Controlador de acceso con reconocimiento facial

Manual del usuario



Versión 1.0.1

Prefacio

General

Este manual presenta las funciones y operaciones del controlador de acceso de reconocimiento facial (en adelante, el "controlador de acceso"). Lea atentamente antes de utilizar el dispositivo y guarde el manual para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de señal	Significado
DANGER	Indica un alto riesgo potencial 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 1.0.1	Se actualizó el manual.	Mayo de 2023
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, es posible que recopile 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 de la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del manual

- El manual es solo de referencia. Pueden 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 de acuerdo con las últimas leyes y regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Pueden encontrarse ligeras diferencias entre 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 pueden provocar que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede 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 explicación final.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas 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 contenido que cubre el manejo adecuado del controlador de acceso, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el controlador de acceso y cumpla con las pautas al usarlo.

Requerimientos 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 humedad y temperatura 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 estándares de seguridad eléctrica locales. Asegúrese de que el voltaje ambiental sea estable y cumpla con los requisitos de suministro de energía del controlador de acceso.
- No conecte el controlador de acceso a dos o más tipos de fuentes de alimentación, para evitar 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 una fuente de alimentación de armario proporcionada 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 en la norma IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de la fuente de alimentación están sujetos a la etiqueta del controlador de acceso.
- El controlador de acceso es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del controlador de acceso esté conectada a una toma de corriente con conexión a tierra de protección.

Requisitos de funcionamiento



- 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.

- Utilice 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 instrucción profesional.

Tabla de contenido

Prólogo..... 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 básico de configuración..... 3

2.2 Iconos comunes.....3

2.3 Inicialización..... 4

2.4 Pantalla de espera..... 4

2.5 Inicio de sesión.....6

2.6 Comunicación en red..... 6

2.6.1 Configuración de IP..... 6

2.6.2 Registro Activo..... 7

2.6.3 Configuración de Wi-Fi.....8

2.6.4 Configuración del puerto serie 9

2.6.5 Configuración de Wiegand..... 9

2.7 Gestión de usuarios..... 10

2.7.1 Agregar usuarios.....10

2.7.2 Visualización de la información del usuario.....12

2.7.3 Configuración de la contraseña del administrador.....13

2.8 Gestión de acceso..... 14

2.8.1 Configuración de combinaciones de desbloqueo..... 14

2.8.2 Configuración de alarmas..... 15

2.8.3 Configuración del estado de la puerta..... 17

2.8.4 Configuración del tiempo de retención de bloqueo..... 17

2.9 Sistema..... 17

2.9.1 Configuración de la hora.....17

2.9.2 Configuración de parámetros faciales..... 19

2.9.3 Ajuste del volumen..... 21

2.9.4 (Opcional) Configuración de parámetros de huellas dactilares..... 21

2.9.5 Configuración de pantalla..... 21

2.9.6 Restauración de valores predeterminados de fábrica..... 21

2.9.7 Reiniciar el dispositivo..... 21

2.10 Gestión USB..... 21

2.10.1 Exportación a USB..... 22

2.10.2 Importación desde USB..... 22
2.10.3 Actualización del sistema..... 23
2.11 Configuración de funciones.....23
2.12 Desbloqueo de la puerta..... 25
2.12.1 Desbloqueo con Tarjetas..... 25
2.12.2 Desbloqueo por reconocimiento facial..... 25
2.12.3 Desbloqueo por contraseña de usuario..... 26
2.12.4 Desbloqueo mediante contraseña de administrador.....26
2.12.5 Desbloqueo mediante código QR..... 26
2.12.6 Desbloqueo por huella dactilar..... 26
2.13 Información del sistema..... 26
2.13.1 Visualización de la capacidad de datos.....27
2.13.2 Visualización de la versión del dispositivo..... 27
3 Operaciones web..... 28
3.1 Inicialización..... 28
3.2 Inicio de sesión.....28
3.3 Restablecimiento de la contraseña.....29
3.4 Configuración de parámetros de la puerta.....30
3.5 Configuración de la vinculación de alarmas.....33
3.5.1 Configuración de la vinculación de alarmas..... 33
3.5.2 Visualización de registros de alarmas..... 35
3.6 Configuración del intercomunicador.....35
3.6.1 Configuración del servidor SIP..... 35
3.6.2 Configuración de parámetros básicos..... 39
3.6.3 Adición del VTO..... 41
3.6.4 Adición del VTH..... 42
3.6.5 Adición del VTS..... 44
3.6.6 Visualización del estado del dispositivo.....44
3.6.7 Visualización de registros de llamadas..... 44
3.7 Personalización..... 45
3.7.1 Agregar recursos.....45
3.7.2 Configuración de temas.....46
3.8 Configuración de horarios..... 49
3.8.1 Configuración de secciones de tiempo.....49
3.8.2 Configuración de grupos de vacaciones.....50
3.8.3 Configuración de planes de vacaciones.....51
3.9 Capacidad de datos..... 52
3.10 Configuración de vídeo e imagen.....52
3.10.1 Configuración de vídeos..... 52
3.10.2 Ajuste del volumen..... 59

3.10.3 Configuración de la codificación local..... 59
3.10.4 Configuración del modo de imagen.....59
3.11 Configuración de la detección de rostros..... 60
3.12 Configuración de la red.....62
3.12.1 Configuración de TCP/IP.....62
3.12.2 Configuración de puertos..... 64
3.12.3 Configuración del registro automático..... 65
3.12.4 Configuración del servicio en la nube.....65
3.12.5 Configuración del puerto serie..... 66
3.12.6 Configuración de Wiegand.....67
3.13 Gestión de la seguridad..... 68
3.13.1 Configuración de la autoridad IP..... 68
3.13.2 Configuración del sistema.....71
3.14 Gestión de usuarios..... 77
3.14.1 Agregar usuarios..... 77
3.14.2 Cómo agregar usuarios ONVIF.....78
3.14.3 Visualización de usuarios en línea..... 80
3.15 Mantenimiento..... 80
3.16 Gestión de la configuración..... 80
3.16.1 Exportación/importación de archivos de configuración..... 80
3.16.2 Restauración de valores predeterminados de fábrica.....81
3.17 Actualización del sistema.....81
3.17.1 Actualización de archivos.....82
3.17.2 Actualización en línea..... 82
3.18 Visualización de la información de la versión..... 82
3.19 Visualización de registros..... 82
3.19.1 Registros del sistema..... 82
3.19.2 Registros de administración..... 83
3.19.3 Desbloqueo de registros..... 83
4 Configuración de Smart PSS Lite..... 84
4.1 Instalación e inicio de sesión..... 84
4.2 Agregar dispositivos..... 84
4.2.1 Agregar dispositivos uno por uno.....84
4.2.2 Agregar dispositivos en lotes..... 85
4.3 Gestión de usuarios..... 87
4.3.1 Configuración del tipo de tarjeta..... 87
4.3.2 Agregar usuarios.....87
4.3.3 Asignación de permisos de acceso.....92
4.4 Gestión de acceso..... 93
4.4.1 Apertura y cierre remoto de la puerta..... 93

4.4.2 Configuración de Siempre abierto y Siempre cerrado.....94
4.4.3 Monitoreo del estado de la puerta..... 94
Apéndice 1 Puntos importantes del funcionamiento del intercomunicador.....96
Apéndice 2 Puntos importantes del escaneo de códigos QR..... 97
Apéndice 3 Puntos importantes de las instrucciones para el registro de huellas dactilares.....98
Apéndice 4 Puntos importantes del registro facial.....100
Apéndice 5 Recomendación de seguridad..... 103

1 Descripción general

1.1 Introducción

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

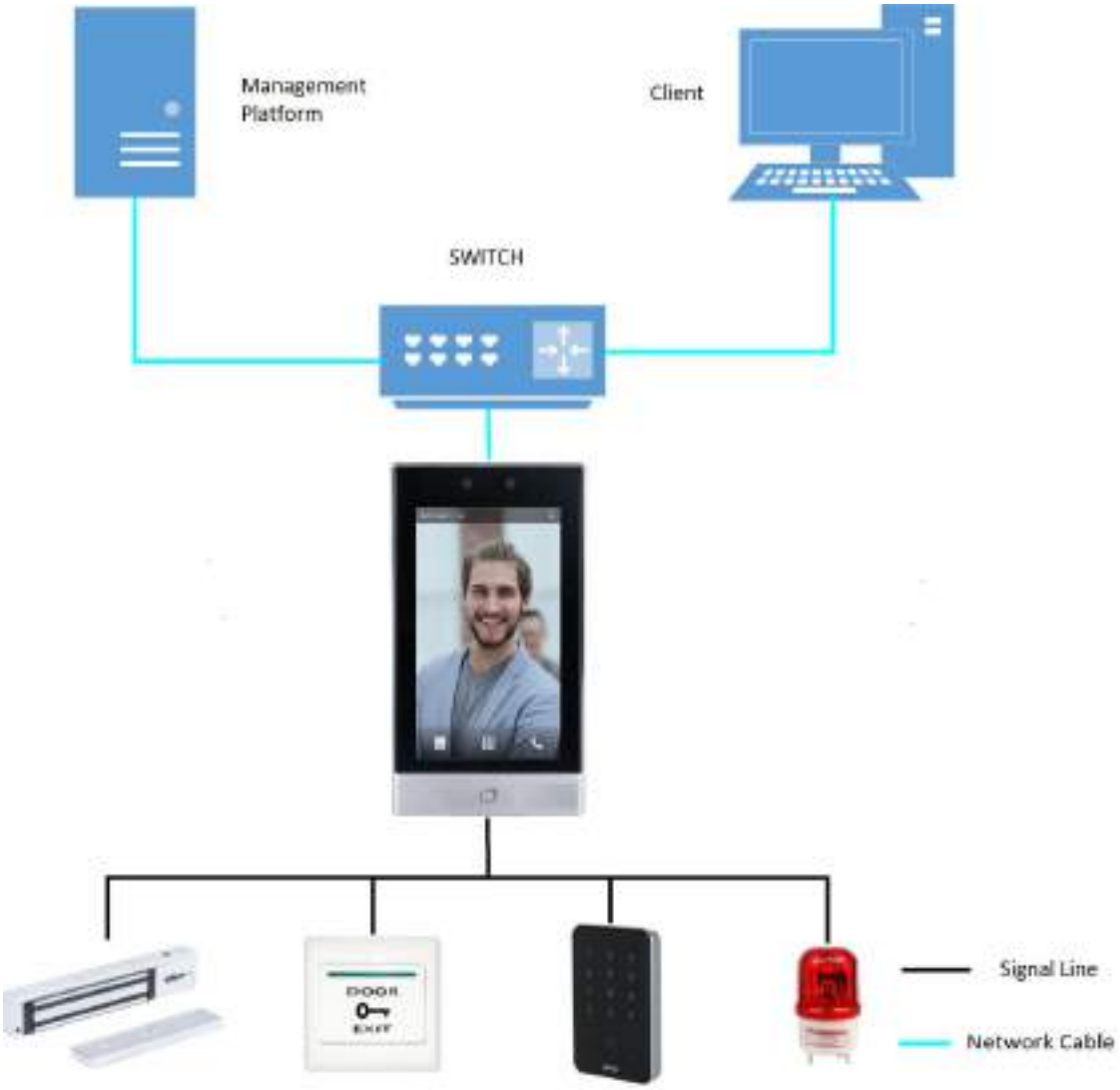
1.2 Características

- LCD de 7" con una resolución de 1024 × 600.
- La cámara CMOS de doble lente de 2 MP y el sensor de imagen de alto rendimiento garantizan un reconocimiento preciso incluso en condiciones de poca luz y en lugares oscuros que carecen de iluminación.
- Cuenta con iluminación automática para reducir eficazmente la contaminación lumínica.
- Admite 50.000 usuarios (hasta 50 administradores), 50.000 caras, 50.000 contraseñas, 100.000 tarjetas, 10.000 huellas dactilares y 300.000 registros.
- Múltiples métodos de desbloqueo, incluidos reconocimiento facial, tarjeta IC, contraseña, huella digital y código QR. También puedes combinarlos para crear tus propios métodos de desbloqueo personales.
- Muestra el cuadro delimitador de rostros y detecta el rostro que ocupa la mayor cantidad de píxeles en tiempo real. También puede configurar el filtrado de rostros objetivo configurando el umbral de píxeles del rostro.
- Reconoce rostros a una distancia de 0,3 m a 2,0 m (0,98 pies a 6,56 pies) y detecta personas entre una altura de 0,9 m y 2,4 m (2,95 pies a 7,87 pies) cuando la cámara está instalada a 1,4 m del suelo.
- Gracias al algoritmo de aprendizaje profundo de reconocimiento facial, el dispositivo puede localizar con precisión más de 360 puntos clave en el rostro de un objetivo.
- Los rostros pueden reconocerse en 0,2 segundos, sin necesidad de que la persona toque el dispositivo.
- Cuenta con detección de mascarilla y detección de casco de seguridad.
- Hay disponibles múltiples modos de visualización y avisos de voz para transmitir los resultados del reconocimiento para proteger la privacidad de los usuarios.
- La detección de vida se utiliza para detectar intentos de suplantación de identidad, como usar una foto o un vídeo para obtener acceso.
- Ofrece múltiples tipos de alarmas, como coacción, manipulación, intrusión, tiempo de espera de desbloqueo y uso excesivo de tarjetas y contraseñas ilegales.
- Admite diferentes tipos de usuarios, incluidos general, patrulla, lista de bloqueo, VIP, invitado y otros.
- Admite realizar videollamadas con monitores interiores, VTS y aplicaciones móviles.
- Conexión TCP/IP y Wi-Fi, registro automático, registro P2P y DHCP.
- Apoya el embellecimiento del rostro.
- Reconoce hasta 6 caras al mismo tiempo.
- Reproduce anuncios en formato de vídeo e imagen.
- Actualización en línea y actualización a través de USB.
- Se conecta a DSS Pro y SmartPSS Lite.

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.

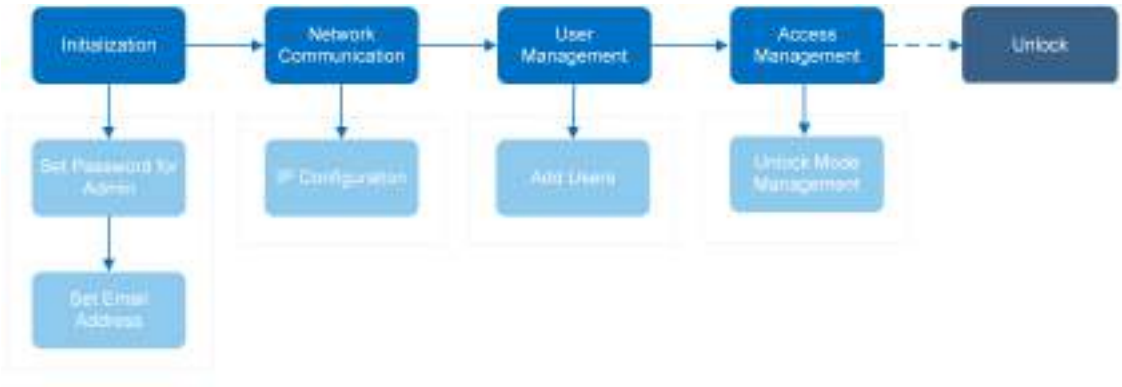
Figura 1-1 Redes



2 Operaciones locales

2.1 Procedimiento de configuración básica

Figura 2-1 Procedimiento de configuración básica



2.2 Iconos comunes

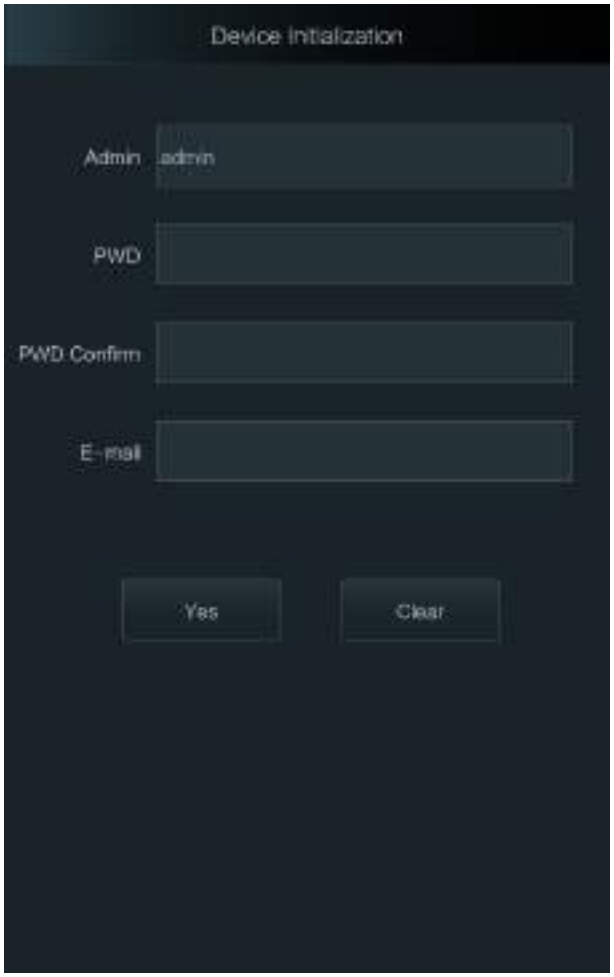
Tabla 2-1 Descripción de los iconos

Icono	Descripción
	Confirmar.
	Pase a la primera página de la lista.
	Pase a la última página de la lista.
	Pase a la página anterior de la lista.
	Pase a la siguiente página de la lista.
	Regresar al menú anterior.
	Encender.
	Apagar.
	Borrar
	Pantalla de inicio
	Buscar

2.3 Inicialización

Para el primer uso o después de restaurar los valores predeterminados de fábrica, debe configurar una contraseña y una dirección de correo electrónico para la cuenta de administrador. Puede usar la cuenta de administrador para iniciar sesión en el menú principal del controlador de acceso y en la página web.

Figura 2-2 Inicialización



- 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: mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &).

2.4 Pantalla de espera

Puedes desbloquear la puerta mediante reconocimiento facial, contraseñas y código QR. También puedes hacer llamadas a través de la función de 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 existan ligeras diferencias entre la pantalla de espera que aparece en este manual y el dispositivo real.

Figura 2-3 Página de inicio



Tabla 2-2 Descripción de la pantalla de inicio

No.	Nombre	Descripción
1	Fecha y hora	Fecha y hora actual.
2	Área de deslizamiento de tarjetas	Pase la tarjeta por esta área.
3	Contraseña	Introduzca la contraseña de usuario o la contraseña pública para desbloquear la puerta.
4	Código QR	Toque el ícono del código QR y escanee el código QR para desbloquear la puerta. El ícono del código QR no está disponible para el modelo de huella digital del controlador de acceso.
5	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 a VTO, VTS y DSS. Toque el ícono e ingrese el número de la habitación para llamar al propietario de la casa.
6	Visualización de estado	Muestra el estado de Wi-Fi, red y USB.

2.5 Iniciar sesión

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

Información de contexto

- 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 y luego deslice el dedo hacia la izquierda o hacia la

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

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

2.6.1 Configuración de IP

Establezca la dirección IP del controlador de acceso para conectarlo a la red. Luego, 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 2-4 Configuración de la dirección IP

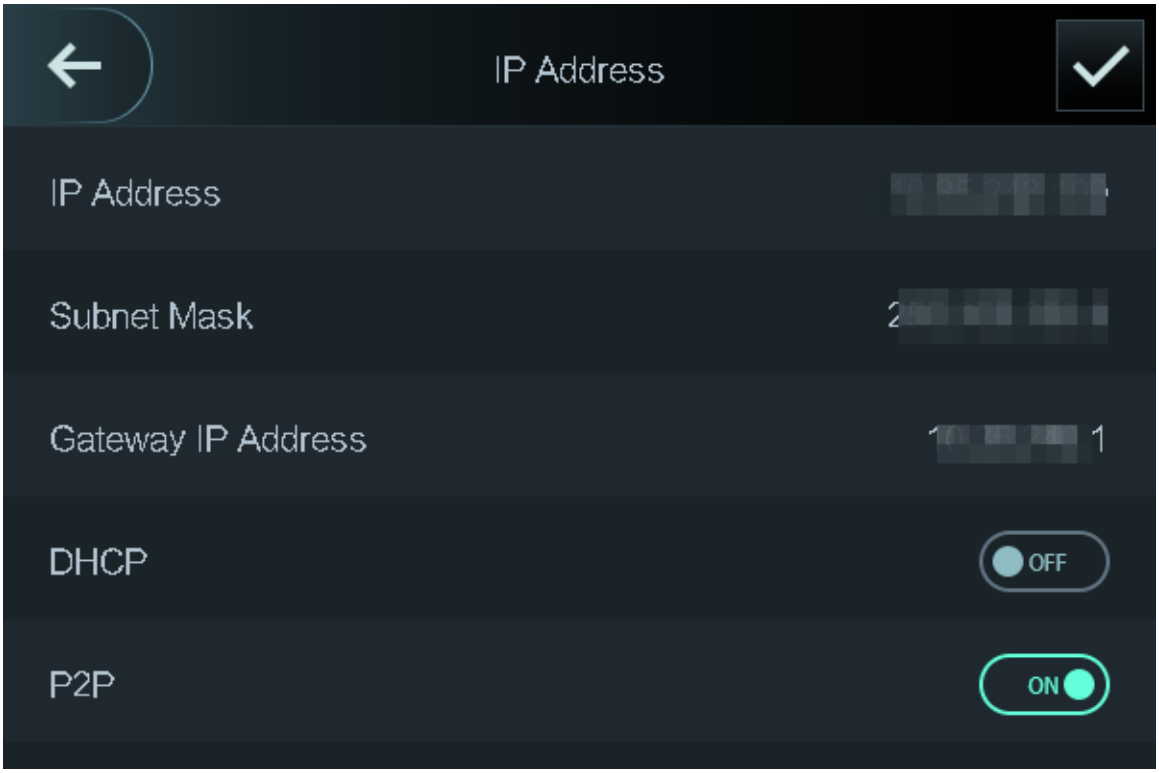


Tabla 2-3 Parámetros de configuración de IP

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 el mapeo de puertos o implementar un servidor de tránsito.

2.6.2 Registro Activo

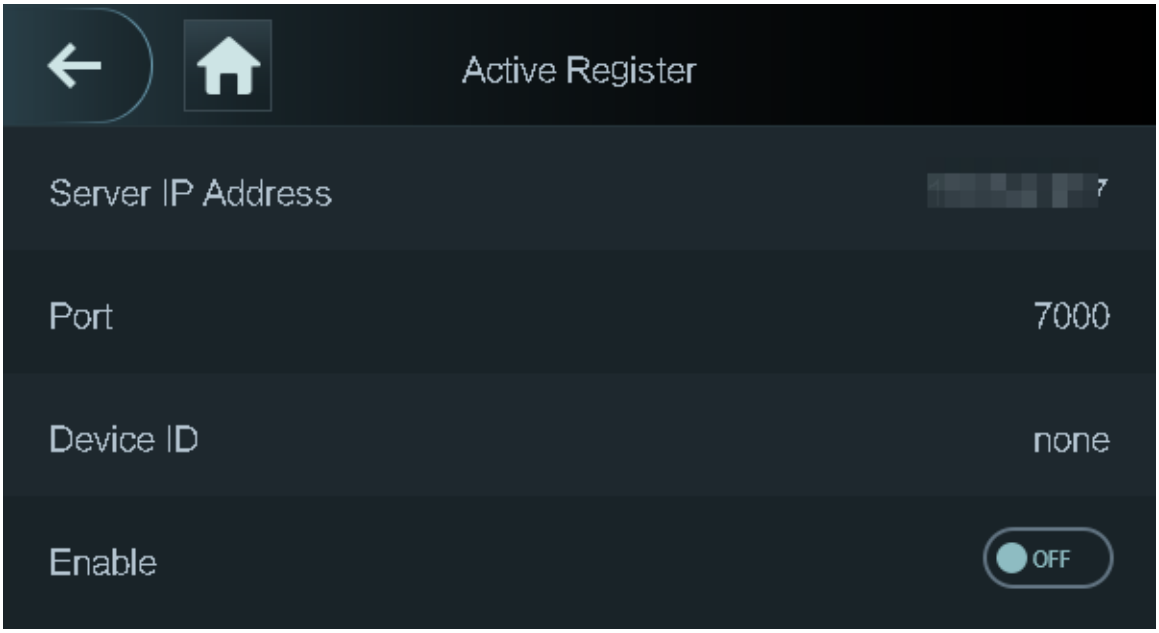
Puede activar la función de registro automático para acceder al Controlador de Acceso a través de la plataforma de gestión.

Procedimiento

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

La plataforma de administración puede borrar todas las configuraciones de personal e inicializar el controlador de acceso. Para evitar la pérdida de datos, mantenga los permisos de la plataforma de administración correctamente.

Figura 2-5 Registro automático



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

Tabla 2-4 Registro automático

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

Paso 3 Habilitar la función de registro activo.

2.6.3 Configuración de Wi-Fi

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

Procedimiento

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

La función Wi-Fi solo está disponible para ciertos modelos del controlador de acceso.

Paso 2 Encienda el Wi-Fi.

Paso 3 Toque 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 introducir el nombre de la red Wi-Fi, pul

Paso 5

2.6.4 Configuración del puerto serie

Procedimiento

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

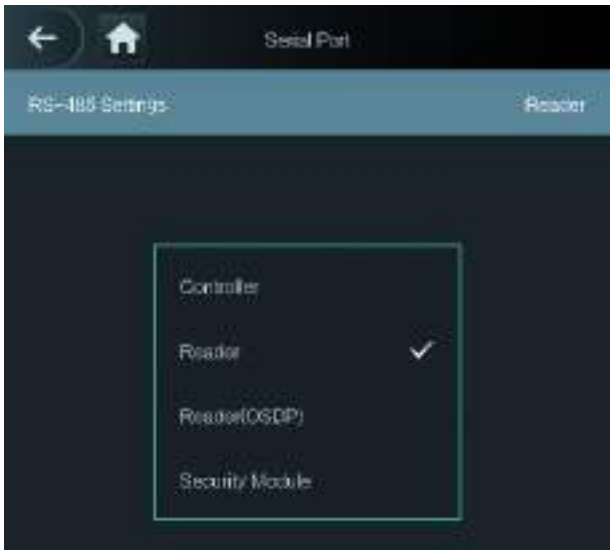
Paso 2 un tipo de puerto.

- 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 enviará datos a otro controlador de acceso externo.

  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 en función del 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, el bloqueo y la conexión de la alarma contra incendios no serán efectivos.

Figura 2-6 Puerto serie



2.6.5 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 otro terminal de acceso.

Figura 2-7 Salida Wiegand



Tabla 2-5 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. ● **Tarjeta Nro.**:Genera datos basados en el primer número de tarjeta del usuario.

2.7 Gestión de usuarios

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

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

2.7.1 Agregar usuarios

Procedimiento

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

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

Figura 2-8 Nuevo usuario



Tabla 2-6 Descripción de los nuevos parámetros de usuario

Parámetro	Descripción
ID de usuario	Introduzca los identificadores de usuario. Los identificadores pueden ser números, letras y combinaciones de estos, y la longitud máxima del identificador es de 32 caracteres. Cada identificador es único.
Nombre	Ingrese un nombre con un máximo de 32 caracteres (incluidos números, símbolos y letras).
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.
Huella dactilar	Cada usuario puede registrar hasta 3 huellas dactilares. Siga las instrucciones en pantalla para registrar las huellas dactilares. Puede configurar la huella dactilar registrada como huella dactilar de coacción y se activará una alarma si la puerta se desbloquea con la huella dactilar de coacción. ● No recomendamos que configure la primera huella digital como huella digital de coacción. ● La función de huella dactilar solo está disponible en modelos seleccionados.

Parámetro	Descripción
Tarjeta	Un usuario puede registrar cinco tarjetas como máximo. Ingrese el número de su tarjeta o deslícela y luego el controlador de acceso leerá la información de la tarjeta. Puedes habilitar el**Tarjeta de coacción**Función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta.  Sólo algunos modelos admiten el desbloqueo de tarjeta.
Personas con discapacidad	Introduzca la contraseña de usuario. La longitud máxima de la contraseña es de 8 dígitos.
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 de la lista de bloqueo desbloqueen la puerta, el personal de servicio recibirá una notificación. ● **Invitado**:Los huéspedes pueden desbloquear la puerta dentro de un período definido o durante un tiempo determinado. Una vez que el período definido o el tiempo de desbloqueo se agoten, 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.

Paso 3 Toqu para guardar la configuración.

2.7.2 Visualización de la información del usuario

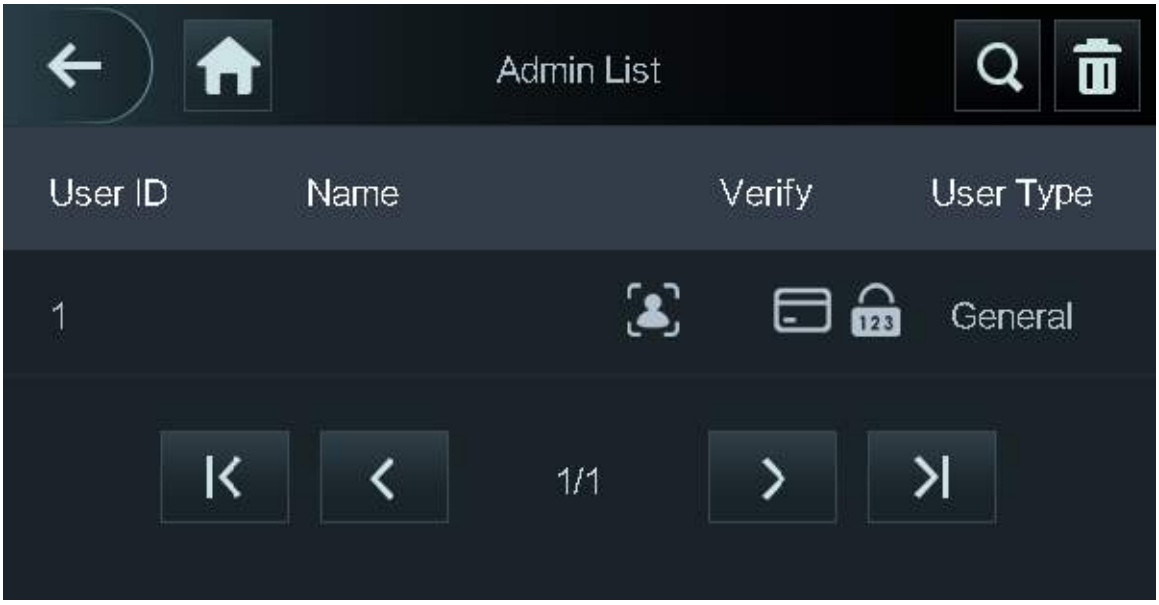
Puede ver la lista de usuarios/administradores y editar la información del usuario.

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.

Figura 2-9 Lista de administradores



- : 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 la información del usuario.
- Eliminar usuarios
  - ◇ Eliminar de forma individual: seleccione un usuario y, a continuación, .
  - ◇ toque . Eliminar en 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.

