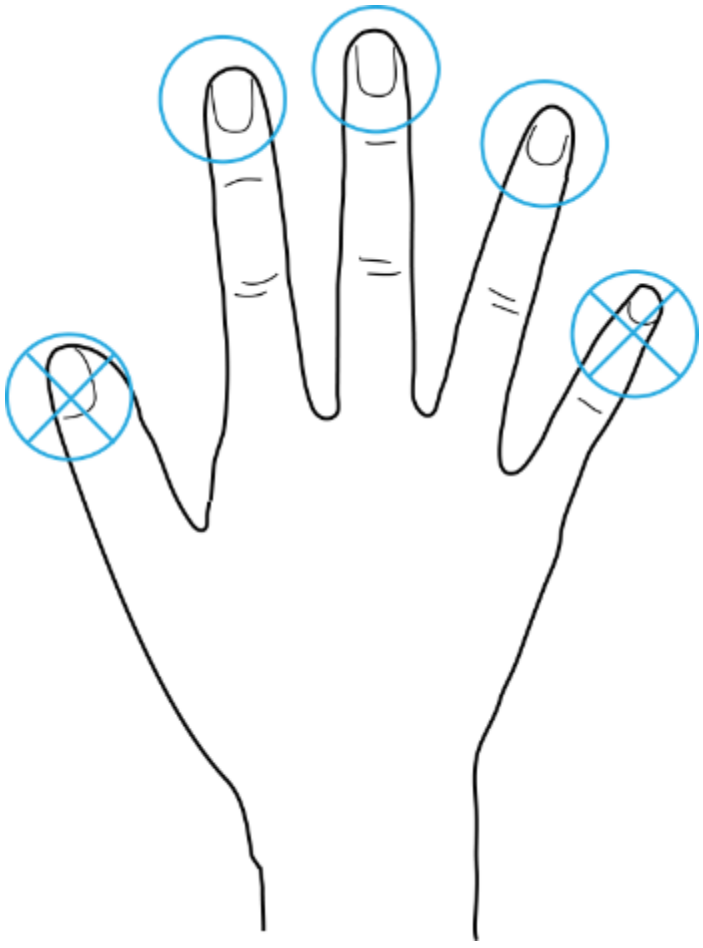
Al registrar la huella dactilar, preste atención a los siguientes puntos:

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

Se recomiendan los dedos

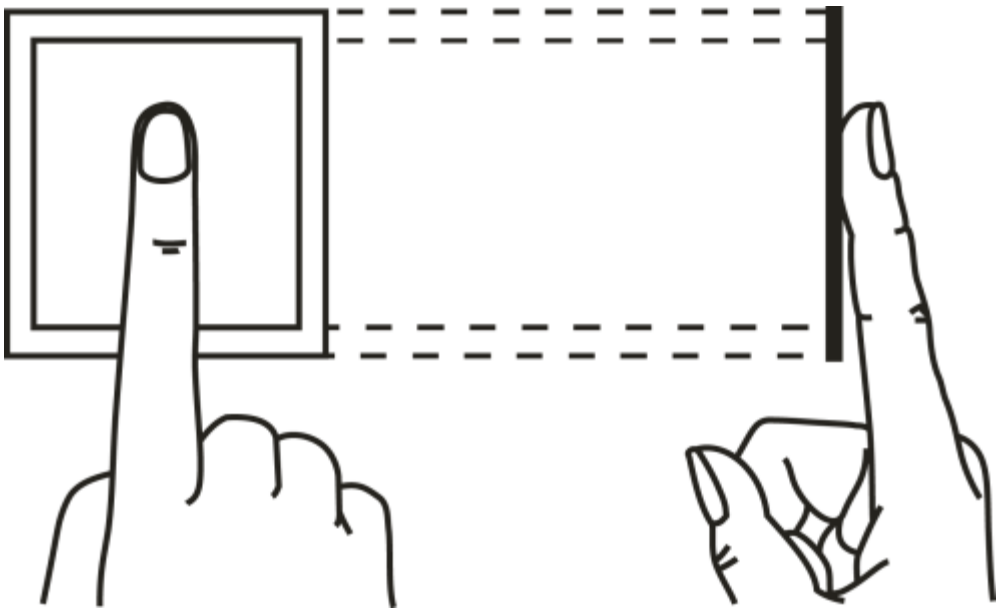
Se recomiendan los dedos índice, medio y anular. Los pulgares y meñiques no se colocan fácilmente en el centro de la grabación.

