Controlador de acceso por reconocimiento facial Web 5.0

Manual de usuario

V1.2.2

Prefacio

General

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

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Significado
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.
ESD	Dispositivos sensibles a la electrostática. Indica un dispositivo que es sensible a descargas electrostáticas.
ELECTRIC SHOCK	Indica alto voltaje peligroso. Tenga cuidado para evitar entrar en contacto con la electricidad.
LASER RADIATION	Indica un peligro de radiación láser. Tenga cuidado de evitar la exposición a un rayo láser.
TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
NOTE	Proporciona información adicional como complemento al texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.2.2	Actualizada la asistencia configuración de permisos.	junio 2024
V1.2.1	Se actualizaron la configuración del intercomunicador, la configuración de control de acceso y más.	mayo 2024
V1.2.0	Comunicación actualizada configuración, configuración de control de acceso y más.	noviembre 2023
V1.1.0	Actualizado el manual.	octubre 2023
V1.0.0	Primer lanzamiento.	junio 2023

Aviso de protección de privacidad

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

Acerca del Manual

- El manual es sólo para referencia. Pueden encontrarse ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas incurridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es sólo para referencia. Es posible que se encuentren ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones de productos pueden provocar que aparezcan algunas diferencias entre el producto real y el manual. Comuníquese con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Pueden existir errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en este manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de dar una explicación final.

Salvaguardias y advertencias importantes

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

Requisito de transporte

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

Requisito de almacenamiento

Guarde el dispositivo en condiciones permitidas de humedad y temperatura.

requerimientos de instalación

- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- Cumpla estrictamente con el código y las normas locales de seguridad eléctrica. Asegúrese de que el voltaje ambiental sea estable y cumpla con los requisitos de suministro de energía del dispositivo.
- No conecte el Dispositivo a dos o más tipos de fuentes de alimentación para evitar daños al Dispositivo.
- El uso inadecuado de la batería podría provocar un incendio o una explosión.
- Siga los requisitos eléctricos para alimentar el dispositivo.
  - A continuación se detallan los requisitos para seleccionar un adaptador de corriente.
    - La fuente de alimentación debe cumplir con los requisitos de las normas IEC 60950-1 e IEC 62368-1.
    - El voltaje debe cumplir con los requisitos SELV (voltaje extra bajo de seguridad) y no exceder los estándares ES-1.
    - Cuando la potencia del dispositivo no supera los 100 W, la fuente de alimentación debe cumplir con los requisitos de LPS y no ser superior a PS2.
  - Recomendamos utilizar el adaptador de corriente proporcionado con el dispositivo.
  - Al seleccionar el adaptador de corriente, los requisitos de la fuente de alimentación (como el voltaje nominal) están sujetos a la etiqueta del dispositivo.

- El personal que trabaja en alturas debe tomar todas las medidas necesarias para garantizar la seguridad personal, incluido el uso de casco y cinturones de seguridad.
- No coloque el Dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- Instale el dispositivo sobre una superficie estable para evitar que se caiga.
- Instale el dispositivo en un lugar bien ventilado y no bloquee su ventilación.

- Utilice un adaptador o fuente de alimentación de gabinete proporcionado por el fabricante.
- Utilice los cables de alimentación recomendados para la región y cumplan con las especificaciones de potencia nominal.
- El Dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del Dispositivo esté conectada a una toma de corriente con conexión a tierra de protección.

Requisitos de operación

- Compruebe si la fuente de alimentación es correcta antes de su uso.
- Conecte el dispositivo a tierra protectora antes de encenderlo.
- No desenchufe el cable de alimentación en el costado del dispositivo mientras el adaptador esté encendido.
- Opere el dispositivo dentro del rango nominal de entrada y salida de energía.
- Utilice el dispositivo en condiciones permitidas de humedad y temperatura.
- No deje caer ni salpique líquido sobre el Dispositivo y asegúrese de que no haya ningún objeto lleno de líquido sobre el Dispositivo para evitar que el líquido fluya hacia él.
- No desmonte el dispositivo sin instrucción profesional.
- Este producto es un equipo profesional.
- El Dispositivo no es adecuado para su uso en lugares donde es probable que haya niños presentes.

Tabla de contenido

1. Información general

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

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

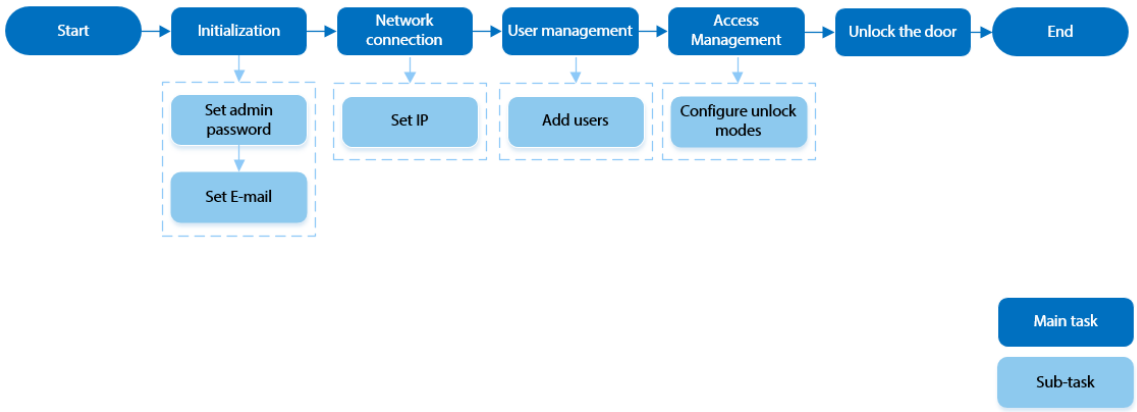
- Las configuraciones pueden diferir según los modelos del producto; consulte el producto real.
- Los dispositivos con pantalla no táctil deben conectarse a un mouse para realizar configuraciones. Este manual utiliza como ejemplo el dispositivo con pantalla táctil.
- Algunos modelos admiten la conexión de módulos de extensión como el módulo de código QR, el módulo de huellas dactilares y más. El tipo de módulos de extensión que los dispositivos admiten pueden diferir; consulte el producto real.

2 operaciones locales

- Las configuraciones pueden diferir según el producto real.
- Los modelos con pantalla no táctil necesitan conectar un mouse USB con cable. Esta sección utiliza como ejemplo los modelos con pantalla táctil.
- Los módulos de expansión externos solo están disponibles en modelos selectos.
- Es posible que vea que algunos textos de la interfaz de usuario no se muestran debido al espacio limitado. Mantenga presionado el texto durante 3 segundos y se mostrará.

2.1 Procedimiento de configuración básica

Figura 2-1 Procedimiento de configuración básica



2.2 Iconos comunes

Tabla 2-1 Descripción de iconos

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

2.3 Pantalla de espera

Puede desbloquear la puerta mediante rostros, tarjetas, contraseñas y códigos QR. También puedes realizar llamadas a través de la función de intercomunicador. Los métodos de desbloqueo pueden diferir según los modelos del producto.

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

Figura 2-2 Pantalla de espera

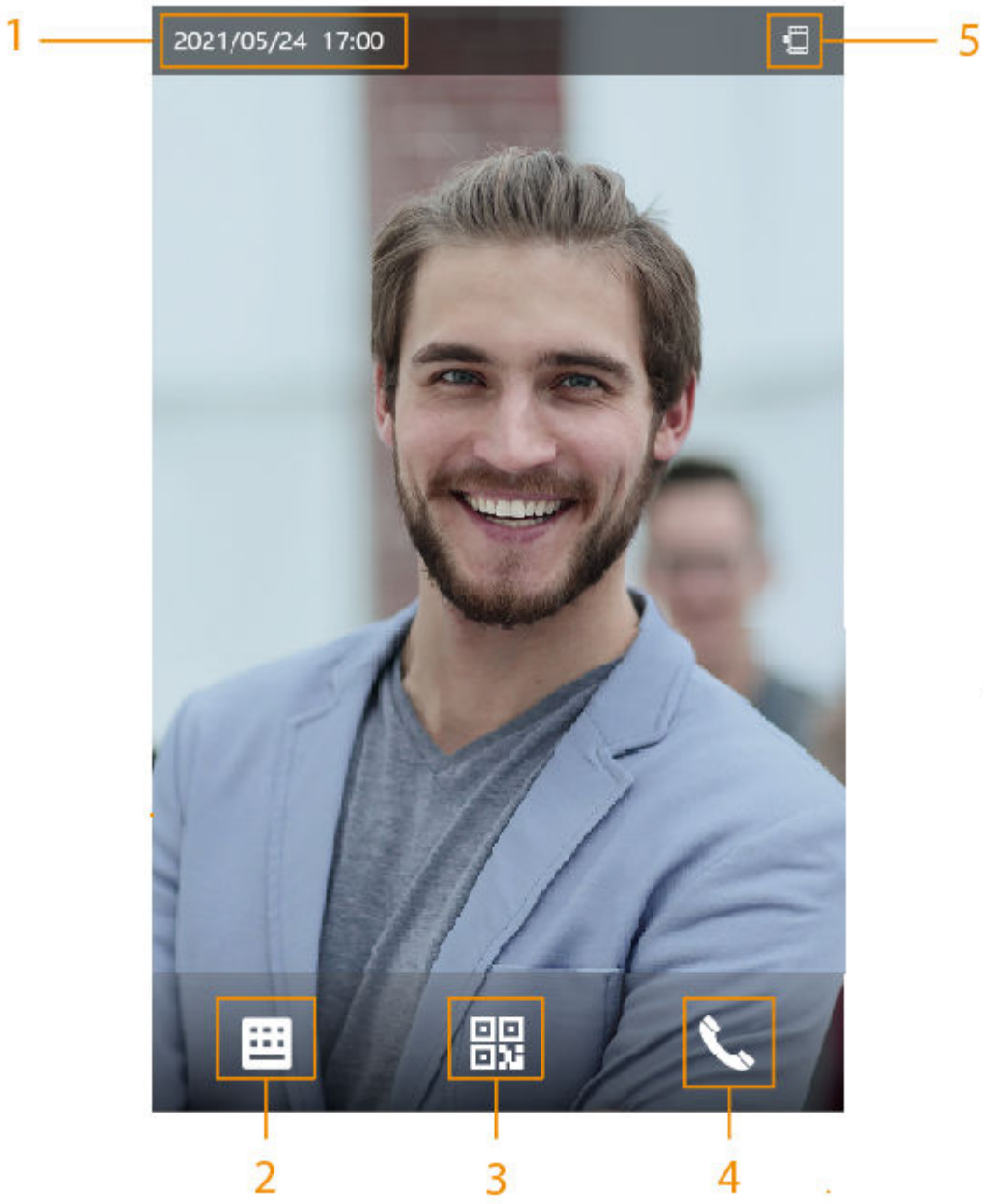


Tabla 2-2 Descripción de la pantalla de inicio

No.	Nombre	Descripción
1	Fecha y hora	Fecha y hora actual.
2	Contraseña	Ingrese la contraseña de usuario o la contraseña de administrador o la contraseña temporal para desbloquear la puerta.
3	Código QR	Toque el ícono del código QR y escanee el código QR para desbloquear la puerta. Para modelos que cuentan con módulo de código QR independiente o se conecta un módulo de expansión QR. El icono no se mostrará. Simplemente puede colocar su código QR frente a la lente del dispositivo o del módulo de expansión y se escaneará automáticamente.
4	Intercomunicador	• Cuando el Dispositivo funciona como servidor, puede llamar al VTO y al VTH. • Cuando la plataforma de gestión funciona como servidor, el Dispositivo puede llamar al VTO, al VTS y a la plataforma de gestión. • Cuando funciona con DMSS, puede llamar a DMSS.
5	Indicación de estado	Muestra el estado de Wi-Fi, red, módulo de extensión, USB y más. Los módulos de extensión y Wi-Fi solo están disponibles en modelos selectos. Puede tocar para ingresar a la pantalla de AP Wi-Fi. Para obtener más información, consulte "2.11.1.4 Configuración de AP Wi-Fi"

2.4 Inicialización

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

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

2.5 Iniciar sesión

Inicie sesión en el menú principal para configurar el Dispositivo. Solo la cuenta de administrador y la cuenta de administrador pueden ingresar al menú principal del Dispositivo. 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 dispositivo, pero no tiene permisos de acceso a la puerta.

- Cuenta de administrador: puede iniciar sesión en el menú principal del dispositivo y tiene permisos de acceso a la puerta.

Procedimiento

Paso 1 Mantenga presionada la pantalla de espera durante 1,5 segundos.

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

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

  La función de huella digital solo está disponible en modelos selectos.
- Card Punch: 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 Restablecer la contraseña

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

Procedimiento

Paso 1 Mantenga presionada la pantalla de espera durante 1,5 segundos.

Paso 2 Grifo**administración**y luego toque una vez en el área en blanco de la pantalla. Hacer clic

Paso 3 **Has olvidado tu contraseña**.

Etapa 4 Lea el mensaje en pantalla y luego haga clic en**Ingresar**.

Paso 5 Grifo**Código QR**y luego escanee el código QR.

Paso 6 Envíe los resultados del escaneo a la dirección de correo electrónico designada.

Recibirás un código de seguridad en tu dirección de correo electrónico.

- Después de escanear el código QR, recibirá un código de seguridad en su dirección de correo electrónico vinculada. Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, dejará de ser válido.
- Se generarán hasta dos códigos de seguridad cuando se escanee el mismo código QR. Si el código de seguridad deja de ser válido, actualice el código QR y escanéelo nuevamente.

Paso 7 Ingrese el código de seguridad.

Si se ingresa el código de seguridad incorrecto 5 veces seguidas, la cuenta de administrador se congelará durante 5 minutos.

Paso 8 Hacer clic**Próximo**.

Paso 9 Restablecer y confirmar la contraseña.

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

Paso 10 Hacer clic**DE ACUERDO**.

2.7 Métodos de desbloqueo

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

2.7.1 Desbloqueo por Tarjetas

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

Esta función solo está disponible en modelos seleccionados.

2.7.2 Desbloqueo facial

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

2.7.3 Desbloqueo por Contraseña de Usuario

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

Procedimiento

Paso 1 Grifo en la pantalla de espera.

Paso 2 Grifo**Desbloquear por contraseña**y luego ingrese el ID de usuario y la contraseña. Grifo**DE**

Paso 3 **ACUERDO**.

2.7.4 Desbloqueo mediante contraseña de administrador

Ingrese solo la contraseña de administrador para desbloquear la puerta. La puerta se puede desbloquear mediante la contraseña de administrador, excepto en el caso de la puerta siempre cerrada. Un dispositivo permite solo una contraseña de administrador.

Requisitos previos

La contraseña de administrador fue configurada. Para obtener más información, consulte "2.8.3 Configuración de la contraseña de desbloqueo del administrador".

Procedimiento

Paso 1 Grifo en la pantalla de espera.

Paso 2 Grifo**Desbloquear mediante contraseña de administrador**y luego ingrese la contraseña de administrador.

Paso 3 Grif

La contraseña de administrador no se puede utilizar para desbloquear cuando el estado de la puerta está configurado en estado siempre cerrado.

2.7.5 Desbloqueo mediante código QR

Procedimiento

Paso 1 En la pantalla de espera, toque

El ícono del código QR se muestra solo después de ir a**Funciones**>**Acceso directo a la interfaz de reconocimiento facial**para permitir**Código QR**.

Paso 2 Coloque su código QR frente a la lente.

2.7.6 Desbloqueo por huella digital

Coloque su dedo en el escáner de huellas digitales. Esta función solo está disponible en modelos selectos.

2.7.7 Desbloqueo mediante contraseña temporal

Desbloquee la puerta con la contraseña temporal.

Procedimiento

Paso 1 Agregue el dispositivo a DMSS.

DMSS generará una contraseña temporal que le permitirá desbloquear la puerta antes de que caduque.

Paso 2 En la pantalla de inicio, toque y luego toque**Desbloquear por contraseña**

Paso 3 **temporal**. Ingrese la contraseña temporal y luego toque .

2.8 Gestión de personas

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

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

2.8.1 Agregar usuarios

Procedimiento

Paso 1 Sobre el**Menú principal**, seleccionar**Gestión de personas**>**Crear**

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

Figura 2-3 Agregar nuevo usuario

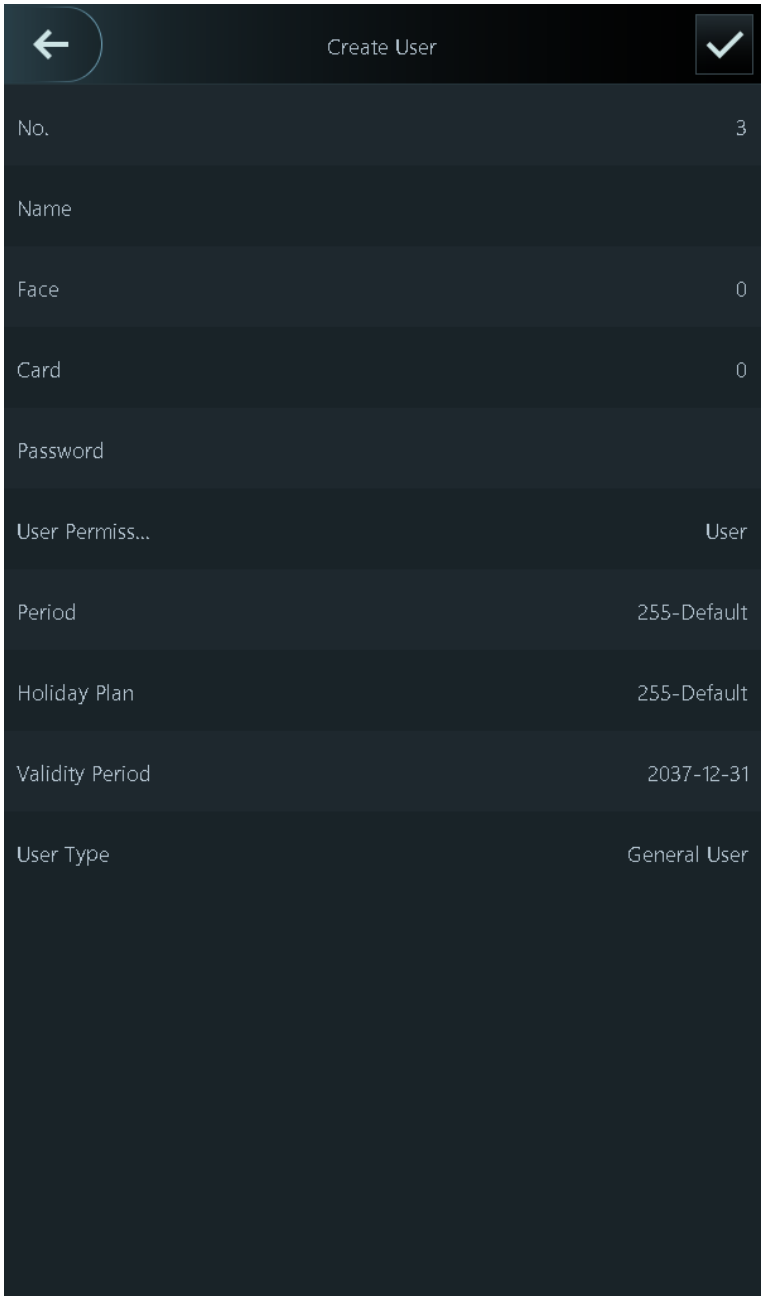


Tabla 2-3 Descripción de los parámetros

Parámetro	Descripción
No.	El número es como una identificación de empleado, que puede ser números, letras y sus combinaciones, y la longitud máxima del número es de 30 caracteres.
Nombre	El nombre puede tener hasta 32 caracteres (incluidos números, símbolos y letras).

Parámetro	Descripción
FP	Registrar huellas dactilares. Un usuario puede registrar hasta 3 huellas digitales y usted puede configurar una huella digital para la huella digital de coacción. Se activará una alarma cuando se utilice la huella digital de coacción para desbloquear la puerta.  ● La función de huella digital solo está disponible en modelos selectos. ● No recomendamos configurar la primera huella digital como huella digital de coacción. ● Un usuario sólo puede establecer una huella digital de coacción. ● La función de huellas dactilares está disponible si el dispositivo admite la conexión de un módulo de extensión de huellas dactilares.
Rostro	Coloque su rostro dentro del marco y se capturará automáticamente una imagen del rostro. Puede registrarse nuevamente si no está satisfecho con el resultado.
Tarjeta	Un usuario puede registrar hasta 5 tarjetas como máximo. Ingrese el número de su tarjeta o pase la tarjeta y luego el dispositivo 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.  ● Esta función solo está disponible en modelos seleccionados. ● Un usuario sólo puede configurar una tarjeta de coacción.
Contraseña	Ingrese la contraseña de usuario. La longitud máxima de la contraseña es de 8 dígitos. La contraseña de coacción suma 1 según el último dígito de la contraseña de desbloqueo. Por ejemplo, si la contraseña de usuario es 12345, la contraseña de coacción será 12346; si la contraseña de usuario es 789 y la contraseña de coacción es 780. Se activará una alarma de coacción cuando se utilice una contraseña de coacción para desbloquear la puerta.
Permiso de usuario	● **Usuario**:Los usuarios solo tienen acceso a la puerta o permisos de asistencia. ● **Administración**:Los administradores pueden configurar el dispositivo además de los permisos de acceso y asistencia.
Período	Las personas pueden desbloquear la puerta o pasar lista durante el período definido. Para obtener detalles sobre cómo configurar períodos, consulte "3.6.8.1 Configuración de períodos de tiempo".
Plan de vacaciones	Las personas pueden desbloquear la puerta o pasar lista durante el feriado definido. Para obtener detalles sobre cómo configurar períodos, consulte "3.6.8.2 Configuración de planes de vacaciones".
Período de validez	Establezca una fecha en la que expirarán los permisos de acceso y asistencia de la persona.