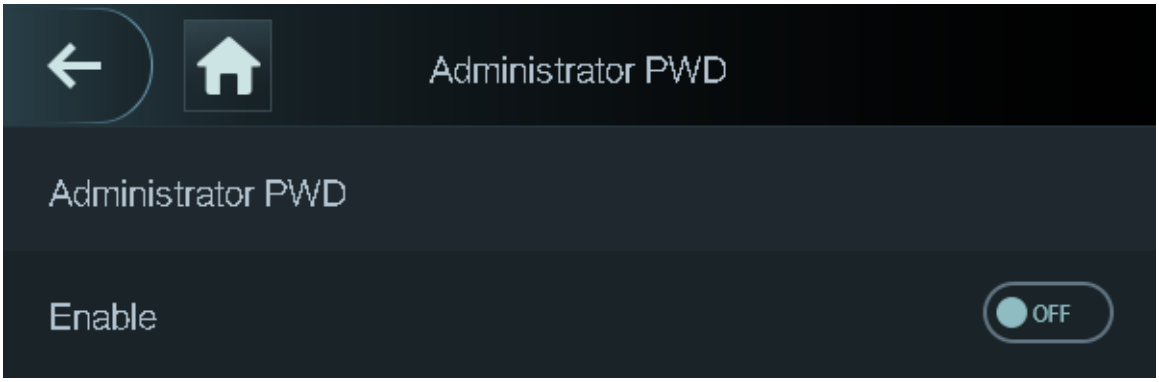
2.7.3 Configuración de la contraseña del administrador

Puede desbloquear la puerta ingresando únicamente la contraseña de administrador. La contraseña de administrador no está limitada por el 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 2-10 Establecer contraseña de administrador



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

Paso 3 Grif

Paso 4 Activar la función de administrador.

2.8 Gestión de acceso

Puede configurar los parámetros de acceso a la puerta, como los modos de desbloqueo, la conexión de alarmas y los horarios de las puertas. Los modos de desbloqueo pueden variar según el producto real.

2.8.1 Configuración de combinaciones de desbloqueo

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

Información de contexto

La función de huella dactilar solo está disponible en modelos seleccionados.

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 2-11 Elemento (opción múltiple)



Paso 4 Toque para guardar los cambios.

2.8.2 Configuración de alarmas

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

Procedimiento

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

Paso 2 Habilitar el tipo de alarma.

Figura 2-12 Alarma

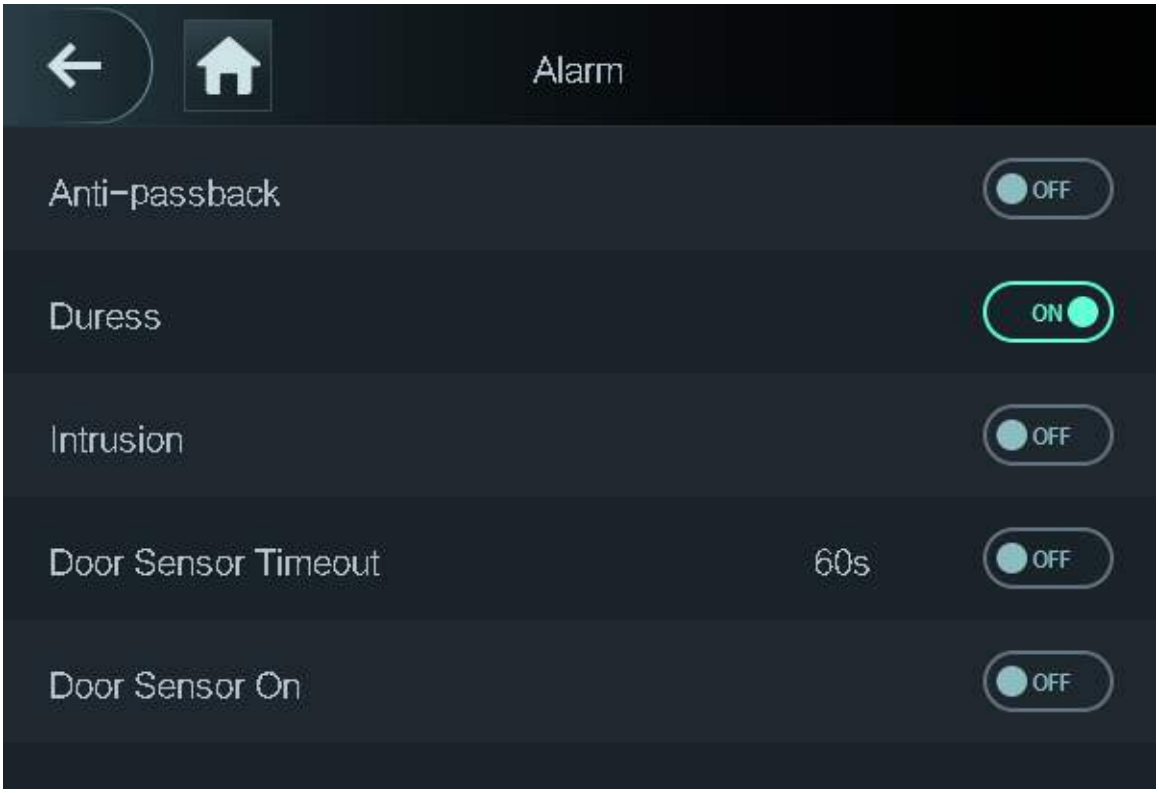


Tabla 2-7 Descripción de los parámetros de alarma

Parámetro	Descripción
Anti-passback	Los usuarios deben verificar su identidad tanto para entrar como para salir; de lo contrario, se activará una alarma. Esto ayuda a evitar que el titular de una tarjeta le pase la tarjeta de acceso a otra persona para que pueda entrar. Cuando se activa la función antirretorno, el titular de la tarjeta debe abandonar el área protegida a través de un lector de salida antes de que el sistema le permita entrar nuevamente. ● Si una persona ingresa después de la 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 entra sin autorización y sale después de la autorización, se activará una alarma cuando intente entrar 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 forma 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.

Parámetro	Descripción
Sensor de puerta activado	Las alarmas de intrusión y de 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 del bloqueo.**

Paso 2 Introduzca la duración del desbloqueo.

Paso 3 Toque para guardar los cambios.

2.9 Sistema

2.9.1 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 2-13 Tiempo

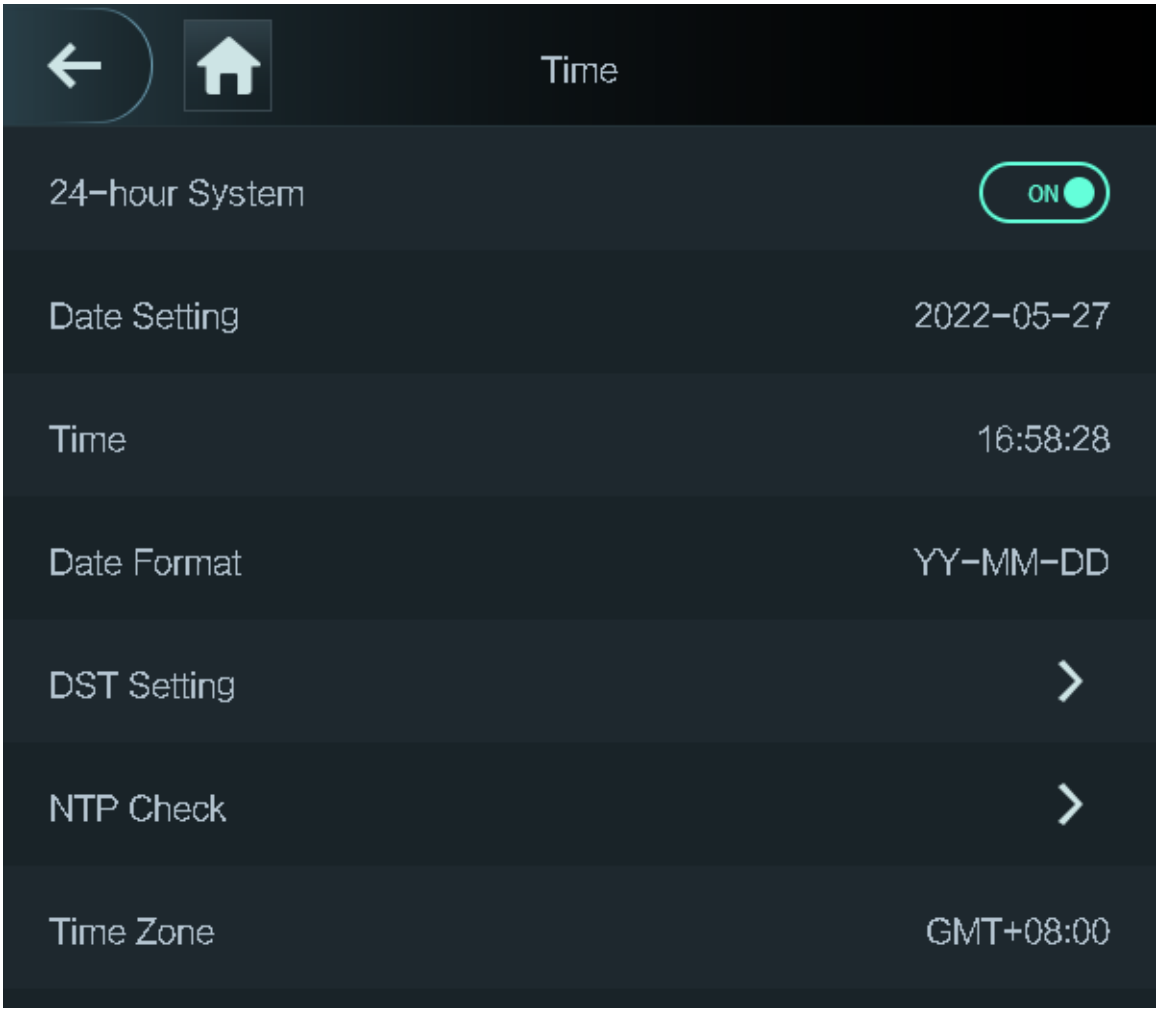


Tabla 2-8 Descripción de los parámetros de tiempo

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.
Configuración del horario de verano	1. Toque**Configuración del horario de verano** 2. Habilite 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. Toqu

Parámetro	Descripción
Comprobación NTP	Un servidor de protocolo de hora de red (NTP) es una máquina dedicada a funcionar como servidor de sincronización horaria para 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 cambia 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**:Introduzca el puerto del servidor NTP. ● **Intervalo (min)**:Introduzca el intervalo de sincronización horaria.
Huso horario	Seleccione la zona horaria.

2.9.2 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 2-14 Parámetros de rostro

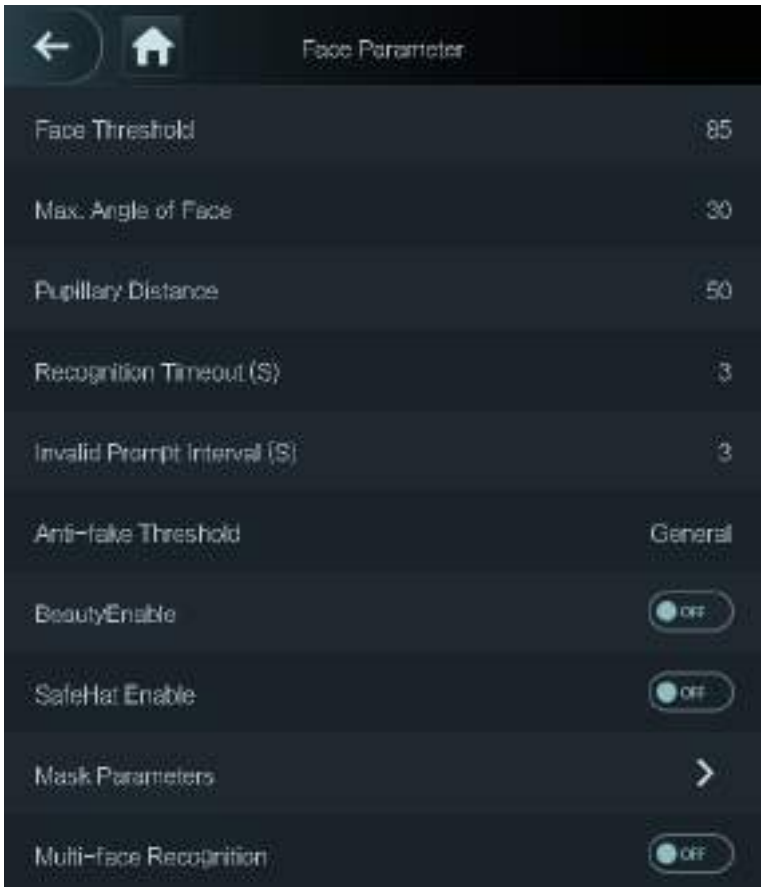


Tabla 2-9 Descripción de los parámetros faciales

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 del rostro para la detección de rostros. Un valor mayor significa un rango de ángulos del rostro más amplio. Si el ángulo de pose del rostro está fuera del rango definido, no aparecerá el cuadro de detección de rostros.
Distancia pupilar	Las imágenes de rostros requieren los píxeles deseados entre los ojos (llamada distancia pupilar) para un reconocimiento exitoso. El píxel predeterminado es 45. El píxel cambia según el tamaño del rostro y la distancia entre los rostros y la lente. Si un adulto está a 1,5 metros de la lente, la distancia pupilar puede ser de 50 px a 70 px.
Tiempo de espera de reconocimiento (S)	Si se reconoce correctamente el rostro de una persona con permiso de acceso, el controlador de acceso indicará que el reconocimiento facial se ha realizado correctamente. Puede introducir el intervalo de tiempo para indicarlo.
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 que se ha producido un error en el reconocimiento facial. Puede introducir el intervalo de tiempo indicado.
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 Habilitar	Embellece las imágenes de rostros capturadas.
Habilitar SafeHat	Detecta si las personas usan cascos seguros.
Parámetros de la máscara	● Modo máscara: ◇ **Sin detección**:No se detecta la máscara durante el reconocimiento facial. ◇ **Recordatorio de uso de mascarilla**:Se detecta la mascarilla durante el reconocimiento facial. Si la persona no lleva mascarilla, el sistema le recordará que debe usarla y se le permitirá el acceso. ◇ **Intercepción de máscara**:Se detecta la mascarilla durante el reconocimiento facial. Si una persona no lleva mascarilla, el sistema le recordará que debe usarla y le negará el acceso. ● Umbral de reconocimiento de máscara: un umbral más alto significa una mayor precisión en la detección de máscara.
Reconocimiento de múltiples caras	Admite la detección de 6 imágenes de rostros al mismo tiempo y el modo de combinación de desbloqueo deja de ser válido. La puerta se desbloquea después de que cualquiera de ellos acceda.

2.9.3 Ajuste del volumen

Procedimiento

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

Paso 2 **Volumen del pitido**o**Volumen del micrófono**.

Paso 3 Toque o para ajustar el volumen.

2.9.4 (Opcional) Configuración de parámetros de huellas dactilares

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

Información de contexto

La función de huella dactilar solo está disponible en modelos seleccionados.

Procedimiento

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

Paso 2 **dactilar**Toque o para ajustar el valor.

2.9.5 Configuración de pantalla

Configure 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 apagado de pantalla**y luego toque o para ajustar la hora.

2.9.6 Restauración de los valores predeterminados de fábrica

Procedimiento

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

Paso 2 valores predeterminados de fábrica si es necesario.

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

2.9.7 Reiniciar el dispositivo

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

2.10 Gestión USB

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

- Asegúrese de que haya un USB insertado en el controlador de acceso antes de exportar datos o actualizar el sistema. Para evitar fallas, no extraiga el USB ni realice ninguna operación en el controlador de acceso durante el proceso.
- Para exportar la información de un controlador de acceso a otros dispositivos, es necesario utilizar un dispositivo USB. No se permite importar imágenes de rostros a través de USB.

2.10.1 Exportación a USB

Puede exportar datos desde el controlador de acceso a un dispositivo 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**.

Figura 2-15 Exportación USB



2.10.2 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**.

Figura 2-16 Importación USB



2.10.3 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.

2.11 Configuración de funciones

En el**Menú principal**interfaz, seleccionar**Características**>**Configuración de privacidad**.

Figura 2-17 Configuración de privacidad

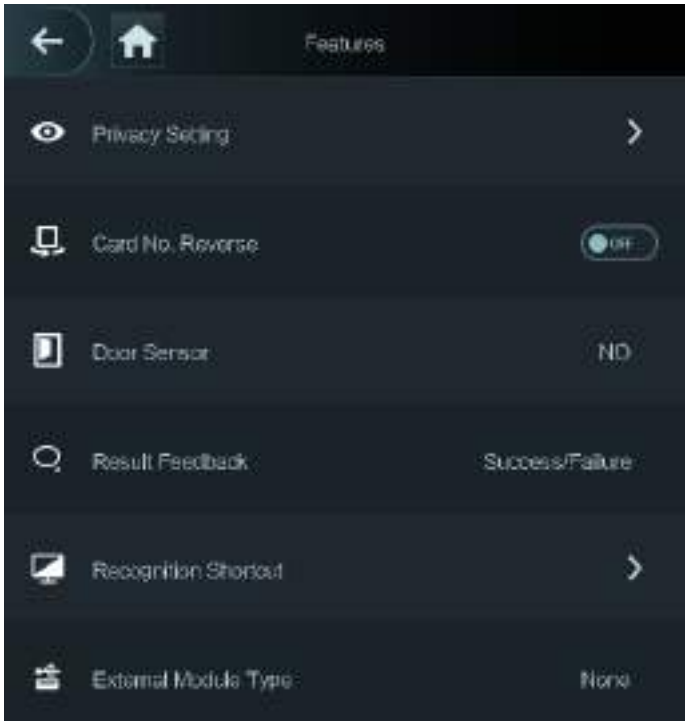


Tabla 2-10 Descripción de características

Parámetro	Descripción
Configuración privada	● Habilitar restablecimiento de contraseña: puede habilitar esta función para restablecer la contraseña. La función Restablecimiento de contraseña está habilitada de manera predeterminada. ● HTTPS: El Protocolo seguro de transferencia de hipertexto (HTTPS) es un protocolo para la comunicación segura a través de una red de computadoras. 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 de rostros automáticamente cuando las personas abran la puerta. La función está habilitada de manera predeterminada.

Parámetro	Descripción
Tarjeta N° Reverso	Cuando el terminal 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 el**Tarjeta N° 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.
Atajo de reconocimiento	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 ícono del método de desbloqueo del código QR se muestra en la pantalla de espera. ● Llamada: El icono de la función de llamada se muestra en la pantalla de espera. ● Tipo de llamada: ◇ Sala de llamadas: toque el ícono de llamada en el modo de espera e ingrese el número de la habitación para realizar llamadas. ◇ Centro de administración de llamadas: toque el ícono de llamada en el modo de espera y luego llame al centro de administración. ◇ Sala de llamadas personalizada: toque el ícono de llamada para llamar al número de sala definido. Primero debe definir el número de sala en la **Atajo de reconocimiento**pantalla.

2.12 Desbloqueo de la puerta

Puedes desbloquear la puerta mediante reconocimiento facial, contraseñas, tarjetas y más. Los métodos de desbloqueo predeterminados son tarjeta/rostro/contraseña.

2.12.1 Desbloqueo por tarjetas

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

2.12.2 Desbloqueo por reconocimiento facial

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

2.12.3 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 contraseña**, y luego ingrese el ID de usuario y la contraseña.

Paso 3 Toque**Sí**.

2.12.4 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 y anti-passback, excepto para puertas normalmente cerradas. Un dispositivo solo permite una contraseña de administrador.

Prerrequisitos

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

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

Paso 3 Grif

2.12.5 Desbloqueo mediante código QR

Procedimiento

Paso 1 En la pantalla de espera, toca Coloca el

Paso 2 código QR frente a la lente.

También puedes colocar el código QR frente a la lente directamente sin tocarlo. .

2.12.6 Desbloqueo por huella dactilar

Coloque el dedo sobre el escáner de huellas dactilares. Esta función solo está disponible en algunos modelos.

2.13 Información del sistema

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

2.13.1 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.

2.13.2 Visualización de la versión del dispositivo

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.

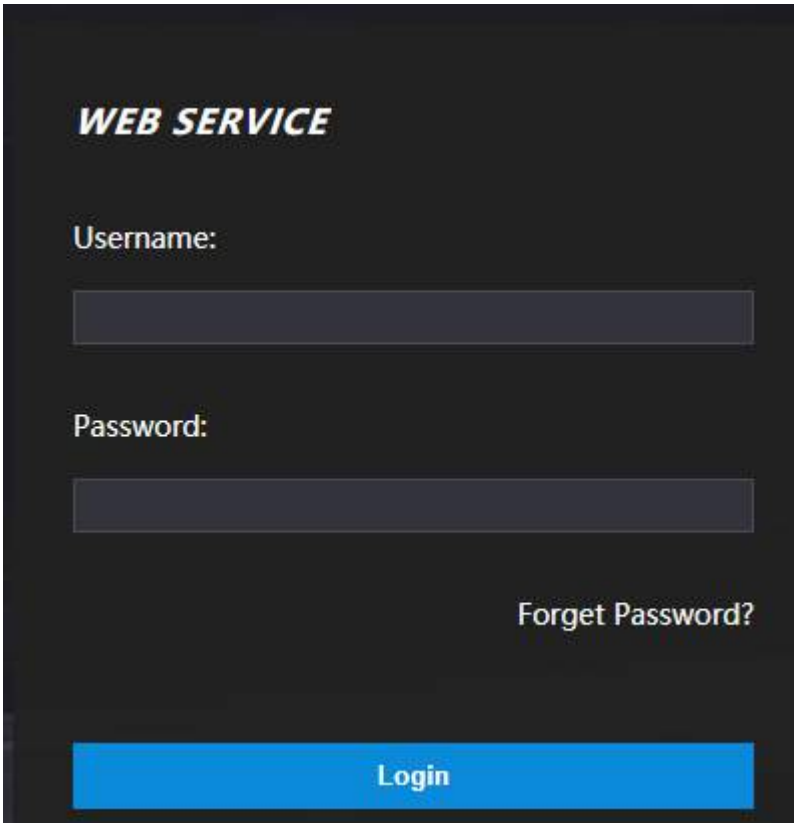
- La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excepto ' " ; : &). Establezca una contraseña de alta seguridad siguiendo las indicaciones de seguridad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

3.2 Iniciar 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 configuraste durante la inicialización. Te recomendamos cambiar la contraseña de administrador con regularidad para aumentar la seguridad.
- Si olvida la contraseña de inicio de sesión del administrador, puede hacer clic en**¿Olvidaste tu contraseña?**Para obtener 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 código de seguridad deja de ser válido, actualice el código QR y escanéelo nuevamente.
- Después de escanear el código QR, recibirá un código de seguridad en la dirección de correo electrónico vinculada. Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, perderá su validez.
- 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 en**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 los 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 Parámetros de la puerta

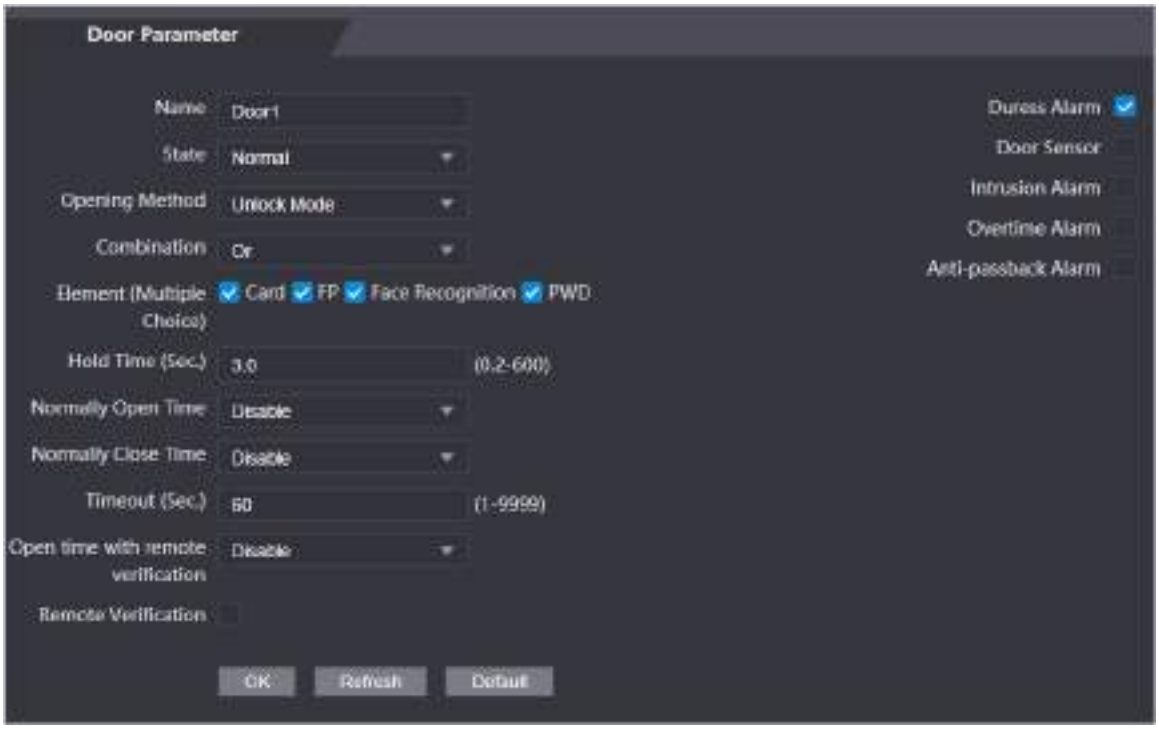


Tabla 3-1 Descripción de los parámetros de la puerta

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 grupos: 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.)	Una vez que se le concede el acceso a una persona, la puerta permanecerá desbloqueada durante un tiempo definido para que pueda pasar. Varía entre 0,2 s y 600 s.
Hora normalmente abierta	La puerta permanece abierta o cerrada durante el período definido.
Hora normalmente cerrada	
Tiempo de espera (seg.)	Se activará una alarma de tiempo de espera si la puerta permanece desbloqueada durante un tiempo superior a este valor.
Abrir con verificación remota	Establezca el período de apertura de la puerta para verificación remota. Una vez que los usuarios obtienen acceso en el controlador de acceso, también se les debe otorgar acceso desde la plataforma de administración antes de que se desbloquee la puerta.

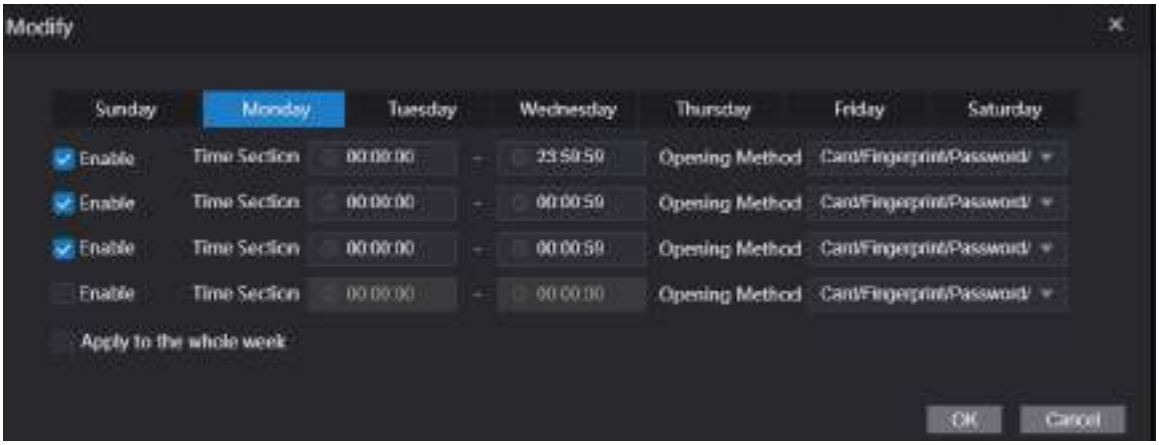
Parámetro	Descripción
Alarma de coacción	Se activará una alarma cuando se utilice una tarjeta de coacción o una contraseña de coacción para desbloquear la puerta.
Sensor de puerta	Las alarmas de intrusión y de horas extras se pueden activar solo después **Sensor de puerta**está habilitado.
Alarma de intrusión	Cuando**Sensor de puerta**está habilitado, se activará una alarma de intrusión si la puerta se abre de 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 para entrar como para salir; de lo contrario, se activará una alarma. Esto ayuda a evitar que el titular de una tarjeta le pase la tarjeta de acceso a otra persona para que pueda entrar. Cuando se activa la función antirretorno, el titular de la tarjeta debe abandonar el área protegida a través de un lector de salida antes de que el sistema le permita entrar nuevamente. ● Si una persona ingresa después de la 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 entra sin autorización y sale después de la autorización, se activará una alarma cuando intente entrar nuevamente y se le negará el acceso al mismo tiempo.

Paso 3 Configurar el método de apertura.

- Desbloqueo por periodo

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

Figura 3-4 Parámetro de la sección de tiempo



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

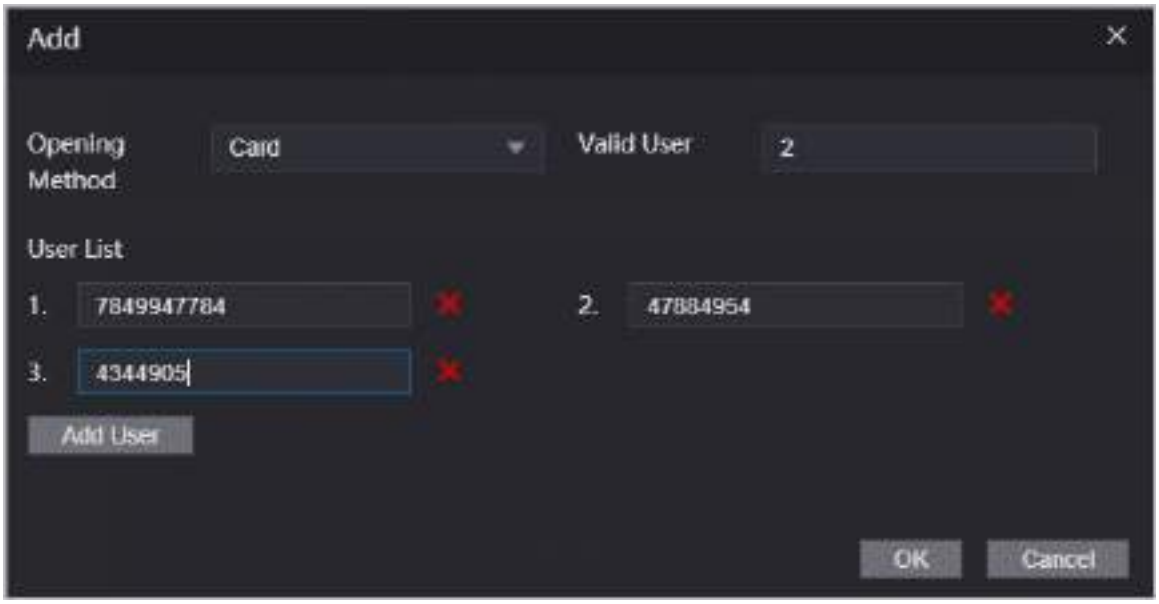
- Combinación de grupos

  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 la cantidad de usuarios válidos es 2 y hay 3 usuarios en la lista de usuarios definida, se requieren dos usuarios en la lista para otorgar acceso.