Apéndice Figura 3-1 Dedos recomendados

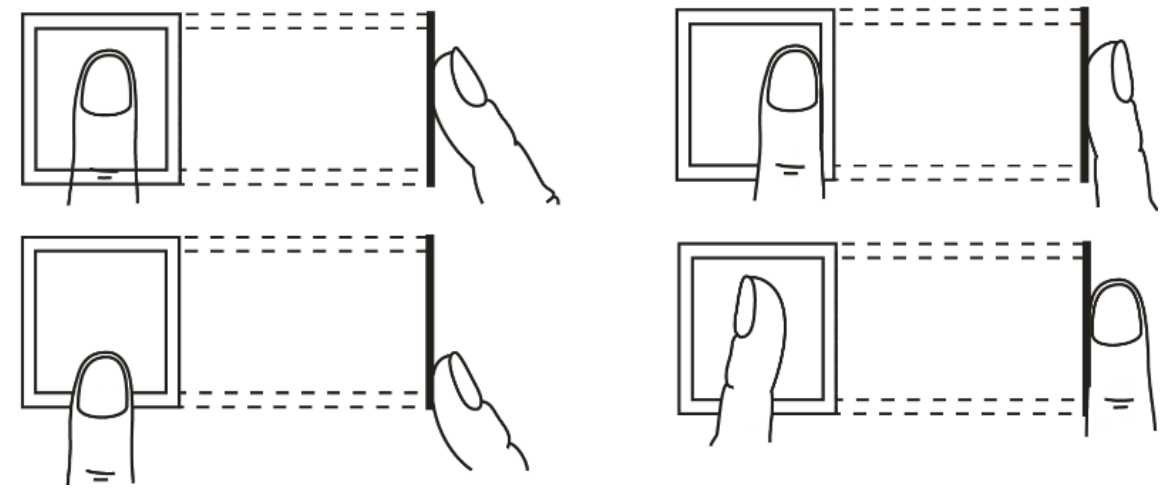


Cómo presionar su huella dactilar en el escáner

Apéndice Figura 3-2 Colocación correcta



Apéndice Figura 3-3 Colocación incorrecta



Apéndice 4 Puntos importantes del rostro

Registro

Antes del registro

- Las gafas, los sombreros y las barbas pueden influir en el rendimiento del reconocimiento facial.
- No te cubras las cejas cuando uses sombreros.
- No cambie mucho el estilo de su barba si usa el controlador de acceso; de lo contrario, el reconocimiento facial podría fallar.
- Mantén tu cara limpia.
- Mantenga el controlador de acceso al menos a 2 metros de distancia de la fuente de luz y al menos a 3 metros de ventanas o puertas; de lo contrario, la luz de fondo y la luz solar directa podrían influir en el rendimiento de reconocimiento facial del controlador de acceso.