Parámetro	Descripción
Tipo de usuario	• **Usuario general**:Los usuarios generales pueden desbloquear la puerta. • **Usuario de la lista de bloqueo**:Cuando los usuarios en la lista de bloqueo desbloquean la puerta, se activará una alarma de lista de bloqueo. • **Usuario invitado**:Los huéspedes pueden desbloquear la puerta dentro de un período definido o durante una determinada cantidad de veces. Una vez transcurrido el período definido o los tiempos de desbloqueo, no pueden desbloquear la puerta. • **Usuario de patrulla**:Los usuarios de patrulla pueden controlar la asistencia en el dispositivo, pero no tienen permisos de entrada. • **Usuario VIP**:Cuando VIP abra la puerta, el personal de servicio recibirá una notificación. • **Otro usuario**:Cuando desbloqueen la puerta, la puerta permanecerá desbloqueada durante 5 segundos más. Esta función no es efectiva cuando la verificación remota está habilitada. • **Usuario personalizado 1/Usuario personalizado 2**:Lo mismo con los usuarios generales.
Departamento	Seleccione departamentos, lo cual es útil al configurar horarios de departamentos. Para saber cómo crear departamentos, consulte "2.10.1 Configurar departamentos". Esta función solo está disponible en modelos seleccionados.
Modo de programación	• Horario de departamento: aplique horarios de departamento al usuario. • Horario personal: Aplicar horarios personales al usuario. Para saber cómo configurar horarios personales o departamentales, consulte "2.10.4 Configuración de horarios de trabajo". ◇ Esta función solo está disponible en modelos seleccionados. ◇ Si configura el modo de programación en programación de departamento aquí, la programación personal que haya configurado para el usuario en**Asistencia**>**Programar configuración**>**Horario personal**quedar inválido.

Paso 3 Grif

2.8.2 Ver información del usuario

Procedimiento

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

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

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

Operaciones relacionadas

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

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

2.8.3 Configuración de la contraseña de desbloqueo del administrador

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

Procedimiento

Paso 1 Sobre el**Menú principal**pantalla, seleccione**Usuario**>**Contraseña de desbloqueo de administrador**.

Paso 2 Grifo**Contraseña de desbloqueo de administrador**y luego ingrese una contraseña. Active la función de

Paso 3 desbloqueo de administrador.

2.9 Gestión del control de acceso

Puede configurar ajustes para puertas como el modo de desbloqueo, vinculación de alarma y horarios de puertas. Los modos de desbloqueo disponibles pueden diferir según el modelo del producto.

2.9.1 Configurar el método de desbloqueo

2.9.1.1 Configurar combinaciones de desbloqueo

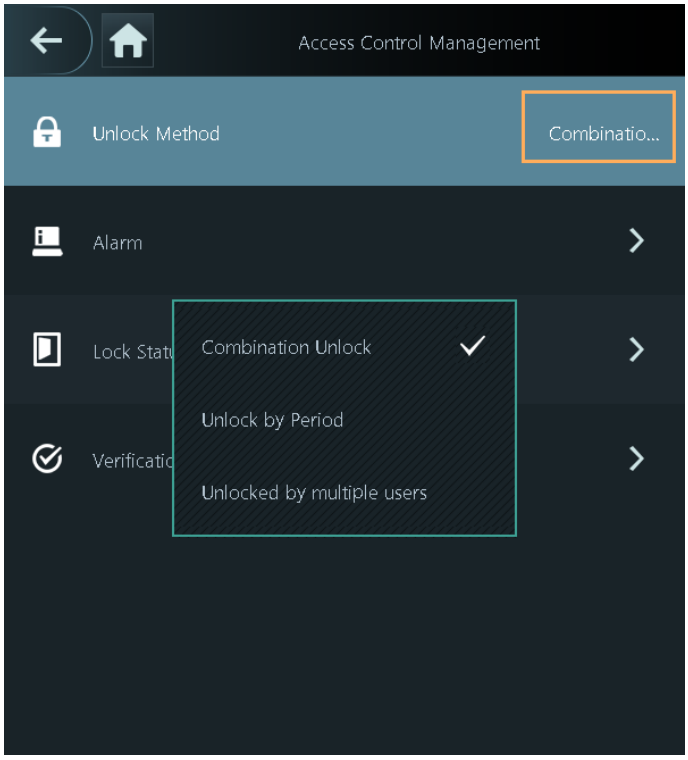
Utilice tarjeta, huella digital, rostro, contraseña o sus combinaciones para desbloquear la puerta. Los modos de desbloqueo disponibles pueden diferir según el modelo del producto.

Procedimiento

Paso 1 Seleccionar**Gestión de control de acceso**>**Método de desbloqueo**.

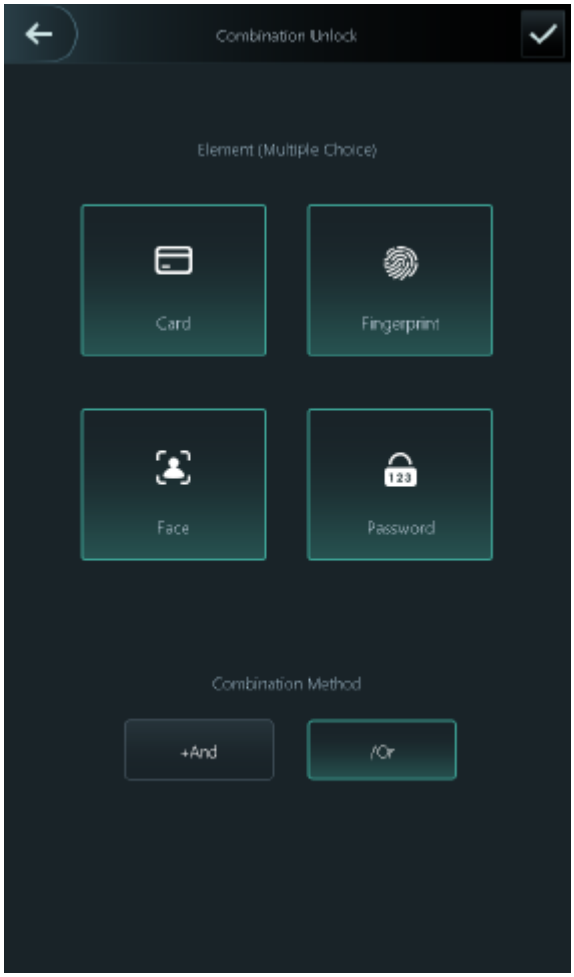
Paso 2 Grifo**Desbloqueo combinado**,y el selecto**Desbloqueo combinado**formar la lista.

Figura 2-4 Desbloqueo combinado



Paso 3 Grifo**Método de desbloqueo**y seleccione métodos de desbloqueo.

Figura 2-5 Método de combinación



Etapa 4 Toca +**Y**o**/O**para configurar combinaciones.

Para cancelar su selección, toque el método seleccionado nuevamente.

- **+Y**:

  Verifique todos los métodos de desbloqueo seleccionados para abrir la puerta.

  Las personas deben completar la verificación en el orden de tarjeta, huella digital, rostro y contraseña.

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

Paso 5 para guardar los cambios.

2.9.1.2 Configuración de desbloqueo por período

Procedimiento

Paso 1 Seleccionar**Gestión de control de acceso**>**Método de desbloqueo**.

Paso 2 Toque el área derecha de**Método de desbloqueo**,y luego seleccione**Desbloquear por período**formar la lista.

Para obtener detalles sobre cómo configurar el desbloqueo por período, consulte "3.6.1.2 Configuración de métodos de desbloqueo".

Paso 3 Toque para guardar los cambios.

2.9.1.3 Configurar el desbloqueo por varios usuarios

Procedimiento

Paso 1 Seleccionar**Gestión de control de acceso**.

Paso 2 Toque el área derecha de**Método de desbloqueo**,y luego seleccione**Desbloqueo por múltiples usuarios**de la lista.

Para obtener detalles sobre cómo configurar el desbloqueo por período, consulte "3.6.1.2 Configuración de métodos de desbloqueo".

Paso 3 Toque para guardar los cambios.

2.9.2 Configuración de alarmas

Se activará una alarma cuando se acceda de forma anormal a la entrada o salida.

Procedimiento

Paso 1 Seleccionar**Gestión de control de acceso**>**Alarma**.

Paso 2 Habilite el tipo de alarma.

Los tipos de alarma pueden diferir según los modelos del producto.

Figura 2-6 Alarma

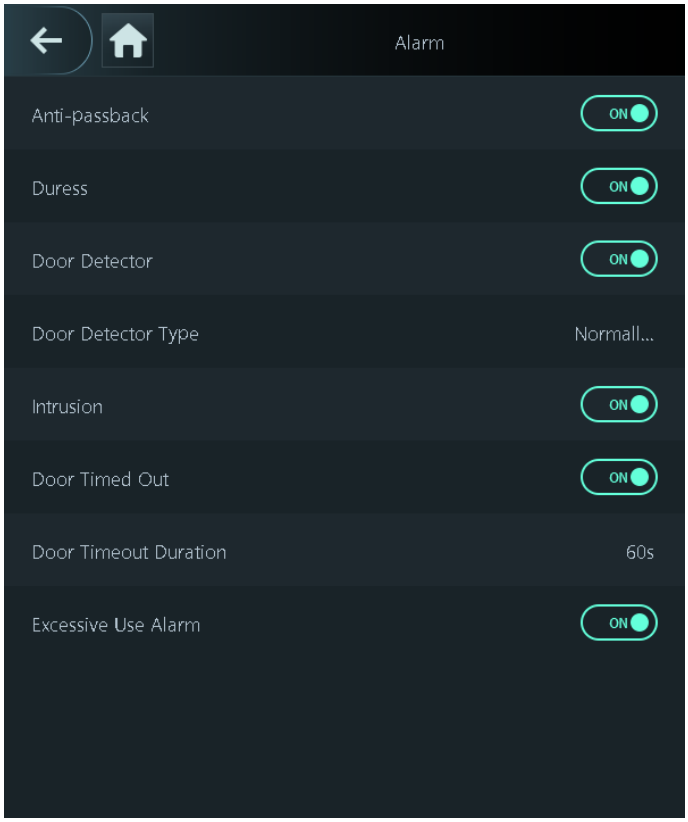


Tabla 2-4 Descripción de los parámetros de alarma

Parámetro	Descripción
Anti-passback	Los usuarios deben verificar sus identidades tanto para entrar como para salir; de lo contrario se activará una alarma. Esto ayuda a evitar que los titulares de tarjetas puedan entregar su tarjeta a otras personas para permitirles el acceso. Cuando el antipassback está habilitado, el titular de la tarjeta debe abandonar el área segura a través de un lector de salida antes de que el sistema le conceda acceso nuevamente. Las personas deben pasar su tarjeta por el lector de "entrada" para ingresar a un área segura y pasarla por el lector de "salida" para salir de ella. ● Si una persona ingresa después de ser verificada, pero sale sin ser verificada, se activará una alarma si intenta ingresar nuevamente y se le negará el acceso. ● Si una persona ingresa sin ser verificada, pero sale después de ser verificada, se activará una alarma si intenta ingresar nuevamente y se le negará el acceso.  Si el Dispositivo solo puede conectarse a una cerradura, la verificación a través del Dispositivo significa que una persona ingresó en la dirección "dentro", y la verificación a través del lector de tarjetas externo significa que salió en la dirección "fuera". Este es el valor predeterminado.
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.
Detector de puerta	Con el detector de puertas conectado a su dispositivo, se pueden activar alarmas cuando las puertas se abren o cierran de manera anormal. Hay 2 tipos de detectores de puertas: detector NC y detector NO. ● Normalmente cerrado: el sensor está en una posición de cortocircuito cuando la puerta o ventana está cerrada. ● Normalmente abierto: se crea un circuito abierto cuando la ventana o puerta está realmente cerrada.
Tipo de detector de puerta	
Intrusión	Si la puerta se abre de forma anormal, se activará una alarma de intrusión que durará un tiempo definido.
Puerta agotada	Cuando la puerta permanece desbloqueada por más tiempo que el tiempo de espera definido, la alarma de tiempo de espera de la puerta se activará y durará el tiempo definido.  El detector de puerta y la función de tiempo de espera de puerta deben habilitarse al mismo tiempo.
Duración del tiempo de espera de la puerta	
Alarma de uso excesivo	Si se utiliza la contraseña o tarjeta incorrecta 5 veces seguidas en 60 segundos, se activará la alarma por uso excesivo de tarjeta ilegal y durará un tiempo definido.

2.9.3 Configurar el estado de la puerta

Procedimiento

Paso 1 Sobre el**Menú principal**pantalla, seleccione**Gestión de control de acceso**>**Configuración de estado de bloqueo**. Establecer el estado

Paso 2 de la puerta.

Figura 2-7 Estado de bloqueo

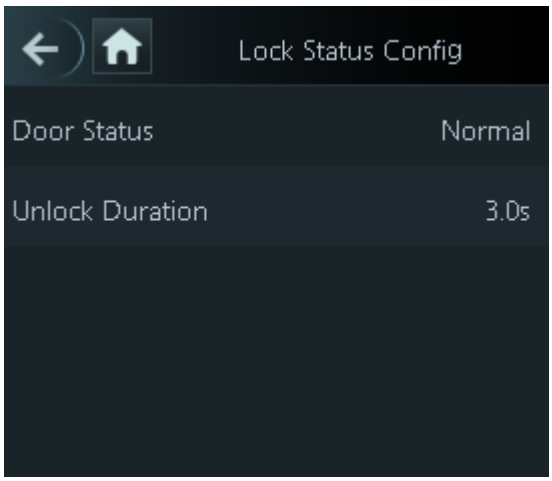


Tabla 2-5 Descripción de los parámetros

Parámetro	Descripción
Estado de la puerta	• **Normalmente abierto**:La puerta permanece abierta todo el tiempo. • **Normalmente cerrado**:La puerta permanece cerrada todo el tiempo. • **Normal**:Si**Normal**Si selecciona , la puerta se bloqueará y desbloqueará según su configuración.
Duración del desbloqueo	Después de que se le conceda acceso a una persona, la puerta permanecerá desbloqueada durante un tiempo definido para que pueda pasar.

2.9.4 Configurar el intervalo de tiempo de verificación

Si verifica su identidad varias veces dentro de un período determinado, solo la primera verificación se considerará válida y la puerta no se abrirá después de la segunda o posteriores verificaciones. Desde el momento en que la puerta no se abre, deberá esperar el intervalo de tiempo de verificación configurado antes de intentar verificar su identidad nuevamente.

Procedimiento

Paso 1 Seleccionar**Gestión de control de acceso**>**Intervalo de verificación (seg)**.

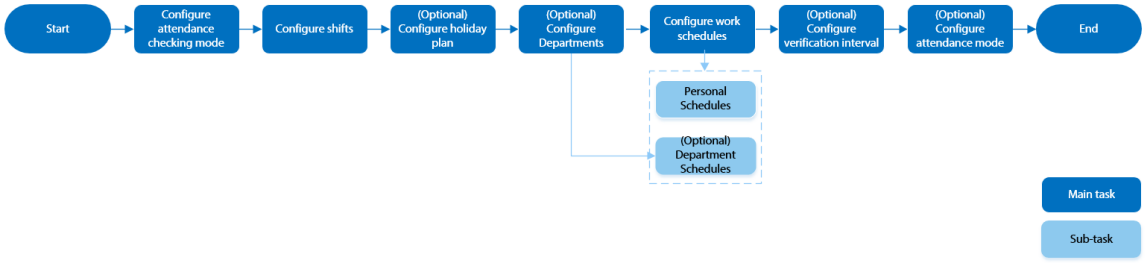
Paso 2 Ingrese el intervalo de tiempo y luego toqu

2.10 Gestión de asistencia

El tiempo de asistencia admite la gestión de asistencia tanto en el dispositivo como en Smart PSS Lite. Esta sección solo utiliza la configuración de asistencia en el dispositivo como ejemplo.

Esta función solo está disponible en modelos seleccionados (dispositivos de la serie de 4,3 pulgadas).

Figura 2-8 Diagrama de flujo de configuración del tiempo de asistencia



2.10.1 Configurar departamentos

Procedimiento

Paso 1 Seleccionar**Asistencia**>**Configuración del departamento**.

Paso 2 Seleccione un departamento y luego cámbiele el nombre.

Hay 20 departamentos predeterminados. Le recomendamos cambiarles el nombre.

Figura 2-9 Crear departamentos

Paso 3 Grif

2.10.2 Configurar turnos

Configure turnos para definir reglas de tiempo de asistencia. Los empleados deben llegar a trabajar a la hora prevista para el inicio de su turno y salir a la hora de finalización, excepto cuando opten por trabajar horas extras.

Procedimiento

Paso 1 Seleccionar**Asistencia**>**Configuración de turnos**.

Paso 2 Seleccione un turno.

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

Paso 3 Configurar los parámetros del turno.

Figura 2-10 Crear turnos

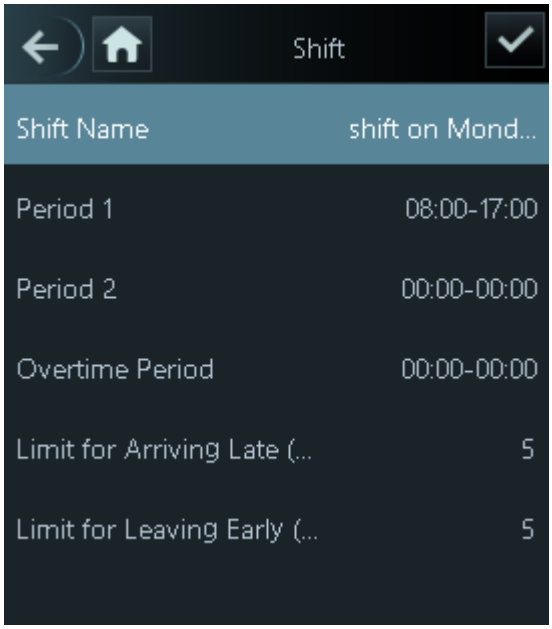
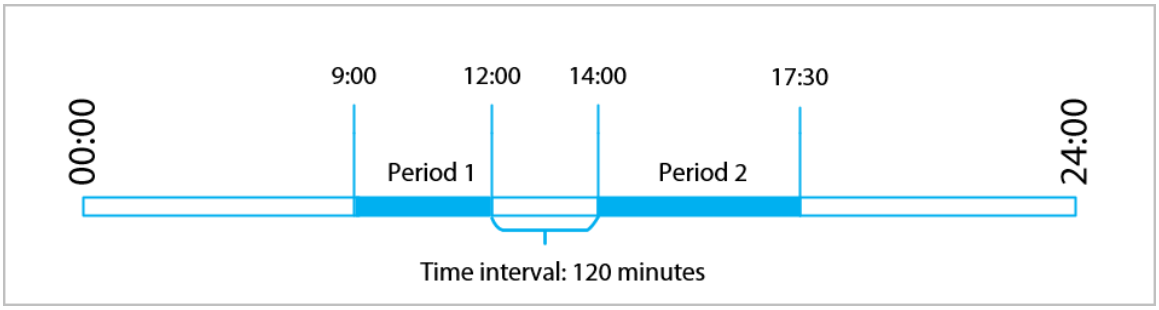


Tabla 2-6 Descripción de los parámetros de cambio

Parámetro	Descripción
Nombre del turno	Ingrese el nombre del turno.
Periodo 1	Especifique un rango de tiempo en el que las personas pueden registrar la entrada y la salida de la jornada laboral. Si solo establece un período de asistencia, los empleados deben registrar su entrada y salida en los horarios designados para evitar que aparezca una anomalía en su registro de asistencia. Por ejemplo, si configura de 08:00 a 17:00, los empleados deben registrar su entrada antes de las 08:00 y su salida a partir de las 17:00. Si establece 2 períodos de asistencia, los 2 períodos no pueden superponerse. Los empleados deben registrar su entrada y salida en ambos períodos.
Periodo 2	
Periodo de horas extras	Se considerará que los empleados que registren su entrada o salida durante el período definido trabajan más allá de su horario normal de trabajo.
Límite por llegar tarde (min)	Se puede conceder una cierta cantidad de tiempo a los empleados para que puedan registrar su entrada un poco tarde y su salida un poco antes. Por ejemplo, si la hora habitual para registrar la entrada es a las 08:00, el período de tolerancia se puede establecer en 5 minutos para que los empleados que lleguen antes de las 08:05 no se consideren retrasados.
Límite de salida anticipada (min)	

- Cuando el intervalo de tiempo entre 2 periodos es un número par, puedes dividir el intervalo de tiempo entre 2 y asignar la primera mitad del intervalo al primer periodo, que será el tiempo de salida. La segunda mitad del intervalo debe asignarse al segundo período como cronómetro.

Figura 2-11 Intervalo de tiempo (número par)

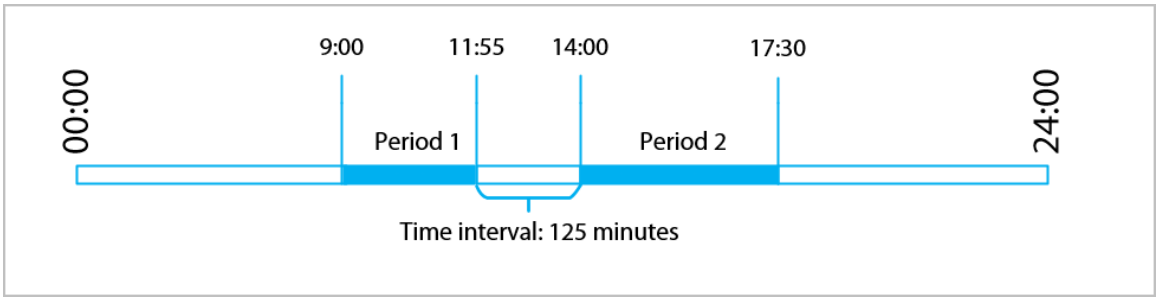


Por ejemplo: si el intervalo es de 120 minutos, entonces la hora de salida para el período 1 es de 12:00 a 12:59, y la hora de entrada para el período 2 es de 13:00 a 14:00.

Si una persona registra su salida varias veces durante el período 1, la última hora será válida, y si registra su entrada varias veces durante el período 2, la hora más temprana será válida.

- Cuando el intervalo de tiempo entre 2 períodos sea un número impar, la porción más pequeña del intervalo se asignará al primer período, que será el tiempo de salida. La mayor parte del intervalo se asignará al segundo período como el reloj en el tiempo.

Figura 2-12 Intervalo de tiempo (número par)



Por ejemplo: si el intervalo es de 125 minutos, entonces la hora de salida para el período 1 es de 11:55 a 12:57, y la hora de entrada para el período 2 es de 12:58 a 14:00. El período 1 tiene 62 minutos y el período 2 tiene 63 minutos.