Figura 3-5 Combinación de grupos



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

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

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 de la vinculación de alarmas

3.5.1 Configuración de la vinculación de alarmas

Configure la vinculación de alarmas para activarlas cuando se produzcan eventos de acceso anormales. Las configuraciones en la página web se sincronizarán con las configuraciones en la plataforma de administración si se agrega el controlador de acceso a la plataforma.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Enlace de alarma**>**Enlace de alarma**.

Figura 3-6 Vinculación de alarma



Paso 3 Haga clic en y luego podrá modificar los parámetros de vinculación de alarma.

Figura 3-7 Modificar parámetros de vinculación de alarma

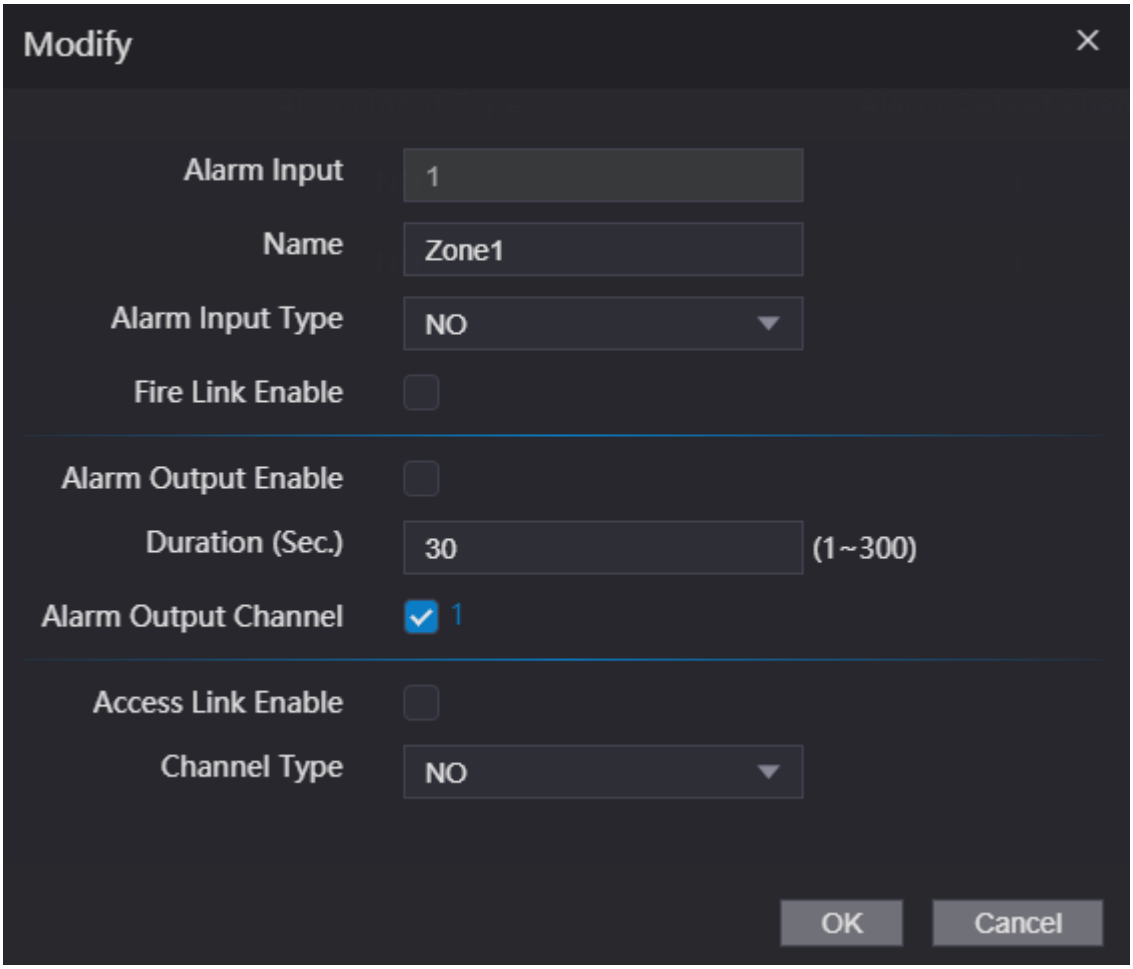


Tabla 3-2 Descripción de los parámetros de vinculación de alarmas

Parámetro	Descripción
Entrada de alarma	El número de la entrada de alarma que no se puede modificar.
Nombre	Introduzca el nombre de la alarma.
Tipo de entrada de alarma	Seleccione el tipo de entrada según el dispositivo de alarma. ● **NO**:El circuito del dispositivo de alarma normalmente está abierto y se cierra cuando se activa una alarma. ● **CAROLINA DEL NORTE**:El circuito del dispositivo de alarma normalmente está cerrado y se abre cuando se activa una alarma.

Parámetro	Descripción
Habilitar enlace de fuego	Si la vinculación contra incendios está habilitada, las alarmas contra incendios se activarán cuando ocurran eventos de incendio y las salidas de alarma y el acceso a las puertas se vincularán.  Si el enlace contra incendios está activado, la salida de alarma se activa de manera predeterminada y el acceso a la puerta estará normalmente abierto cuando ocurran eventos de incendio de manera predeterminada.
Habilitar salida de alarma	Si la salida de alarma está activada, el relé generará mensajes de alarma.
Duración (seg.)	Duración de la alarma. Varía entre 1 s y 300 s.
Canal de salida de alarma	Seleccione el canal de salida de alarma según su dispositivo de alarma.
Habilitar enlace de acceso	Una vez activado el enlace de control de acceso, la puerta estará normalmente abierta o normalmente cerrada cuando haya señales de alarma de entrada. ● NO: La puerta normalmente está abierta cuando hay señales de alarma de entrada. ● NC: La puerta normalmente está cerrada cuando hay señales de alarma de entrada.
Tipo de canal	

Paso 4 Hacer clic**DE ACUERDO**.

3.5.2 Visualización de registros de alarmas

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Enlace de alarma**>**Registro de alarmas**.

Paso 3 Seleccione un rango de tiempo y un tipo de alarma y luego haga clic en**Consulta**.

3.6 Configuración del intercomunicador

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

3.6.1 Configuración del servidor SIP

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

Información de contexto



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

Procedimiento

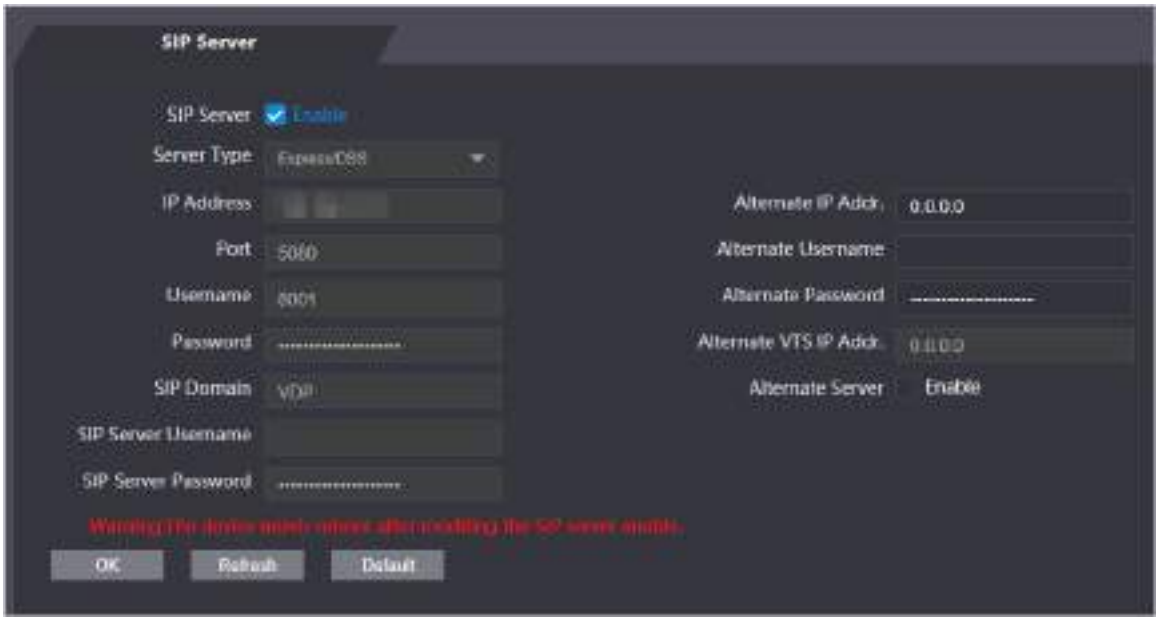
Paso 1 Seleccionar**Intercomunicador**>**Servidor SIP**.

Paso 2 Seleccione un tipo de servidor.

- Utilice el controlador de acceso como servidor SIP.

  Encender**Servidor SIP**y mantener los demás parámetros como predeterminados.

  Figura 3-8 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**DE ACUERDO**.

Figura 3-9 Utilice VTO como servidor SIP

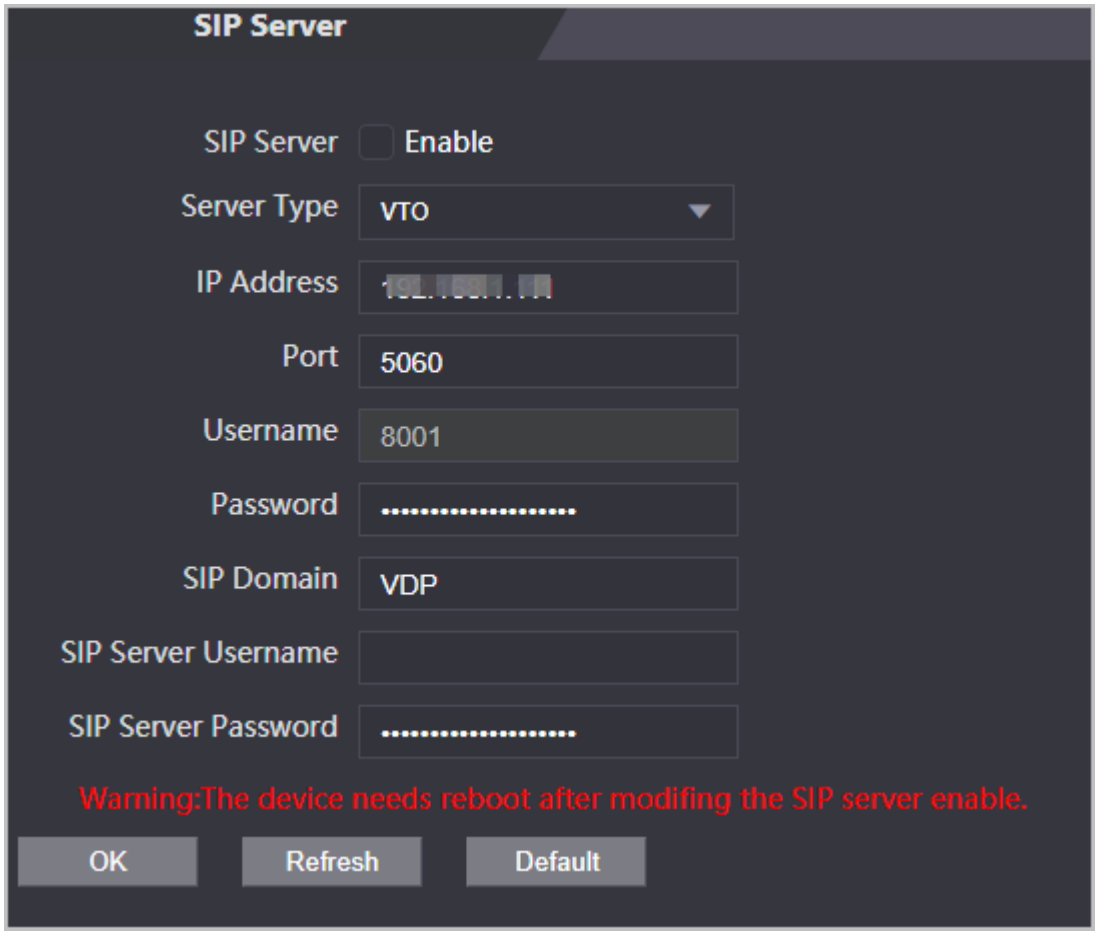


Tabla 3-3 Configuración del servidor SIP

Parámetro	Descripción
Dirección IP	Dirección IP de la plataforma.
Puerto	◇ 5060 por defecto cuando VTO funciona como servidor SIP. 5080 por ◇ defecto cuando la plataforma funciona como servidor SIP.
Nombre de usuario	Déjalos como predeterminados.
Contraseña	
Dominio SIP	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**Expresar/DSS**desde**Tipo de servidor**.

Figura 3-10 Utilice DSS Express o DSS Pro como servidor SIP

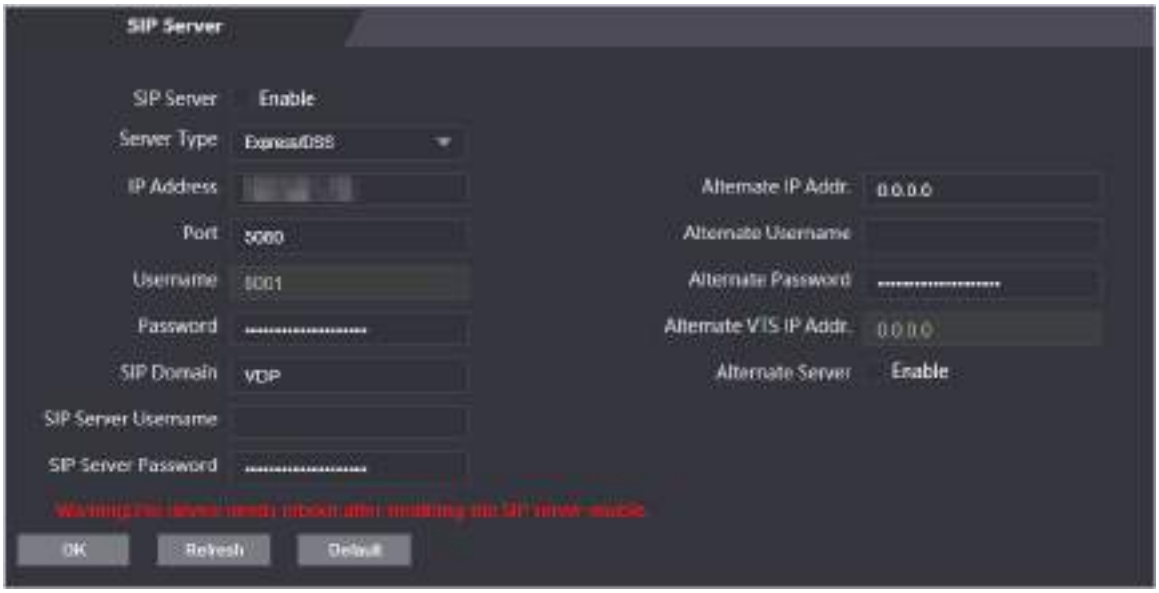


Tabla 3-4 Configuración del servidor SIP

Parámetro	Descripción
Dirección IP	Dirección IP de la plataforma.
Puerto	◇ 5060 de forma predeterminada cuando VTO funciona como servidor SIP. 5080 de forma ◇ predeterminada cuando la plataforma funciona como servidor SIP.
Nombre de usuario	Déjalos como predeterminados.
Contraseña	
Dominio SIP	Déjalo como predeterminado.
Nombre de usuario del servidor SIP	El nombre de usuario y la contraseña de inicio de sesión de la plataforma.
Contraseña del servidor SIP	
Dirección IP alternativa.	El servidor alternativo se utilizará como servidor SIP cuando DSS Express o DSS Pro no respondan. Le recomendamos que configure 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 ingresar la dirección IP, el nombre de usuario y la contraseña del VTO. No habilite **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. Cuando la plataforma de administración no responda, se activará el VTS alternativo para garantizar que VTO, VTH y VTS aún puedan realizar la función de intercomunicador de video.

Paso 3 Hacer clic**DE ACUERDO**.

3.6.2 Configuración de parámetros básicos

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

Procedimiento

Paso 1 Seleccionar**Hablar de nuevo**>

Paso 2 **Local**. Configure los parámetros.

- Utilice el controlador de acceso como servidor SIP.

Figura 3-11 Parámetro básico



Tabla 3-5 Descripción de parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccionar**Estación de puerta de la unidad**.
VTO N.º	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 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 3-12 Parámetro básico



Tabla 3-6 Descripción de parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccionar**Estación de puerta de la unidad**.
VTO N.º	El número del VTO. ◇ El número debe tener cuatro dígitos. Los dos primeros dígitos son 80 y los dos últimos dígitos empiezan por 01. Por ejemplo, 8001. ◇ Si existen varios VTO en una unidad, el número de VTO no se puede repetir.
Número de llamada del centro	El número de teléfono predeterminado para el centro de 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 3-13 Parámetro básico



Tabla 3-7 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 se encuentra la estación de puerta de la unidad. instalado.	Si el edificio y la unidad están habilitados en DSS, ingrese 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. Tomemos como ejemplo la habitación 1001, unidad 2 y el edificio 1. Si el número de edificio está habilitado en el Si el DSS y la unidad no están habilitados, el número de habitación es "1#1001". Si tanto el edificio como la unidad están habilitados, el número de habitación es "1#2#1001". Si el edificio no está habilitado y la unidad tampoco lo está, el número de habitación es "1001". Para obtener más información, consulte el manual del usuario del DSS.
Unidad No.	Seleccione la casilla de verificación y luego ingrese el número de la unidad donde está instalada la estación de puerta de la unidad.	
VTO N.º	El número de la estación de puerta de la unidad. Si existen varios VTO en una unidad, el número de VTO no se puede repetir.	
Número de llamada del centro	El número de teléfono predeterminado es 888888 cuando el VTO llama al VTS. Manténgalo como predeterminado.	

Parámetro	Descripción
Modo de transmisión	El modo 1 está seleccionado de forma predeterminada.

Paso 3 Hacer clic**Confirmar**.

3.6.3 Adición del VTO

Cuando el controlador de acceso funciona como servidor SIP y usted 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 3-14 Agregar VTO

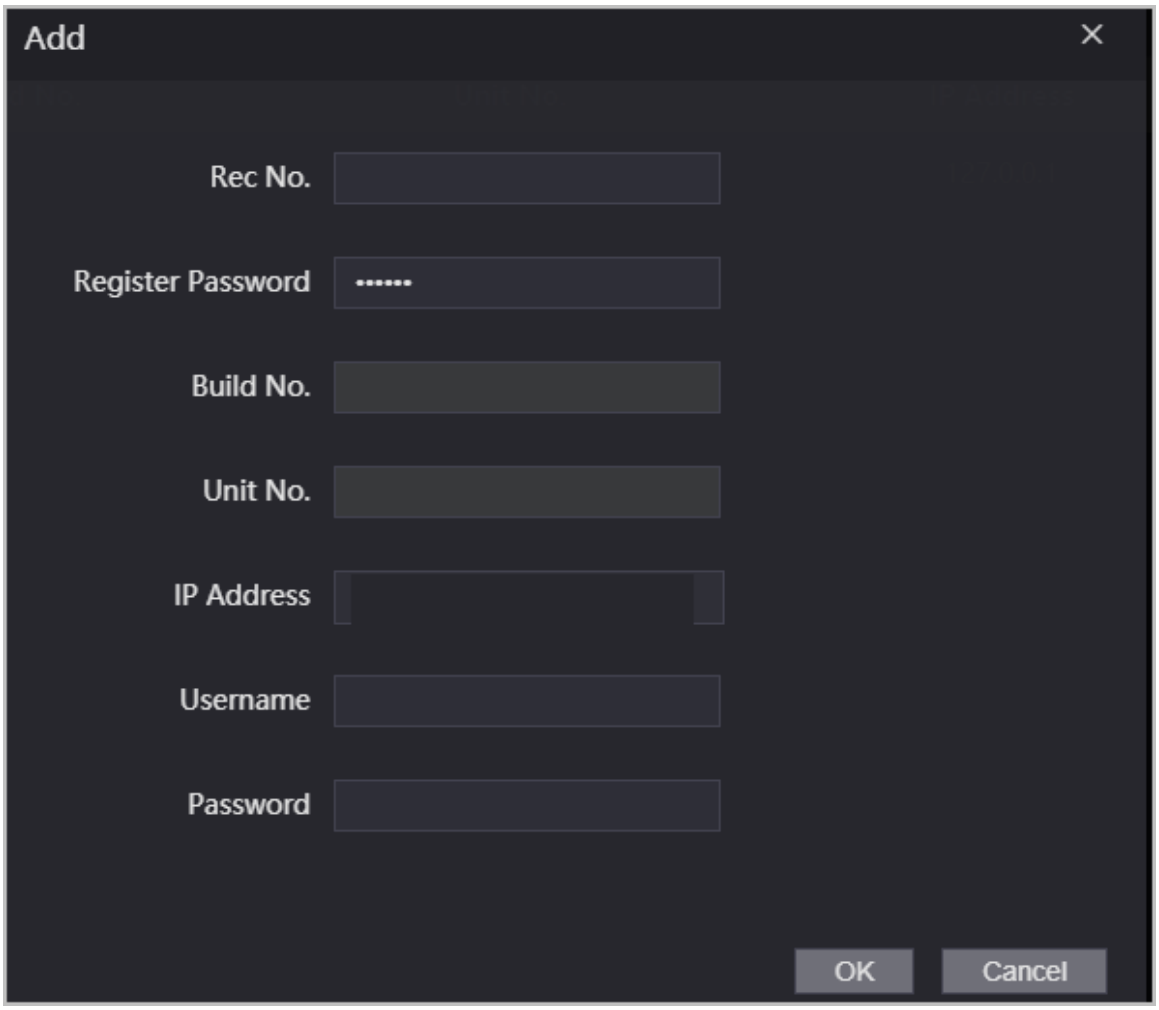


Tabla 3-8 Agregar configuración de VTO

Parámetro	Descripción
Rec. Nro.	El número del VTO añadido. Puede consultar el número en la **Dispositivo**Página en la página web de la VTO.

Parámetro	Descripción
Registro Contraseña	Mantenlo por defecto
Número de compilación	No se puede configurar.
Unidad No.	
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**.

3.6.4 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 contexto

- Cuando hay un VTH principal y una extensión, primero debe activar la función de llamada grupal y luego agregar el VTH principal y la extensión en el**Gestión de VTH**Para saber cómo activar la función de llamada grupal, consulte "3.6.2 Configuración de parámetros básicos".
- No se puede agregar 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 3-15 Agregar individualmente

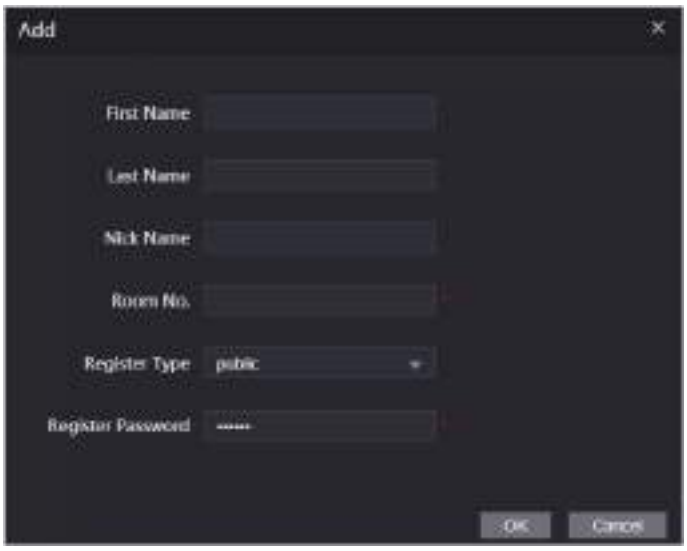


Tabla 3-9 Información de la habitación

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 un VTH principal y extensiones, el número de habitación del VTH principal termina en -0 y el número de habitación de la extensión termina en -1, -2 o -3. Por ejemplo, el VTH principal es 101-0 y el número de habitación de la extensión es 101-1, 101-2... ◇ Si la función de llamada grupal no está activada, no se puede configurar el número de habitación en el formato 9901-xx.
Nombre de pila	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 3-16 Adición por lotes



Tabla 3-10 Adición de lotes

Parámetro	Descripción
Cantidad de capas unitarias	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 de 1 a 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.

3.6.5 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**Haga clic

Paso 2 en**Agregar**y establecer parámetros.

Figura 3-17 Gestión de VTS

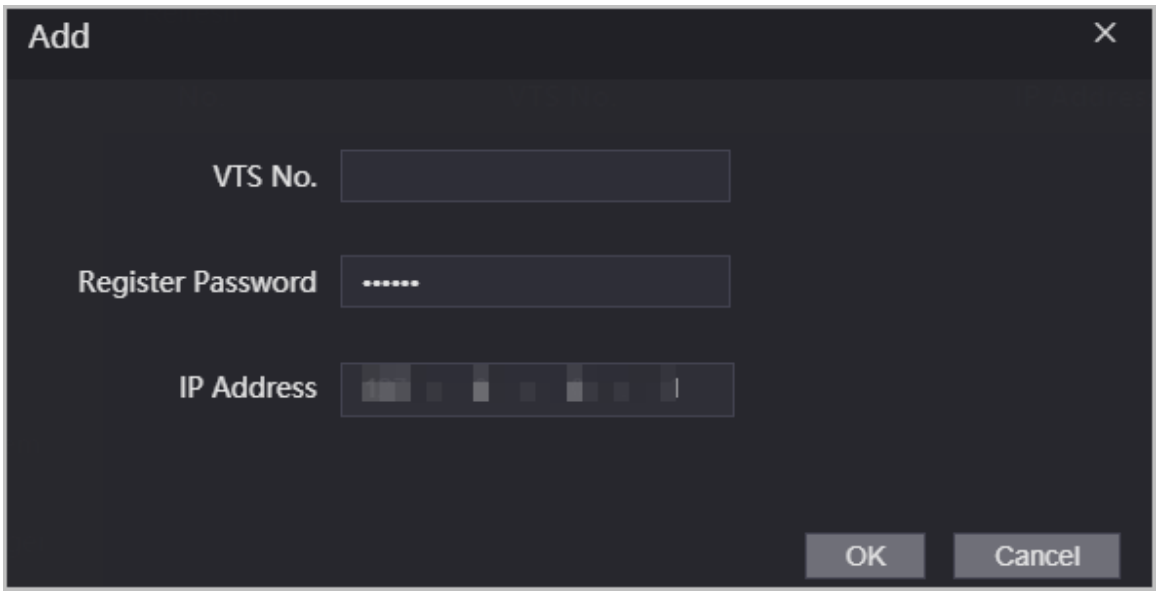


Tabla 3-11 Parámetros VTS

Parámetro	Descripción
N.º VTS	El número del VTS, que puede tener hasta 9 dígitos.
Contraseña de registro	La contraseña de registro es la contraseña de inicio de sesión del VTS. Le recomendamos que la mantenga como predeterminada.
Dirección IP	La dirección IP del VTS.

Paso 3 Hacer clic**DE ACUERDO**.

3.6.6 Visualización del estado del dispositivo

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

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

3.6.7 Visualización de registros de llamadas

Ver todo el registro de llamadas salientes y entrantes.

En la página de inicio, seleccione**Configuración de Talkback**>**Llamar**.

3.7 Personalización

Configure temas y agregue recursos de video o imagen al controlador de acceso.

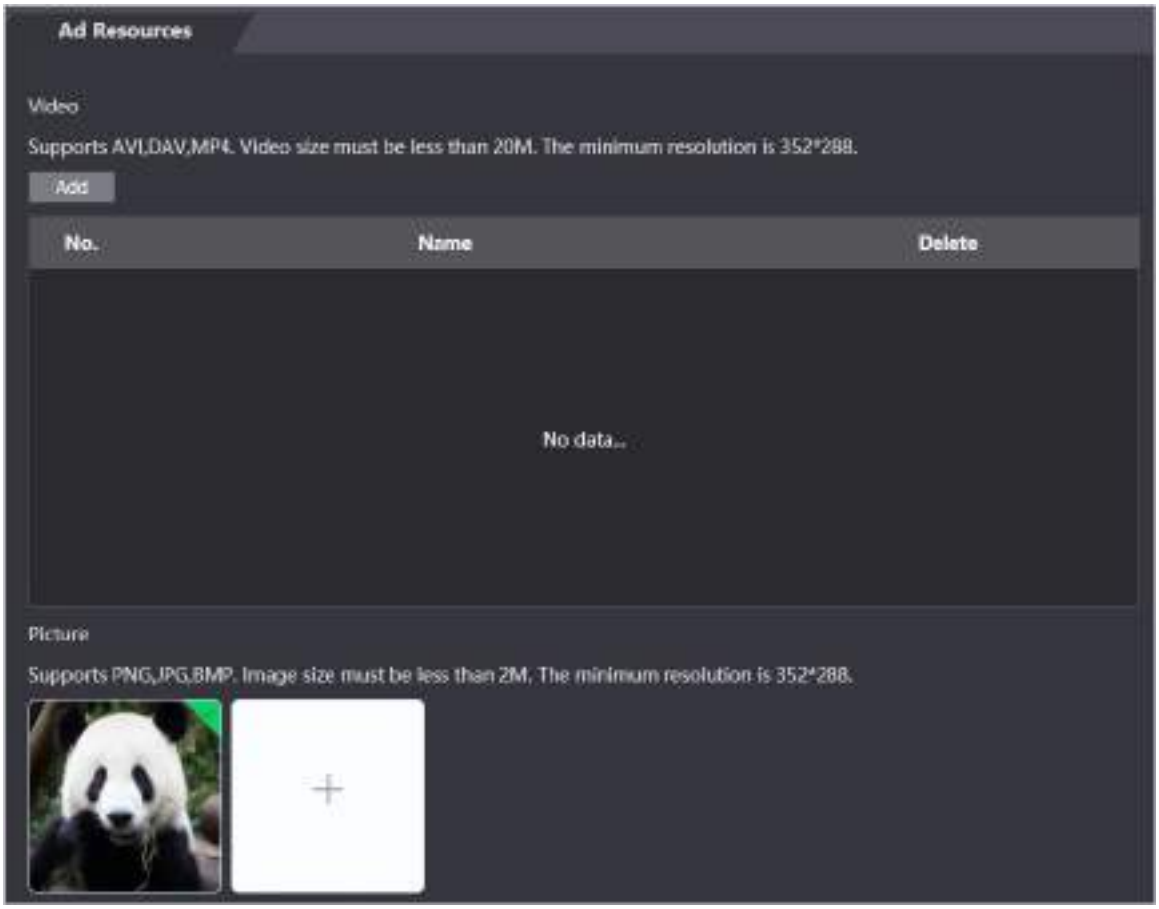
3.7.1 Agregar recursos

Agregue imágenes o vídeos para que se muestren en la pantalla de espera del Terminal de Acceso.

Procedimiento

Paso 1 En la página de inicio, seleccione**Personalización**>**Recursos publicitarios**.

Figura 3-18 Agregar recursos



Paso 2 Añadir vídeos o imágenes.