Durante el registro

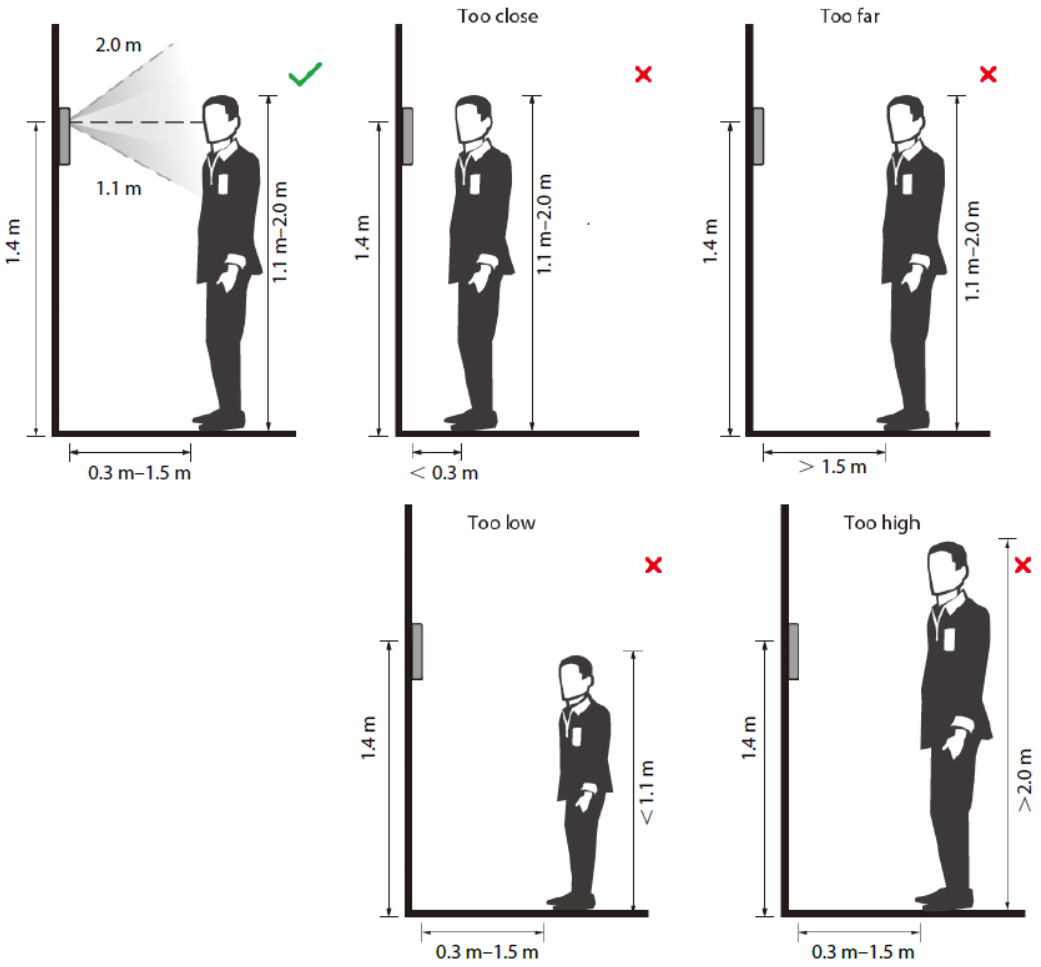
- Puede registrar rostros a través del Controlador de Acceso o de la plataforma. Para el registro a través de la plataforma, consulte el manual de usuario.
- Centra tu cabeza en el marco de captura de fotos. La imagen del rostro se capturará automáticamente.

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

Posición de la cara

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

Apéndice Figura 4-1 Posición adecuada de la cara



Requisitos de las caras

- Asegúrese de que la cara esté limpia y la frente no esté cubierta de pelo.
- No use anteojos, sombreros, barbas pobladas ni otros adornos faciales que influyan en la grabación de imágenes del rostro.
- Con los ojos abiertos, sin expresiones faciales y dirige tu cara hacia el centro de la cámara.
- Al grabar su rostro o durante el reconocimiento facial, no mantenga su rostro demasiado cerca ni 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; los píxeles de la imagen son más de 500 × 500 píxeles; el tamaño de la imagen es inferior a 100 KB y el nombre de la imagen y la identificación de la persona son los mismos.
- Asegúrese de que el rostro ocupe más de 1/3 pero no más de 2/3 del área total de la imagen. y la relación de aspecto no exceda 1:2.

Apéndice 5 Recomendaciones de ciberseguridad

Acciones obligatorias a tomar para la seguridad de la red de equipos básicos:

1.**Utilice contraseñas seguras**

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

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

Recomendaciones "deseables" para mejorar la seguridad de la red de sus equipos:

1.**Protección física**

Le sugerimos que implemente protección física para los equipos, especialmente los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en una sala de computadoras y un gabinete especiales, e implemente un control de acceso y una gestión de claves rigurosos para evitar que personal no autorizado realice contactos físicos, como dañar el hardware o conectar sin autorización equipos extraíbles (como memorias USB o puertos serie), etc.

2.**Cambie las contraseñas periódicamente**

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

3.**Establecer y actualizar contraseñas Restablecer información oportunamente**

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

4.**Habilitar bloqueo de cuenta**

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

5.**Cambiar el puerto HTTP predeterminado y otros puertos de servicio**

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

6.**Habilitar HTTPS**

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

7.**Vinculación de direcciones MAC**

Le recomendamos vincular la dirección IP y MAC del gateway al equipo, reduciendo así el riesgo de suplantación de ARP.

8.**Asignar cuentas y privilegios de manera razonable**

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios de manera razonable y asigne un

conjunto mínimo de permisos para ellos.

9. **Desactivar servicios innecesarios y elegir modos seguros**

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

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

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

10. **Transmisión cifrada de audio y vídeo**

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

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

11. **Auditoría segura**

- Comprobar usuarios en línea: le sugerimos que compruebe periódicamente los usuarios en línea para ver si el dispositivo ha iniciado sesión sin autorización.
- Consultar registro de equipos: Al visualizar los registros, podrás conocer las direcciones IP que se utilizaron para iniciar sesión en tus dispositivos y sus operaciones clave.

12. **Registro de red**

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

13. **Construir un entorno de red seguro**

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

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