Si una persona registra su salida varias veces durante el período 1, la última hora será válida, y si registra su entrada varias veces durante el período 2, la hora más temprana será válida.

Todos los tiempos de asistencia son precisos al segundo. Por ejemplo, si la hora normal de entrada se establece en las 8:05 a. m., el empleado que registre su entrada a las 8:05:59 a. m. no se considerará que llega tarde. Sin embargo, el empleado que llegue a las 8:06 a. m. se marcará como retrasado por 1 minuto.

Etapa 4 Grif

2.10.3 Configurar planes de vacaciones

Configure planes de vacaciones para establecer períodos en los que no se realizará un seguimiento de la asistencia.

Procedimiento

Paso 1 Seleccionar**Asistencia**>**Configuración de turnos**>**Día festivo**.

Paso 2 Hacer clic + para agregar planes de vacaciones.

Paso 3 Configure los parámetros.

Figura 2-13 Crear planes de vacaciones

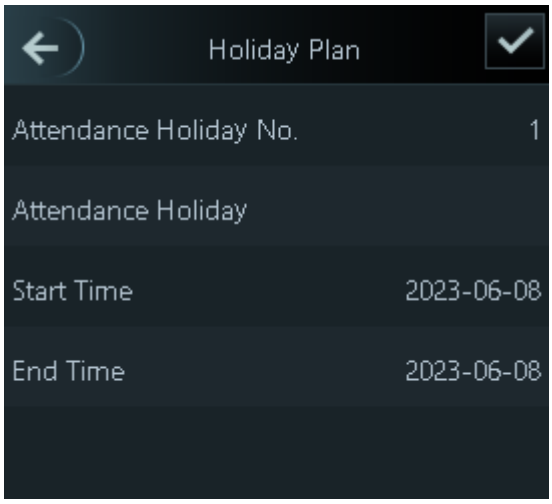


Tabla 2-7 Descripción de los parámetros

Parámetro	Descripción
Asistencia Día festivo No.	El número de las vacaciones.
Asistencia vacaciones	El nombre de la festividad.
Hora de inicio	La hora de inicio y finalización de las vacaciones.
Hora de finalización	

Etapa 4 Grif

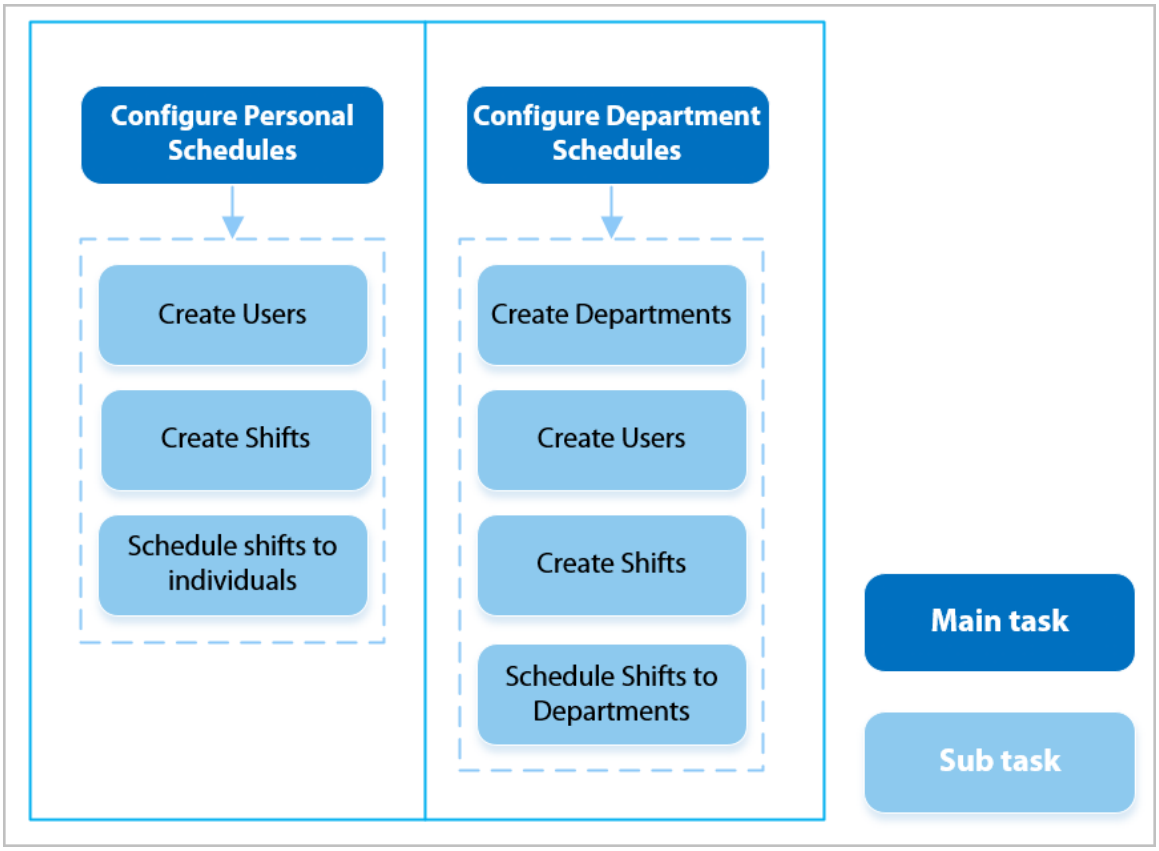
2.10.4 Configurar horarios de trabajo

Un horario de trabajo generalmente se refiere a los días por mes y las horas por día que se espera que un empleado esté en su trabajo. Puede crear diferentes tipos de horarios de trabajo basados en diferentes personas o departamentos, y luego los empleados deben seguir los horarios de trabajo establecidos.

Información de contexto

Consulte el diagrama de flujo para configurar horarios personales o horarios de departamento.

Figura 2-14 Configuración de horarios de trabajo



Procedimiento

Paso 1 Seleccionar**Asistencia**>**Programar configuración**.

Paso 2 Establecer horarios de trabajo para individuos.

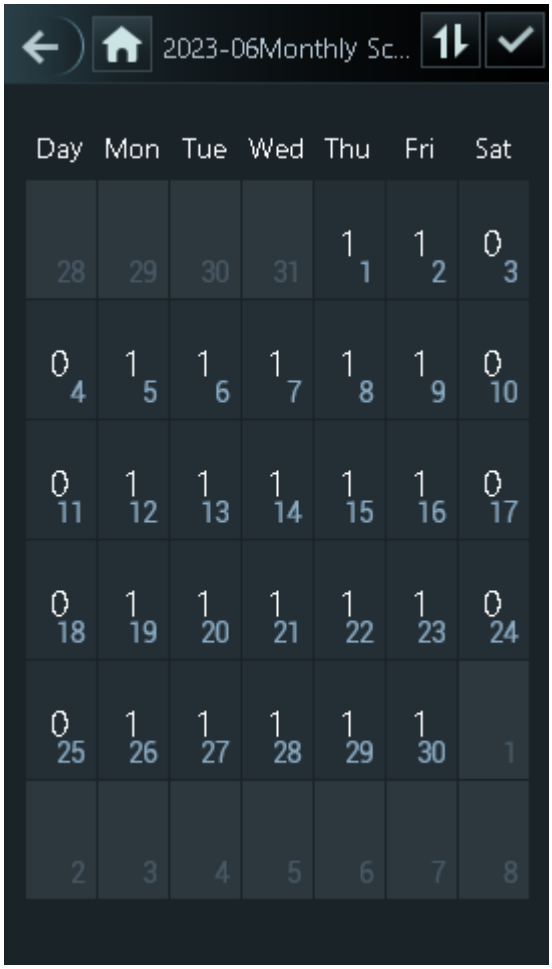
1. Toque**Horario personal**.
2. Ingrese la ID de usuario y luego toque
3. En el calendario, seleccione un día y luego seleccione un turno.

   El turno está programado para el día.

Solo puede establecer horarios de trabajo para el mes actual y el mes siguiente.

- 0 indica ruptura.
- Del 1 al 24 indica el número de turnos definidos. Para saber cómo configurar turnos, consulte "2.10.2 Configuración de turnos".
- 25 indica viaje de negocios.
- 26 indica excedencia.

Figura 2-15 Cambios de horario a individuos



4. Toqu

Paso 3 Establecer horarios de trabajo para los departamentos.

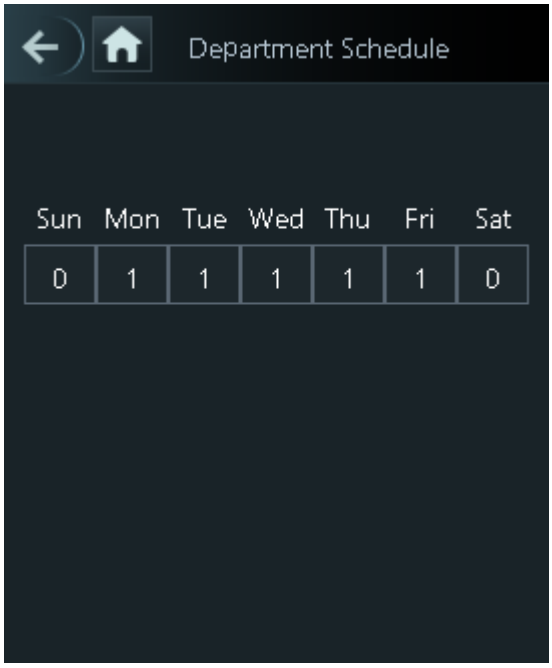
1. Toque**Horario del departamento**.

2. Toque un departamento y luego seleccione turnos para una semana.

Los turnos están programados para la semana.

- 0 indica descanso.
- Del 1 al 24 indica el número de turnos definidos. Para saber cómo configurar turnos, consulte "2.10.2 Configuración de turnos".
- 25 indica viaje de negocios.
- 26 indica excedencia.

Figura 2-16 Horario de turnos a un departamento



El horario de trabajo definido es en un ciclo semanal y se aplicará a todos los empleados del departamento.

Etapa 4 Grif

2.10.5 Configurar modos de asistencia

Cuando marca su entrada o salida, puede configurar los modos de asistencia para definir el estado de asistencia.

Procedimiento

Paso 1 En la pantalla del menú principal, haga clic en**Asistencia**.

Paso 2 Permitir**Local o Remoto**y luego configure el modo de asistencia.

Los registros de asistencia también se sincronizarán con la plataforma de gestión.

Figura 2-17 Modo de asistencia

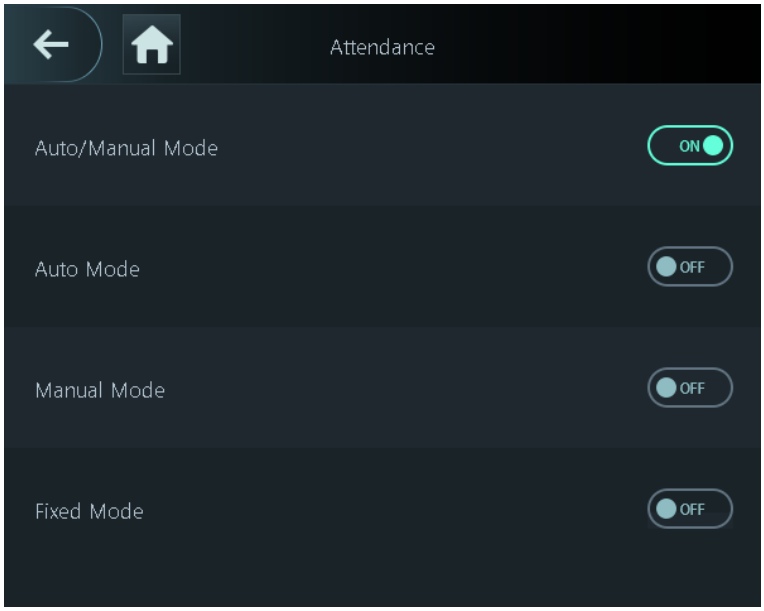


Tabla 2-8 Modo de asistencia

Parámetro	Descripción
Modo automático/manual	La pantalla muestra el estado de asistencia automáticamente después de registrar su entrada o salida, pero también puede cambiar manualmente su estado de asistencia.
Modo automático	La pantalla muestra su estado de asistencia automáticamente después de registrar su entrada o salida.
Modo manual	Seleccione manualmente su estado de asistencia cuando registre su entrada o salida.
Modo fijo	Cuando registre su entrada o salida, la pantalla mostrará el estado de asistencia definido todo el tiempo.

Paso 3 Seleccione un modo de asistencia.

Etapa 4 Configure los parámetros para el modo de asistencia.

Figura 2-18 Modo automático/modo manual

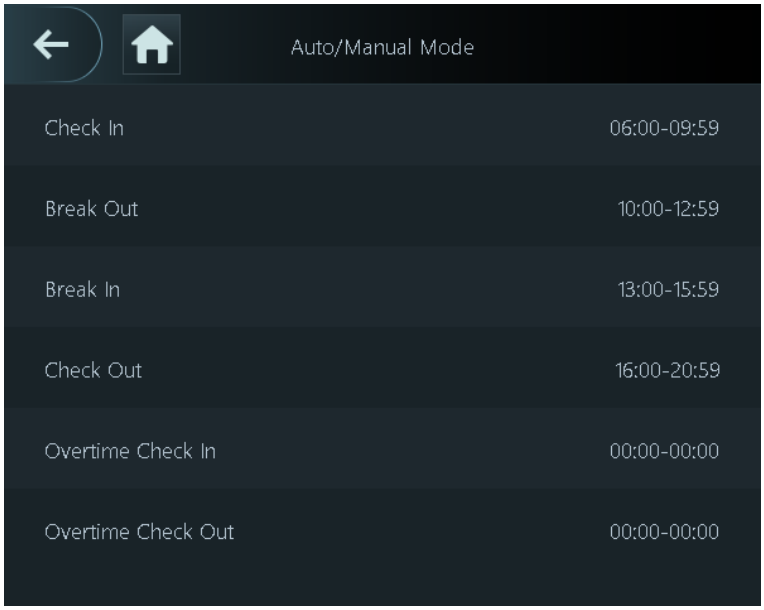


Figura 2-19 Modo fijo

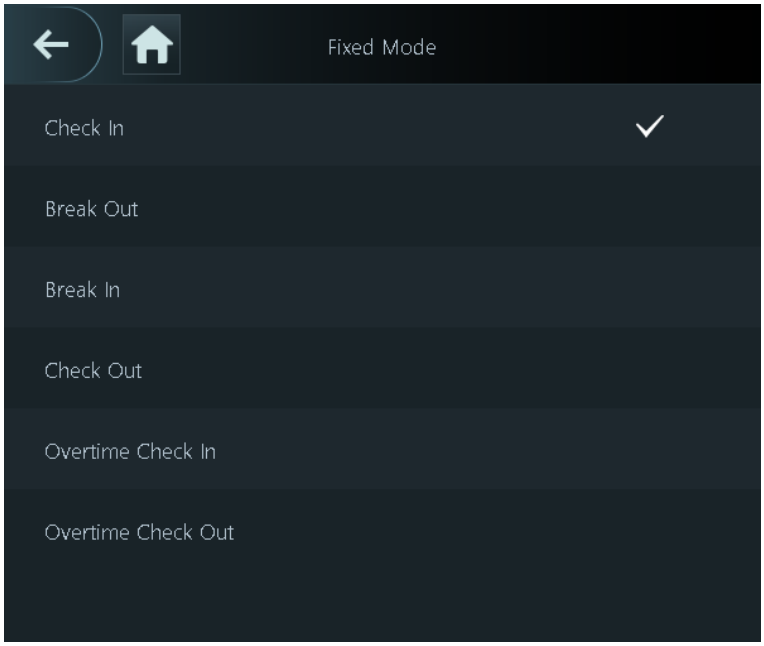


Tabla 2-9 Parámetros del modo de asistencia

Parámetros	Descripción
Registrarse	Registre cuándo comienza su jornada laboral normal.
Fugarse	Regístrese cuando comience su descanso.
Interrumpir	Registre cuando termine su descanso.
Verificar	Regístrese cuando comience su jornada laboral normal.
Registro de horas extras	Regístrese cuando comience su período de horas extra.
Salida de horas extras	Regístrese cuando finalice su período de horas extra.

2.11 Configuración de comunicación

Configure la red, el puerto serie y el puerto Wiegand para conectar el Dispositivo a la red.

El puerto serie y el puerto Wiegand pueden diferir según los modelos de dispositivo.

2.11.1 Configuración de la red

2.11.1.1 Configurar la dirección IP

Configure una dirección IP para que el dispositivo lo conecte a la red. Después de eso, puede iniciar sesión en la página web y en la plataforma de administración para administrar el Dispositivo.

Procedimiento

Paso 1 Sobre el**Menú principal**, seleccionar**Configuración de comunicación**>**Red**>**Dirección IP**.

Paso 2 Configure la dirección IP.

Figura 2-20 Configuración de la dirección IP

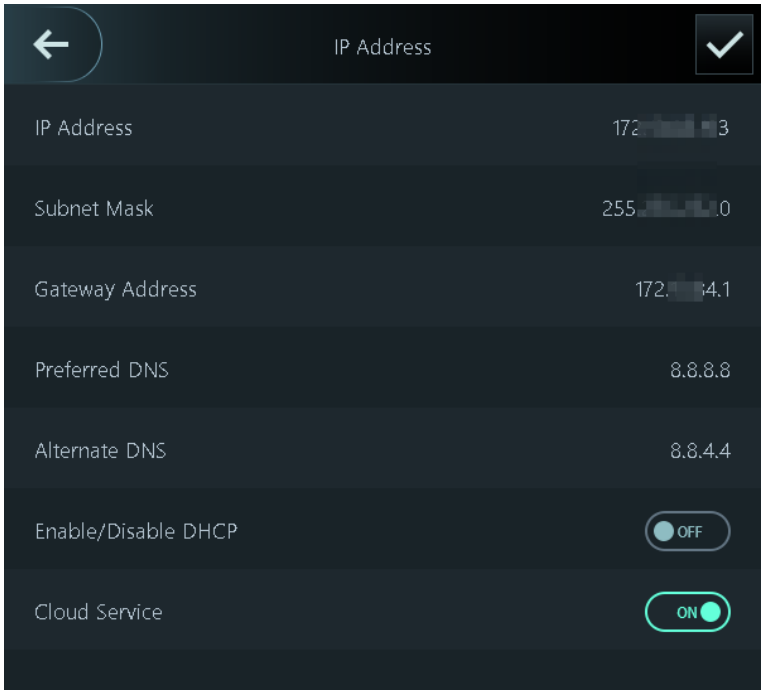


Tabla 2-10 Parámetros de configuración IP

Parámetro	Descripción
Dirección IP/Máscara de subred/Dirección de puerta de enlace	La dirección IP, la máscara de subred y la dirección IP de la puerta de enlace deben estar en el mismo segmento de red.
DNS preferido	La IP del servidor DNS.
DNS alternativo	La IP alternativa del servidor DNS.

Parámetro	Descripción
Activar/Desactivar DHCP	Significa Protocolo de configuración dinámica de host. Cuando DHCP está activado, al dispositivo se le asignará automáticamente una dirección IP, una máscara de subred y una puerta de enlace.
Servicio de almacenamiento en la nube	Administre dispositivos sin solicitar DDNS, configure el mapeo de puertos e implemente servidores de tránsito.

2.11.1.2 Configuración del registro automático

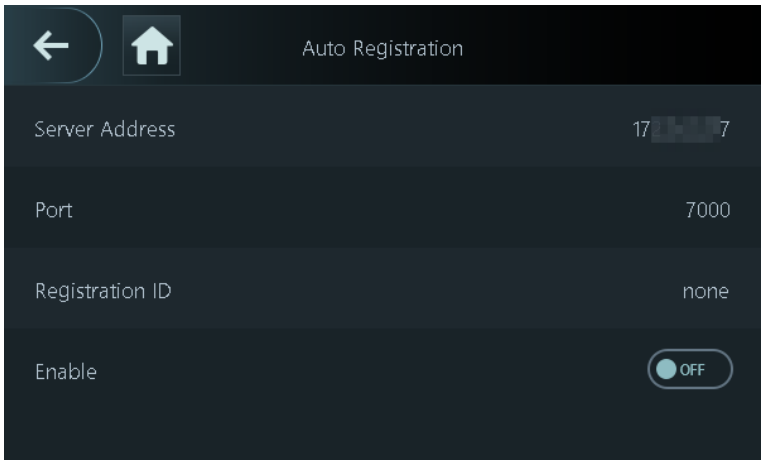
Agregue el dispositivo a una plataforma de administración para que pueda administrarlo en la plataforma.

Procedimiento

Paso 1 Sobre el**Menú principal**, seleccionar**Configuración de comunicación**>**Red**>**Registro automático**.

Para evitar exponer el sistema a riesgos de seguridad y pérdida de datos, controle los permisos de la plataforma de gestión.

Figura 2-21 Registro activo



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

Tabla 2-11 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 de Registro	Ingrese la ID del dispositivo (definida por el usuario). Cuando agrega el Dispositivo a la plataforma de administración, la ID de registro que ingresa en la plataforma de administración debe ajustarse a la ID de registro definida en el Dispositivo.

2.11.1.3 Configuración de Wi-Fi

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

Información de contexto

Esta función solo está disponible en modelos seleccionados.

Procedimiento

Paso 1 Sobre el**Menú principal**, seleccionar**Configuración de comunicación**>**Red**>**Wifi**.

Paso 2 Enciende el wifi.