- Añadir vídeos.

  1. Haga clic**Agregar**.
  2. Haga clic**Navegar**,Seleccione el archivo de vídeo y luego haga clic en**Próximo**.

  ◇ Puedes cargar hasta 5 archivos de vídeo.
  ◇ Admite FLV, AVI, ASF, DAV, PS, TS, MP4. El tamaño del video debe ser inferior a 20 M. Solo es
  ◇ compatible con Firefox y la última versión de Chrome para cargar archivos de video.

  3. Haga clic**DE ACUERDO**.

- Añadir imágenes

  1. Haga clic en .

2. Seleccione una imagen del local y cárguela.

- Puedes subir hasta 10 imágenes.
- Admite PNG, JPG y BMP. El tamaño de la imagen debe ser inferior a 2 M.

Operaciones relacionadas

- Haga clic para eliminar las imágenes o vídeos cargados.

  Los vídeos y las imágenes en uso no se pueden eliminar.
- Haga clic para obtener una vista previa de la imagen cargada.

3.7.2 Configuración de temas

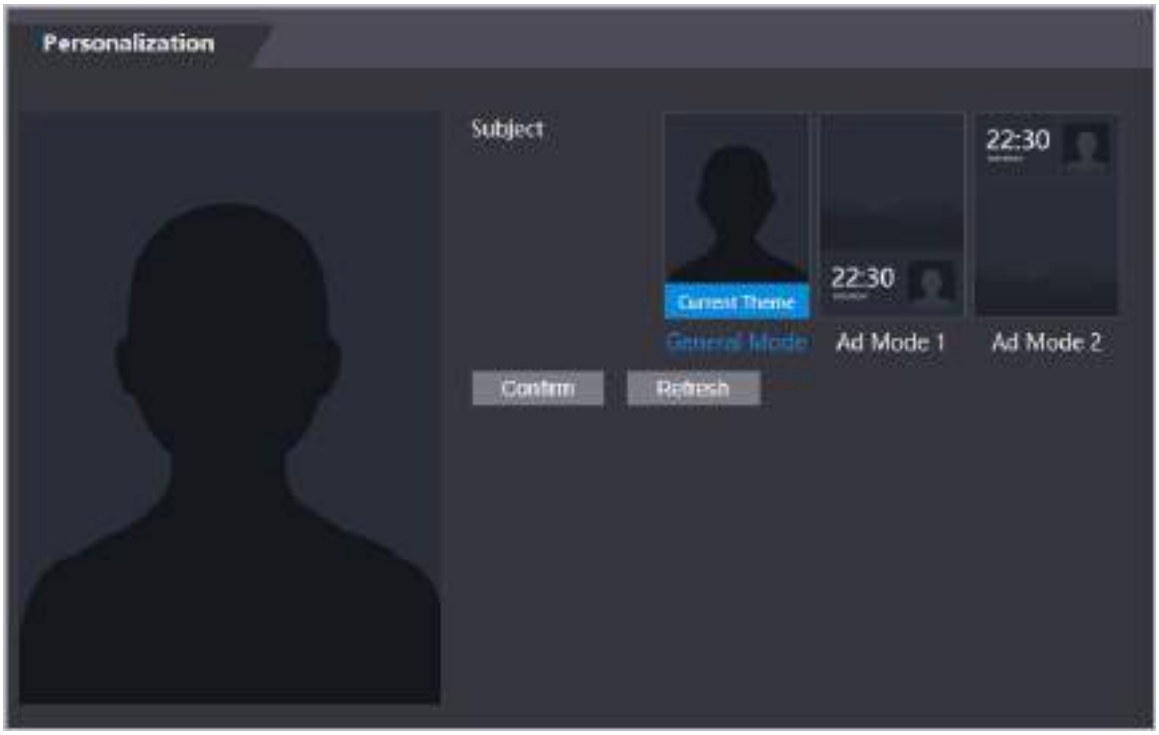
Procedimiento

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

Paso 2 Seleccione el tema.

- Modo general: muestra la imagen del rostro en pantalla completa.
- Modo de anuncio 1: el área superior muestra los anuncios y el área inferior muestra la hora y el cuadro de detección de rostro.
- Modo de anuncio 2: el área superior muestra la hora y el cuadro de detección de rostro, y el área inferior muestra los anuncios.

Figura 3-19 Tema

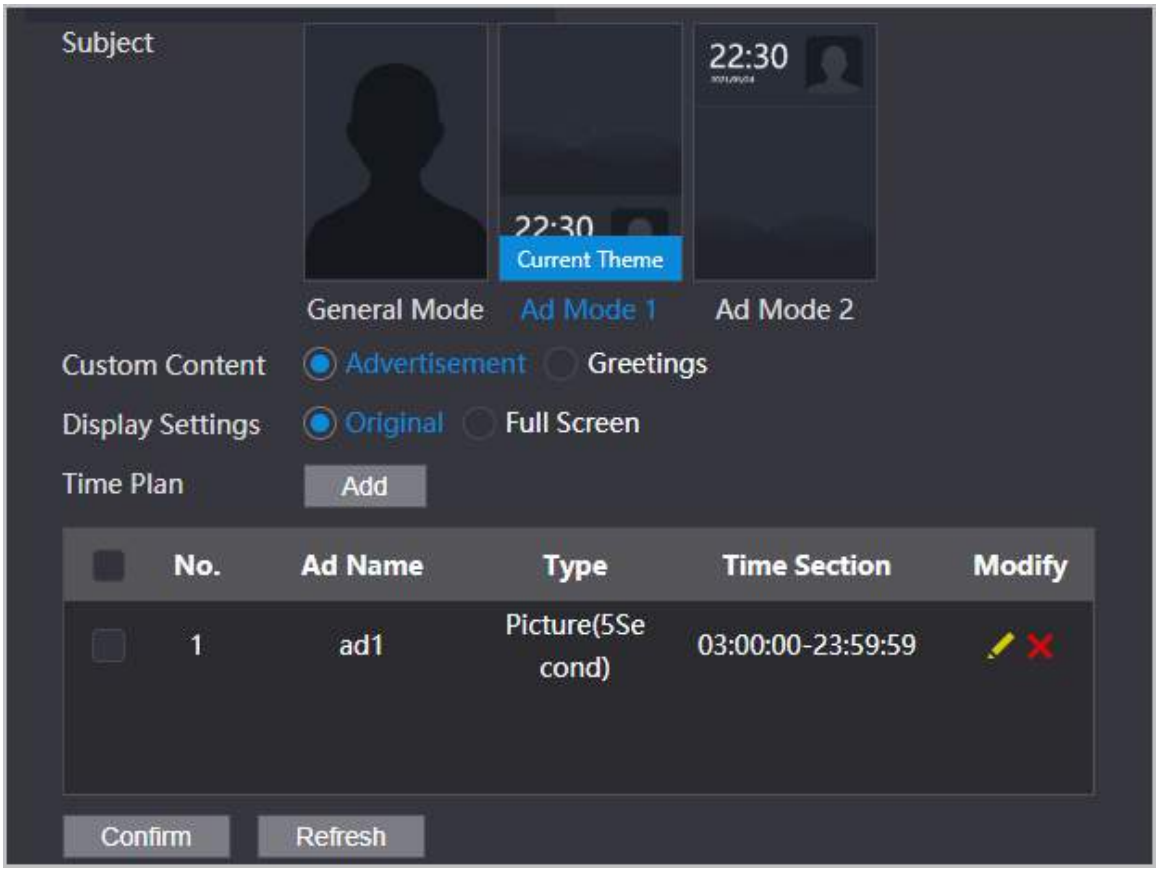


Paso 3 Seleccione el mensaje de voz para verificar la identidad correctamente.

Paso 4 Configure la visualización de anuncios.

1. Seleccione el modo de anuncio 1 o el modo de anuncio 2 y, a continuación, seleccione**Anuncio**.

Figura 3-20 Modo de anuncio



2. Seleccione el modo de visualización.

- Original: reproduce la imagen y el vídeo en el tamaño original.
- Pantalla completa: reproduce la imagen y el vídeo en pantalla completa.

3. Haga clic**Agregar**para agregar horarios.

Puedes agregar hasta 10 horarios.

4. Ingrese el nombre del anuncio,

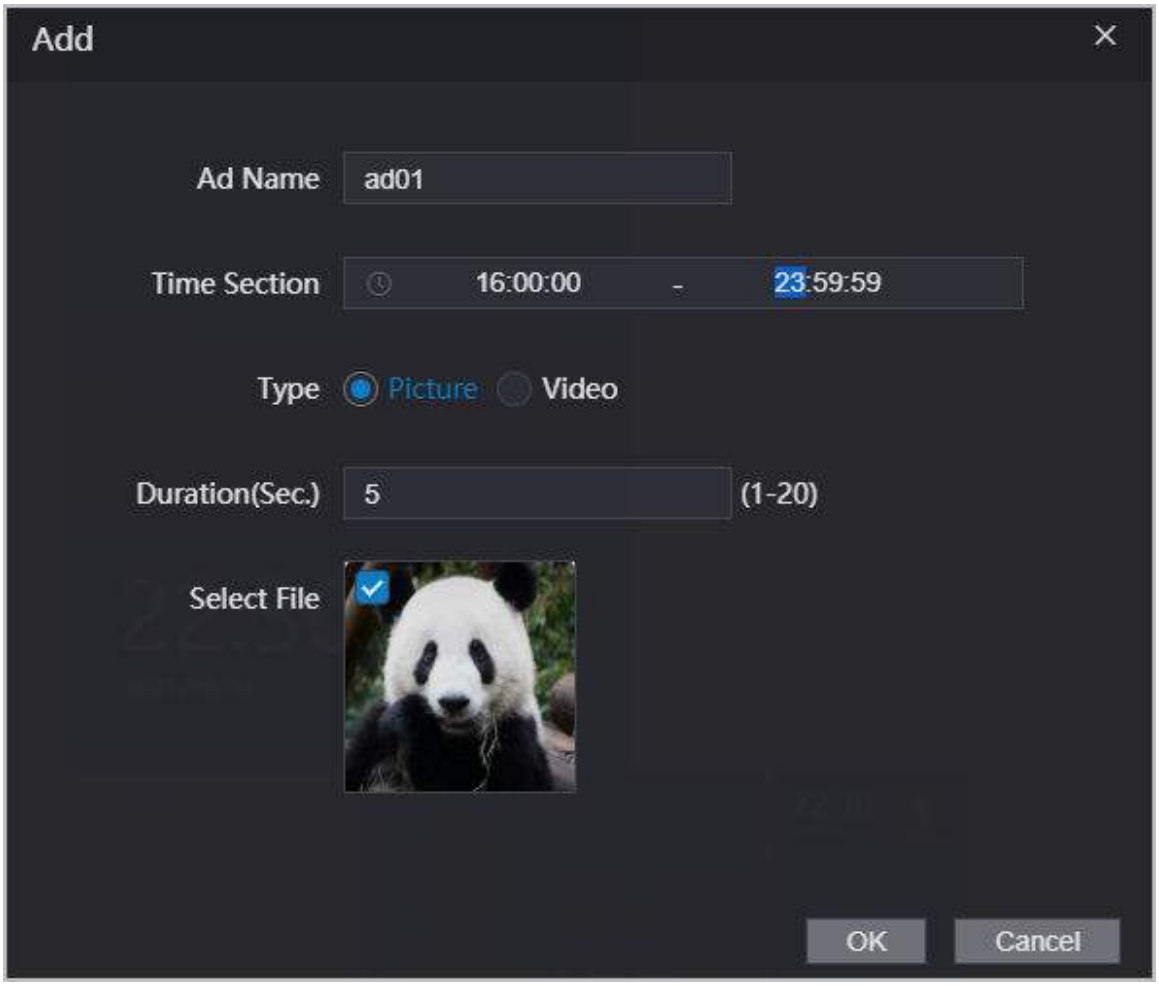
5. Seleccione la sección de tiempo, tipo y archivo.

6. Ingrese la duración y luego haga clic en**DE ACUERDO**.

Establezca la duración de una sola imagen cuando las imágenes se reproduzcan en bucle. La duración varía de 1 s a 20 s y es de 5 s de forma predeterminada.

7. Seleccione el tipo y el archivo.

Figura 3-21 Agregar horarios

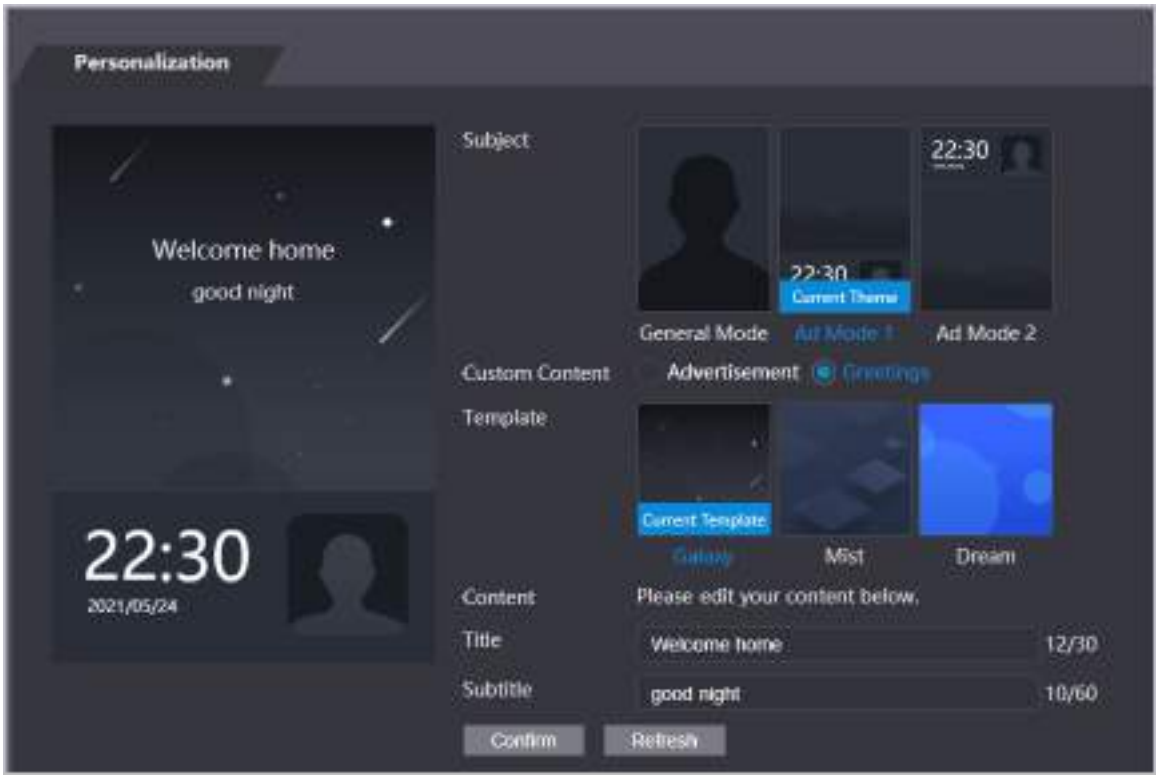


8. Seleccione el horario agregado y luego haga clic en**DE ACUERDO**

Paso 5 . Configurar saludos.

1. Seleccione**Saludos**desde**Contenido personalizado**.
2. Seleccione la plantilla.
3. Ingrese el título y el subtítulo.

Figura 3-22 Saludos



4. Haga clic**Confirmar**.

3.8 Configuración de horarios

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

3.8.1 Configuración de secciones de tiempo

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

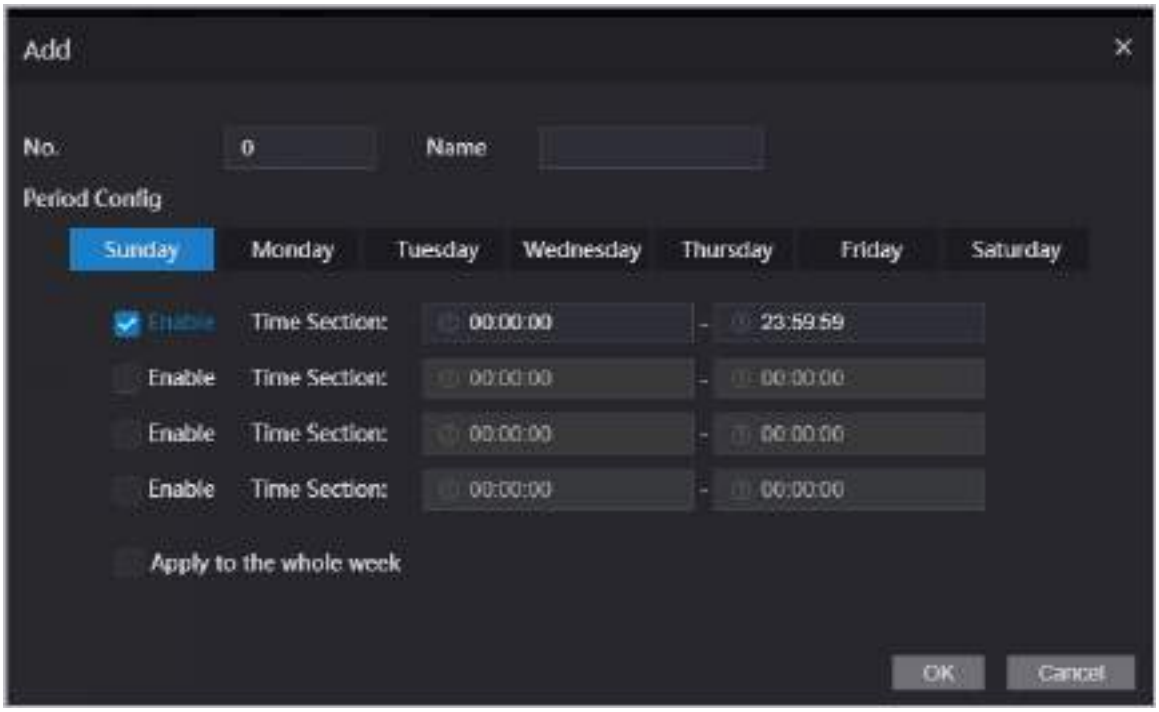
Procedimiento

Paso 1 Inicie sesión en la página web.

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

Paso 3 clic en**Agregar**.

Figura 3-23 Parámetros de la sección de tiempo



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

- **No.**:Introduzca el número de la hora. Varía entre 0 y 127.
- **Nombre**:Introduzca un nombre para cada sección de tiempo. Puede introducir un máximo de 32 caracteres (que pueden incluir números, caracteres especiales y caracteres en inglés).

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

Paso 5 Configurar secciones de tiempo para cada día.

Paso 6 (Opcional) Haga clic en**Aplicar a toda la semana**Para copiar la configuración al resto de días, haga clic en**DE**

Paso 7 **ACUERDO**.

3.8.2 Configuración de grupos de vacaciones

Establezca franjas horarias para diferentes grupos de vacaciones. Puede configurar hasta 128 grupos de vacaciones (desde el n.º 0 hasta el n.º 127) y hasta 16 franjas horarias para un solo grupo de vacaciones. Los usuarios pueden desbloquear puertas en las franjas horarias definidas.

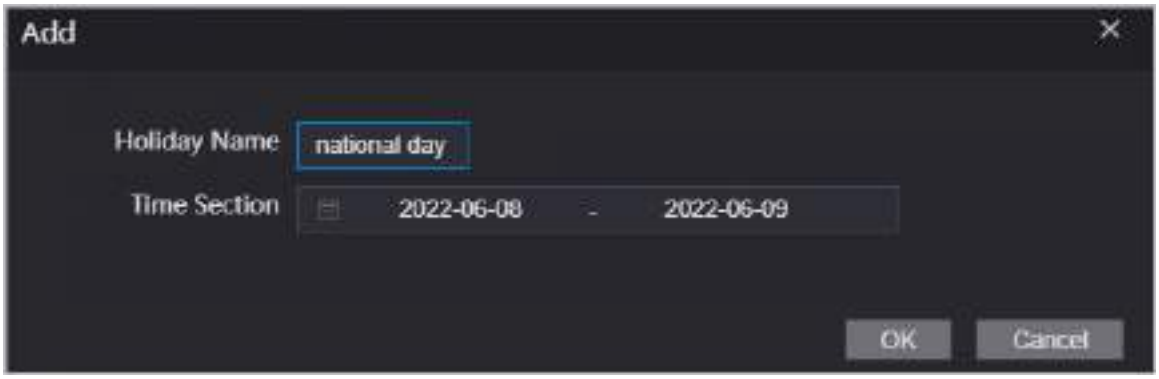
Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Sección de tiempo**>**Grupo de vacaciones**>**Configuración**Haga clic en

Paso 3 **Agregar**.

Figura 3-24 Agregar un grupo de vacaciones



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

- **Nombre de la fiesta**:Introduzca el nombre del grupo de vacaciones. Introduzca un nombre para cada sección horaria. Puede introducir un máximo de 32 caracteres (que 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**DE**

Paso 5 **ACUERDO**.

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

Paso 6 Hacer clic**DE ACUERDO**.

3.8.3 Configuración de planes de vacaciones

Asignar los grupos de vacaciones configurados a los planes de vacaciones. Los usuarios solo pueden desbloquear la puerta en el horario definido en el plan de vacaciones.

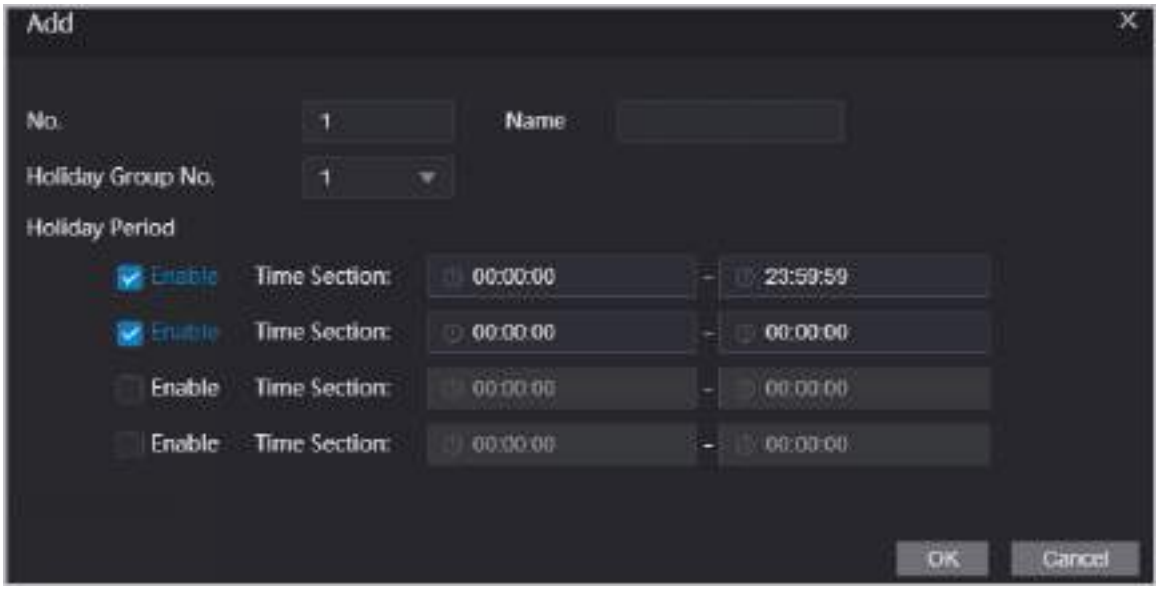
Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Sección de tiempo**>**Configuración del plan de vacaciones**Haga clic en

Paso 3 **Agregar**.

Figura 3-25 Agregar plan de vacaciones



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

- **No.**:Introduzca un número de sección. Puede ser de 0 a 127.
- **Nombre**:Introduzca un nombre para cada sección de tiempo. Puede introducir un máximo de 32 caracteres (que 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**Periodo de vacaciones**Área, configure tramos horarios en el grupo de vacaciones. Puede configurar hasta cuatro tramos horarios.

Paso 7 Hacer clic**DE ACUERDO**.

3.9 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**.

3.10 Configuración de vídeo e imagen

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

Información de contexto

Le recomendamos que utilice los parámetros predeterminados en esta sección.

3.10.1 Configuración de vídeos

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

- Estándar de vídeo: Seleccionar**Sistema de clasificación de números arábigos (NTSC)**.
- Id. de canal: el canal 1 es para configuraciones de imagen de luz visible. El canal 2 es para configuraciones de imagen de luz infrarroja.
- Predeterminado: restaurar la configuración predeterminada.
- Capturar: 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.

3.10.1.1 Configuración del canal 1

Procedimiento

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

Paso 2 **de vídeo**. Seleccionar**1**desde**Canal No.**Lista.

Paso 3 Configurar la tarifa de fecha.

Figura 3-26 Tasa de fecha

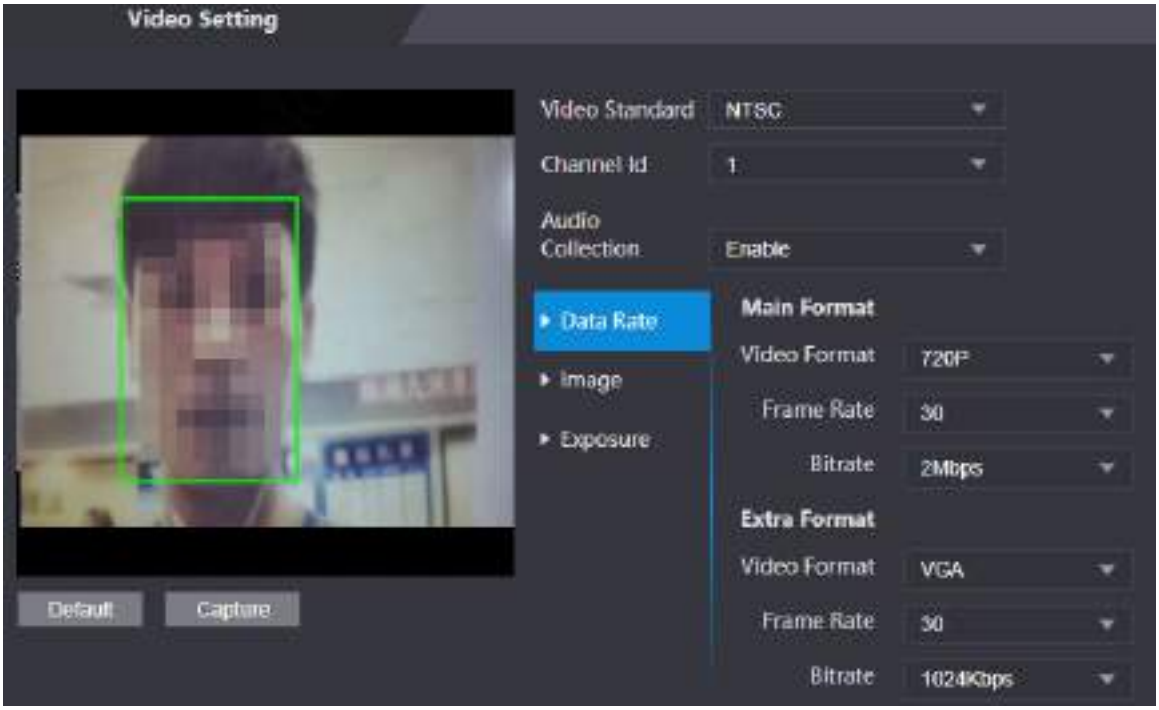


Tabla 3-12 Descripción de la tasa de fecha

Parámetro		Descripción
Formato principal	Formato de vídeo	Cuando el controlador de acceso funciona como un VTO y se conecta al VTH, el límite de flujo adquirido del VTH es 720p. Cuando la resolución se cambia a 1080p, la función de llamada y monitoreo podría verse afectada.
	Velocidad de cuadros	La cantidad de fotogramas (o imágenes) por segundo. El rango de velocidad de fotogramas es de 1 a 25 fps.
	Tasa de bits	Indica la cantidad de datos que se transmiten a través de una conexión a Internet en un período de tiempo determinado. Seleccione un ancho de banda adecuado en función de la velocidad de su red.
Transmisión adicional	Formato de vídeo	La subtransmisión admite D1, VGA y QVGA.
	Velocidad de cuadros	La cantidad de fotogramas (o imágenes) por segundo. El rango de velocidad de fotogramas es de 1 a 25 fps.
	Tasa de bits	Indica la cantidad de datos transmitidos a través de una conexión a Internet en un período de tiempo determinado.

Paso 4 Configurar la imagen.

Figura 3-27 Imagen

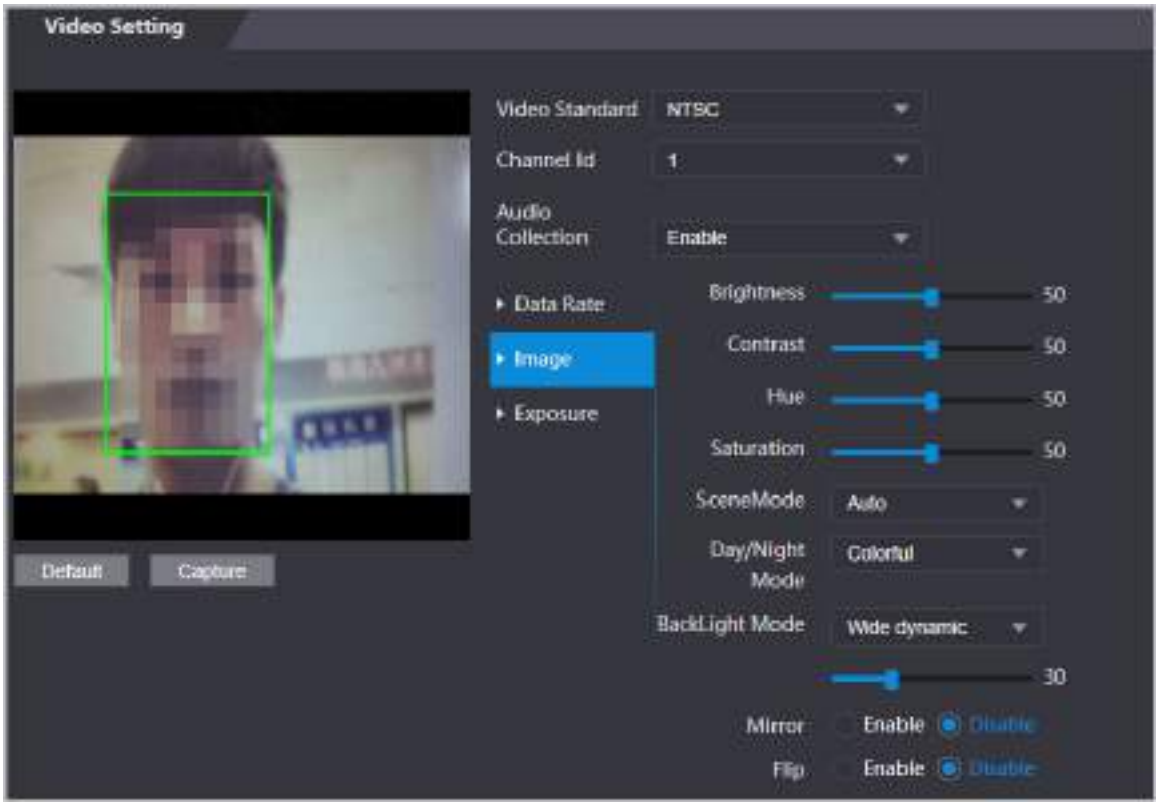


Tabla 3-13 Descripción de la imagen

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 permite distinguir un objeto. Cuanto mayor sea el valor de contraste, mayor será el contraste de color.
Matiz	Se refiere a la fuerza o saturación de un color. Describe la intensidad del color o su pureza.
Saturación	La saturación del color indica la intensidad del color en una imagen. A medida que aumenta la saturación, el color se ve 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 en función de 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.

Parámetro	Descripción
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.
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 luces altas (HLC) es una tecnología que se utiliza en las cámaras de seguridad CCTV/IP para tratar imágenes expuestas a luces como faros o focos. El sensor de imagen de la cámara detecta luces fuertes en el video y reduce la exposición en esos puntos para mejorar la calidad general de la imagen.
Espejo	Cuando la función está activada, las imágenes se mostrarán con el lado izquierdo y el derecho invertidos.
Voltear	Cuando esta función está activada, las imágenes se pueden voltear.

Paso 5 Configurar los parámetros de exposición.

Figura 3-28 Exposición

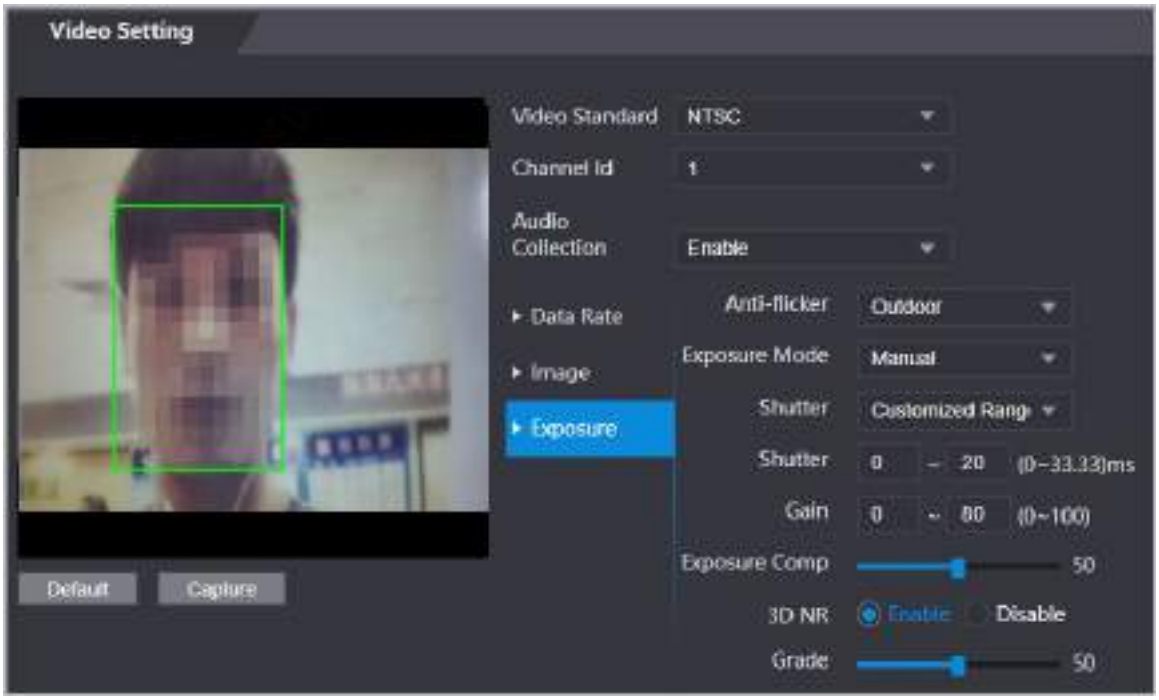


Tabla 3-14 Descripción de los parámetros de exposición

Parámetro	Descripción
Anti-parpadeo	Configure el antiparpadeo para reducir el parpadeo y 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**Se selecciona, se puede cambiar el modo de exposición.
Modo de exposición	Puede configurar la exposición para ajustar el brillo de la imagen. ● **Auto**:El 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 no es suficiente y el valor del obturador ha alcanzado su límite superior o inferior, el controlador de acceso ajustará automáticamente el valor de 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**Anti-parpadeo**lista, puedes seleccionar **Prioridad de obturador**como el modo de exposición. ◇ El modo de exposición puede variar según los diferentes modelos de controlador de acceso.
Obturador	El obturador es un componente que permite el paso de la luz durante un tiempo determinado. Cuanto mayor sea la velocidad de obturación, menor será el tiempo de exposición y más oscura será la imagen.
Ganar	Cuando se establece el rango de valores de ganancia, se mejorará la calidad del video.
Exposición Compensación	Puede hacer que una foto sea más brillante o más oscura ajustando el valor de compensación de exposición.
Reducción de ruido 3D	Cuando la Reducción de ruido 3D (RD) está activada, se puede reducir el ruido del video para garantizar videos de alta definición.
Calificación	Puede establecer su calificación cuando esta función esté activada.

3.10.1.2 Configuración del canal 2

Procedimiento

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

Paso 2 **de vídeo**Seleccione 2 de los**Canal No.**. Configure el

Paso 3 estado del vídeo.

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

Figura 3-29 Imagen

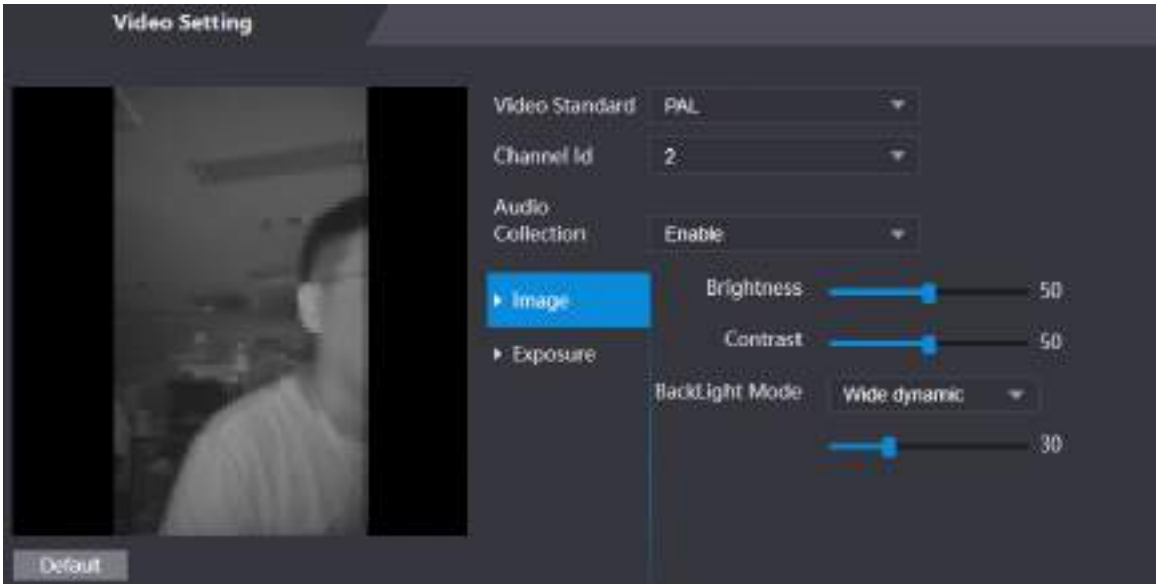


Tabla 3-15 Descripción de la imagen

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 permite distinguir 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 luces altas (HLC) es una tecnología que se utiliza en las cámaras de seguridad CCTV/IP para tratar imágenes expuestas a luces como faros o focos. El sensor de imagen de la cámara detecta luces fuertes en el video y reduce la exposición en esos puntos para mejorar la calidad general de la imagen.

Paso 4 Configurar los parámetros de exposición.

Figura 3-30 Parámetro de exposición

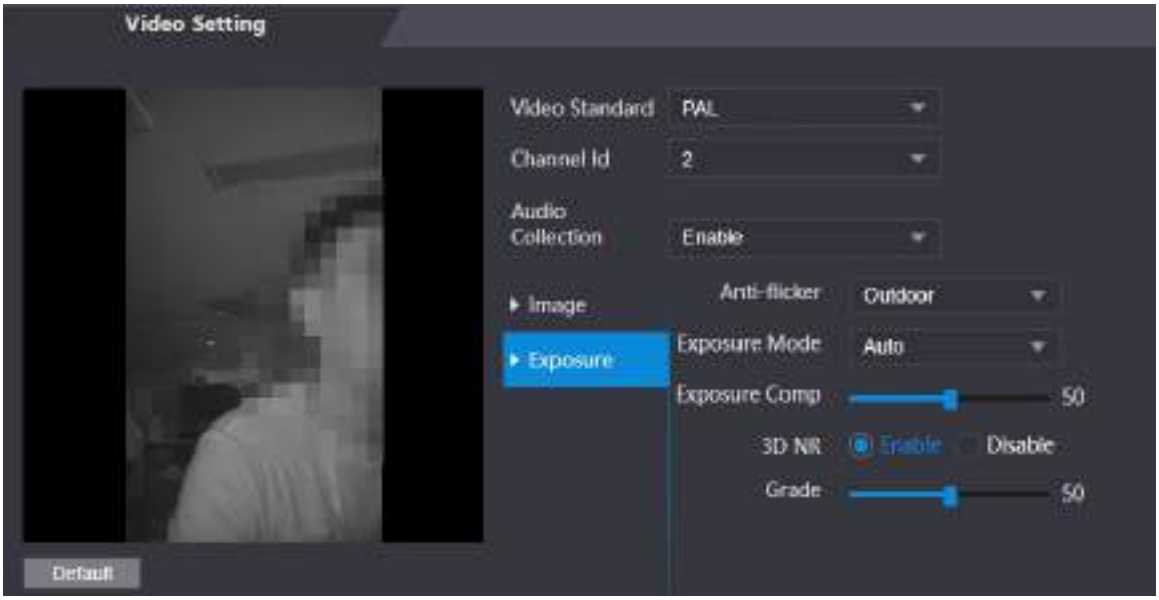


Tabla 3-16 Descripción de los parámetros de exposición

Parámetro	Descripción
Anti-parpadeo	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**Se selecciona, se puede cambiar el modo de exposición.
Modo de exposición	Puede configurar la exposición para ajustar el brillo de la imagen. ● **Auto**:El 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 no es suficiente y el valor del obturador ha alcanzado su límite superior o inferior, el controlador de acceso ajustará automáticamente el valor de 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**Anti-parpadeo**lista, puedes seleccionar **Prioridad de obturador**como el modo de exposición. ◇ El modelo de exposición puede variar según los diferentes modelos de controlador de acceso.

Parámetro	Descripción
Obturador	El obturador es un dispositivo que permite el paso de la luz durante un tiempo determinado. Cuanto mayor sea la velocidad de obturación, menor será el tiempo de exposición y más oscura será la imagen.
Ganar	Cuando se establece el rango de valores de ganancia, se mejorará la calidad del video.
Compensación de exposición	Puede hacer que una foto sea más brillante o más oscura ajustando el valor de compensación de exposición.
Reducción de ruido 3D	Cuando la Reducción de ruido 3D (RD) está activada, se puede reducir el ruido del video para garantizar videos de alta definición. Puede establecer su calificación cuando esta función esté activada.
Calificación	

3.10.2 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 de volumen**

Paso 3 Arrastre el control deslizante para ajustar el volumen. Haga clic

Paso 4 **DE ACUERDO**.

3.10.3 Configuración de la codificación local

Configure el área de monitoreo en el VTO y el VTH puede proporcionar una pantalla de monitoreo en tiempo real.

Información de contexto

Para evitar la pérdida de datos de video, le recomendamos que active la función de codificación local cuando el VTO esté conectado a VTH.

Procedimiento

Paso 1 Seleccionar**Vídeo y audio**>**Codificación local**.

Paso 2 Seleccionar**Permitir**Para activar la función, haga clic en

Paso 3 **DE ACUERDO**.

3.10.4 Configuración del modo de imagen

Seleccione el modo de imagen según el sitio de instalación del controlador de acceso.

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración de vídeo**>**Modo de imagen**.

Paso 2 Seleccione el modo de imagen según la ubicación de instalación del controlador de acceso.

- Interior: El controlador de acceso se instala en interiores, como oficinas. La luz artificial se distribuye uniformemente por toda la habitación y no hay luz natural.
- Exterior: El controlador de acceso se instala en exteriores y la luz del día es brillante y uniforme.

- Otros: el rostro humano se encuentra a contraluz, lo que hace que se oscurezca. Le recomendamos que seleccione otro modo para que el controlador de acceso lo detecte con mayor facilidad.

Paso 3 Hacer clic**DE ACUERDO**.

3.11 Configuración de la detección de rostros

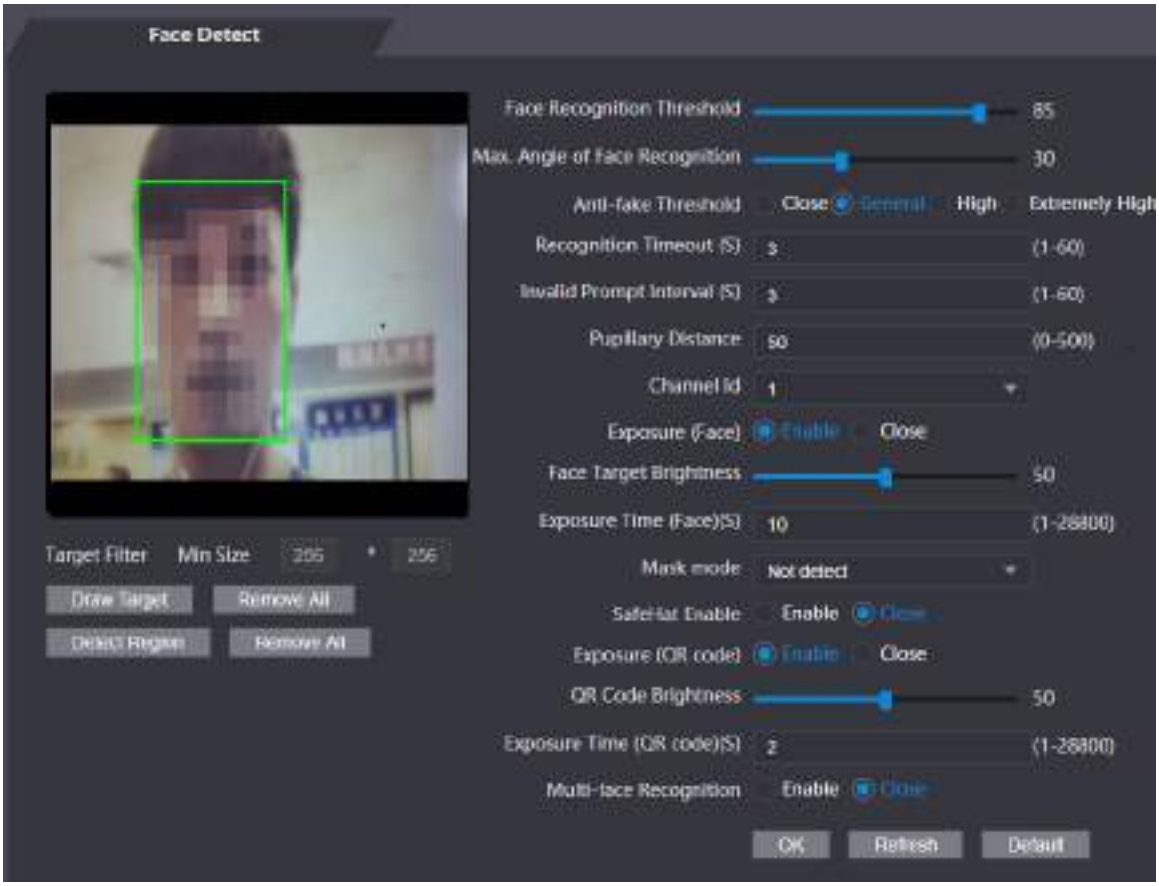
Puede configurar parámetros relacionados con el rostro humano en esta interfaz para aumentar la precisión del reconocimiento facial.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccione**Detección de rostro**.

Figura 3-31 Detección de rostro



Paso 3 Configurar los parámetros.

Tabla 3-17 Descripción de los parámetros de detección de rostros

Parámetro	Descripción
Umbral de reconocimiento facial	Ajuste la precisión del reconocimiento facial. Un umbral más alto significa mayor precisión.
Ángulo máximo de reconocimiento facial	Establezca el ángulo máximo de pose del rostro para la detección de rostros. Un valor mayor significa un rango de ángulos del rostro más amplio. Si el ángulo de pose del rostro está fuera del rango definido, no aparecerá el cuadro de detección de rostros.

Parámetro	Descripción
Umbral anti-falsificación	Evite el reconocimiento facial falso cuando las personas utilicen 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 indicarlo.
Intervalo de aviso 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 que se ha producido un error en el reconocimiento facial. Puede introducir el intervalo de tiempo indicado.
Distancia pupilar	Las imágenes de rostros requieren los píxeles deseados entre los ojos (llamada distancia pupilar) para un reconocimiento exitoso. El píxel predeterminado es 45. El píxel cambia según el tamaño del rostro y la distancia entre los rostros y la lente. Si un adulto está a 1,5 metros de la lente, la distancia pupilar puede ser de 50 px a 70 px.
Identificación del canal	1 es para la cámara de luz blanca y 2 es para la cámara de luz infrarroja.
Exposición (Rostro)	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**:No se detecta la máscara durante el reconocimiento facial. ● **Recordatorio de uso de mascarilla**:La mascarilla se detecta durante el reconocimiento facial. Si la persona no lleva mascarilla, el sistema le recordará que debe usarla y se le permitirá el acceso. ● **Intercepción de máscara**:La mascarilla se detecta durante el reconocimiento facial. Si una persona no lleva mascarilla, el sistema le recordará que se la ponga y le negará el acceso.
Habilitar SafeHat	Detecta si las personas usan cascos seguros.
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.
Código QR Brillo	

Parámetro	Descripción
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 emitirá luz nuevamente hasta que haya transcurrido el tiempo de exposición definido.
Reconocimiento de múltiples caras	Admite la detección de 6 imágenes de rostros al mismo tiempo y el modo de combinación de desbloqueo deja de ser válido. La puerta se desbloquea después de que cualquiera de ellos acceda.
Dibujar objetivo	• Hacer clic**Dibujar objetivo**y luego dibuje el cuadro mínimo de detección de rostros. • Hacer clic**Eliminar todo**, y puedes eliminar todos los marcos que hayas dibujado.
Detectar región	• Hacer clic**Detectar región**Mueva el mouse y podrá ajustar la región de detección de rostro. • Hacer clic**Eliminar todo**, y puedes eliminar todas las regiones de detección.

Paso 4 Dibuja el cuadro de detección de rostros.

1. Haga clic**Dibujar objetivo**,
2. Dibuje un rectángulo arrastrando el mouse y luego suelte el botón izquierdo del mouse.

Se detectará el objetivo en el área definida. Dibuje el

Paso 5 tamaño del objetivo.

1. Haga clic**Dibujar objetivo**
2. Haga clic derecho para dibujar el cuadro de reconocimiento facial para definir el tamaño mínimo del rostro detectado.

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**.

3.12 Configuración de la red

3.12.1 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**>**Protocolo**

Paso 2 **TCP/IP**. Configurar parámetros.

Figura 3-32 TCP/IP

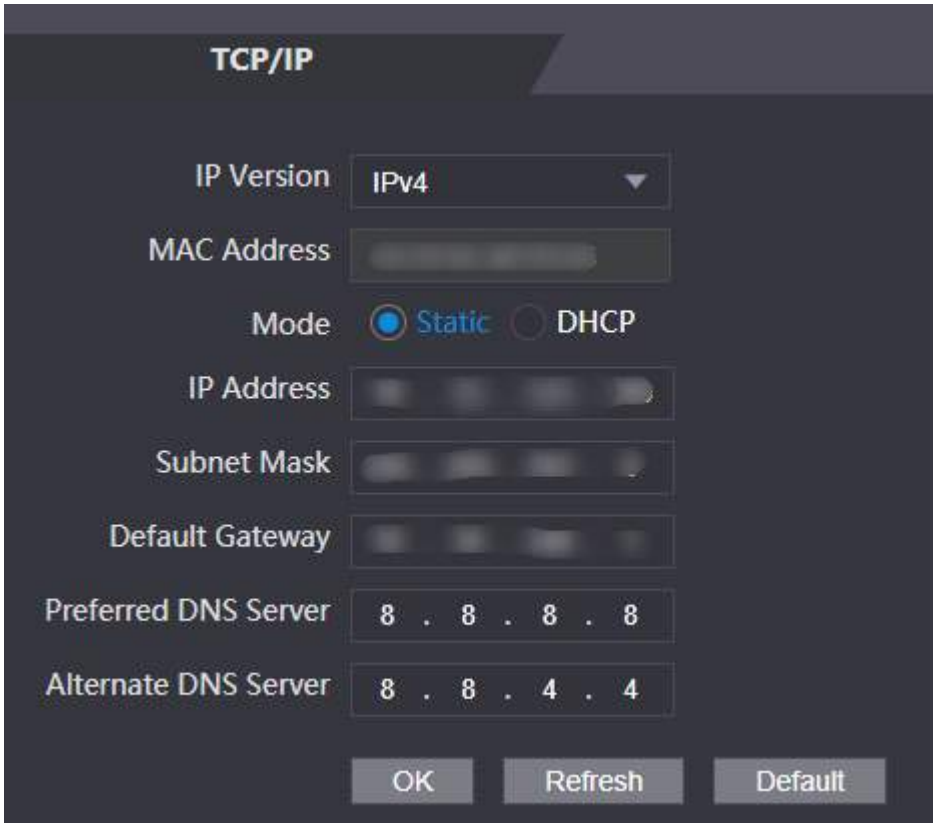


Tabla 3-18 Descripción de TCP/IP

Parámetro	Descripción
Versión IP	IPv4
Dirección MAC	Dirección MAC del controlador de acceso.
Modo	• **Estático**:Ingrese manualmente la dirección IP, la máscara de subred y la puerta de enlace. • **DHCP**:Significa Protocolo de configuración dinámica de host. Cuando se activa DHCP, se le asignará automáticamente una dirección IP, una máscara de subred y una puerta de enlace al controlador de acceso.
Dirección IP	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.
Máscara de subred	
Puerta de enlace predeterminada	
DNS preferido	Establezca la dirección IP del servidor DNS preferido.
DNS alternativo	Establecer la dirección IP del servidor DNS alternativo.

Paso 3 Hacer clic**DE ACUERDO**.

3.12.2 Configuración de puertos

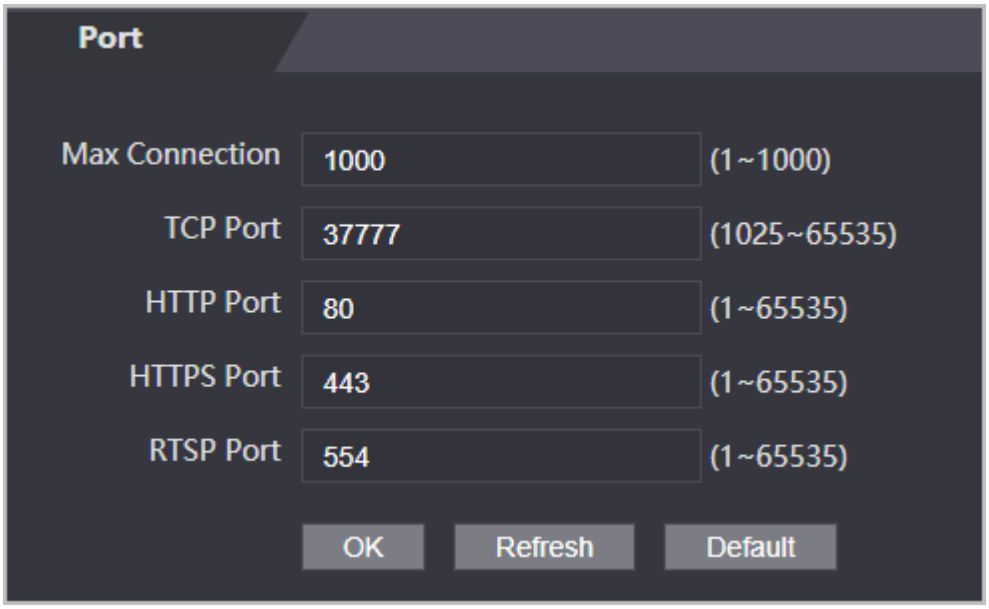
Puede limitar el acceso al Controlador de Acceso al mismo tiempo a través de la web, el cliente de escritorio y el teléfono.

Procedimiento

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

Paso 2 Configurar números de puerto.

Figura 3-33 Configurar puertos



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

Tabla 3-19 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 Terminal 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**.

3.12.3 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 3-34 Registro

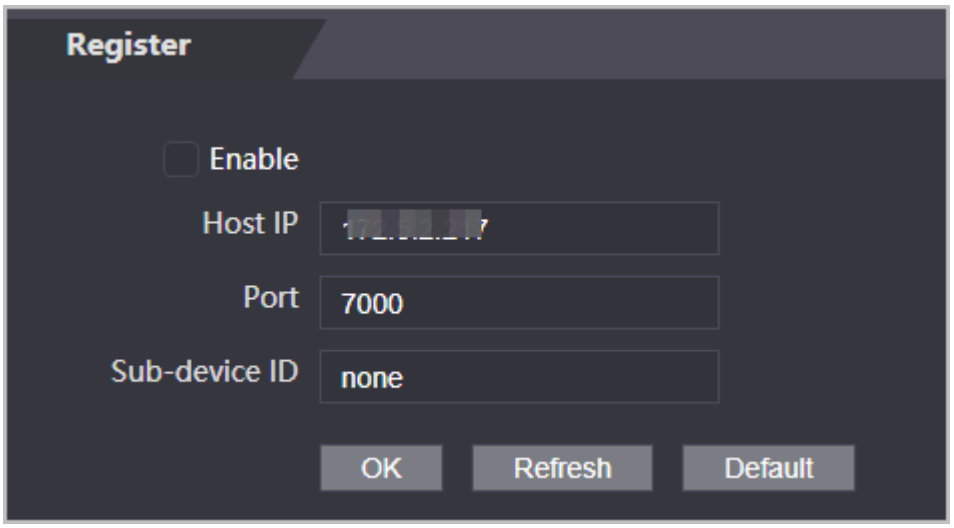


Tabla 3-20 Descripción del registro automático

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

Paso 3 Hacer clic**Aplicar**.

3.12.4 Configuración del servicio en la nube

El servicio en la nube ofrece un servicio de penetración de NAT. Los usuarios pueden administrar varios dispositivos a través de 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 3-35 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.

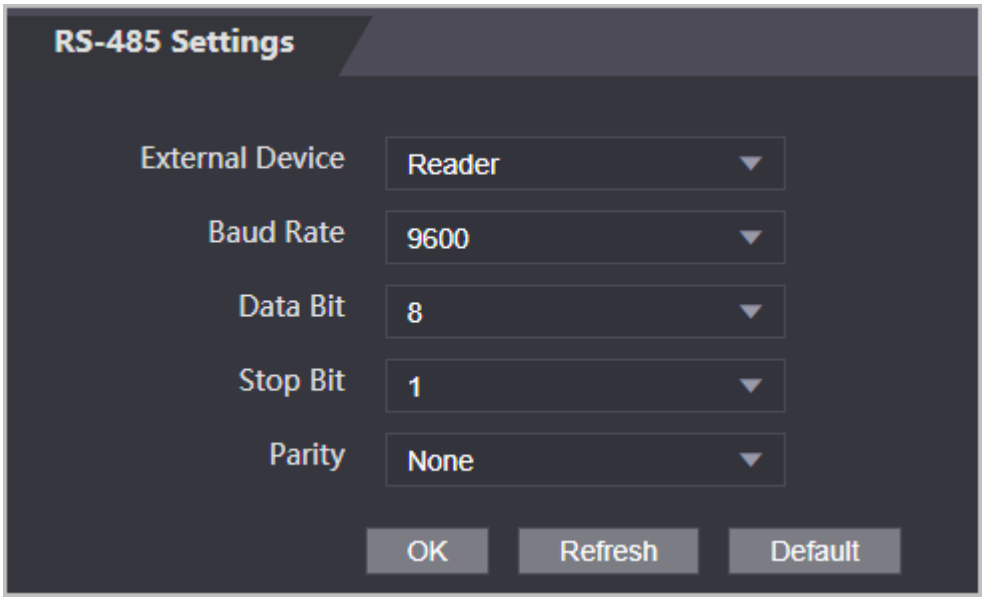
3.12.5 Configuración del puerto serie

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 3-36 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 en función del 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, el bloqueo y la conexión de la alarma contra incendios no serán efectivos.

3.12.6 Configuración de Wiegand

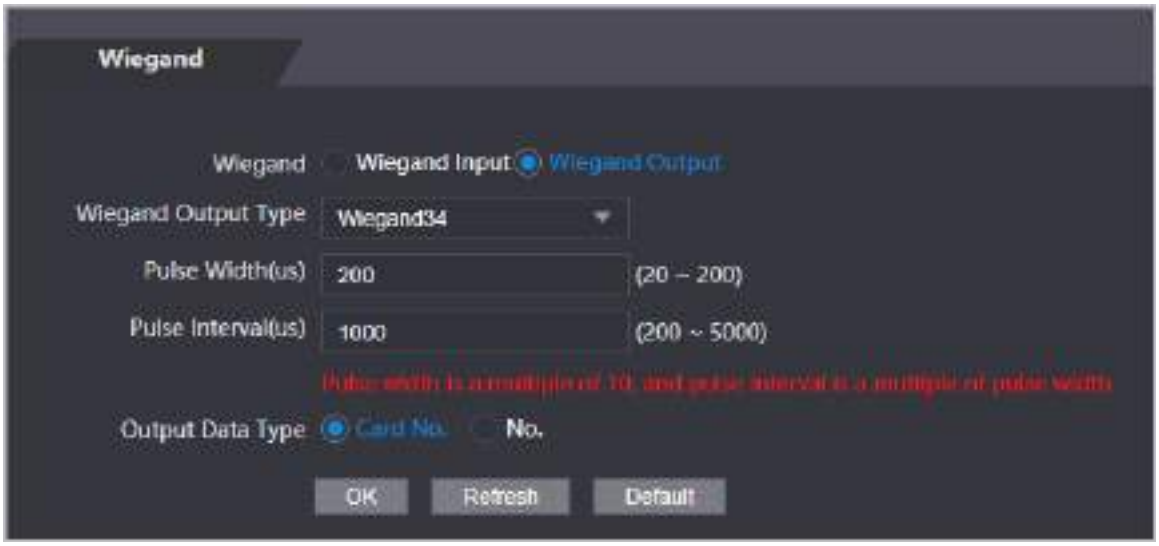
El controlador de acceso permite el modo de entrada y salida Wiegand.

Procedimiento

Paso 1 En el**Menú principal**, seleccionar**Conexión**>**Wiegand**

Paso 2 Seleccione un Wiegand.

Figura 3-37 Salida Wiegand



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

Tabla 3-21 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.