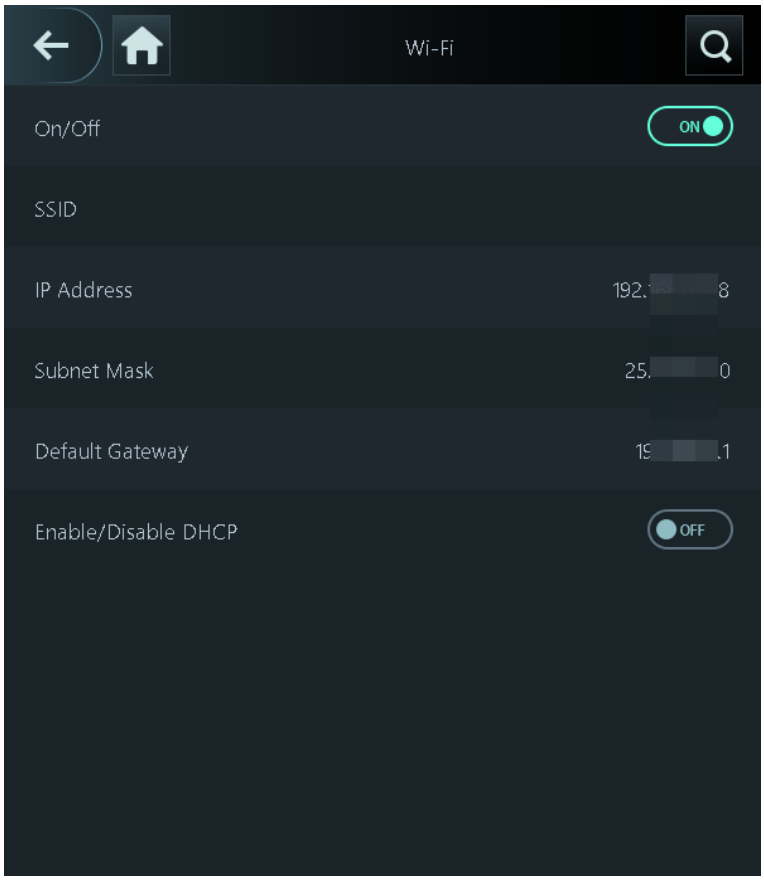
- La función Wi-Fi solo está disponible en modelos seleccionados.
- Wi-Fi AP y la función Wi-Fi no se pueden habilitar al mismo tiempo.
- Después de habilitar Wi-Fi, espere aproximadamente 1 minuto para conectarse a Wi-Fi.

Paso 3 Grifo para buscar redes inalámbricas disponibles.

Etapa 4 Seleccione una red inalámbrica e ingrese la contraseña.

Si el sistema no encuentra una red Wi-Fi, toque**SSID**para ingresar el nombre del Wi-Fi.

Figura 2-22 Conexión a Wi-Fi



Operaciones relacionadas

Activar/Desactivar DHCP: habilite esta función y al dispositivo se le asignará automáticamente una dirección Wi-Fi.

2.11.1.4 Configuración del punto de acceso Wi-Fi

Esta función solo está disponible en modelos seleccionados.

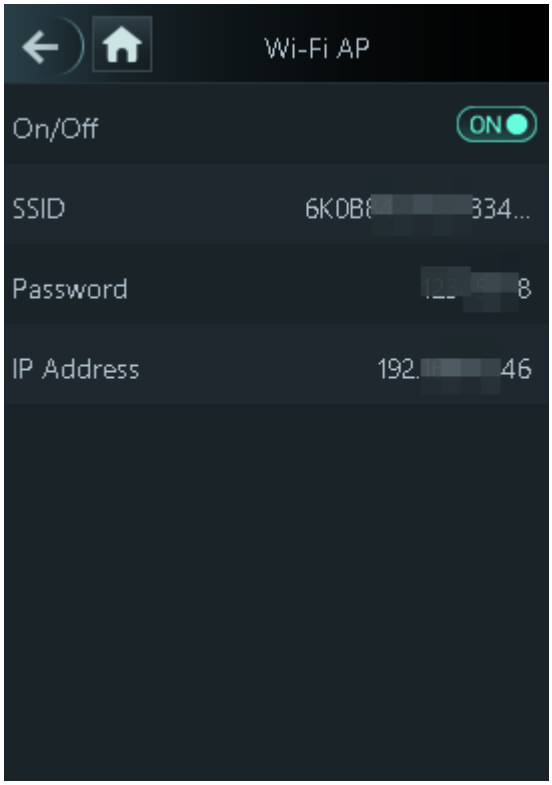
Procedimiento

Paso 1 Sobre el**Menú principal**, seleccionar**Configuración de comunicación**>**Red**>**Punto de acceso Wi-Fi**. Encienda el punto

Paso 2 de acceso Wi-Fi.

Wi-Fi AP y la función Wi-Fi no se pueden habilitar al mismo tiempo.

Figura 2-23 Conexión al AP Wi-Fi



Resultados

Utilice su computadora para conectarse al AP Wi-Fi del dispositivo para acceder a su página web.

2.11.2 Configuración del puerto serie

Esta función solo está disponible en modelos seleccionados.

Procedimiento

Paso 1 Sobre el**Menú principal**, seleccionar**Configuración de comunicación**>**Puerto serial**.

Paso 2 Seleccione un dispositivo externo.

Figura 2-24 Tipo de dispositivo externo

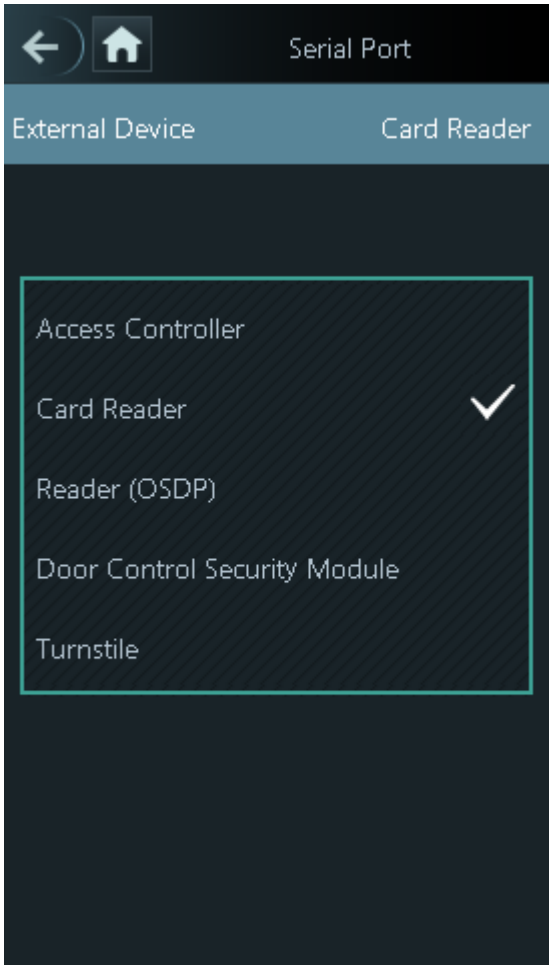


Tabla 2-12 Descripción del puerto

Dispositivo externo	Descripción
Controlador de acceso	El Dispositivo funciona como un lector de tarjetas y envía datos a otros controladores de acceso externos para controlar el acceso. Tipo de datos de salida: ● Número de tarjeta: genera datos basados en el número de tarjeta cuando los usuarios deslizan sus tarjetas para desbloquear puertas; genera datos basados en el primer número de tarjeta del usuario cuando los usuarios utilizan otros métodos de desbloqueo. ● No.: genera datos basados en la identificación del usuario.
Lector de tarjetas	El Dispositivo funciona como un controlador de acceso y se conecta a un lector de tarjetas externo.
Lector (OSDP)	El Dispositivo está conectado a un lector de tarjetas basado en el protocolo OSDP.
Módulo de seguridad de control de puertas	Después de habilitar el módulo de seguridad, el botón de salida de la puerta, el control de bloqueo y la conexión contra incendios del Dispositivo dejan de ser efectivos, pero el botón de salida de la puerta y el control de bloqueo que se conecta al módulo de seguridad sí se vuelven efectivos.

Dispositivo externo	Descripción
Torniquete	Cuando el Dispositivo está conectado a un torniquete y la placa controladora de acceso del torniquete está conectada a un módulo de código QR externo o módulo de deslizamiento de tarjeta, la placa transmitirá los datos de verificación al torniquete.

2.11.3 Configuración de Wiegand

El dispositivo permite el modo de entrada y salida Wiegand.

Esta función solo está disponible en modelos seleccionados.

Procedimiento

Paso 1 En la página web, seleccione**Configuración de comunicación**>**Wiegand**.

Paso 2 Seleccione un Wiegand.

- Seleccionar**Entrada Wiegand**cuando conecta un lector de tarjetas externo al Dispositivo.

  Cuando el Dispositivo se conecta a un dispositivo de terceros a través del puerto de entrada Wiegand y el número de tarjeta leído por el Dispositivo está en el orden inverso al número de tarjeta real. En este caso, puede activar**Inversión del número de tarjeta**función.
- Seleccionar**Salida Wiegand**cuando el Dispositivo funciona como lector de tarjetas y es necesario conectarlo a un controlador u otro terminal de acceso.

Figura 2-25 Salida Wiegand

Tabla 2-13 Descripción de la salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	Seleccione un formato Wiegand para leer números de tarjetas o números de identificación. ● **Wiegand26**:Lee 3 bytes o 6 dígitos. ● **Wiegand34**:Lee 4 bytes u 8 dígitos. ● **Wiegand66**:Lee 8 bytes o 16 dígitos.
Ancho de pulso	Ingrese el ancho del pulso y el intervalo de pulso de la salida Wiegand.
Intervalo de pulso	
Tipo de datos de salida	Seleccione el tipo de datos de salida. ● **No.**:El sistema genera datos basados en la identificación del usuario. El formato de datos es hexadecimal o decimal. ● **Número de tarjeta**:El sistema genera datos basados en el primer número de tarjeta del usuario.

2.12 Configuración del sistema

2.12.1 Configurar la hora

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

Procedimiento

Paso 1 Sobre el**Menú principal**, seleccionar**Ajustes del sistema**>**Tiempo**.

Paso 2 Configurar la hora del sistema.

Figura 2-26 Hora

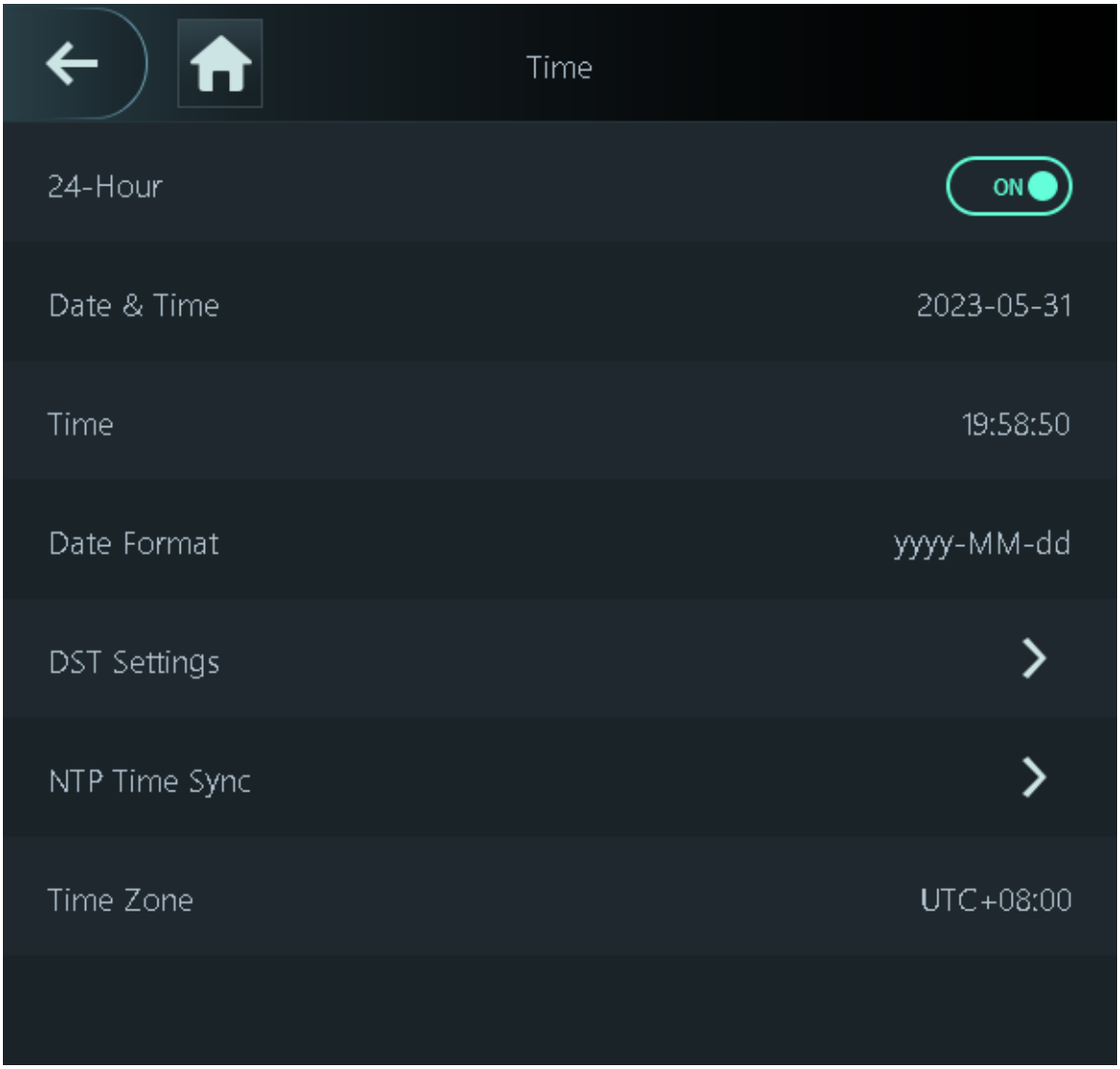


Tabla 2-14 Descripción de los parámetros de tiempo

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

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

2.12.2 Configuración de parámetros de cara

Los parámetros faciales pueden diferir según los modelos del dispositivo.

Procedimiento

Paso 1 En el menú principal, seleccione**Ajustes del sistema**>**Configuración de parámetros de cara**.

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

Figura 2-27 Parámetro de cara

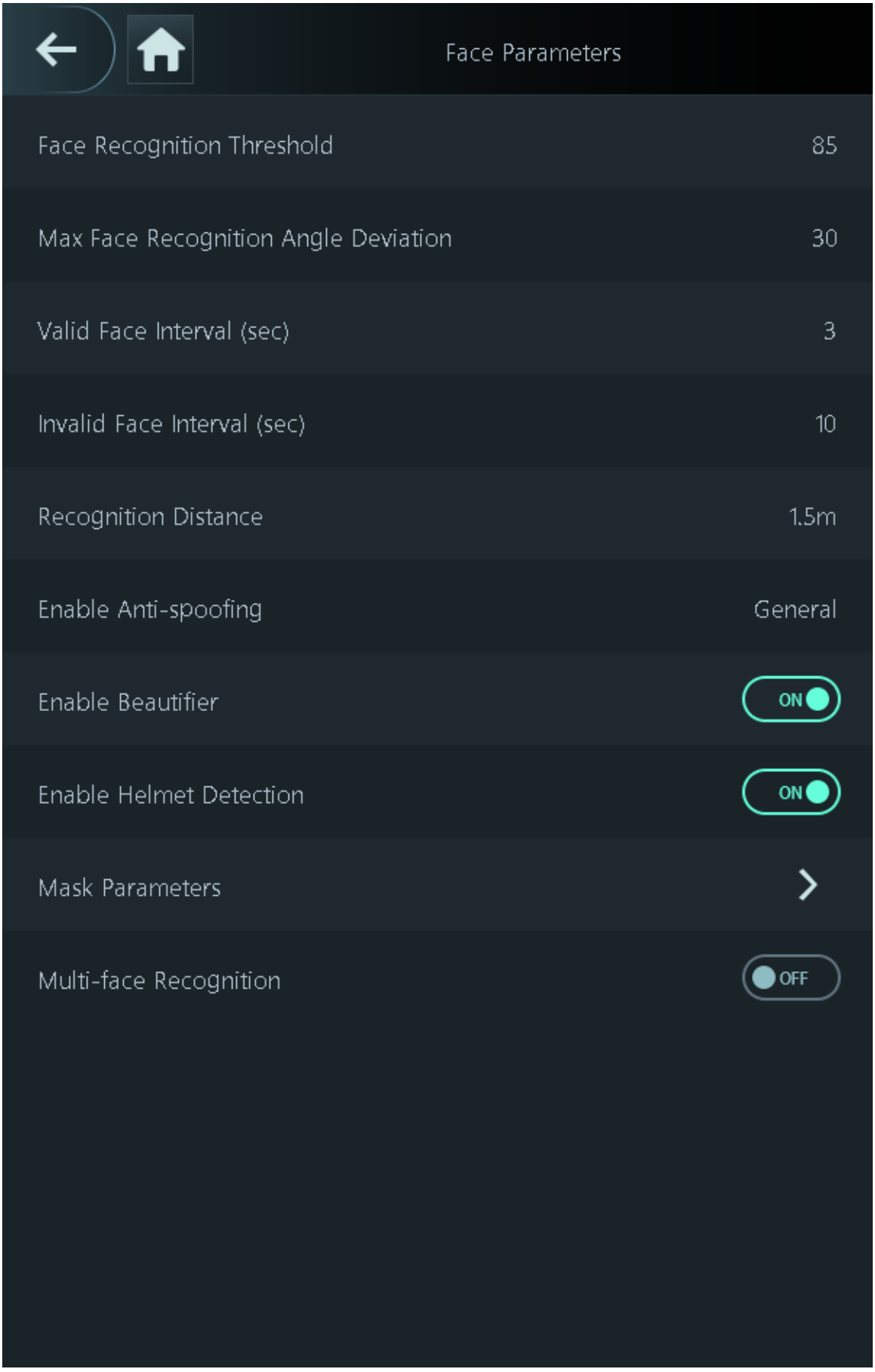


Tabla 2-15 Descripción de los parámetros de la cara

Nombre	Descripción
Umbral de reconocimiento facial	Ajuste el nivel de precisión del reconocimiento facial. Un umbral más alto significa una mayor precisión y una menor tasa de reconocimiento falso. Cuando el umbral es demasiado bajo, como 0, la tasa de reconocimiento falso será extremadamente alta. Por favor tenga en cuenta.
Desviación máxima del ángulo de reconocimiento facial	Establezca el ángulo más grande en el que se puede colocar una cara para la detección de caras. Cuanto mayor sea el valor, mayor será el rango del ángulo de la cara. Si el ángulo en el que se coloca una cara no está dentro del rango definido, es posible que no se detecte correctamente.
Intervalo de cara válido (seg)	Cuando la misma cara permanece frente a la lente después del primer reconocimiento exitoso, el Dispositivo realizará nuevamente el reconocimiento de la cara después de un intervalo definido.
Intervalo de cara no válido (seg)	Cuando la misma cara permanece frente a la lente después del primer reconocimiento fallido, el Dispositivo realizará nuevamente el reconocimiento de la cara después de un intervalo definido.
Distancia de reconocimiento	La distancia entre la cara y la lente.
Habilitar antisuplantación de identidad	Esto evita que las personas puedan utilizar fotos, vídeos, máscaras y otros sustitutos para obtener acceso no autorizado.
Habilitar embellecedor	Embellece las imágenes de rostros capturados.
Habilitar detección de casco	Detecta cascos de seguridad. La puerta no se desbloqueará para las personas que no lleven casco.
Parámetros de máscara	● Modo máscara: ◇ **No detectar**:La máscara no se detecta durante el reconocimiento facial. ◇ **Recordatorio de máscara**:La máscara se detecta durante el reconocimiento facial. Si la persona no lleva mascarilla, el sistema le recordará que la use, pero aún así se le permitirá el acceso. ◇ **Sin autorización sin usar mascarilla**:La máscara se detecta durante el reconocimiento facial. Si una persona no lleva mascarilla, el sistema le recordará que la use y se le negará el acceso. ● Umbral de reconocimiento de máscara: cuanto más alto sea el umbral, más preciso será el reconocimiento facial cuando una persona use una máscara y habrá una menor tasa de reconocimiento falso.
Reconocimiento multicara	Detecta de 4 a 6 imágenes de rostros a la vez. El desbloqueo combinado no se puede usar con esto y la puerta se desbloqueará cuando una de las personas sea verificada exitosamente. La cantidad de imágenes de rostros admitidas puede variar según el modelo del producto.

Nombre	Descripción
Modo iluminador	● Automático: el iluminador se enciende en condiciones de poca luz. ● Desactivar: El iluminador está apagado todo el tiempo. Esta función solo está disponible en modelos seleccionados.

2.12.3 Configuración del volumen

Procedimiento

Paso 1 Sobre el**Menú principal**, seleccionar**Ajustes del sistema**>**Configuración de volumen**

Paso 2 . Configure los parámetros.

Tabla 2-16 Descripción de parámetros

Parámetros	Descripción
Volumen del pitido	y luego toque + o − para ajustar el volumen.
Volumen del micrófono	
Sonido de toque de pantalla	Cuando esta función está habilitada, los dispositivos con pantalla táctil producirán un sonido de toque y los dispositivos sin pantalla táctil producirán un sonido de clic del mouse.

2.12.4 Configurar el idioma

Cambie el idioma en el dispositivo. Sobre el**Menú principal**, seleccionar**Ajustes del sistema**>**Idioma**, seleccione el idioma del dispositivo.

2.12.5 Configuración de pantalla

Configure cuándo se debe apagar la pantalla y el tiempo de cierre de sesión.

Procedimiento

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

Paso 2 Grifo**Hora de cerrar sesión**,**Configuración de pantalla apagada**o**Configuración de brillo de la pantalla**y luego toque + o − para ajustar la hora o el brillo de la pantalla.

- Tiempo de cierre de sesión: El sistema vuelve a la pantalla de espera después de un tiempo definido de inactividad.
- Configuración de pantalla apagada: el sistema vuelve a la pantalla de espera y luego la pantalla se apaga después de un tiempo definido de inactividad.

  Por ejemplo, si el tiempo de cierre de sesión se establece en 15 segundos y el tiempo de apagado de la pantalla se establece en 30 segundos, el sistema vuelve a la pantalla de espera después de 15 segundos y luego la pantalla se apagará después de otros 15 segundos.

  El tiempo de cierre de sesión debe ser menor que el tiempo de apagado de la pantalla.

2.12.6 (Opcional) Configuración de parámetros de huellas digitales

Configure la precisión de la detección de huellas dactilares. Cuanto mayor sea el valor, mayor será el umbral de similitud y la precisión.

Información de contexto

Esta función solo está disponible en modelos selectos y algunos admiten la conexión a un módulo de extensión de huellas digitales.

Procedimiento

Paso 1 Sobre el**Menú principal**, seleccionar**Ajustes del sistema**>**Configuración de parámetros de huellas**

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

2.12.7 Restauración de los valores predeterminados de fábrica

Procedimiento

Paso 1 Sobre el**Menú principal**, seleccionar**Ajustes del sistema**>**Fallas de fábrica**.

Paso 2 Restaure los valores predeterminados de fábrica si es necesario. Restaure la configuración predeterminada de fábrica si es necesario.

- **Fallas de fábrica**:Restablece todas las configuraciones y datos excepto la configuración de IP y el tipo de módulo de extensión.
- **Restaurar la configuración predeterminada (excepto la información y los registros del usuario)**:Restablece todas las configuraciones excepto la información del usuario y los registros.

2.12.8 Reiniciar el dispositivo

Sobre el**Menú principal**, seleccionar**Ajustes del sistema**>**Reanudar**y el dispositivo se reiniciará.

2.13 Configuración de funciones

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

Las funciones pueden diferir según el modelo del producto.

Figura 2-28 Funciones

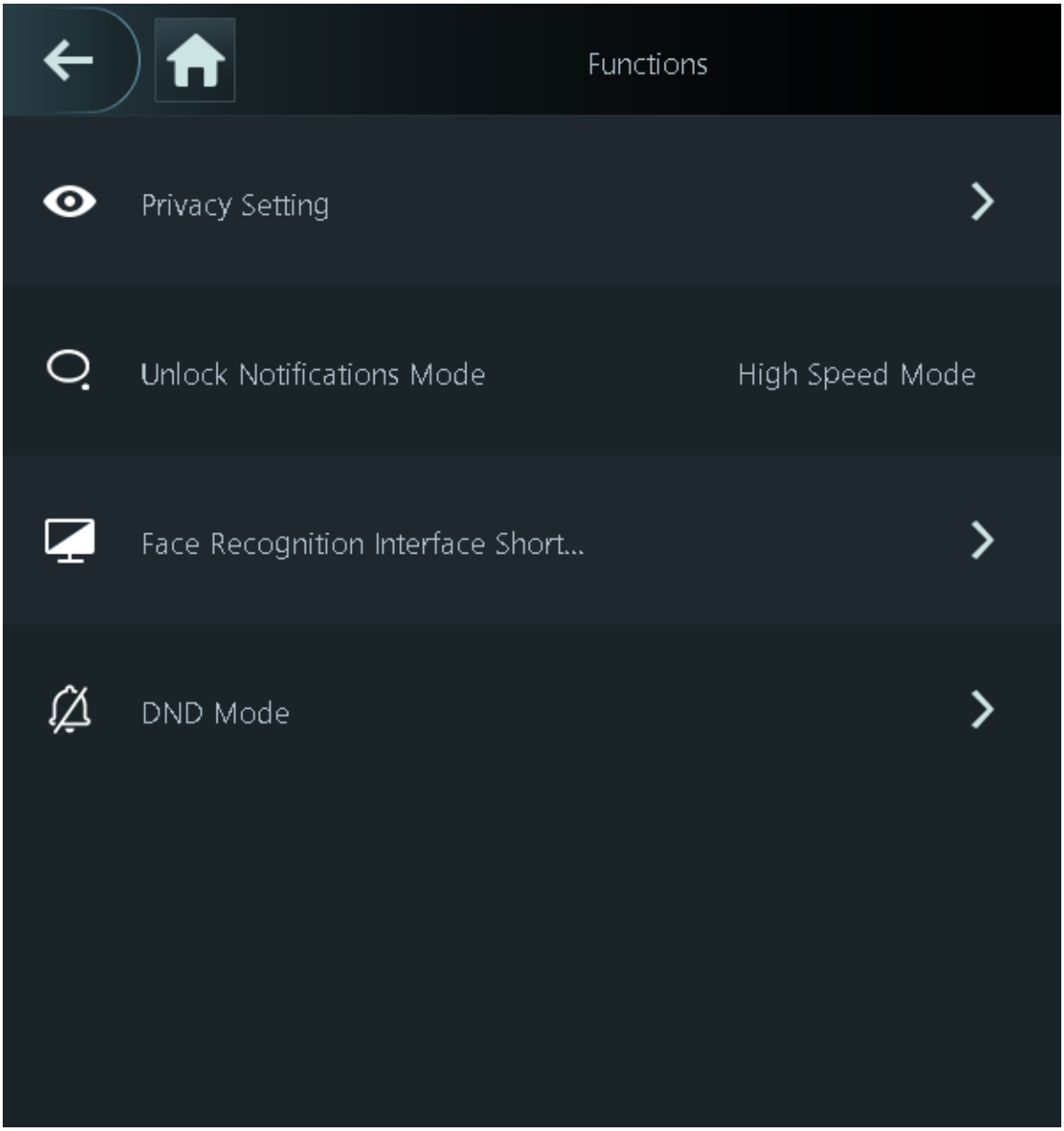


Tabla 2-17 Descripción de la función

Parámetro	Descripción
Entorno privado	● Restablecer contraseña: la contraseña se puede restablecer cuando activa esta función. ● Habilitar HTTPS: El Protocolo seguro de transferencia de hipertexto (HTTPS) es un protocolo para la comunicación segura a través de una red informática. Cuando HTTPS está habilitado, HTTPS se utilizará para acceder a los comandos CGI; de lo contrario, se utilizará HTTP.  Cuando HTTPS está habilitado, el dispositivo se reiniciará automáticamente. ● Habilitar CGI: Common Gateway Interface (CGI) ofrece un protocolo estándar para que los servidores web ejecuten programas similares a cómo se ejecutan las aplicaciones de consola en un servidor que genera dinámicamente una página web. El CGI está habilitado de forma predeterminada. ● Habilitar 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. Los datos transmitidos se cifrarán después de habilitar esta función. ● Imagen de huella digital: la imagen de la huella digital se muestra cuando desbloquea mediante la huella digital.  Esta función solo está disponible en modelos seleccionados. ● Captura: las imágenes de rostros se capturarán automáticamente cuando las personas abran la puerta. ● Borrar todas las instantáneas: elimina todas las fotos capturadas automáticamente.
Notificaciones push	Muestra la notificación en la pantalla cuando una persona está verificando su identidad en el Dispositivo. ● Modo de alta velocidad: el sistema le indica**Verificado con éxito** o**No autorizado**en la pantalla. ● Modo simple: muestra la identificación del usuario, el nombre y la hora de verificación después de otorgar el acceso, y muestra**No autorizado**y el tiempo de autorización después de que se deniega el acceso. ● Estándar: muestra la imagen de la cara registrada del usuario, la ID de usuario, el nombre y la hora de verificación después de que se le concede el acceso, y muestra **No autorizado** y el tiempo de verificación después de que se deniega el acceso. ● Modo de contraste: muestra la imagen del rostro capturada y una imagen del rostro registrada de un usuario, la identificación del usuario, el nombre y la hora de autorización después de otorgar el acceso, y muestra**No autorizado**después de que se le niegue el acceso.

Parámetro	Descripción
Acceso directo a la interfaz de reconocimiento facial	Seleccione métodos de verificación de identidad en la pantalla de espera. ● Contraseña: su icono se muestra en la pantalla de espera. ● Código QR: su icono se muestra en la pantalla de espera. Esta función solo está disponible en modelos seleccionados. ● Timbre: su icono se muestra en la pantalla de espera. ◇ Timbre del dispositivo local: toque el ícono de campana en la pantalla de espera y el dispositivo sonará. ◇ Configuración de tono de llamada: seleccione un tono de llamada ◇ Tiempo del tono de llamada (seg): establece el tiempo de timbre (1-30 segundos). El valor predeterminado es 3. ◇ Alarma: toque el ícono de campana y sonará el dispositivo de alarma externo. Esta función solo está disponible en modelos seleccionados. Cuando se comparten el cable de alarma y el cable del timbre, asegúrese de que la interfaz funcional esté configurada en**Timbre de la puerta**. Para obtener más información, consulte "3.6.11 Configuración de funciones de puerto". ● Llamar: su icono 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 una llamada. ◇ 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 en la pantalla de espera para llamar a la sala predefinida. Puede llamar a DMSS solo en este tipo de llamada. ● Servidor SIP: puede activar SIP para configurar el dispositivo como servidor SIP.
Módulo de expansión	Seleccione un módulo de expansión y el dispositivo se reiniciará. ● se muestra en la esquina derecha de la pantalla de espera, lo que significa que se configuró correctamente. ● aparece en la esquina derecha de la pantalla de espera, lo que significa que falló la configuración. ● El módulo de expansión solo está disponible en modelos selectos. ● El módulo de expansión no admite el intercambio en caliente. ● La configuración del módulo de expansión permanece sin cambios incluso después de que el sistema se restablezca a su configuración de fábrica.
Modo No Molestar	No hay mensajes de voz durante el tiempo establecido cuando verifica su identidad en el Dispositivo. Puede configurar hasta 4 períodos.

2.14 Gestión de USB

Puede utilizar un USB para actualizar el dispositivo y exportar o importar información de usuario o registros de asistencia a través de USB.

- Asegúrese de que haya un USB insertado en el dispositivo antes de exportar datos o actualizar el sistema. Para evitar fallas, no extraiga el USB ni realice ninguna operación en el dispositivo durante el proceso.
- Puede utilizar un USB para exportar la información de un Dispositivo a otro Dispositivo. No se permite importar imágenes de rostros a través de USB.
- La importación/exportación de registros de asistencia solo está disponible en modelos seleccionados.

2.14.1 Exportar a USB

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

Procedimiento

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

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

- Cuando los datos se exportan en Excel, se pueden editar.
- El disco USB admite el formato FAT32 y la capacidad de almacenamiento es de 4 GB a 128 GB.

  La información personal, los rasgos faciales, los datos de la tarjeta y los datos de las huellas dactilares se cifran al exportar.

2.14.2 Importar desde USB

Puede importar datos desde USB al dispositivo.

Procedimiento

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

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

2.14.3 Actualización del sistema

Actualice el sistema del Dispositivo a través de USB.

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 dispositivo.

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

Paso 3 **ACUERDO**.

El dispositivo se reiniciará cuando se complete la actualización.

No apague el dispositivo durante la actualización.

2.15 Gestión de registros

En el menú principal, seleccione**Gestión de registros**>**Buscar registros de desbloqueo**. Se muestran los registros de desbloqueo. Puede buscar registros por ID de usuario.

2.16 Información del sistema

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

2.16.1 Visualización de la capacidad de datos

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

2.16.2 Visualización de la versión del dispositivo

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

Operaciones relacionadas

Grifo**Código QR del material del producto**, escanee el código QR con su teléfono para ver los documentos del producto.

Esta función solo está disponible en modelos seleccionados.

3 operaciones web

En la página web, también puede configurar y actualizar el Dispositivo.

Las configuraciones web difieren según los modelos del Dispositivo.

3.1 Inicialización

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

Requisitos previos

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

Procedimiento

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

Le recomendamos utilizar la última versión de Chrome o Firefox.

Paso 2 Seleccione un idioma en el Dispositivo.

Paso 3 Configure la contraseña y la dirección de correo electrónico de acuerdo con las instrucciones en pantalla.

- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excluidos ' " ; : &). Establezca una contraseña de alta seguridad mediante siguiendo la indicación 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 Dispositivo en el**DIRECCIÓN**barra y presione la tecla Intro.

Paso 2 Ingrese el nombre de usuario y la contraseña.

- El nombre del administrador predeterminado es admin y la contraseña es la que configuró durante la inicialización. Le recomendamos cambiar la contraseña de administrador periódicamente para aumentar la seguridad.
- Si olvida la contraseña de inicio de sesión del administrador, puede hacer clic en**¿Contraseña olvidada?**para restablecer la contraseña.

Paso 3 Hacer clic**Acceso**.

3.3 Restablecer la contraseña

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

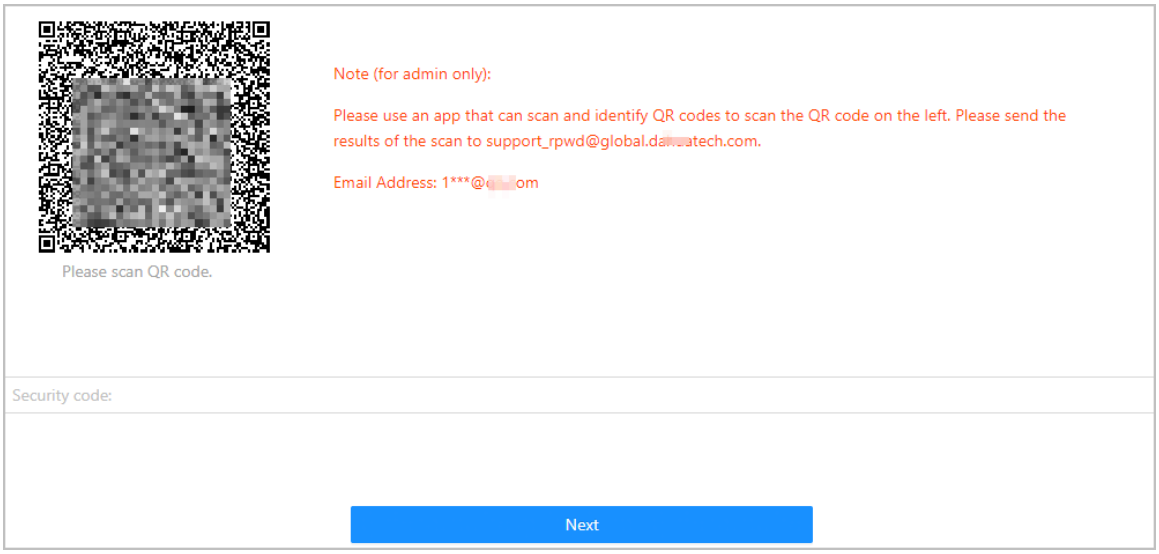
Procedimiento

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

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

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

Figura 3-1 Restablecer contraseña



- Se generarán hasta dos códigos de seguridad cuando se escanee 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 su dirección de correo electrónico vinculada. Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, dejará de ser válido.
- Si se ingresa el código de seguridad incorrecto 5 veces seguidas, la cuenta de administrador se congelará durante 5 minutos.

Etapa 4 Ingrese el código de seguridad.

Paso 5 Hacer clic**Próximo**.

Paso 6 Restablecer y confirmar la contraseña.

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

Paso 7 Hacer clic**DE ACUERDO**.

3.4 Página de inicio

La página de inicio se muestra después de iniciar sesión correctamente.

Figura 3-2 Página de inicio

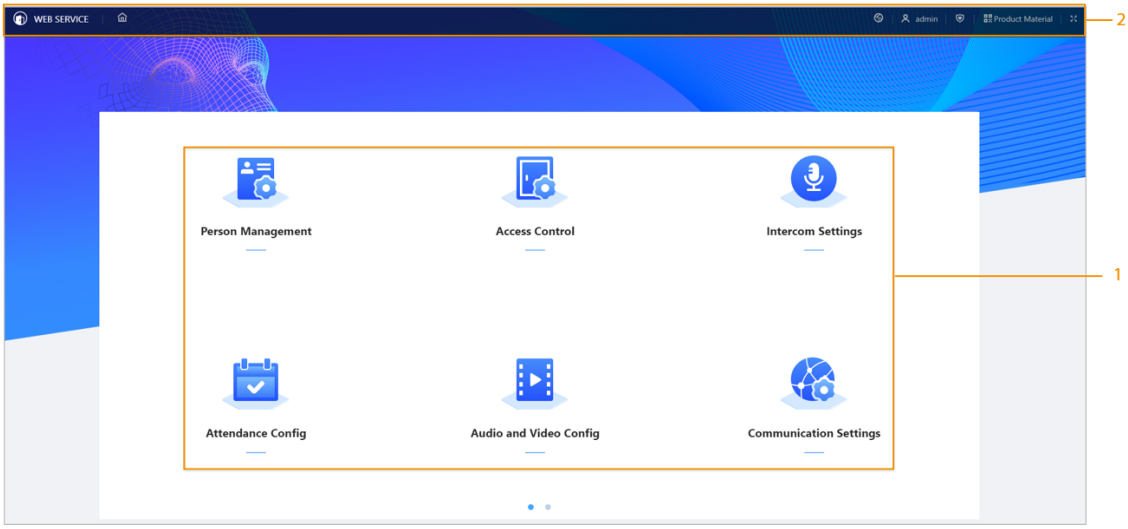


Tabla 3-1 Descripción de la página de inicio

No.	Descripción
1	Menú principal.
2	• : Ingrese a la página de inicio. • : Visualización en pantalla completa. • : Introducir el**Seguridad**página. • Product Material: Escanee el código QR con su teléfono para ver los documentos del producto. Esta función solo está disponible en modelos seleccionados. • admin: cierre sesión o reinicie el dispositivo. • : seleccione un idioma en el dispositivo.

3.5 Gestión de personas

Procedimiento

Paso 1 En la página de inicio, seleccione**Gestión de personas**,y luego haga clic**Agregar**. Configurar

Paso 2 la información del usuario.

Figura 3-3 Agregar usuarios

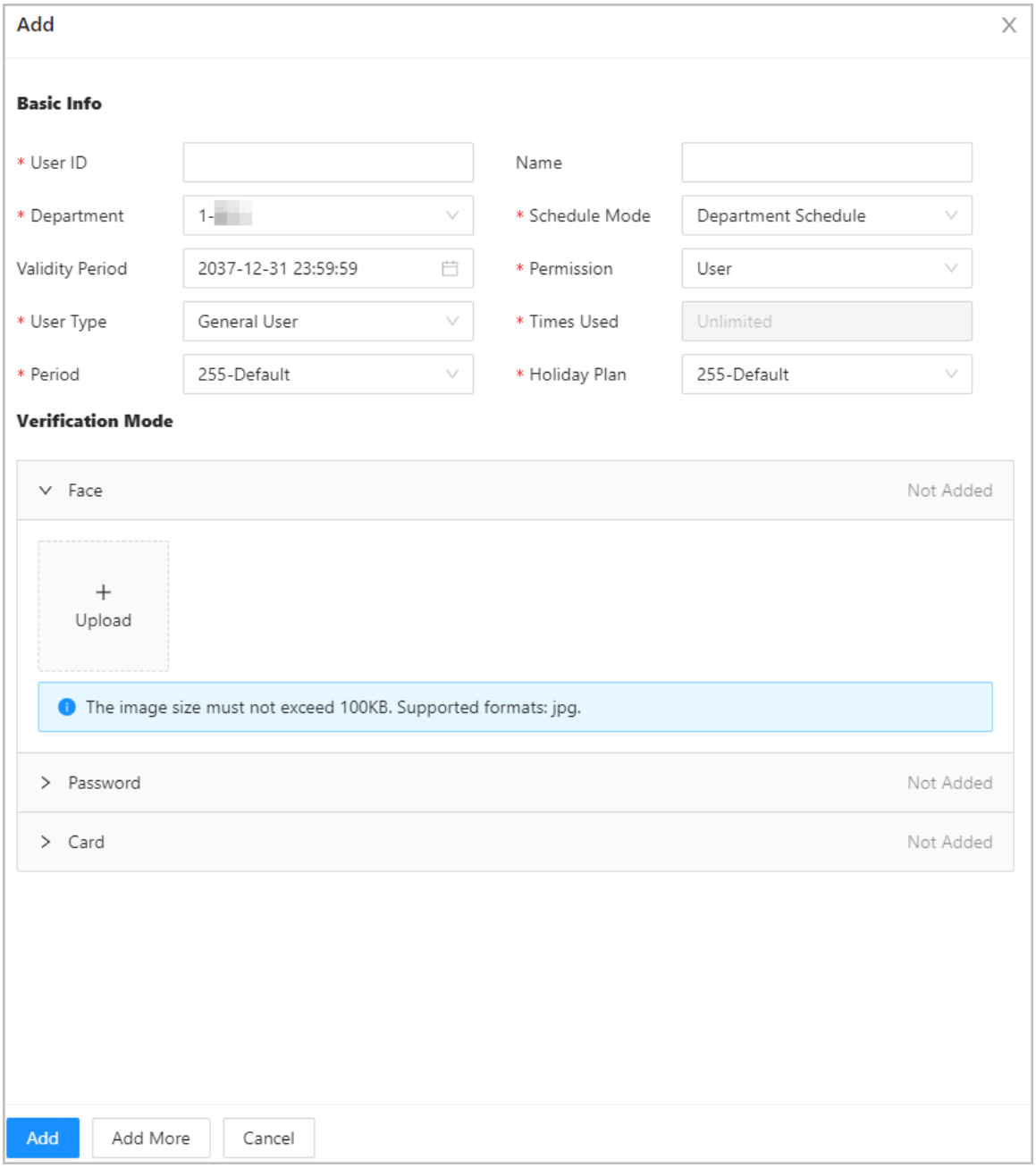


Tabla 3-2 Descripción de los parámetros

Parámetro	Descripción
ID de usuario	La ID de usuario es como la ID de empleado, que puede consistir en números, letras y sus combinaciones, y la longitud máxima del número es de 30 caracteres.
Nombre	El nombre puede tener hasta 32 caracteres (incluidos números, símbolos y letras).

Parámetro	Descripción
Departamento	Agregar usuarios a un departamento. Si se asigna un horario de departamento a la persona, seguirá el horario de departamento establecido. Para saber cómo crear un departamento, consulte "2.10.1 Configurar departamentos".
Modo de programación	● Horario del departamento: Asigne el horario del departamento al usuario. Para obtener más información, consulte "2.10.4 Configuración de horarios de trabajo". ● Horario personal: Asigne un horario personal al usuario. Para obtener más información, consulte "2.10.4 Configuración de horarios de trabajo".  ◇ Esta función solo está disponible en modelos seleccionados. ◇ Si configura el modo de programación en programación de departamento aquí, la programación personal que haya configurado para el usuario en**Asistencia**>**Programar configuración**>**Horario personal**es inválido.
Período de validez	Establezca una fecha en la que expirarán los permisos de acceso y asistencia de la persona.
Permiso	● **Usuario**:Los usuarios solo tienen acceso a la puerta o permisos de asistencia. ● **Administración**:Los administradores pueden configurar el dispositivo además de los permisos de acceso y asistencia.
Tipo de usuario	● **Usuario general**:Los usuarios generales pueden desbloquear la puerta. ● **Usuario de la lista de bloqueo**:Cuando los usuarios en la lista de bloqueo desbloquean la puerta, el personal de servicio recibirá una notificación. ● **Usuario invitado**:Los huéspedes pueden desbloquear la puerta dentro de un período definido o durante una determinada cantidad de veces. Una vez transcurrido el período definido o los tiempos de desbloqueo, no pueden desbloquear la puerta. ● **Usuario de patrulla**:Los usuarios de patrulla pueden controlar la asistencia en el dispositivo, pero no tienen permisos de entrada. ● **Usuario VIP**:Cuando VIP abra la puerta, el personal de servicio recibirá un aviso. ● **Otro usuario**:Cuando desbloqueen la puerta, la puerta permanecerá desbloqueada durante 5 segundos más. ● Usuario personalizado 1/Usuario personalizado 2: Lo mismo con los usuarios generales.
Tiempo utilizado	Establezca un límite de desbloqueo para usuarios invitados. Una vez transcurrido el tiempo de desbloqueo, no pueden desbloquear la puerta.
Período	Las personas pueden desbloquear la puerta o pasar lista durante el período definido.  Puede seleccionar más de un período.