Parámetro	Descripción
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. ● **Tarjeta Nro.**:Genera datos basados en el primer número de tarjeta del usuario.

3.13 Gestión de la seguridad

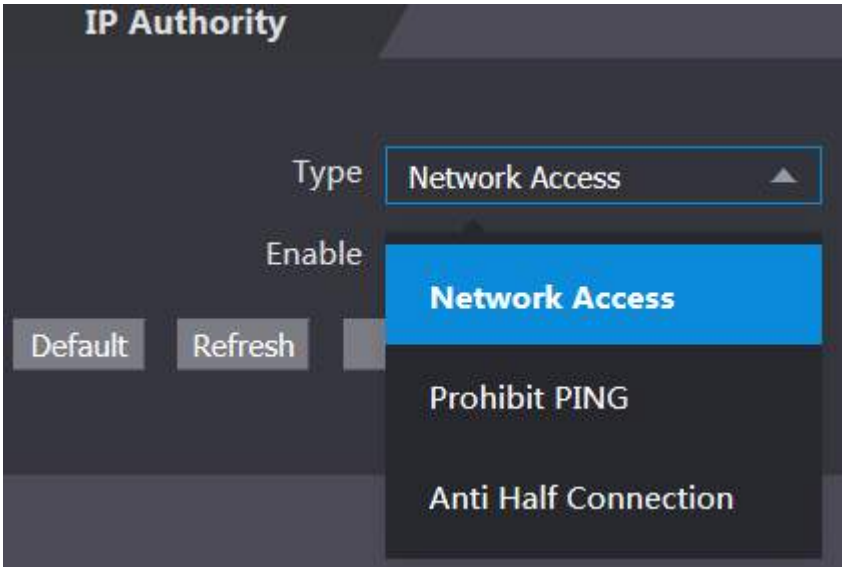
3.13.1 Configuración de la autoridad IP

Procedimiento

Paso 1 Inicie sesión en la página web.

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

Figura 3-38 Autoridad de propiedad intelectual



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

- **Acceso a la red**:Establecer 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.

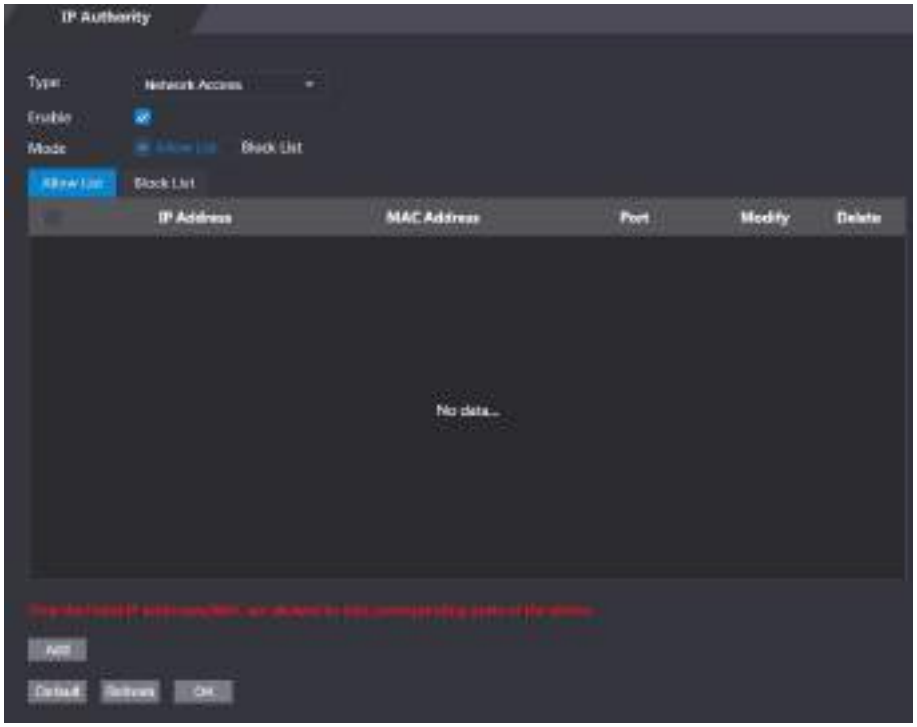
3.13.1.1 Acceso a la red

Procedimiento

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

Paso 2 la**Permitir**Casilla de verificación.

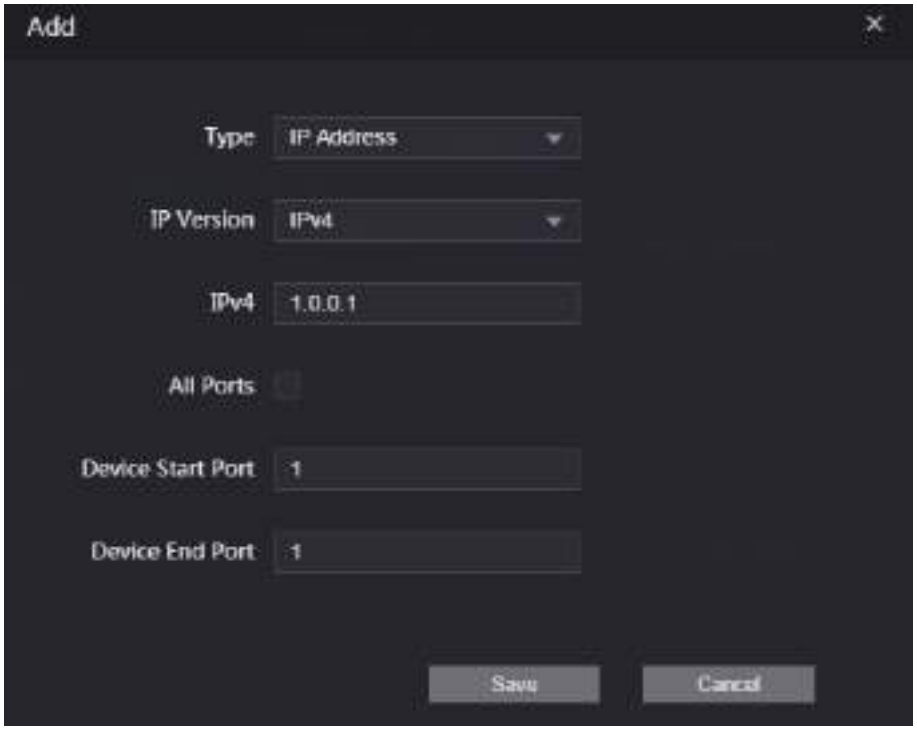
Figura 3-39 Acceso a la red



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

Paso 4 clic en**Agregar**.

Figura 3-40 Agregar IP



Paso 5 Configurar parámetros.

Tabla 3-22 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 aclaras**Todos los puertos**Casilla de verificación, establece 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 blanca o la lista negra. para
- Hacer clic eliminar la lista blanca o la lista negra

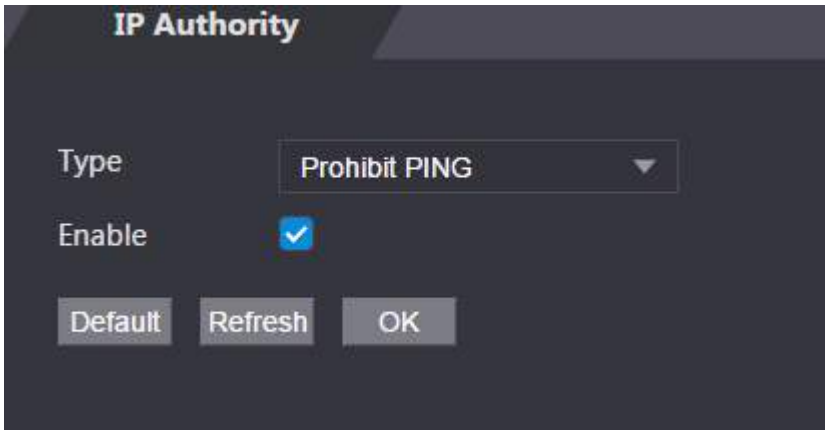
3.13.1.2 Prohibir PING

Procedimiento

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

Paso 2 la**Permitir**Casilla de verificación.

Figura 3-41 Prohibir PING



Paso 3 Hacer clic**DE ACUERDO**.

3.13.1.3 Conexión anti-media

Procedimiento

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

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

Paso 3

3.13.2 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 3-42 Servicio del sistema

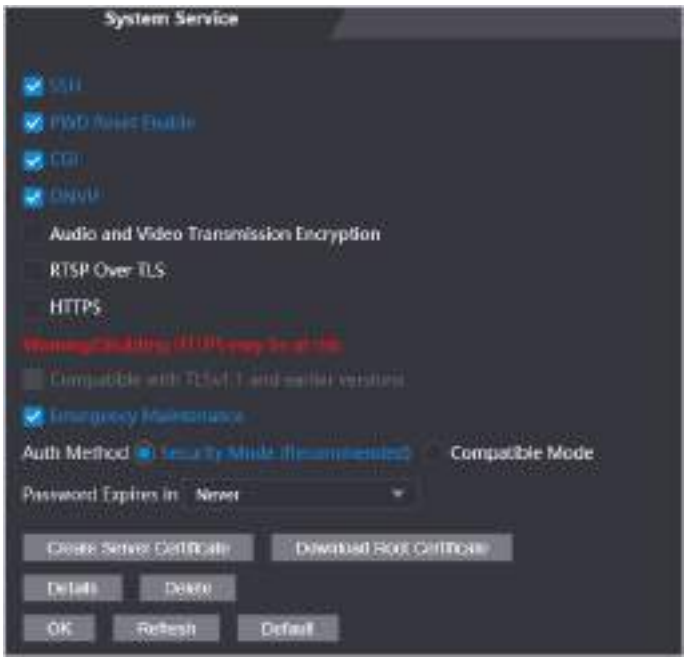


Tabla 3-23 Descripción del servicio del sistema

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 contraseña	Si está habilitada, puede restablecer la contraseña. Esta función está habilitada de manera predeterminada.
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 de manera predeterminada.
ONVIF	Permitir que otros dispositivos extraigan la transmisión de video del VTO a través del protocolo ONVIF.
Audio y vídeo Transmisión Encriptación	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 video se encripta 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 de computadoras. 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.
La contraseña caduca en	Establecer la fecha de expiración de la contraseña.

Paso 4 Hacer clic**DE ACUERDO**.

3.13.2.1 Creación de un certificado de servidor

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

Información de contexto

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

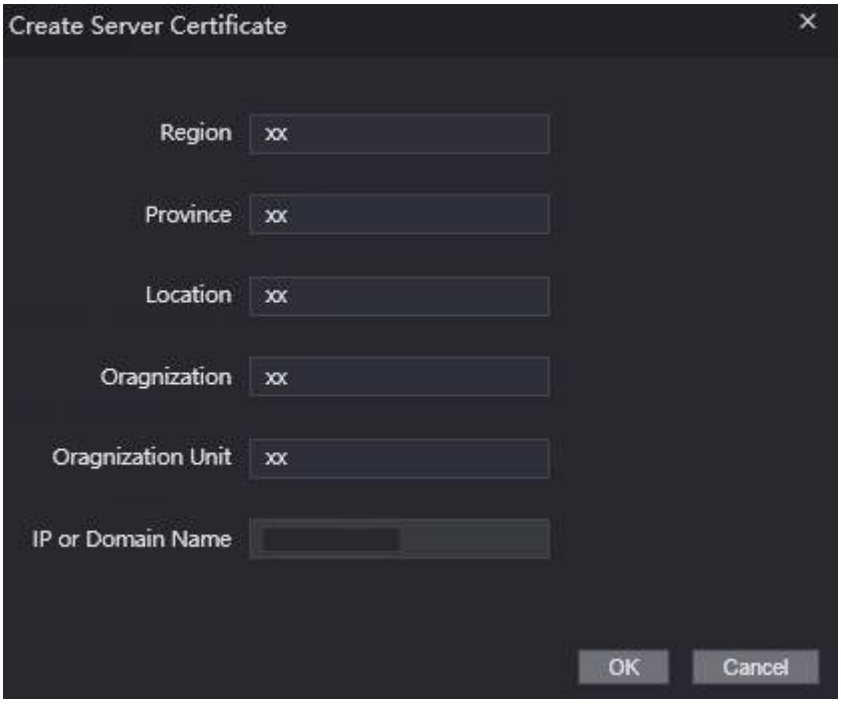
Procedimiento

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

Paso 2 información y haga clic**DE ACUERDO**.

El controlador de acceso se reiniciará.

Figura 3-43 Crear certificado de servidor



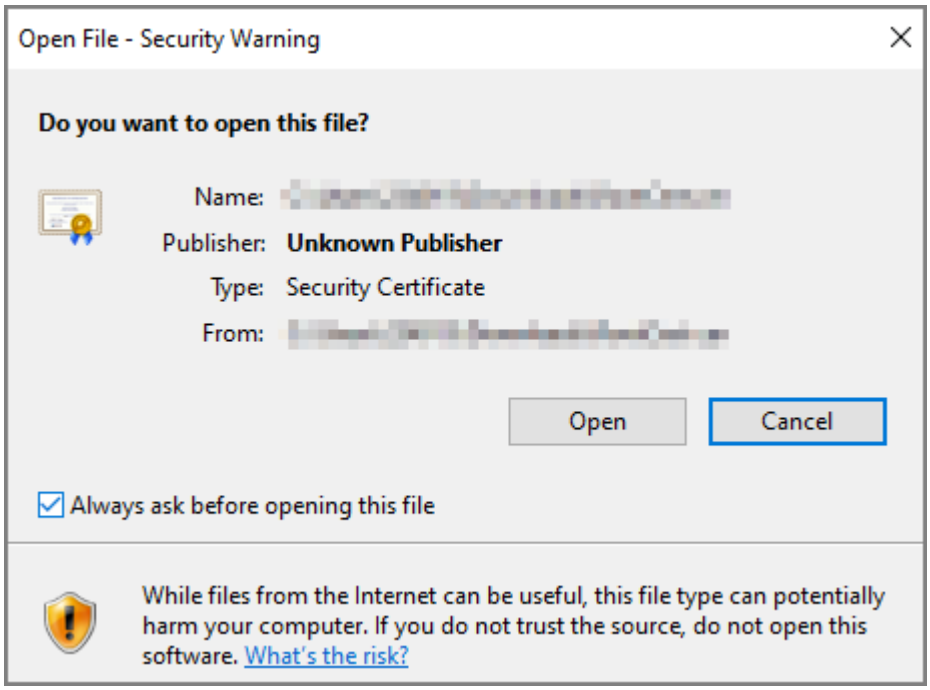
3.13.2.2 Descarga del certificado raíz

Procedimiento

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

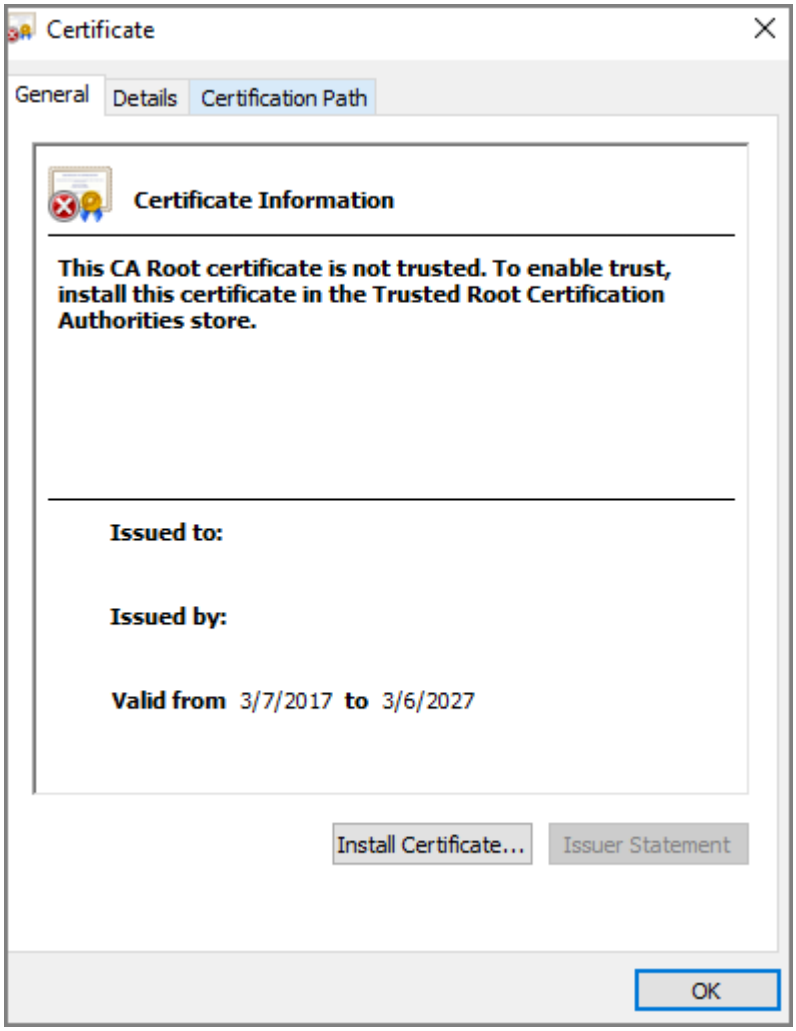
Paso 2 doble clic en el archivo que ha descargado y luego haga clic en**Abierto**.

Figura 3-44 Descarga de archivos



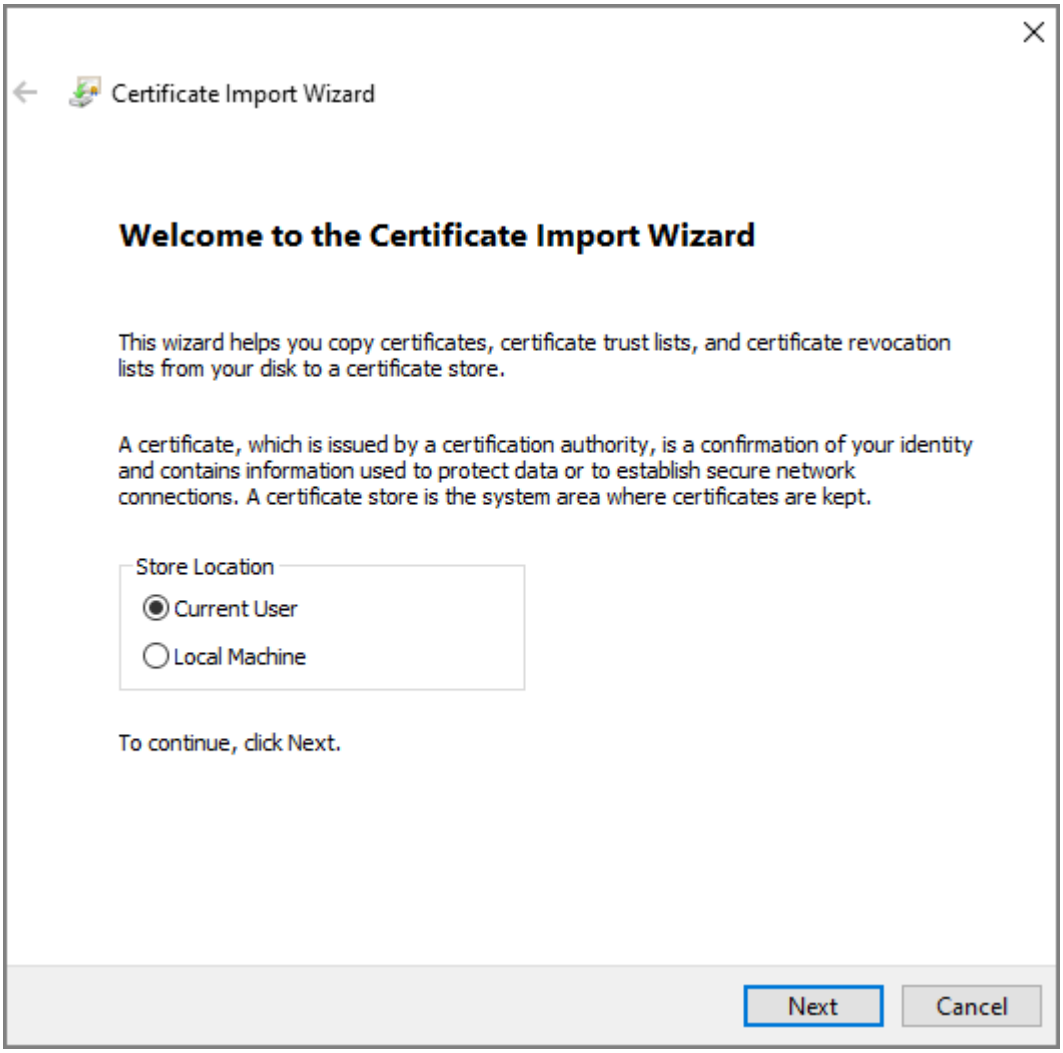
Paso 3 Hacer clic**Instalar certificado**.

Figura 3-45 Información del certificado



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

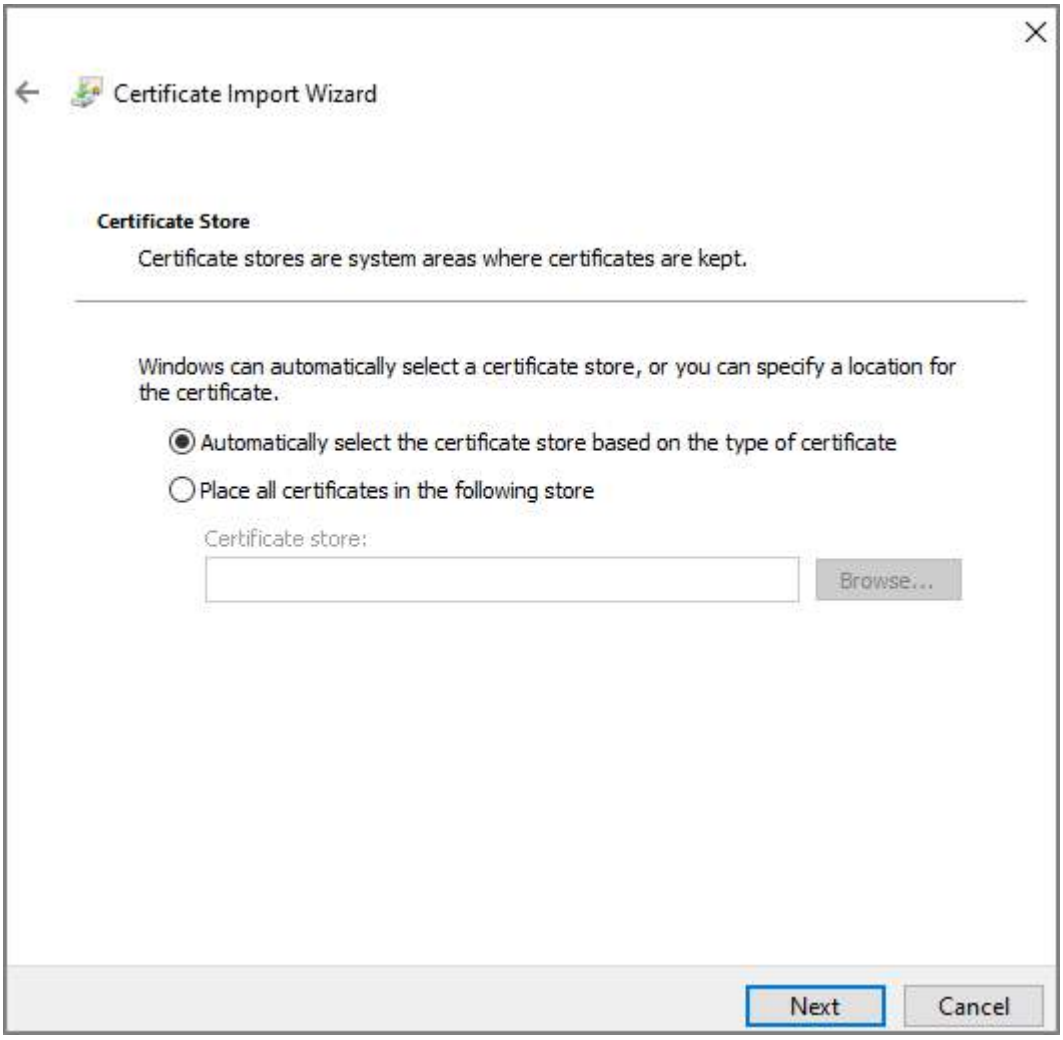
Figura 3-46 Asistente de importación de certificados (1)



Paso 5 Seleccione la ubicación de almacenamiento adecuada.

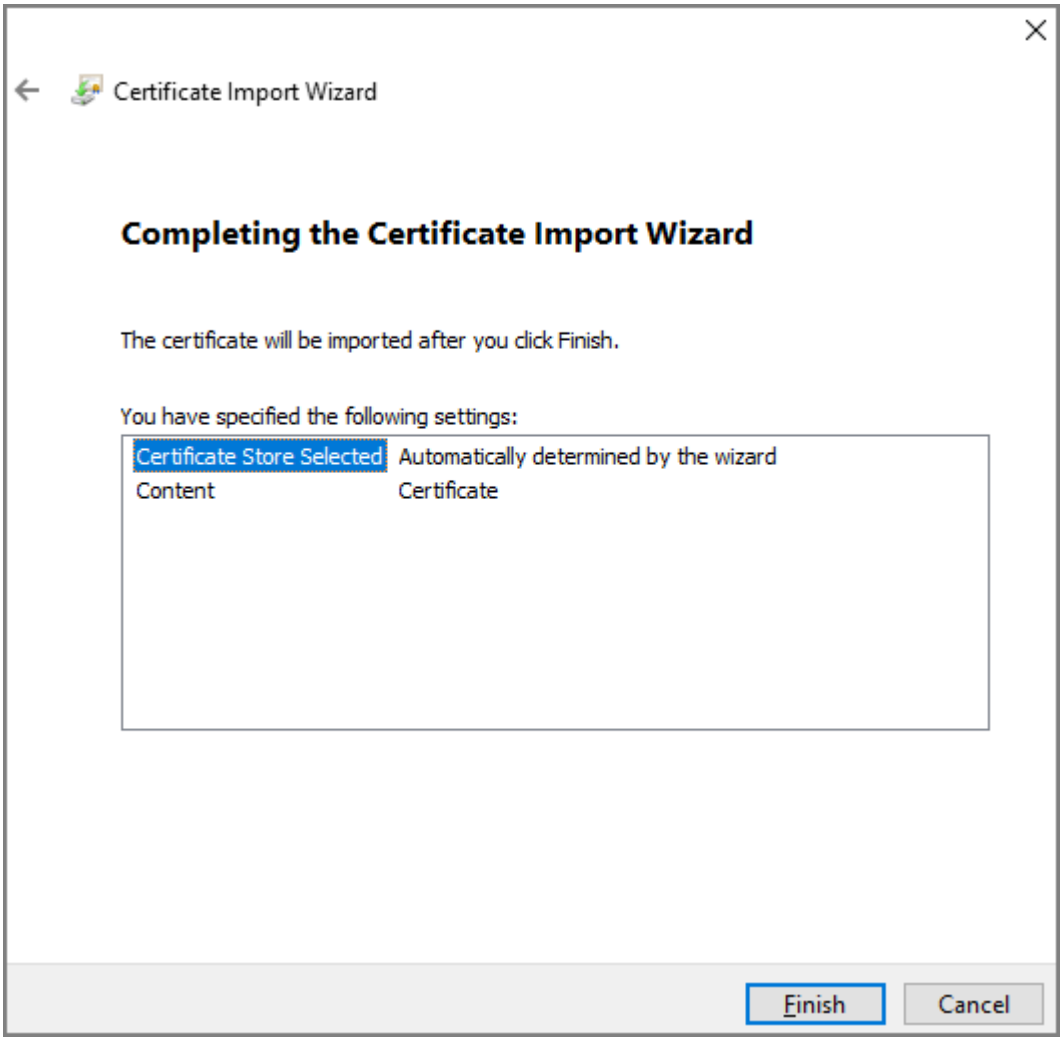
1. Seleccione**Coloque todos los certificados en el siguiente almacén**.
2. Haga clic**Navegar**para importar el certificado a la**Autoridades de certificación raíz de confianza** tienda y luego haga clic en**Próximo**.

Figura 3-47 Asistente de importación de certificados (2)



Paso 6 Hacer clic**Finalizar**.

Figura 3-48 Asistente de importación de certificados (3)



3.14 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.

3.14.1 Agregar usuarios

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

Procedimiento

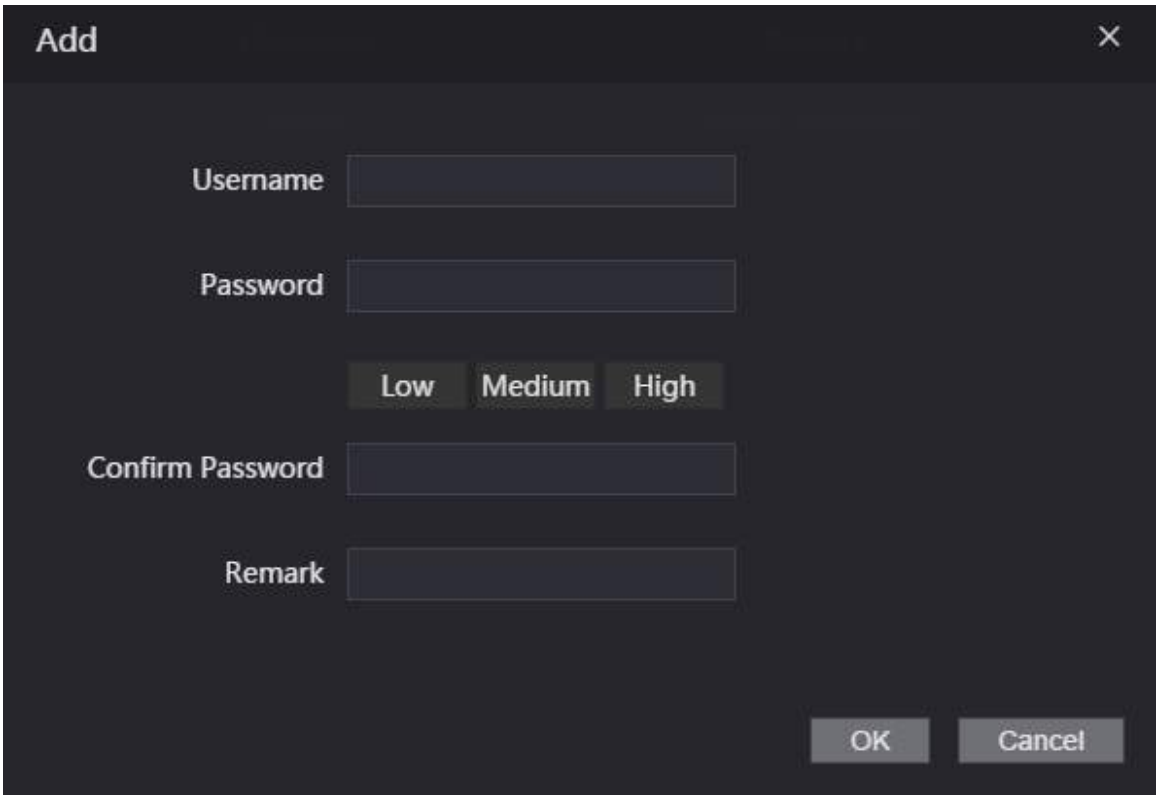
Paso 1 En la página de inicio, seleccione**Gestión de usuarios.**>**Gestión de usuarios.**

Paso 2 Haga clic en**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 puede tener hasta 31 caracteres y solo admite 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 caracteres especiales (excluyendo ' " ; : &).