Parámetro	Descripción
Plan de vacaciones	Las personas pueden desbloquear la puerta o pasar lista durante el feriado definido.  Puede seleccionar más de un día festivo.
Rostro	Hacer clic**Subir**para cargar una imagen de cara. Cada persona sólo puede agregar hasta 2 imágenes de rostros. Puede ver o eliminar la imagen de la cara después de cargarla.  La imagen del rostro está en formato jpg, jpeg, png y debe tener menos de 100 KB.
Tarjeta	 Esta función solo está disponible en modelos seleccionados. ● Ingrese el número de tarjeta manualmente. 1. Haga clic**Agregar**. 2. Ingrese el número de tarjeta y luego haga clic en**Agregar**. ● Lea el número automáticamente a través del lector de inscripción o del Dispositivo. 1. Haga clic**Agregar**,y luego haga clic**Modificar**para seleccionar un lector de inscripción o el Dispositivo. 2. Haga clic**Leer tarjeta**y luego pase las tarjetas por el lector de tarjetas. Se muestra una cuenta regresiva de 60 segundos para recordarle que pase las tarjetas y el sistema leerá el número de la tarjeta automáticamente. Si la cuenta regresiva de 60 segundos expira, haga clic en**Leer tarjeta**nuevamente para iniciar una nueva cuenta regresiva. 3. Haga clic**Agregar**. Un usuario puede registrar hasta 5 tarjetas como máximo. Ingrese el número de su tarjeta o pase la tarjeta y luego el dispositivo 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. ●  : Establecer tarjeta de coacción. : ●  Cambiar número de tarjeta.  Un usuario sólo puede configurar una tarjeta de coacción.
Contraseña	Ingrese la contraseña de usuario. La longitud máxima de la contraseña es de 8 dígitos. La contraseña de coacción es la contraseña de desbloqueo + 1. Por ejemplo, si la contraseña de usuario es 12345, la contraseña de coacción será 12346. Se activará una alarma de coacción cuando se utilice una contraseña de coacción para desbloquear la puerta.

Parámetro	Descripción
FP	Registrar huellas dactilares. Un usuario puede registrar hasta 3 huellas digitales y usted puede configurar una huella digital para la huella digital de coacción. Se activará una alarma cuando se utilice la huella digital de coacción para desbloquear la puerta. Registre huellas digitales a través de un lector de inscripción o el Dispositivo. 1. Haga clic**Agregar**,y luego haga clic**Modificar**para seleccionar un lector de inscripción o el Dispositivo. 2. Presione con el dedo el escáner según las instrucciones que aparecen en pantalla. 3. Haga clic**Agregar**. ● La función de huella digital solo está disponible en modelos selectos. ● No recomendamos configurar la primera huella digital como huella digital de coacción. ● Un usuario sólo puede establecer una huella digital de coacción. ● La función de huellas dactilares está disponible si el dispositivo admite la conexión de un módulo de huellas dactilares.

Paso 3 Hacer clic**DE ACUERDO**.

Operaciones relacionadas

- Importar información del usuario: haga clic**Plantilla de exportación**,y descargue la plantilla e ingrese la información del usuario en ella. Coloque las imágenes de rostros y la plantilla en la misma ruta de archivo y luego haga clic en **Importar información de usuario**para importar la carpeta.

  Se pueden importar hasta 10.000 usuarios a la vez.
- Borrar: borra todos los usuarios.
- Actualizar: actualiza la lista de usuarios.
- Buscar: busque por nombre de usuario o ID de usuario.

3.6 Configurar el control de acceso

3.6.1 Configuración de parámetros de control de acceso

3.6.1.1 Configuración de parámetros básicos

Procedimiento

Paso 1 Seleccionar**Control de acceso**>**Parámetros de control de acceso**.

Paso 2 En**Ajustes básicos**, configurar parámetros básicos para el control de acceso.

Figura 3-4 Parámetros básicos

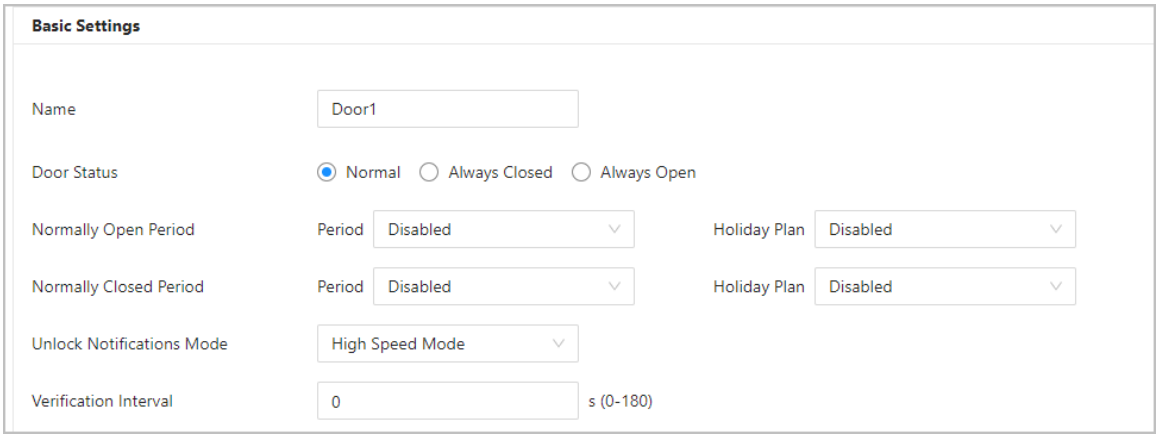


Tabla 3-3 Descripción de los parámetros básicos

Parámetro	Descripción
Nombre	El nombre de la puerta.
Estado de la puerta	Establecer el estado de la puerta. ● Normal: la puerta se desbloqueará y bloqueará según su configuración. ● Siempre abierta: la puerta permanece desbloqueada todo el tiempo. ● Siempre Cerrada: La puerta permanece cerrada todo el tiempo.
Periodo normalmente abierto Periodo normalmente cerrado	Cuando seleccionas**Normal**, puede seleccionar una plantilla de tiempo de la lista desplegable. La puerta permanece abierta o cerrada durante el tiempo definido. Para obtener detalles sobre cómo configurar períodos y planes de vacaciones, consulte "3.6.8 Configuración de horarios". ● Cuando el período normalmente abierto entra en conflicto con el período normalmente cerrado, el período normalmente abierto tiene prioridad sobre el período normalmente cerrado. ● Cuando el período entra en conflicto con el plan de vacaciones, los planes de vacaciones tienen prioridad sobre los períodos.
Notificación de desbloqueo	Muestra la notificación en la pantalla cuando una persona verifica su identidad en el Dispositivo. ● Modo de alta velocidad: el sistema le indica**Verificado con éxito**o **No autorizado**en la pantalla. ● Modo simple: muestra la identificación del usuario, el nombre y la hora de verificación después de otorgar el acceso; muestra**No autorizado**y tiempo de autorización después del acceso denegado. ● Estándar: muestra la imagen del rostro registrado del usuario, la identificación del usuario, el nombre y la hora de verificación después de otorgar el acceso; muestra**No autorizado** y tiempo de verificación después del acceso denegado. ● Modo de contraste: muestra la imagen del rostro capturada y una imagen del rostro registrada de un usuario, ID de usuario, nombre y hora de autorización después de otorgar el acceso; muestra**No autorizado**y tiempo de autorización después del acceso denegado.

Parámetro	Descripción
Intervalo de verificación	Si verifica su identidad varias veces dentro de un período determinado, solo la primera verificación se considerará válida y la puerta no se abrirá después de la segunda o posteriores verificaciones. Desde el momento en que la puerta no se abre, deberá esperar el intervalo de tiempo de verificación configurado antes de intentar verificar su identidad nuevamente.

Paso 3 Hacer clic**Aplicar**.

3.6.1.2 Configurar métodos de desbloqueo

Puede utilizar varios métodos de desbloqueo para desbloquear la puerta, como huella digital, tarjeta y contraseña. También puedes combinarlos para crear tu propio método de desbloqueo personal.

Procedimiento

Paso 1 Seleccionar**Control de acceso**>**Parámetros de control de acceso**. En

Paso 2 **Configuración de desbloqueo**, selecciona un modo de desbloqueo.

- Desbloqueo combinado

  1. Seleccione**Desbloqueo combinado**desde el**Modo de desbloqueo**lista.
  2. Seleccione**O**o**Y**.
     - ◇ O: utilice uno de los métodos de desbloqueo seleccionados para abrir la puerta. Y: utilice
     - ◇ todos los métodos de desbloqueo seleccionados para abrir la puerta.
  3. Seleccione los métodos de desbloqueo y luego configure otros parámetros.

Figura 3-5 Configuración de desbloqueo

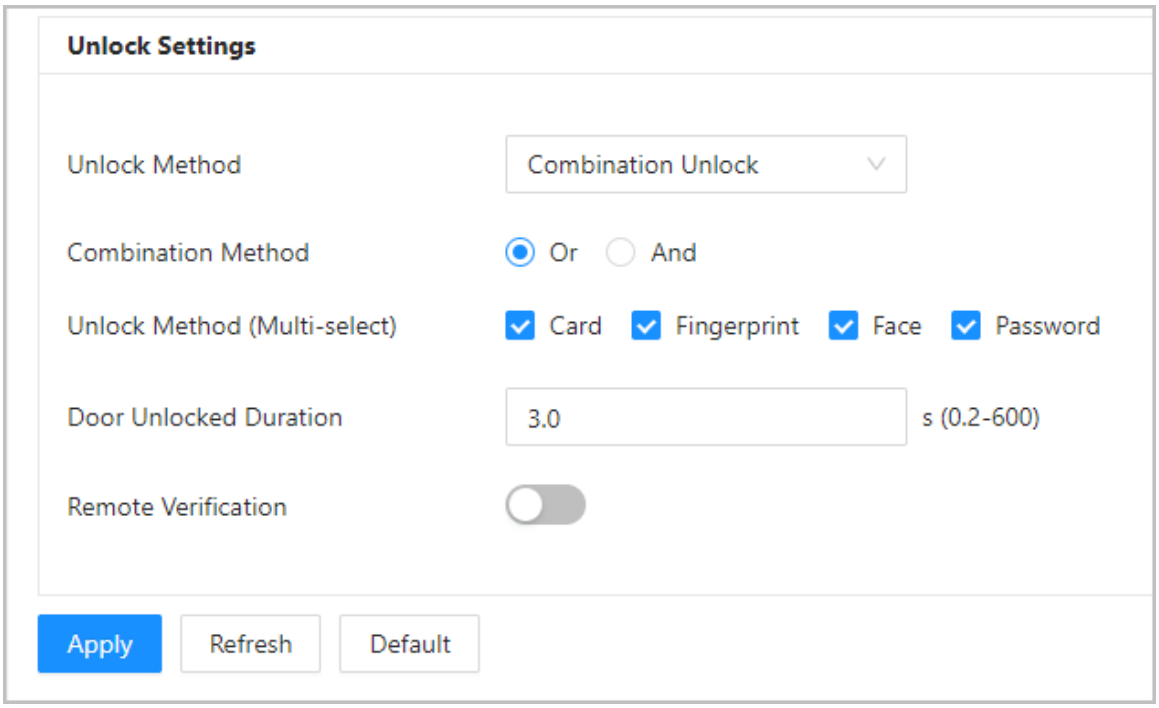


Tabla 3-4 Descripción de la configuración de desbloqueo

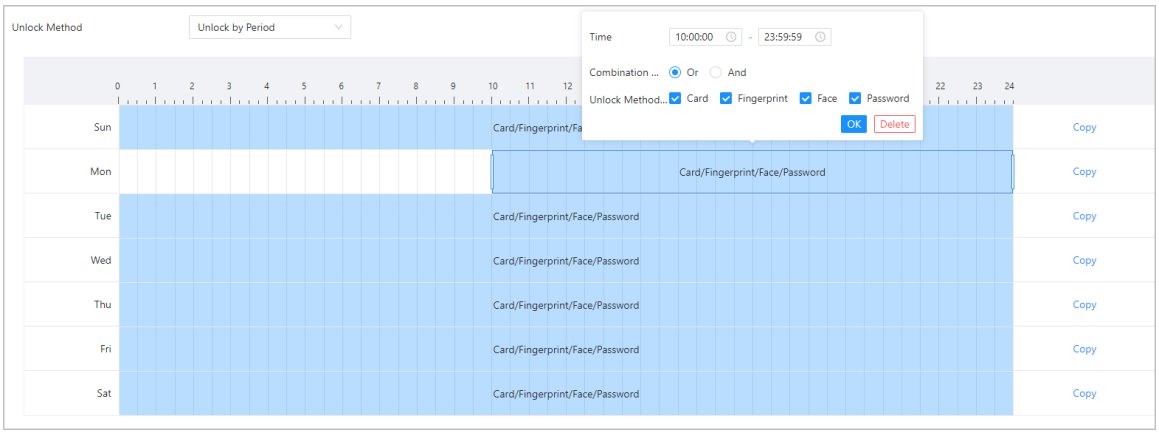
Parámetro	Descripción
Método de desbloqueo (selección múltiple)	Los métodos de desbloqueo pueden diferir según los modelos de producto.
Duración del desbloqueo de la puerta	Después de que se le conceda acceso a una persona, la puerta permanecerá desbloqueada durante un tiempo definido para que pueda pasar. Varía de 0,2 a 600 segundos.
Tiempo de espera de desbloqueo	Cuando el detector de puerta y la alarma de tiempo de espera de desbloqueo están habilitados, se activará una alarma de tiempo de espera si la puerta permanece desbloqueada por más tiempo que el tiempo de desbloqueo definido.
Verificación Remota	Abra la puerta de forma remota.

- Desbloquear por período

1. En el**Modo de desbloqueo**lista, seleccione**Desbloquear por período**.
2. Arrastre el control deslizante para ajustar el período de tiempo para cada día.

   También puedes hacer clic**Copiar**para aplicar el periodo de tiempo configurado a otros días.
3. Seleccione un método de desbloqueo para el período de tiempo y luego configure otros parámetros.

Figura 3-6 Desbloqueo por período



- Desbloqueo por múltiples usuarios.

1. En el**Modo de desbloqueo**lista, seleccione**Desbloqueo por múltiples usuarios**.
2. Haga clic**Agregar**para agregar grupos.
3. Seleccione el método de desbloqueo, el número válido y la lista de usuarios.
   - ◇ Si solo se agrega un grupo, la puerta se desbloquea solo después de que el número de personas del grupo que otorgan acceso sea igual al número válido definido.
   - ◇ Si se agregan más de un grupo, la puerta se desbloquea solo después de que el número de personas de cada grupo que otorgan acceso sea igual al número válido definido.

◇ Puedes agregar hasta 4 grupos.

◇ El número válido indica la cantidad de personas en cada grupo que necesitan verificar sus identidades en el Dispositivo antes de que se desbloquee la puerta. Por ejemplo, si el número válido se establece en 3 para un grupo, 3 personas cualesquiera del grupo deberán verificar sus identidades para desbloquear la puerta.

Paso 3 Hacer clic**Aplicar**.

3.6.2 Configuración de alarmas

Se activará una alarma cuando ocurra un evento de acceso anormal.

Procedimiento

Paso 1 Seleccionar**Control de acceso**>**Alarma**>**Alarma**.

Paso 2 Configurar los parámetros de alarma.

Figura 3-7 Alarma

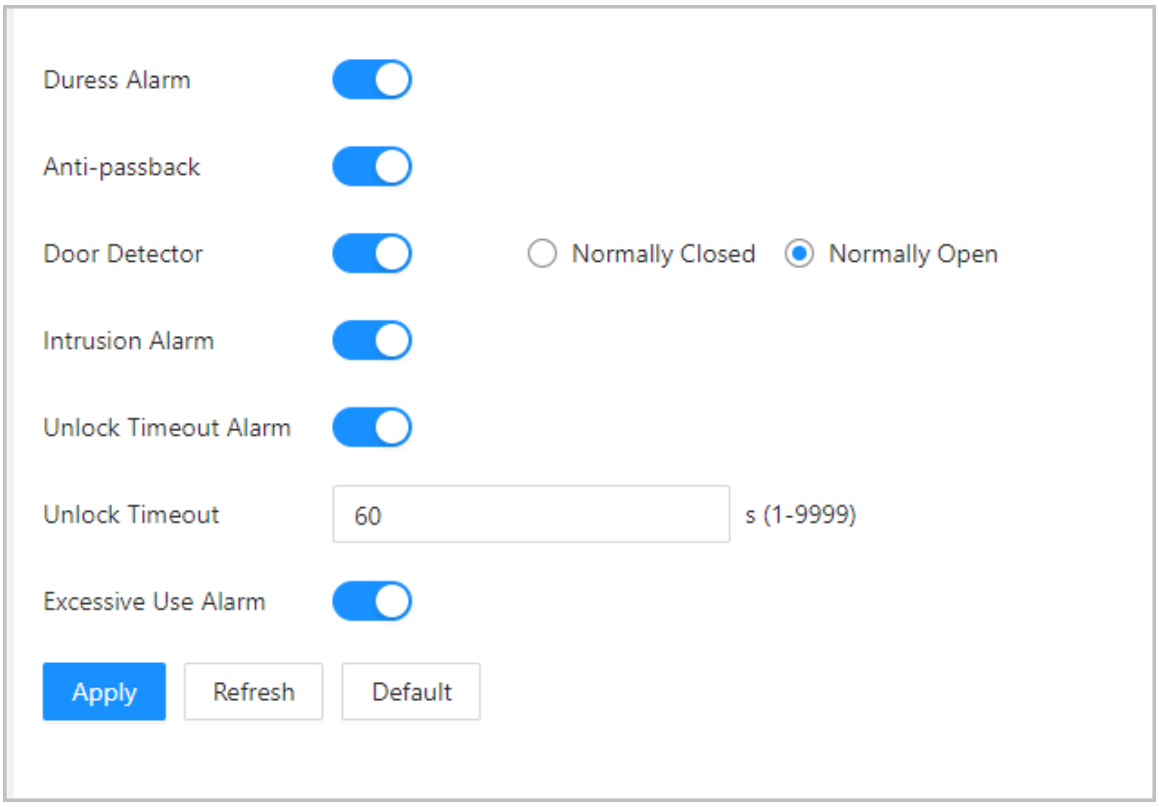


Tabla 3-5 Descripción de los parámetros de alarma

Parámetro	Descripción
Alarma de 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.

Parámetro	Descripción
Anti-passback	Los usuarios deben verificar sus identidades tanto para entrar como para salir; de lo contrario se activará una alarma. Ayuda a evitar que el titular de una tarjeta le pase una tarjeta de acceso a otra persona para poder entrar. Cuando el anti-passback está habilitado, el titular de la tarjeta debe abandonar el área segura a través de un lector de salida antes de que el sistema le permita otra entrada. ● Si una persona entra sin autorización y sale sin autorización, se activará una alarma cuando intente volver a entrar y al mismo tiempo se le negará el acceso. ● Si una persona entra sin autorización y sale después de la autorización, se activará una alarma cuando intente entrar nuevamente y al mismo tiempo se le negará el acceso.  Si el Dispositivo solo puede conectar una cerradura, verificar en el Dispositivo significa la dirección de entrada y verificar en el lector de tarjetas externo significa la dirección de salida de forma predeterminada. Puede modificar la configuración en la plataforma de gestión.
Detector de puerta	Con el detector de puertas conectado a su dispositivo, la alarma se puede activar cuando las puertas se abren o cierran de manera anormal. El detector de puerta incluye 2 tipos, incluido el detector NC y el detector NO. ● Normalmente cerrado: el sensor está en una posición de cortocircuito cuando la puerta o ventana está cerrada. ● Normalmente abierto: se crea un circuito abierto cuando la ventana o puerta está realmente cerrada.
Alarma de intrusión	Si la puerta se abre de forma anormal, se activará una alarma de intrusión que durará un tiempo definido.  Es necesario habilitar al mismo tiempo el detector de puerta y el de intrusión.
Desbloquear alarma de tiempo de espera Tiempo de espera de desbloqueo	Cuando la puerta permanece desbloqueada por más tiempo que el tiempo de espera definido, la alarma de tiempo de espera de la puerta se activará y durará el tiempo definido.  El detector de puerta y la función de tiempo de espera de puerta deben habilitarse al mismo tiempo.
Alarma de uso excesivo	Si se utiliza la contraseña o tarjeta incorrecta 5 veces seguidas en 60 segundos, se activará la alarma por uso excesivo de tarjeta ilegal y durará un tiempo definido.

Paso 3 Hacer clic**Aplicar**.

3.6.3 Configuración de enlaces de alarma (opcional)

Puede configurar enlaces de alarma.