Establezca una contraseña de alta seguridad siguiendo las indicaciones sobre la fortaleza de la contraseña.

Figura 3-49 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.

3.14.2 Agregar usuarios ONVIF

Información de contexto

Open Network Video Interface Forum (ONVIF), un foro industrial abierto y global creado para desarrollar un estándar abierto global para la interfaz de productos de seguridad basados en IP físicos, que permite la compatibilidad de diferentes fabricantes. Los usuarios de ONVIF tienen sus identidades verificadas a través del protocolo ONVIF. El usuario ONVIF predeterminado es admin.

Procedimiento

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

Paso 2 Haga clic en**Agregar**y luego configurar los parámetros.

Figura 3-50 Agregar usuario ONVIF

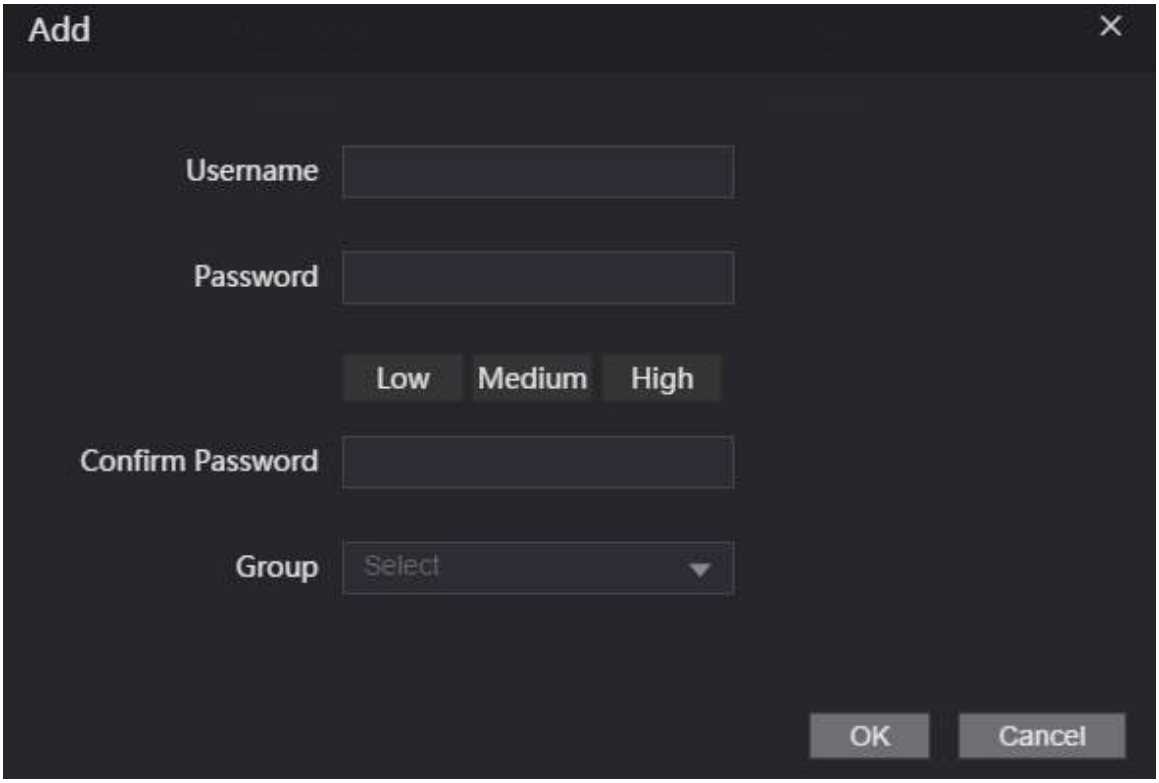


Tabla 3-24 Descripción del usuario de ONVIF

Parámetro	Descripción
Nombre de usuario	El nombre de usuario no puede ser el mismo que el de la cuenta existente. El nombre de usuario consta de hasta 31 caracteres y solo permite números, letras, guiones bajos, líneas intermedias, puntos o @.
Contraseña	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 caracteres especiales (excluyendo ' " ; : &).
Grupo	Hay tres grupos de permisos que representan diferentes niveles de permiso. ● admin: Puede ver y administrar otras cuentas de usuario en el Administrador de dispositivos ONVIF. ● Operador: No puede ver ni administrar otras cuentas de usuario en el Administrador de dispositivos ONVIF. ● Usuario: No puede ver ni administrar otras cuentas de usuario y registros del sistema en el Administrador de dispositivos ONVIF.

Paso 3 Hacer clic**DE ACUERDO**.

3.14.3 Visualización de usuarios en línea

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

3.15 Mantenimiento

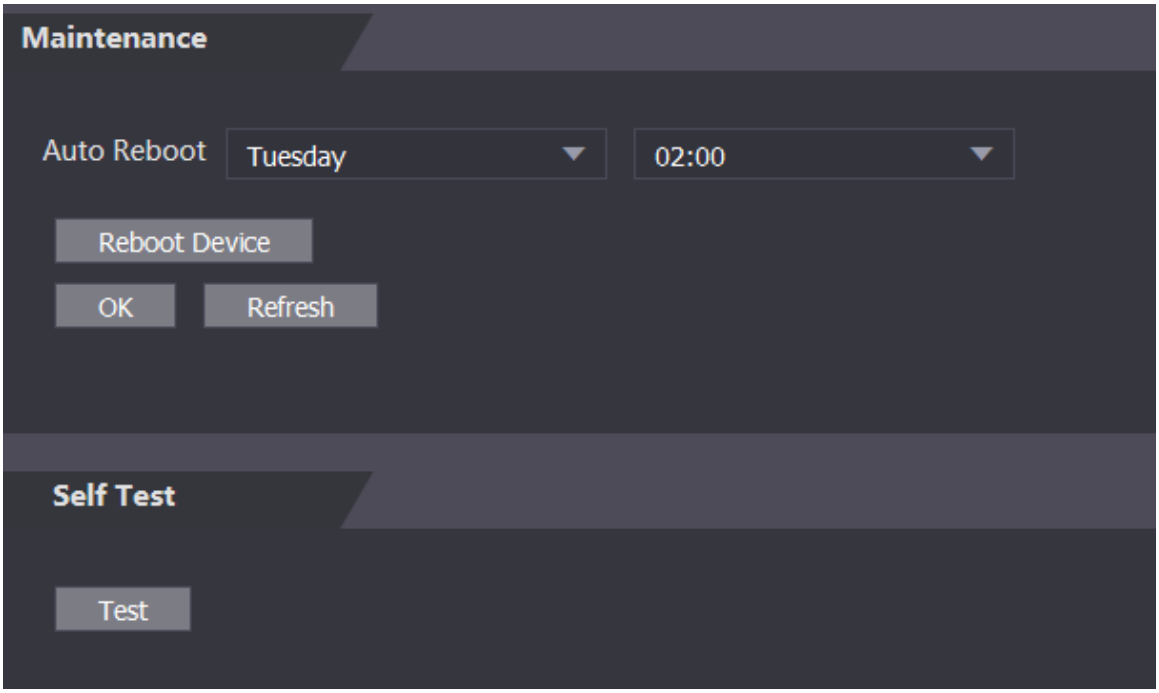
Puede reiniciar periódicamente el controlador de acceso durante el tiempo de inactividad para mejorar su rendimiento.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccione**Mantenimiento**.

Figura 3-51 Mantenimiento



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

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

3.16 Gestión de la configuración

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

3.16.1 Exportación/importación de archivos de configuración

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

Procedimiento

Paso 1 Inicie sesión en la página web.

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

Figura 3-52 Gestión de configuración



Paso 3 Exportar o importar archivos de configuración.

- Exportar archivo de configuración.

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

  La 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.

3.16.2 Restauración de los valores predeterminados de fábrica

Información de contexto

Restaurando el**Controlador de acceso**El cambio a las configuraciones predeterminadas provocará la 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.

3.17 Actualización del sistema

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

3.17.1 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 después de que se complete la actualización.

3.17.2 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.

3.18 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.

3.19 Visualización de registros

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

3.19.1 Registros del sistema

Ver y buscar registros del sistema.

Procedimiento

Paso 1 Inicie sesión en la página web.

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

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

Hacer clic**Respaldo**para descargar el registro del sistema.

3.19.2 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**.

3.19.3 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 log.

4. Configuración inteligente de PSS Lite

Esta sección presenta cómo administrar y configurar el controlador de acceso a través de Smart PSS Lite.

4.1 Instalación e inicio de sesión

Instale e inicie sesión en Smart PSS Lite. Para obtener más información, consulte el manual del 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 preguntas de seguridad para restablecer su contraseña cuando la olvide.

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

4.2 Agregar dispositivos

Debes agregar el dispositivo a Smart PSS Lite. Puedes agregarlos en lotes o de forma individual.

4.2.1 Agregar dispositivos uno por uno

Puede agregar dispositivos uno por uno ingresando sus direcciones IP o nombres de dominio.

Procedimiento

Paso 1 En el**Administrador de dispositivos**página, haga clic

Paso 2 **Agregar**. Configurar la información del dispositivo.

Figura 4-1 Agregar dispositivos

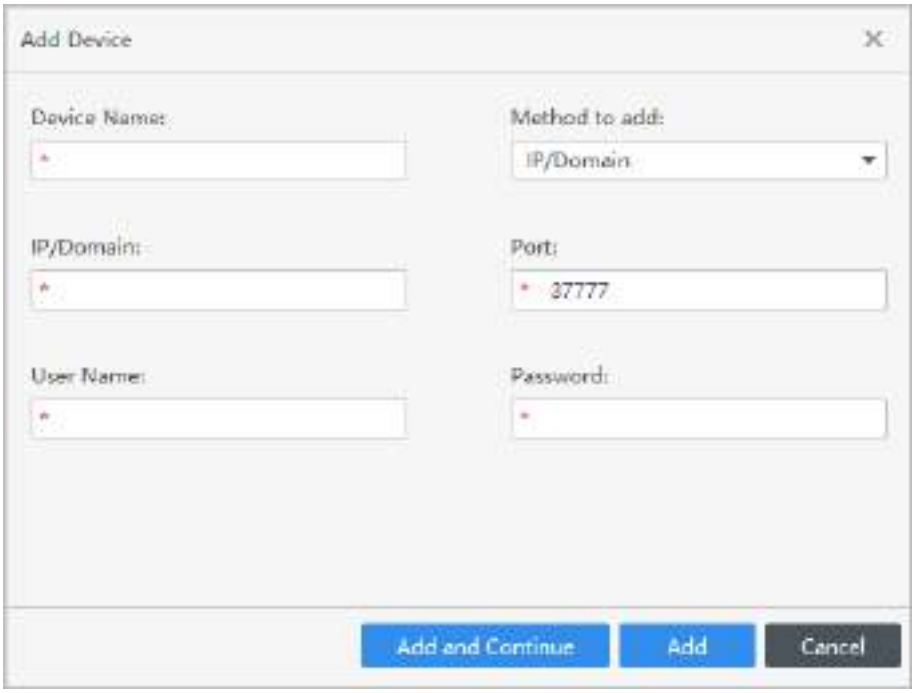


Tabla 4-1 Parámetros de adición de IP

Parámetro	Descripción
Nombre del dispositivo	Le recomendamos que nombre los dispositivos con el área de monitoreo para una fácil identificación.
Método para agregar	Seleccionar**IP/Dominio**. ● IP/Dominio: Ingrese la dirección IP o el nombre de dominio del dispositivo. ● SN: Ingrese el número de serie del dispositivo.
Puerto	Ingrese el número de puerto. El número de puerto predeterminado es 37777. El número de puerto real puede variar según los distintos modelos.
Nombre de usuario	Introduzca el nombre de usuario del dispositivo.
Contraseña	Introduzca la contraseña del dispositivo.

Paso 3 Hacer clic**Agregar**.

Puedes hacer clic**Agregar y continuar**para agregar más dispositivos.

4.2.2 Agregar dispositivos en lotes

Información de contexto

- Le recomendamos que agregue dispositivos mediante la búsqueda automática cuando necesite agregar dispositivos en lotes dentro del mismo segmento de red, o cuando se conoce el segmento de red pero no se conocen las direcciones IP exactas de los dispositivos.
- Cierre ConfigTool y DSS cuando configure dispositivos; de lo contrario, es posible que no pueda encontrar todos los dispositivos.

Procedimiento

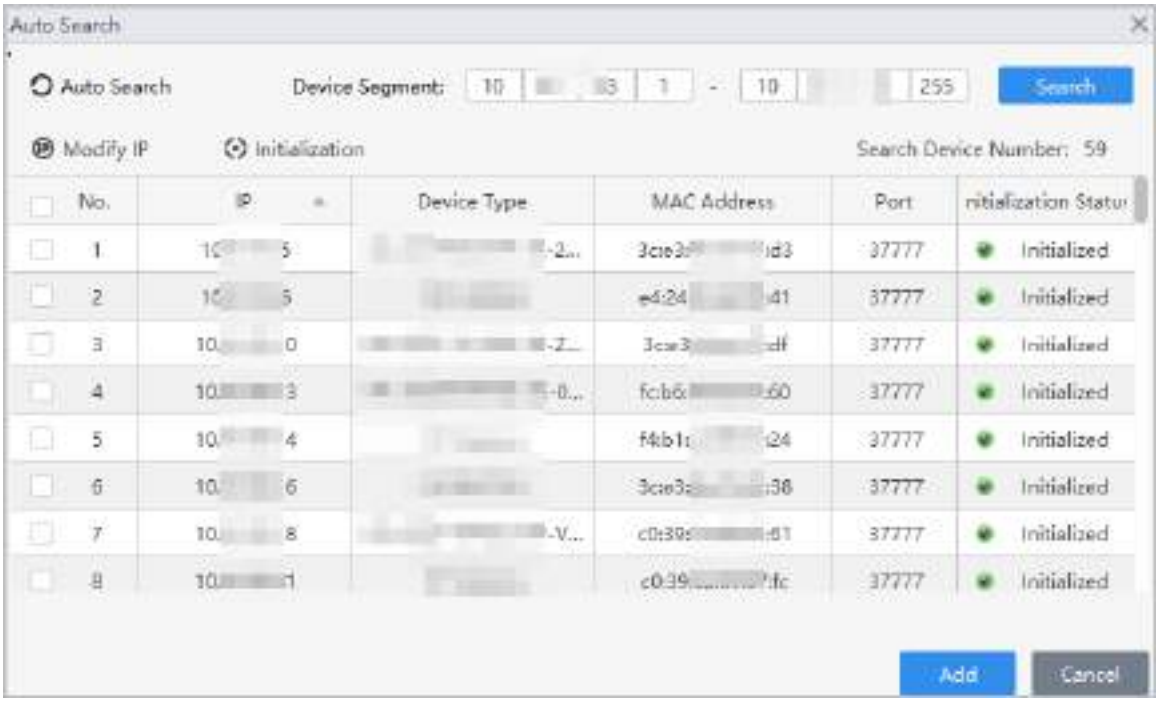
Paso 1 En el**Administrador de dispositivos**página, haga clic**Búsqueda automática**.

Paso 2 Seleccione un método de búsqueda.

- Búsqueda automática: Ingrese el nombre de usuario y la contraseña del dispositivo. El sistema buscará automáticamente los dispositivos que se encuentren en la misma red que su computadora.
- Búsqueda de segmentos de dispositivos: Ingrese el nombre de usuario y la contraseña del dispositivo y luego defina la IP inicial y la IP final. El sistema buscará automáticamente dispositivos en este rango de IP.

Puede seleccionar ambos métodos para que el sistema busque automáticamente dispositivos en la red a la que está conectada su computadora y otras redes.

Figura 4-2 Búsqueda de dispositivos



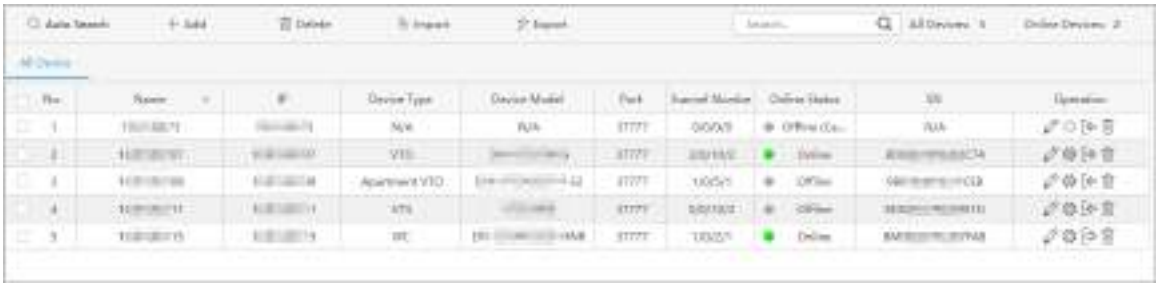
Paso 3 Haga clic en dispositivos y, a continuación, haga clic en**Agregar**.

Paso 4 Ingrese el nombre de usuario y la contraseña de inicio de sesión y luego haga clic en**DE ACUERDO**.

Resultados

Una vez que los dispositivos se hayan agregado correctamente, se mostrarán en esta página.

Figura 4-3 Dispositivos añadidos



4.3 Gestión de usuarios

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

4.3.1 Configuración del tipo de tarjeta

Establezca el tipo de tarjeta antes de asignar tarjetas a los usuarios. Por ejemplo, si la tarjeta asignada es una tarjeta de identificación, establezca el tipo de tarjeta en 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, no se podrá leer el número de tarjeta.

Paso 4 Hacer clic**DE ACUERDO**.

4.3.2 Agregar usuarios

4.3.2.1 Agregar usuarios uno por uno

Procedimiento

Paso 1 Seleccionar**Personal**>**Gerente de personal**>**Agregar**.

Paso 2 Ingrese información básica del personal.

1. Seleccione**Información básica**.
2. Agregue información básica del personal.
3. Tome una instantánea o cargue una imagen y luego haga clic**Finalizar**.

- El número de tarjeta se puede leer automáticamente o completar manualmente. Para leer automáticamente el número de tarjeta, seleccione el lector de tarjetas junto a**Tarjeta Nro.**, y luego coloque la tarjeta en el lector de tarjetas. El número de tarjeta se leerá automáticamente.
- Puede seleccionar varias cámaras USB para tomar fotografías.

- Establecer contraseña

  Hacer clic**Agregar**para agregar la contraseña.
- Configurar tarjeta

  a. Haga clic para seleccionar**Dispositivo**o**Emisor de la tarjeta**como lector de tarjetas.

  b. Agregar tarjetas.

  c. Después de agregarla, puede seleccionar la tarjeta como tarjeta principal o tarjeta de coacción, o reemplazar la tarjeta por una nueva, o eliminar la tarjeta.

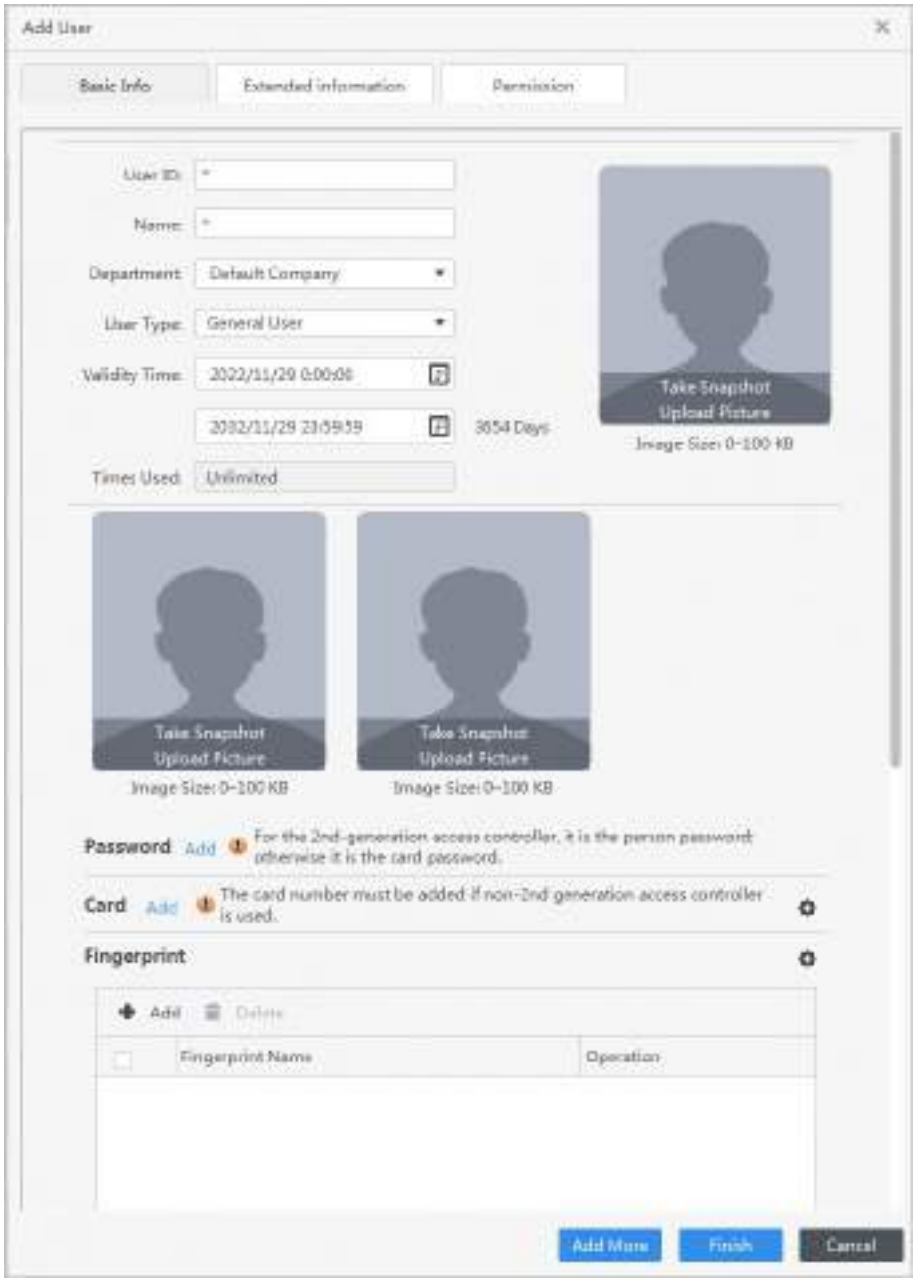
  d. Haga clic para mostrar el código QR de la tarjeta.

  Solo el número de tarjeta de 8 dígitos en modo hexadecimal puede mostrar el código QR de la tarjeta.
- Configurar huella digital

a. Haga clic para seleccionar**Dispositivo**o**Escáner de huellas dactilares**como recolector de huellas dactilares.

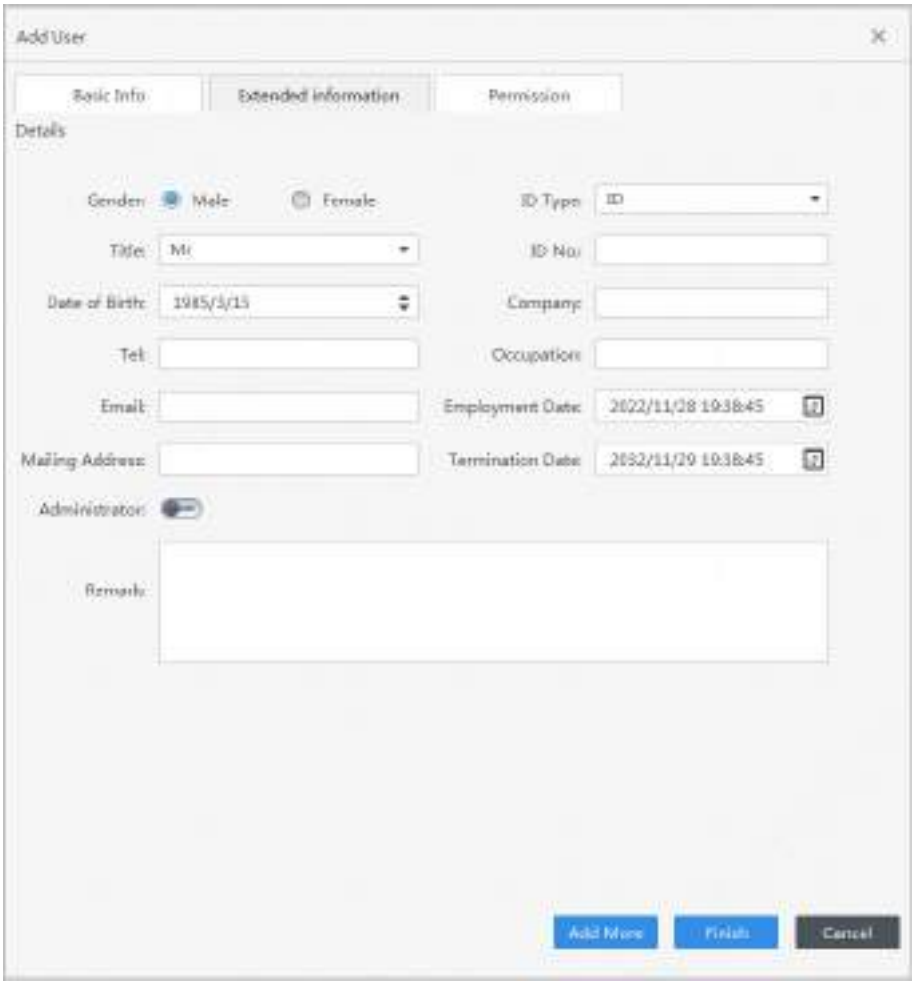
b. Agregar huella digital. Seleccionar**Agregar**>**Agregar huella digital**y luego presione el dedo sobre el escáner tres veces seguidas.

Figura 4-4 Agregar información básica



Paso 3 Hacer clic**Información ampliada**para agregar información ampliada del personal y luego haga clic en **Finalizar**Para salvar.

Figura 4-5 Agregar información extendida



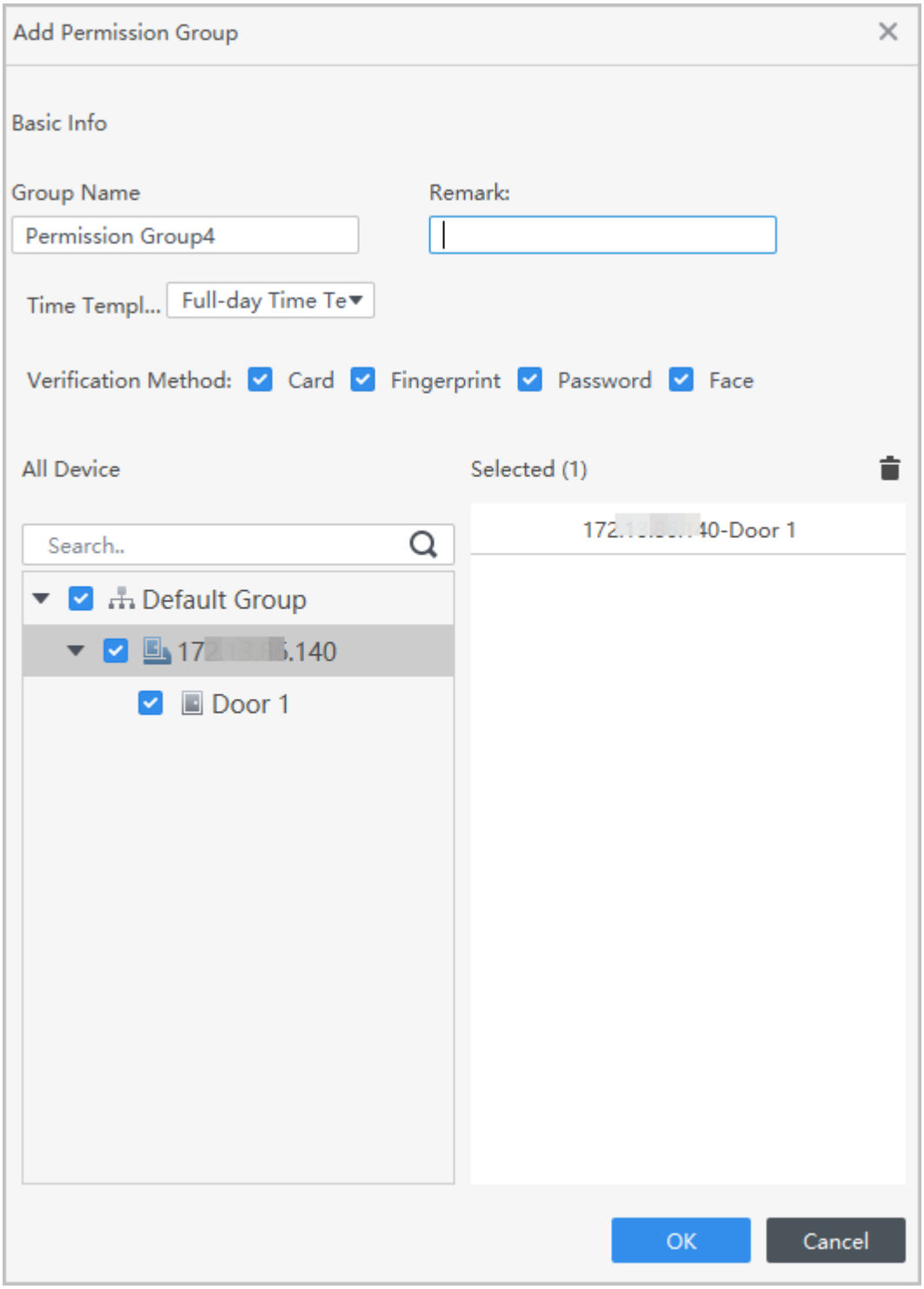
Paso 4 Configurar permisos.

1. Haga clic en .
2. Ingrese el nombre del grupo, observaciones (opcionales) y seleccione una plantilla de tiempo.
3. Seleccione los métodos de verificación y las puertas.

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

1. Seleccione**Grupo**.
2. Ingrese el nombre del grupo, observaciones (opcionales) y seleccione una plantilla de tiempo.
3. Seleccione los métodos de verificación y las puertas.
4. Haga clic**DE ACUERDO**.

Figura 4-6 Configurar grupos de permisos



Paso 6 Hacer clic**Finalizar**.

Después de completar la adición, puede hacer clic en el Para modificar información o agregar detalles en la lista personal.

4.3.2.2 Agregar usuarios en lotes

Procedimiento

Paso 1 Hacer clic**Gerente de personal**>**Actualización por lotes**>**Agregar por lotes**.

Paso 2 Seleccionar**Emisor de la tarjeta**o**Dispositivo**desde**Dispositivo**lista y luego configure los parámetros.