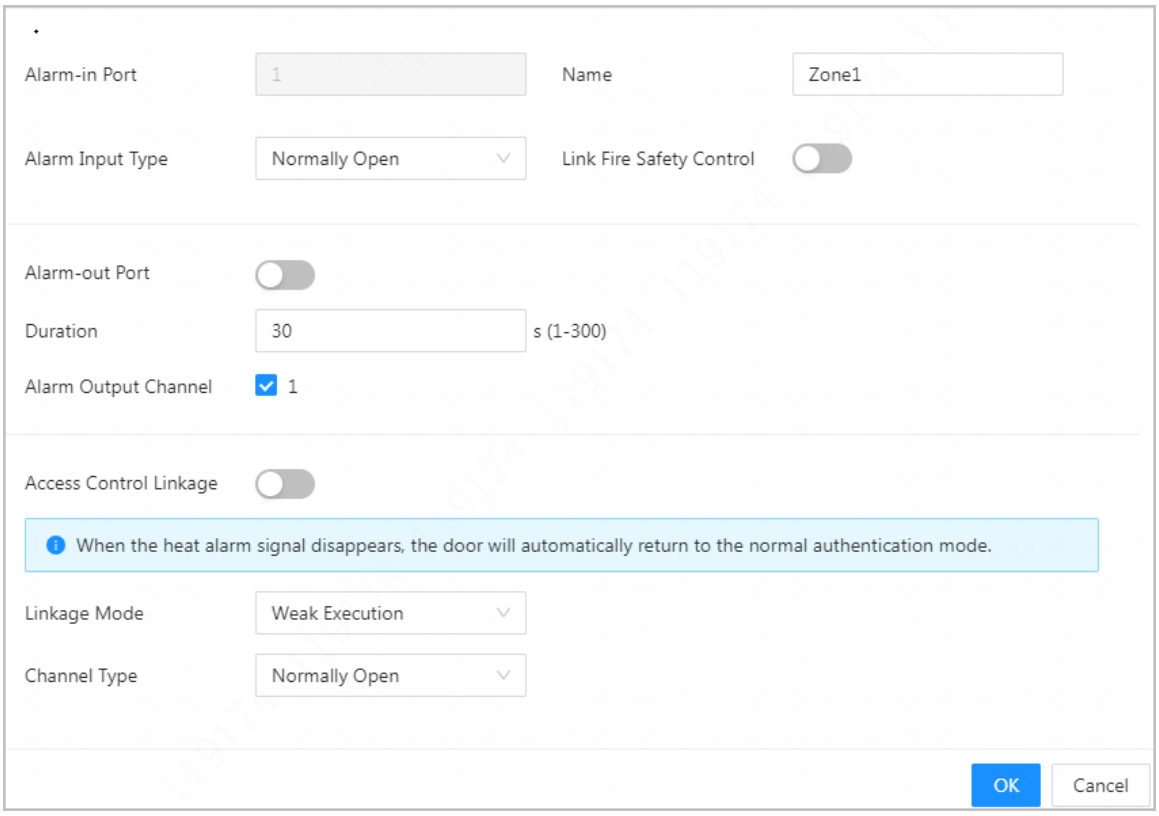
Procedimiento

Paso 1 Seleccionar**Control de acceso**>**Alarma**>**Configuración de vinculación de alarma**.

- Si el Dispositivo se agrega a una plataforma de administración, la configuración de la alarma se sincronizará con la plataforma.
- Esta función solo está disponible en modelos que tienen puertos de entrada y salida de alarma.
- La cantidad de puertos de entrada y salida de alarma varía según los modelos del producto.

Paso 2 Hacer clic para configurar la alarma.

Figura 3-8 Vinculación de alarma



Paso 3 Cree un nombre para la zona de alarma.

Etapa 4 Permitir**Enlace de control de seguridad contra incendios**y seleccione un tipo para el dispositivo de entrada de alarma.

- Normalmente cerrado: la entrada de alarma está en un estado de circuito normalmente cerrado (NC) cuando la alarma no se ha disparado. La apertura de un circuito normalmente cerrado activa la alarma.
- Normalmente abierto: el dispositivo de entrada de alarma está en un estado de circuito normalmente abierto (NO) cuando la alarma no se ha disparado. Cerrar el circuito activa la alarma.

Paso 5 Si desea vincular el control de acceso cuando se activa la alarma de incendio, habilite**Enlace de control de acceso**.

Esta función surte efecto sólo después**Enlace de control de seguridad contra incendios**está habilitado.

Paso 6 Seleccione un modo de vinculación.

- Ejecución sólida: cuando la señal de alarma contra incendios desaparece, la puerta permanece en el estado actual. Cambie manualmente a la configuración anterior del estado de la puerta si lo desea.
- Ejecución débil: cuando la señal de alarma contra incendios desaparece, la puerta vuelve automáticamente a su estado anterior.

Paso 7 Seleccione un tipo de canal.

- Normalmente abierta: la puerta se abre automáticamente cuando se activa la alarma contra incendios.
- Normalmente cerrada: la puerta se cierra automáticamente cuando se activa la alarma contra incendios.

Paso 8 Hacer clic**DE ACUERDO**.

3.6.4 Configuración de la vinculación de eventos de alarma

Procedimiento

Paso 1 Sobre el**Menú principal**, seleccionar**Control de acceso**>**Alarma**>**Vinculación de eventos de alarma**.

Paso 2 Configurar enlaces de eventos de alarma.

Figura 3-9 Vinculación de eventos de alarma

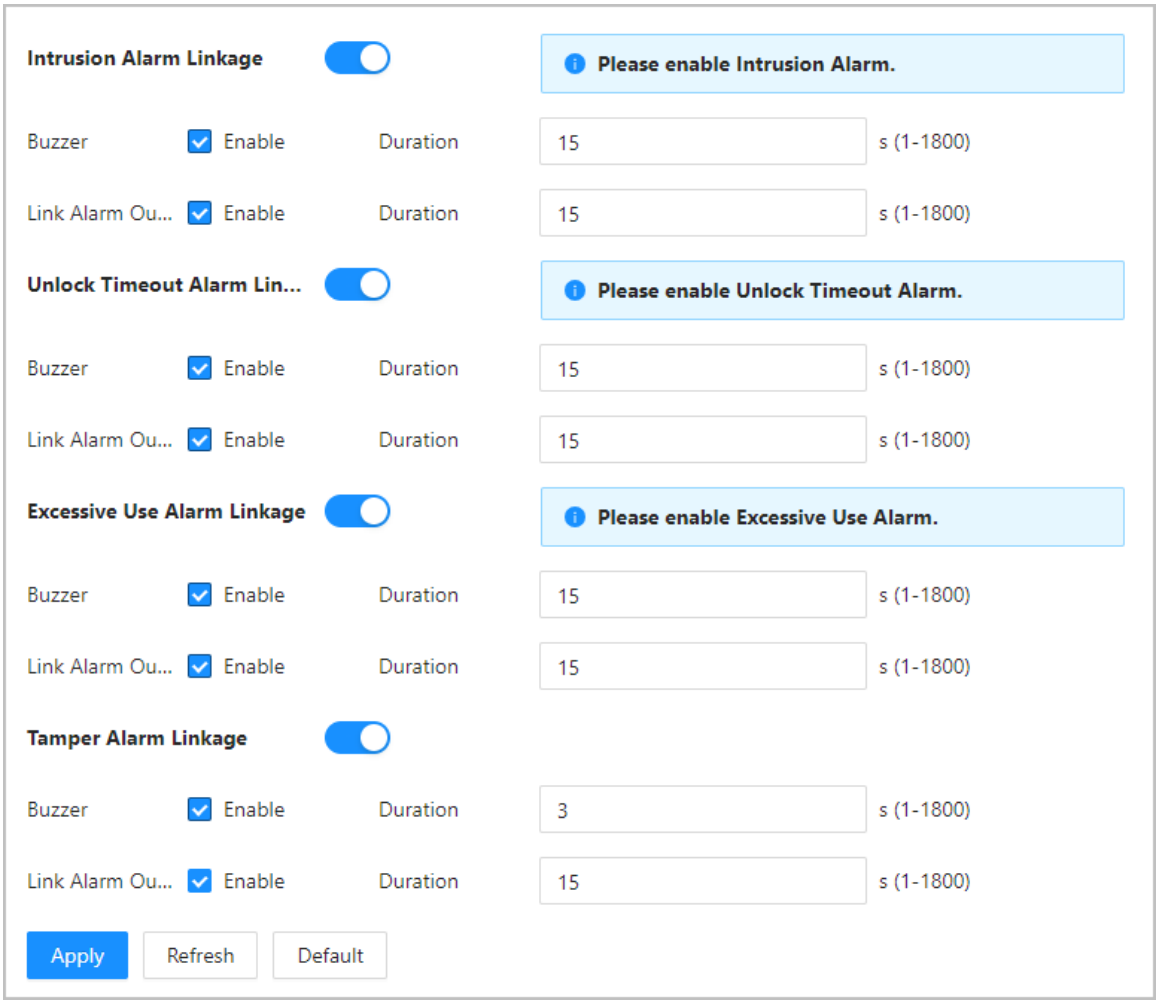


Tabla 3-6 Vinculación de eventos de alarma

Parámetro	Descripción
Enlace de alarma de intrusión	Si la puerta se abre de forma anormal, se activará una alarma de intrusión. ● Zumbador: El zumbador suena cuando se activa una alarma de intrusión. Puede configurar la duración de la alarma. ● Enlace de salida de alarma: el dispositivo de alarma externo genera alarmas cuando se activa la alarma de intrusión. Puede configurar la duración de la alarma.
Desbloquear alarma de tiempo de espera Enlace	Cuando la puerta permanece desbloqueada por más tiempo que el tiempo de espera definido, la alarma de tiempo de espera de la puerta se activará y durará el tiempo definido. ● Zumbador: El zumbador suena cuando se activa la alarma de tiempo de espera de desbloqueo. Puede configurar la duración de la alarma. ● Salida de alarma local: el dispositivo de alarma externo genera alarmas cuando se activa la alarma de tiempo de espera de desbloqueo. Puede configurar la duración de la alarma.
Alarma de uso excesivo Enlace	Si se utiliza la contraseña o tarjeta incorrecta 5 veces seguidas en 60 segundos, se activará la alarma por uso excesivo de tarjeta ilegal y durará un tiempo definido. ● Zumbador: El zumbador suena cuando se activa la alarma de uso excesivo. Puede configurar la duración de la alarma. ● Salida de alarma local: el dispositivo de alarma externo genera alarmas cuando se activa la alarma de tiempo de espera de desbloqueo. Puede configurar la duración de la alarma.
Conexión de alarma de manipulación	La alarma de manipulación se activa cuando alguien intenta dañar físicamente el Dispositivo. ● Zumbador: El zumbador suena cuando se activa la alarma de manipulación. Puede configurar la duración de la alarma. ● Salida de alarma local: el dispositivo de alarma externo genera alarmas cuando se activa la alarma de manipulación. Puede configurar la duración de la alarma.

3.6.5 Configurar la detección de rostros

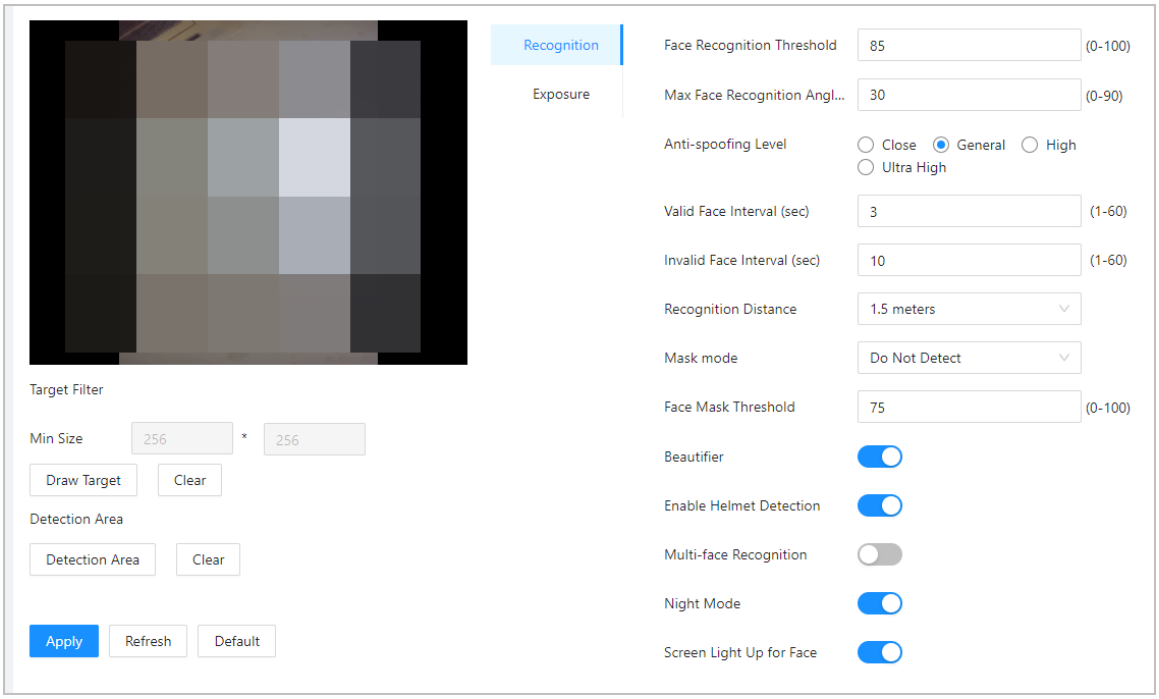
Configure los parámetros de detección de rostros. Los parámetros faciales pueden diferir según los modelos del producto.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Control de acceso**>**Detección de rostro**.

Figura 3-10 Parámetros de detección de rostros



Paso 3 Configure los parámetros.

Tabla 3-7 Descripción de los parámetros de la cara

Nombre	Descripción
Umbral de reconocimiento facial	Ajuste el nivel de precisión del reconocimiento facial. Un umbral más alto significa una mayor precisión y una menor tasa de reconocimiento falso. Cuando el umbral es demasiado bajo, como 0, la tasa de reconocimiento falso será extremadamente alta. Por favor tenga en cuenta.
Desviación máxima del ángulo de reconocimiento facial	Establezca el ángulo más grande en el que se puede colocar una cara para la detección de caras. Cuanto mayor sea el valor, mayor será el rango del ángulo de la cara. Si el ángulo en el que se coloca una cara no está dentro del rango definido, es posible que no se detecte correctamente.
Nivel anti-suplantación de identidad	Esto evita que las personas puedan utilizar fotos, vídeos, máscaras y otros sustitutos para obtener acceso no autorizado.
Iluminador	• Automático: el iluminador se enciende en condiciones de poca luz. • Desactivar: El iluminador está apagado todo el tiempo. Esta función solo está disponible en modelos seleccionados.
Intervalo de cara válido (seg)	Cuando la misma cara permanece frente a la lente después del primer reconocimiento exitoso, el Dispositivo realizará nuevamente el reconocimiento de la cara después de un intervalo definido.

Nombre	Descripción
Intervalo de cara no válido (seg)	Cuando la misma cara permanece frente a la lente después del primer reconocimiento fallido, el Dispositivo realizará nuevamente el reconocimiento de la cara después de un intervalo definido.
Distancia de reconocimiento	La distancia entre la cara y la lente.
Modo máscara	• **No detectar**:La máscara no se detecta durante el reconocimiento facial. • **Recordatorio de máscara**:La máscara se detecta durante el reconocimiento facial. Si la persona no lleva mascarilla, el sistema le recordará que la use, pero aún así se le permitirá el acceso. • **Sin autorización sin usar mascarilla**:La máscara se detecta durante el reconocimiento facial. Si una persona no lleva mascarilla, el sistema le recordará que la use y se le negará el acceso.
Umbral de mascarilla	Cuanto más alto sea el umbral, más preciso será el reconocimiento facial cuando una persona use una máscara y habrá una menor tasa de falso reconocimiento.
embellecedor	Embellece las imágenes de rostros capturados.
Habilitar detección de casco	Detecta gorros de seguridad. La puerta no se desbloqueará si una persona no usa casco.
Reconocimiento multicara	Detecta de 4 a 6 imágenes de rostros a la vez. El desbloqueo combinado no se puede usar con esto y la puerta se desbloqueará cuando una de las personas sea verificada exitosamente.  La cantidad de imágenes de rostros admitidas puede variar según el modelo del producto.
Modo nocturno	En ambientes oscuros, la pantalla de espera muestra una imagen de fondo blanca para mejorar el brillo al verificar el rostro o el código QR.
Pantalla iluminada para la cara	En el estado de pantalla apagada, la pantalla se iluminará cuando se detecte una cara.

Etapa 4 Configure los parámetros de exposición.

Figura 3-11 Parámetros de exposición

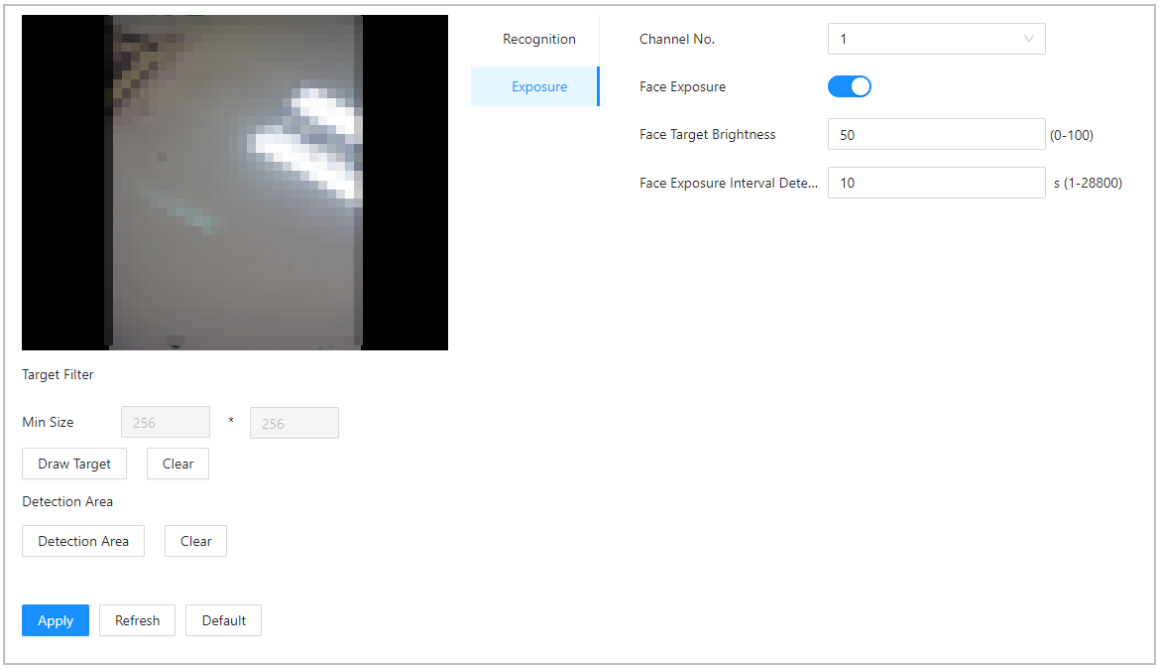


Tabla 3-8 Descripción de los parámetros de exposición

Parámetro	Descripción
Canal No.	• El canal 1 es el modo de luz blanca. • El canal 2 es el modo de luz infrarroja.
Exposición facial	Una vez habilitada la función de exposición del rostro, el rostro se expondrá con el brillo definido para detectar la imagen del rostro con claridad.
Brillo del objetivo de la cara	
Detección de intervalo de exposición facial	La cara quedará expuesta sólo una vez en un intervalo definido.

Paso 5 Dibuja el área de detección de rostros.

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

Se detectará el rostro en el área definida. Dibuja el

Paso 6 tamaño del objetivo.

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

Solo cuando el tamaño de la cara es mayor que el tamaño definido, el dispositivo puede detectar la cara.

Paso 7 Dibuja el área de detección. Hacer clic**DE**

Paso 8 **ACUERDO**.

3.6.6 Configuración de los ajustes de la tarjeta

Información de contexto

Esta función solo está disponible en modelos seleccionados.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Control de acceso**>**Configuración de tarjeta**

Paso 3 . Configure los parámetros de la tarjeta.