Figura 4-7 Agregar usuarios en lotes

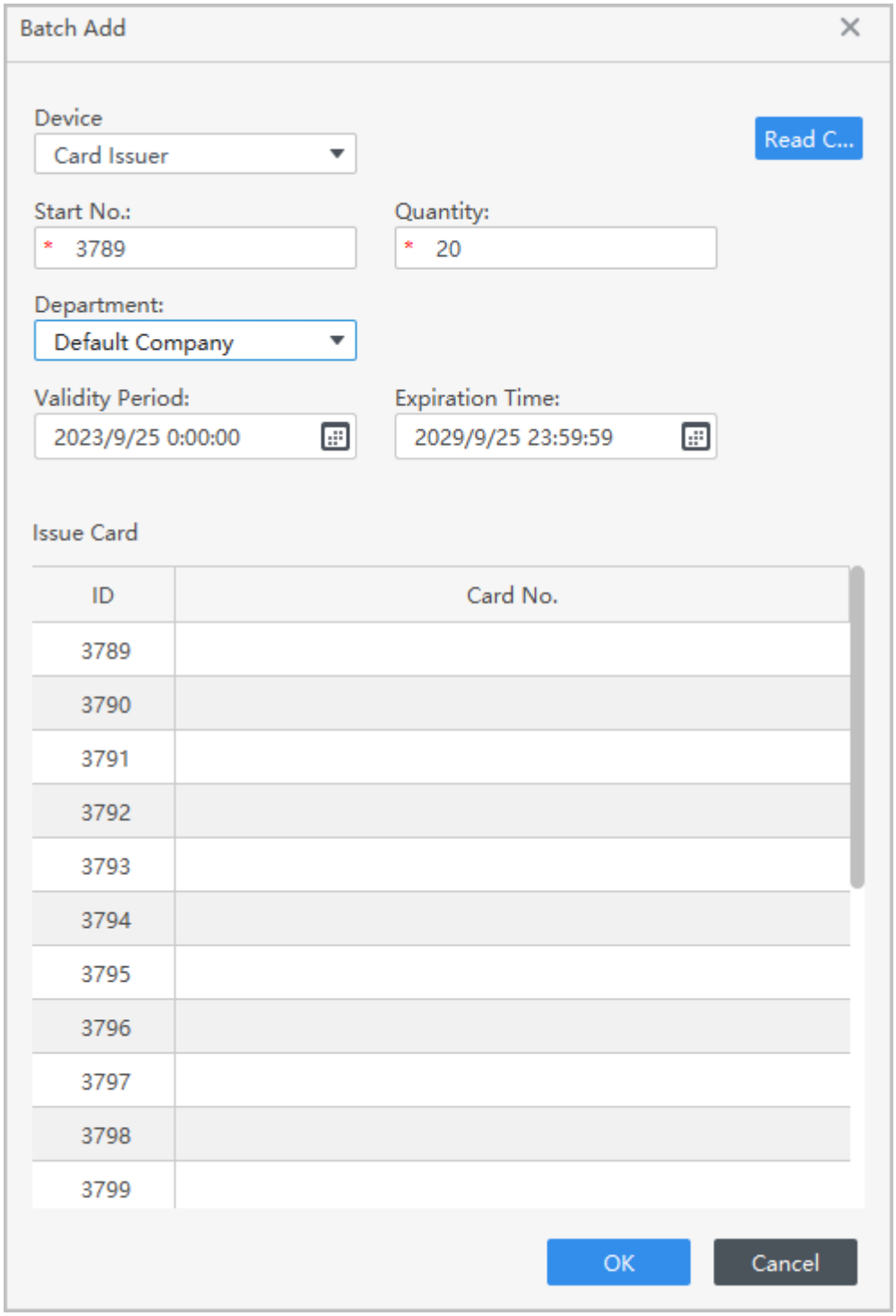


Tabla 4-2 Parámetros para agregar usuarios en lotes

Parámetro	Descripción
Inicio No.	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 3 Hacer clic**Leer la tarjeta n.°**y pase las tarjetas por el lector de tarjetas.

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

Paso 4 **ACUERDO**.

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 vincule a los usuarios con el grupo para que puedan desbloquear las puertas asociadas con el grupo de permisos.

Procedimiento

Paso 1 Hacer clic**Solución de acceso**>**Gerente de personal**>**Permiso**.

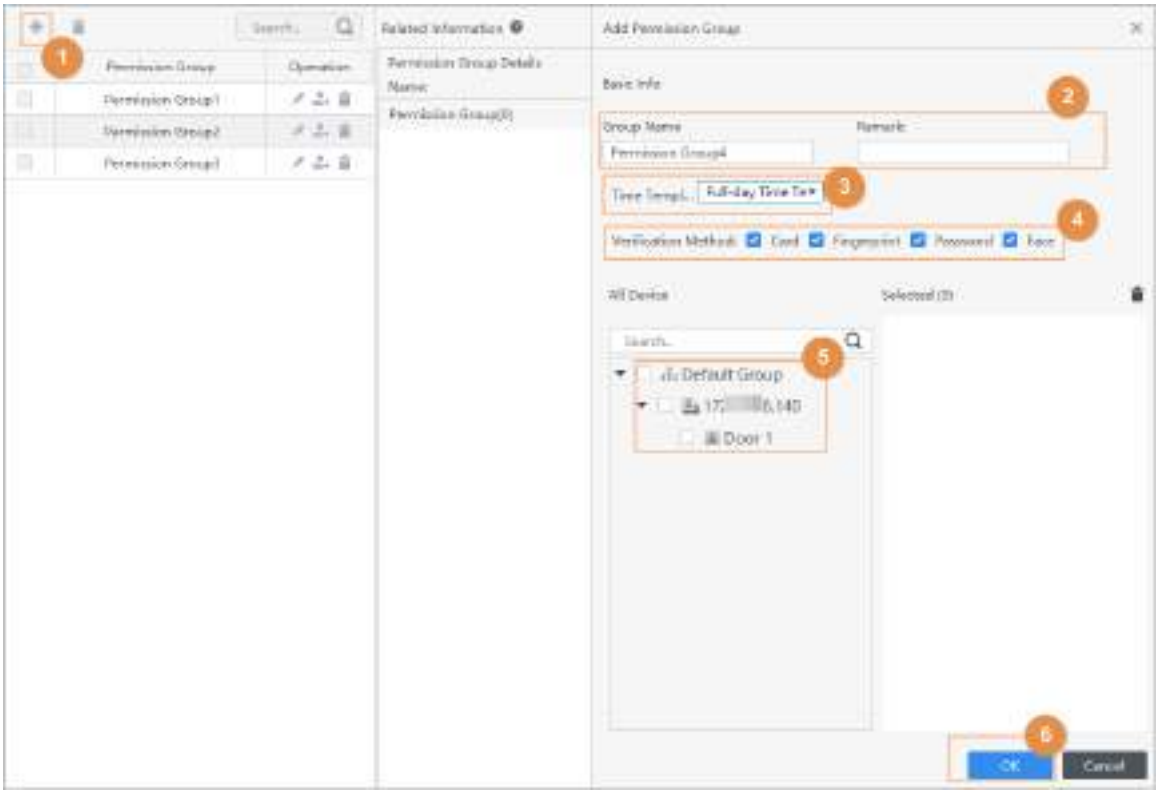
Paso 2 Haga clic en .

Paso 3 Ingrese el nombre del grupo, las observaciones (opcionales) y seleccione una plantilla de tiempo.

Paso 4 Seleccione los métodos de verificación y las puertas.

Paso 5 Hacer clic**DE ACUERDO**.

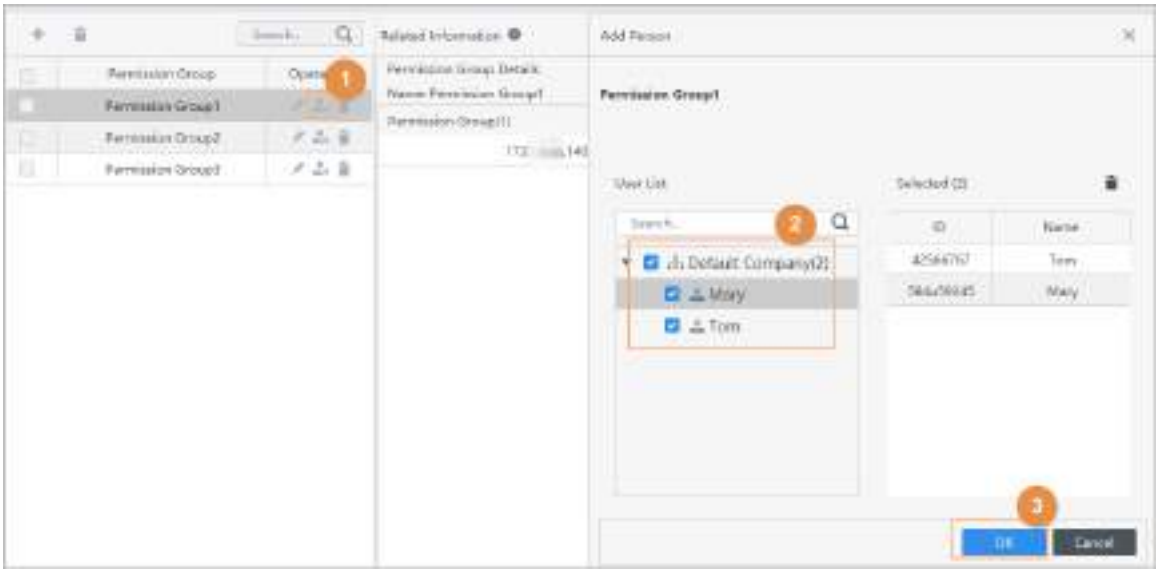
Figura 4-8 Crear un grupo de permisos



Paso 6 Hacer clic del grupo de permisos.

Paso 7 Seleccione usuarios para asociarlos con el grupo de permisos.

Figura 4-9 Agregar usuarios a un grupo de permisos



Paso 8 Hacer clic**DE ACUERDO**.

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

4.4 Gestión de acceso

4.4.1 Apertura y cierre remoto de la puerta

Puede supervisar y controlar la puerta de forma remota a través de la plataforma. Por ejemplo, puede abrir o cerrar la puerta de forma remota.

Procedimiento

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

Paso 2 Controla la puerta de forma remota.

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

Figura 4-10 Puerta abierta



- :Abre o cierra la puerta.
- :Ver el video en vivo de la puerta.

Operaciones relacionadas

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

4.4.2 Configuración de Siempre abierto y Siempre cerrado

Después de configurar siempre 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, haga

Paso 2 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

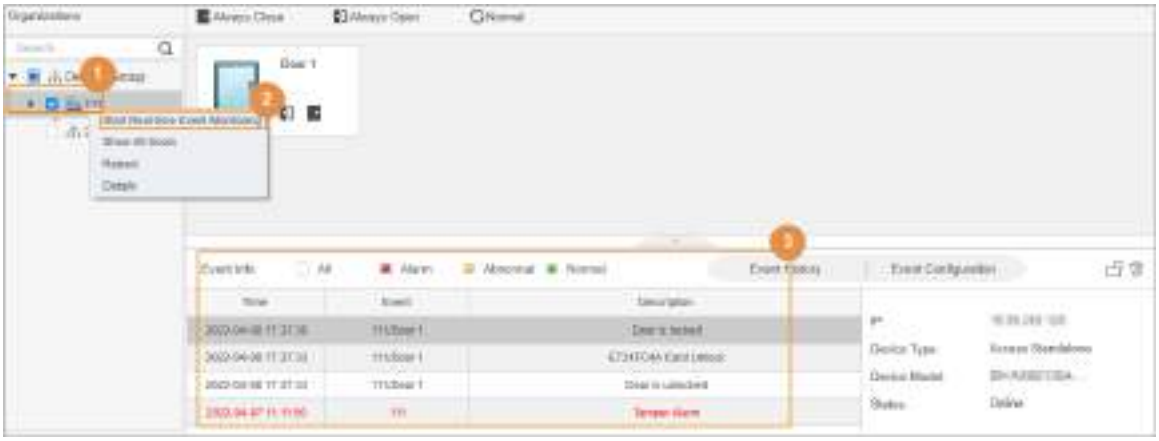
Paso 1 Hacer clic**Solución de acceso**>**Administrador de acceso**en la página de inicio.

Paso 2 Seleccione el dispositivo en el árbol de dispositivos, haga clic derecho en el dispositivo y luego seleccione**Iniciar el monitoreo de eventos en tiempo real**.

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

Hacer clic**Detener 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 dispositivo.
- Reiniciar: reiniciar el dispositivo.
- 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 intercomunicador.

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 Ingresa el número

Paso 2 de la habitación y luego toque .

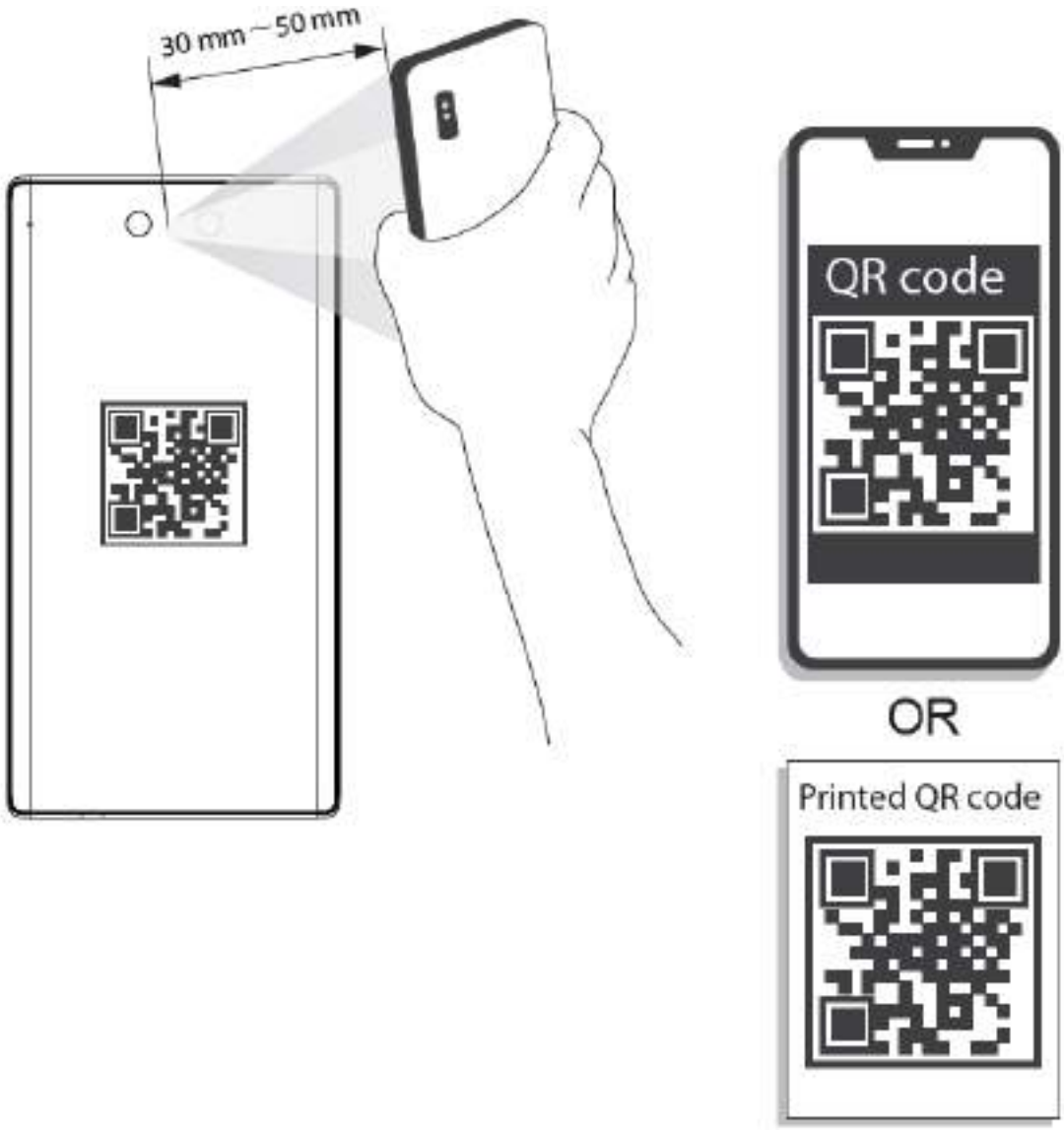
Apéndice 2 Puntos importantes del código QR

Exploración

Controlador de acceso: coloque el código QR en su teléfono a una distancia de 30 mm a 50 mm de la lente de lectura del código QR. Admite códigos QR de 22 mm × 22 mm a 50 mm × 50 mm y de menos de 128 bytes de tamaño.

- La distancia de detección del código QR varía según los bytes y el tamaño del código QR.
- Asegúrese de que el código QR esté alineado con la lente y evite la luz solar directa.

Apéndice Figura 2-1 Escaneo de código QR



Apéndice 3 Puntos importantes de la toma de huellas dactilares

Instrucciones de registro

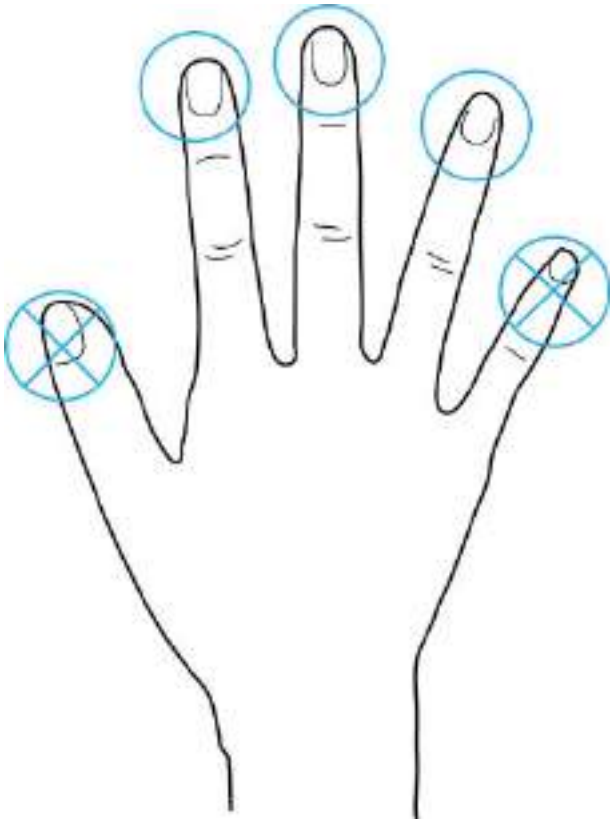
Al registrar la huella dactilar, preste atención a los siguientes puntos:

- 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

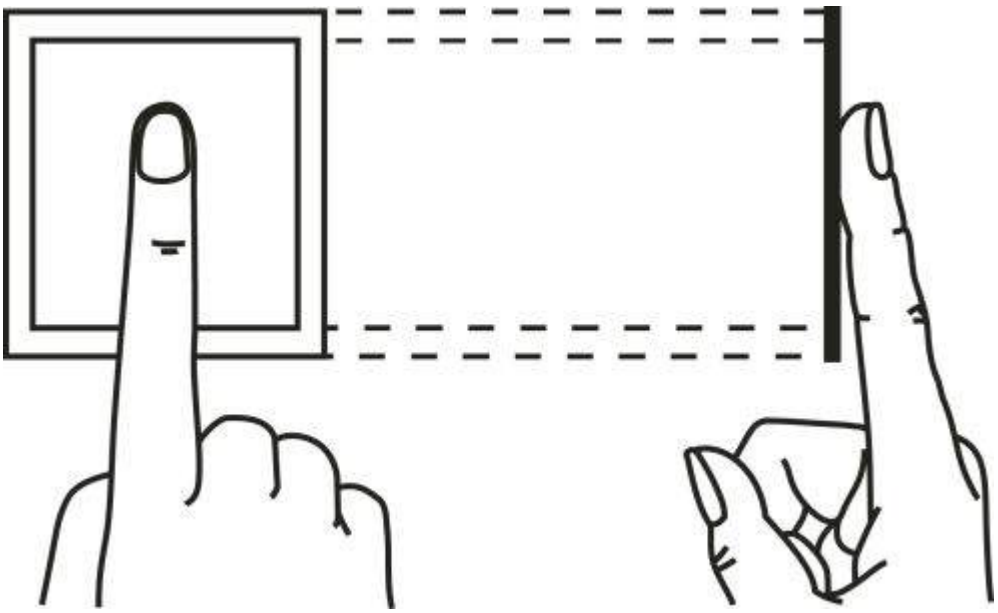
Se recomiendan los dedos índice, medio y anular. Los pulgares y meñiques no se pueden colocar fácilmente en el centro de la grabación.

Apéndice Figura 3-1 Dedos recomendados

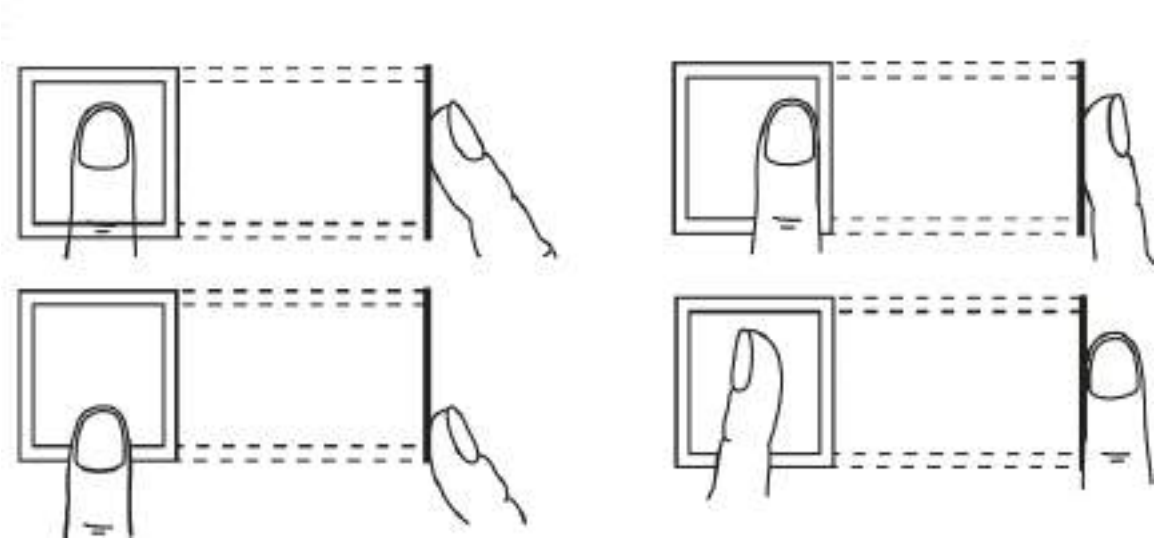


Cómo presionar su huella digital en el escáner

Apéndice Figura 3-2 Colocación correcta



Apéndice Figura 3-3 Colocación incorrecta



Apéndice 4 Puntos importantes del rostro

Registro

Antes de la inscripción

- Las gafas, los sombreros y las barbas podrían influir en el rendimiento del reconocimiento facial.
- No te cubras las cejas cuando uses sombrero.
- No cambie mucho su estilo de barba si usa el dispositivo; de lo contrario, el reconocimiento facial podría fallar.
- Mantén tu cara limpia.
- Mantenga el dispositivo al menos a 2 metros de distancia de fuentes 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

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

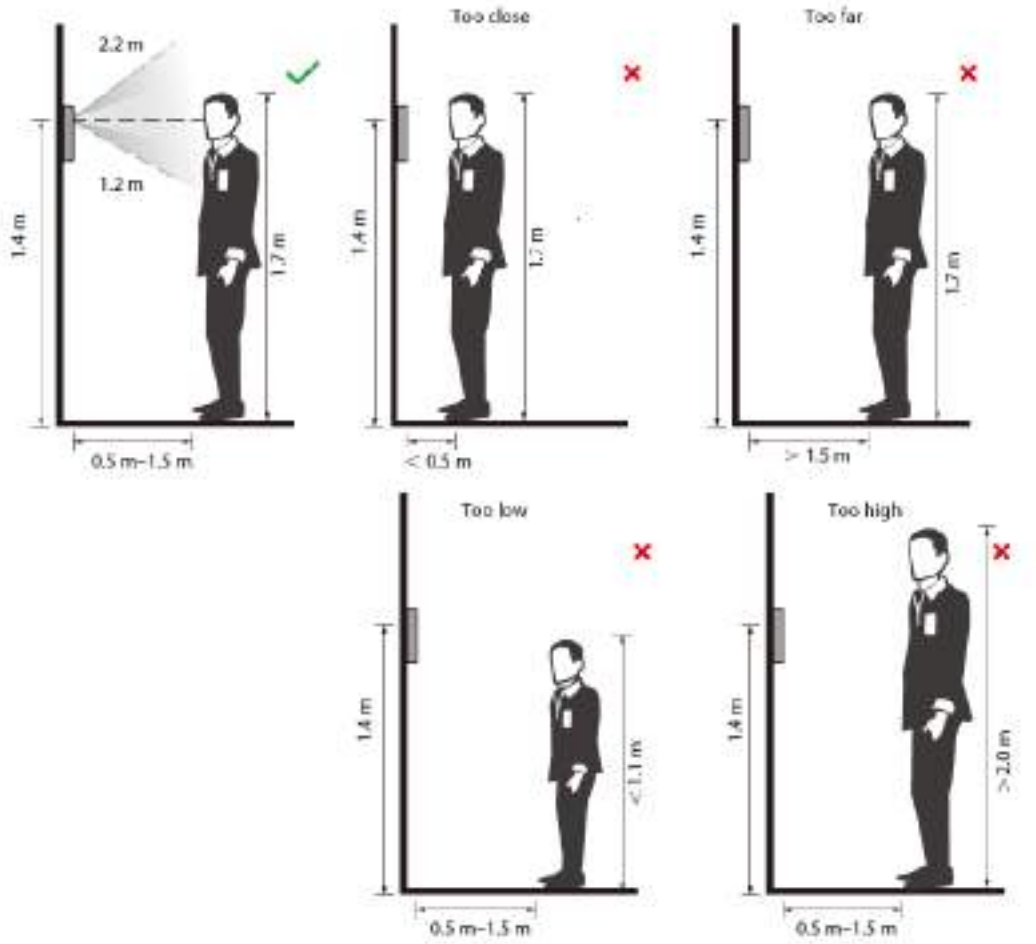
- No mueva la cabeza ni el cuerpo, de lo contrario el registro podría fallar.
- Evite que aparezcan 2 caras en el cuadro de captura al mismo tiempo.

Posición de la cara

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

La posición de la cara que se muestra a continuación es solo de referencia y puede diferir de la situación real.

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 gafas, sombreros, barbas pobladas ni otros adornos faciales que influyan en la grabación de imágenes del rostro.
- Con los ojos abiertos, sin expresiones faciales y dirigiendo la 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 entre caras



- Al importar imágenes de rostros a través de la plataforma de administración, asegúrese de que la resolución de la imagen esté dentro del rango de 150 × 300 píxeles a 600 × 1200 píxeles. Se recomienda que la resolución sea mayor a 500 × 500 píxeles, el tamaño de la imagen sea menor a 100 KB y el nombre de la imagen y el ID de la persona sean iguales.
- Asegúrese de que el rostro ocupe más de 1/3 pero no más de 2/3 del área total de la imagen y que la relación de aspecto no exceda 1:2.

Apéndice 5 Recomendaciones de seguridad

Gestión de cuentas

1.**Utilice contraseñas complejas**

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de caracteres: 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 repetidos, como 111, aaa, etc.

2.**Cambie las contraseñas periódicamente**

Se recomienda cambiar periódicamente la contraseña del dispositivo para reducir el riesgo de que sea adivinada o descifrada.

3.**Asignar cuentas y permisos de forma adecuada**

Agregue usuarios de forma adecuada según los requisitos de servicio y administración y asigne conjuntos de permisos mínimos a los usuarios.

4.**Habilitar la función de bloqueo de cuenta**

La función de bloqueo de cuenta está habilitada de forma predeterminada. Se recomienda mantenerla habilitada para proteger la seguridad de la cuenta. Después de varios intentos fallidos de ingresar la contraseña, se bloquearán la cuenta correspondiente y la dirección IP de origen.

5.**Establecer y actualizar la información de restablecimiento de contraseña de manera oportuna**

El dispositivo admite la función de restablecimiento de contraseña. Para reducir el riesgo de que esta función sea utilizada por actores maliciosos, si hay algún cambio en la información, modifíquela a tiempo. Al configurar las preguntas de seguridad, se recomienda no utilizar respuestas fáciles de adivinar.

Configuración del servicio

1.**Habilitar HTTPS**

Se recomienda que habilite HTTPS para acceder a servicios web a través de canales seguros.

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

Si el contenido de sus datos de audio y video es muy importante o confidencial, se recomienda utilizar la función de transmisión encriptada para reducir el riesgo de que sus datos de audio y video sean espiados durante la transmisión.

3.**Desactiva los servicios no esenciales y utiliza el modo seguro**

Si no es necesario, se recomienda desactivar algunos servicios como SSH, SNMP, SMTP, UPnP, AP hotspot, etc., para reducir las superficies de ataque.

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

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

4.**Cambiar HTTP y otros puertos de servicio predeterminados**

Se recomienda cambiar el puerto predeterminado de HTTP y otros servicios a cualquier puerto entre 1024 y 65535 para reducir el riesgo de ser adivinado por actores de amenazas.

Configuración de red

1.**Habilitar lista de permitidos**

Se recomienda activar la función de lista de permitidos y permitir que solo las direcciones IP de la lista de permitidos accedan al dispositivo. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del dispositivo compatible a la lista de permitidos.

2.**Vinculación de dirección MAC**

Se recomienda vincular la dirección IP de la puerta de enlace a la dirección MAC del dispositivo para reducir el riesgo de suplantación de ARP.

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

Para garantizar mejor la seguridad de los dispositivos y reducir los posibles riesgos cibernéticos, se recomienda lo siguiente:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde la red externa;
- De acuerdo con las necesidades reales de la red, particione la red: si no hay demanda de comunicación entre las dos subredes, se recomienda utilizar VLAN, puerta de enlace y otros métodos para particionar la red para lograr el aislamiento de la red;
- Establecer un sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso ilegal a terminales de la red privada.

Auditoría de seguridad

1.**Comprobar usuarios en línea**

Se recomienda revisar periódicamente a los usuarios en línea para identificar usuarios ilegales.

2.**Comprobar el registro del dispositivo**

Al ver los registros, puede obtener información sobre las direcciones IP que intentan iniciar sesión en el dispositivo y las operaciones clave de los usuarios registrados.

3.**Configurar el registro de red**

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

Seguridad del software

1.**Actualizar el firmware a tiempo**

De acuerdo con las especificaciones operativas estándar de la industria, el firmware de los dispositivos debe actualizarse a la última versión a tiempo para garantizar que el dispositivo tenga las últimas funciones y seguridad. Si el dispositivo está conectado a la red pública, se recomienda habilitar la función de detección automática de actualizaciones en línea, para obtener la información de actualización de firmware publicada por el fabricante de manera oportuna.

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

Se recomienda descargar y utilizar el software de cliente más reciente.

Protección física

Se recomienda que realice una protección física para los dispositivos (especialmente los dispositivos de almacenamiento), como colocar el dispositivo en una sala de máquinas y un gabinete dedicados y tener control de acceso.

y gestión de claves para evitar que personal no autorizado dañe el hardware y otros equipos periféricos (por ejemplo, disco flash USB, puerto serie).