Figura 3-12 Parámetros de la tarjeta

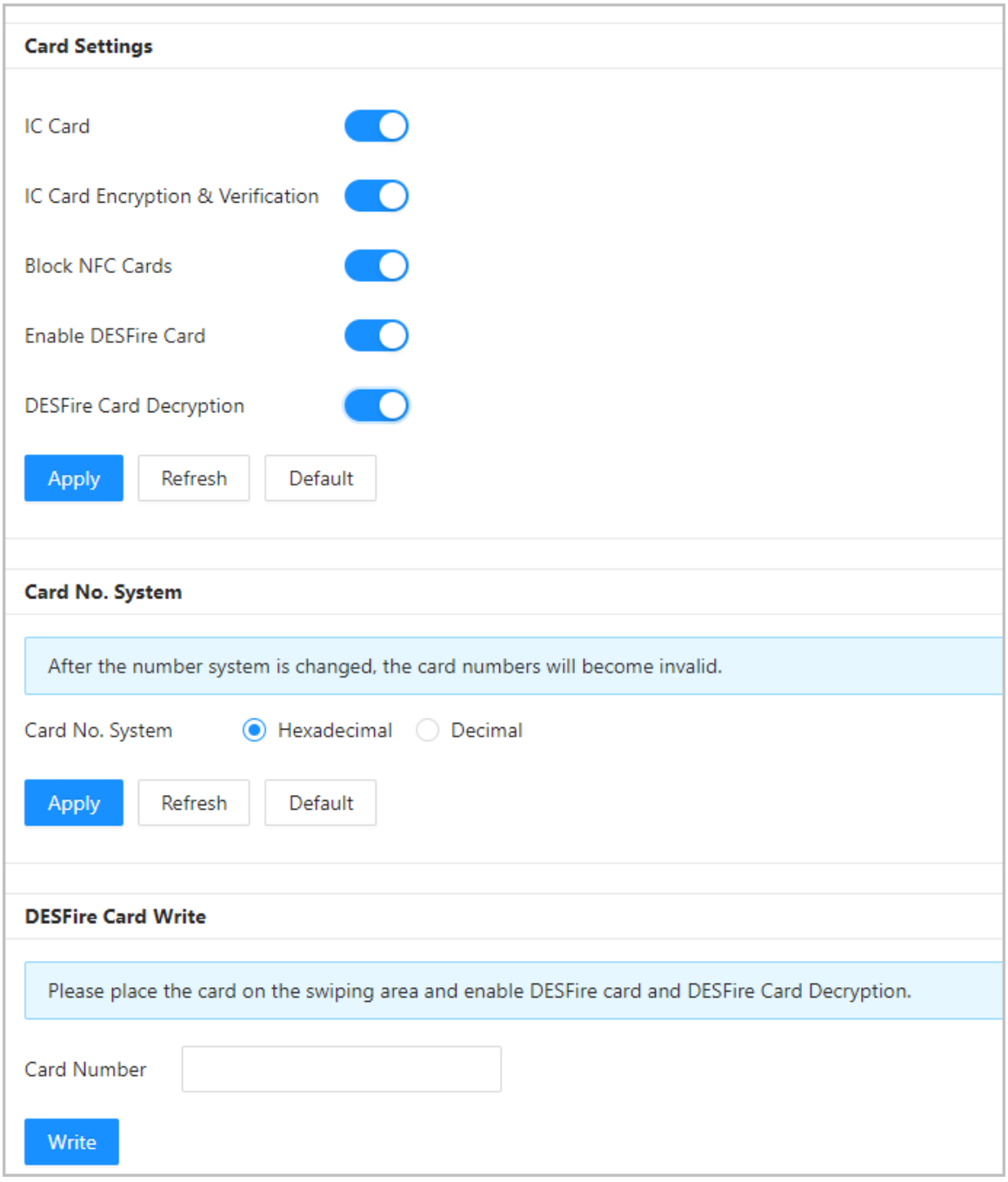


Tabla 3-9 Descripción de los parámetros de la tarjeta

Artículo	Parámetro	Descripción
Configuración de tarjeta	Tarjeta IC	La tarjeta IC se puede leer cuando esta función está habilitada. Esta función solo está disponible en modelos seleccionados.
	Cifrado y verificación de tarjetas IC	La tarjeta cifrada se puede leer cuando esta función está habilitada. Cerciorarse**Tarjeta IC**está habilitado.
	Bloquear tarjetas NFC	Evite el desbloqueo mediante tarjeta NFC duplicada después de habilitar esta función. ● Esta función solo está disponible en modelos que admiten tarjetas IC. ● Cerciorarse**Tarjeta IC**está habilitado. ● La función NFC solo está disponible en determinados modelos de teléfonos.
	Habilitar tarjeta Desfire	El dispositivo puede leer el número de tarjeta de Desfire cuando esta función está habilitada. ● Esta función solo está disponible en modelos que admiten tarjetas IC. ● Sólo admite formato hexadecimal.
	Descifrado de la tarjeta Desfire	La información de la tarjeta Desfire se puede leer cuando**Habilitar tarjeta Desfire**y**Descifrado de la tarjeta Desfire**están habilitados al mismo tiempo. ● Esta función solo está disponible en modelos que admiten tarjetas IC. ● Asegúrese de que la tarjeta Desfire esté habilitada.
Sistema de número de tarjeta	Sistema de número de tarjeta	Seleccione el formato decimal o hexadecimal para el número de tarjeta cuando el lector de tarjetas Wiegand esté conectado. El sistema de número de tarjeta es el mismo tanto para la entrada como para la salida del número de tarjeta.

Artículo	Parámetro	Descripción
Escritura de tarjeta DESFire	Número de tarjeta	Coloque la tarjeta en el lector, ingrese el número de tarjeta y luego haga clic en**Escribir**para escribir el número de tarjeta en la tarjeta. ● La función de la tarjeta Desfire debe estar habilitada. ● Sólo admite formato hexadecimal. ● Admite hasta 8 caracteres.

Etapa 4 Hacer clic**Aplicar**.

3.6.7 Configurar el código QR

Procedimiento

Paso 1 En la página web, seleccione**Control de acceso**>**Configuración de tarjeta**.

Figura 3-13 Código QR

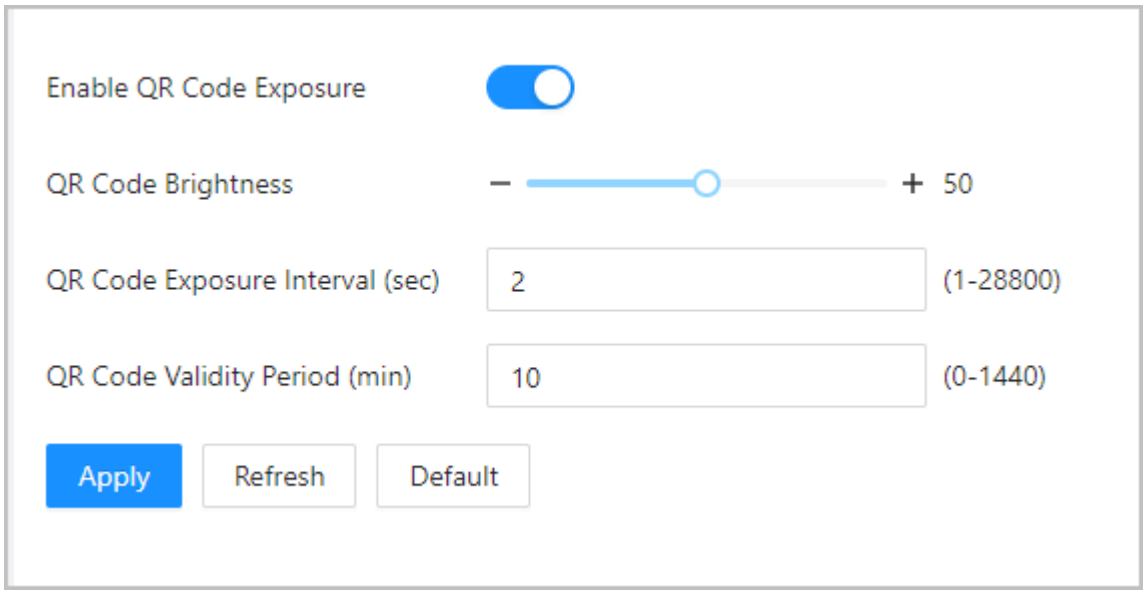


Tabla 3-10 Parámetros del código QRR

Parámetros	Descripción
Habilitar la exposición del código QR	El código QR quedará expuesto con el brillo definido y podrá detectarse y leerse claramente.
Brillo del código QR	
Intervalo de exposición del código QR (seg)	El código QR será expuesto sólo una vez durante el intervalo definido.
Período de validez del código QR (min)	Después de que se genere el código QR, la validez de sus códigos QR durará un tiempo definido antes de que caduque.

3.6.8 Configuración de horarios

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

3.6.8.1 Configurar períodos de tiempo

Puede configurar hasta 128 períodos (del No.0 al No.127) de períodos de tiempo. En cada período, es necesario configurar horarios de acceso a puertas para una semana completa. Las personas solo pueden abrir la puerta durante el horario programado.

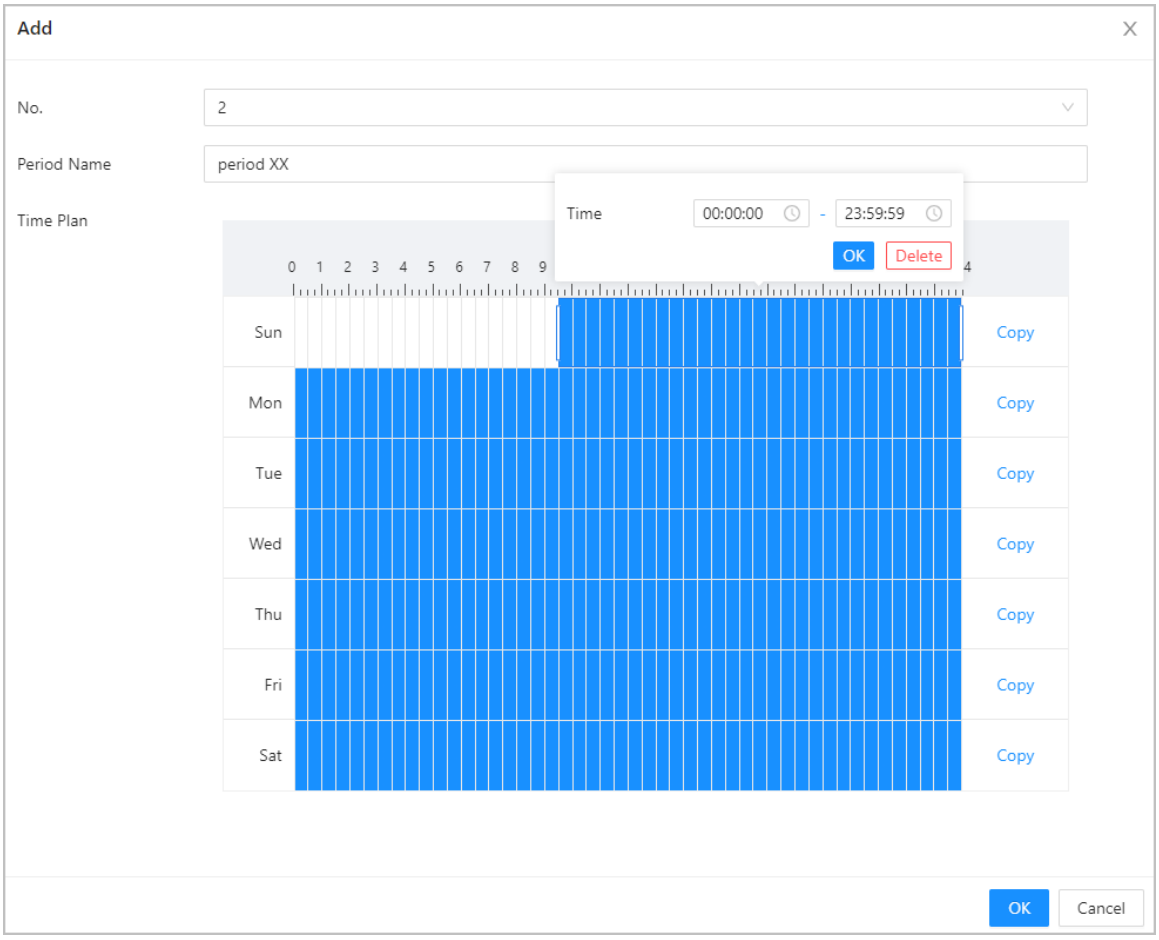
Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Control de acceso**>**Configuración del período**>**Período**. Hacer

Paso 3 clic**Agregar**.

Figura 3-14 Configurar períodos de tiempo



Etapa 4 Arrastre el control deslizante de tiempo para configurar la hora de cada día.

Paso 5 (Opcional) Haga clic**Copiar**para copiar la configuración al resto de días. Hacer clic**DE**

Paso 6 **ACUERDO**.

3.6.8.2 Configurar planes de vacaciones

Puede configurar hasta 128 grupos de días festivos (del 0 al 127) y, para cada grupo de días festivos, puede agregar hasta 16 días festivos. A continuación podrá asignar los grupos de vacaciones configurados al plan de vacaciones. Los usuarios sólo pueden desbloquear la puerta durante el tiempo definido del plan de vacaciones.

Procedimiento

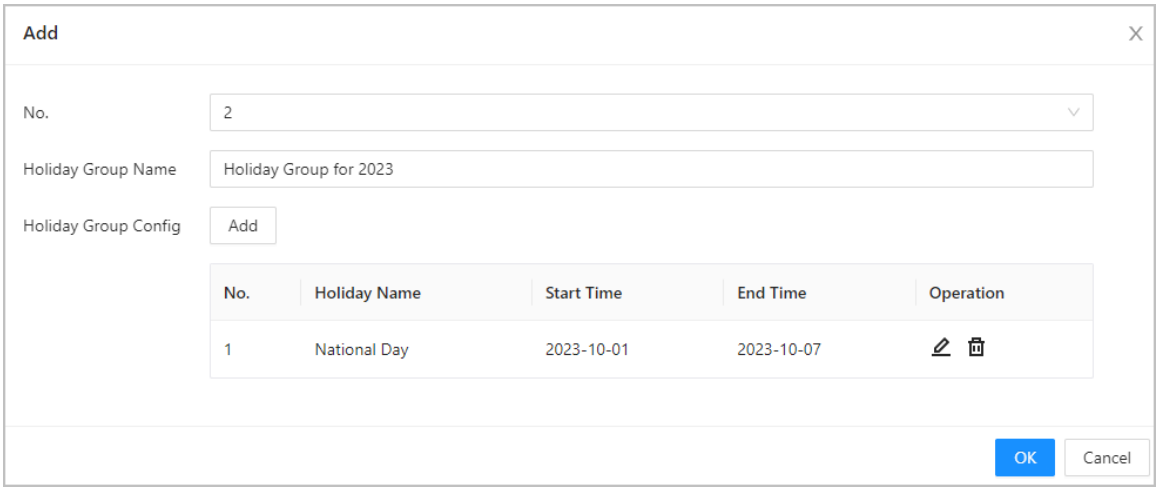
Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Control de acceso**>**Configuración del período**>**Plan de vacaciones**.

Paso 3 Hacer clic**Gestión de vacaciones**,y luego haga clic**Agregar**.

Etapa 4 Seleccione un número para el grupo de vacaciones y luego ingrese un nombre para el grupo.

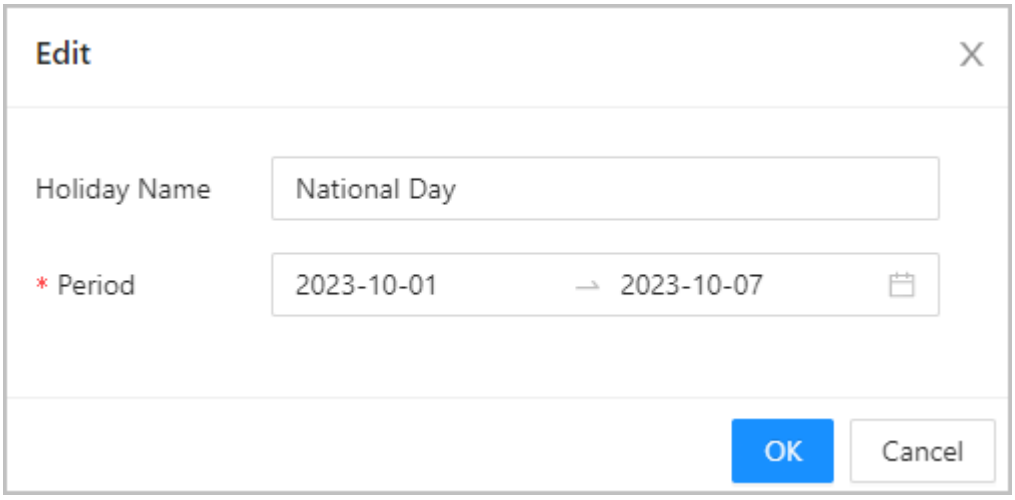
Figura 3-15 Agregar un grupo de vacaciones



Paso 5 Hacer clic**Agregar**y luego agregue un día festivo a un grupo de días festivos. Hacer clic**DE**

Paso 6 **ACUERDO**.

Figura 3-16 Agregar un día festivo a un grupo de días festivos



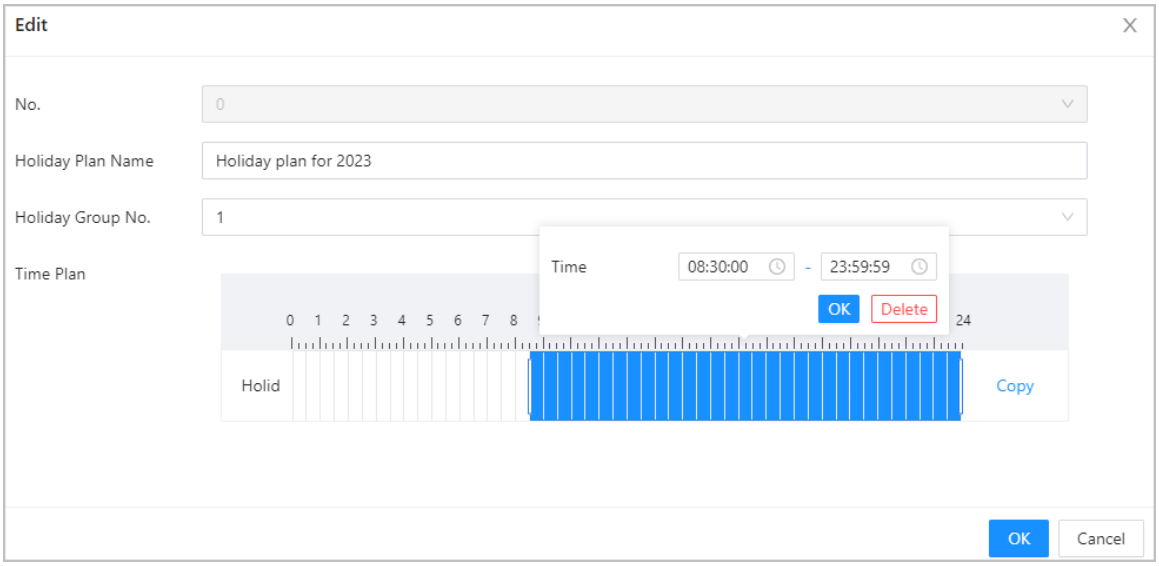
Paso 7 Hacer clic**Gestión de planes**,y luego haga clic**Agregar**.

Paso 8 Seleccione un número para el plan de vacaciones y luego ingrese un nombre.

Paso 9 Seleccione un grupo de vacaciones y luego arrastre el control deslizante para configurar la hora de cada día.

Admite agregar hasta 4 secciones de tiempo en un día.

Figura 3-17 Agregar plan de vacaciones



Paso 10 Hacer clic**DE ACUERDO**.

3.6.9 Configuración de privacidad

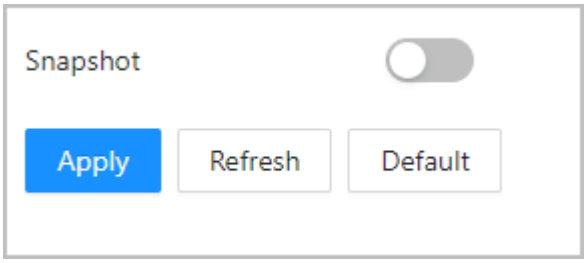
Procedimiento

Paso 1 En la página web, seleccione**Control de acceso**>**La configuración de privacidad**.

Paso 2 Habilite la función de instantánea.

Las imágenes de rostros se capturarán automáticamente cuando las personas abran la puerta.

Figura 3-18 Habilitar instantánea



Paso 3 Hacer clic**Aplicar**.

3.6.10 Configuración de módulos de expansión

Para Dispositivo que admite la conexión de módulos de expansión, configure el tipo de módulo que admite el Dispositivo.

Información de contexto

- El tipo de módulo de expansión puede variar según los modelos del dispositivo.
- La configuración del módulo de expansión permanece después de restaurar el dispositivo a los valores predeterminados de fábrica.

Procedimiento

Paso 1 En la página web, seleccione**Control de acceso**>**Módulo de expansión**.

Paso 2 Seleccione el tipo de módulo que admite el dispositivo. Hacer

Paso 3 clic**Aplicar**.

Las configuraciones entran en vigor después de reiniciar el dispositivo.

- Se muestra en la esquina derecha del dispositivo si la configuración es efectiva.
- se muestra en la esquina derecha del Dispositivo, lo que significa que el tipo de módulo de expansión que configuró no coincide con el módulo de expansión real que está conectado al Dispositivo.
- Si**Ninguno**Si se selecciona y no hay ningún módulo de expansión conectado al dispositivo, no se mostrará el icono del módulo de expansión.

3.6.11 Configuración de funciones del puerto

Algunos puertos pueden funcionar como puertos diferentes; puede configurarlos en puertos diferentes según las necesidades reales.

Información de contexto

- Esta función solo está disponible en modelos seleccionados.
- Los puertos pueden diferir según los modelos del producto.

Procedimiento

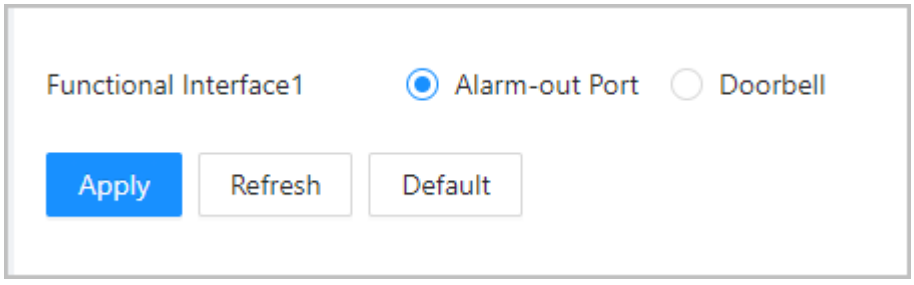
Paso 1 En la página web, seleccione**Control de acceso**>**Configuración de**

Paso 2 **puerto**. Seleccione el tipo de puerto.

Cuando se comparten el cable de alarma y el cable del timbre, configure la interfaz para **Timbre de la puerta**para asegurarse de que suene el timbre.

Paso 3 Hacer clic**Aplicar**.

Figura 3-19 Configurar puertos



3.6.12 Configurar la comparación de back-end

Pasar datos directamente, como el código QR o el número de tarjeta, a la plataforma de terceros para la validación de datos en lugar de validarlos en el Dispositivo.

Seleccionar**Control de acceso**>**Comparación de back-end**.

Figura 3-20 Comparación de back-end

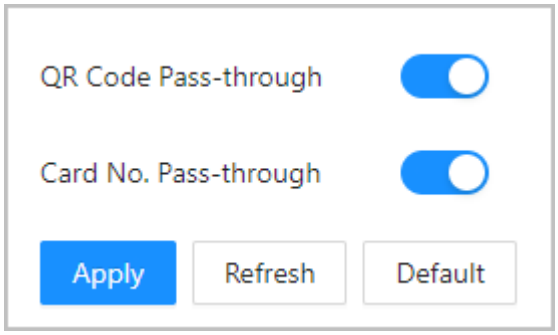


Tabla 3-11 Comparación de back-end

Parámetros	Descripción
Transferencia de código QR	Una vez habilitado, el código QR escaneado se pasa a la plataforma de terceros para la validación de los datos.
Número de tarjeta Transferencia	Una vez habilitado, el número de tarjeta pasa a la plataforma de terceros para la validación de datos.

3.7 Configuración del intercomunicador

El Dispositivo puede funcionar como una estación de puerta para realizar un videoportero.

La función de intercomunicación solo está disponible en modelos selectos.

3.7.1 Uso del dispositivo como servidor SIP

3.7.1.1 Configurar el servidor SIP

Cuando el dispositivo funciona como servidor SIP, puede conectar hasta 500 VTH.

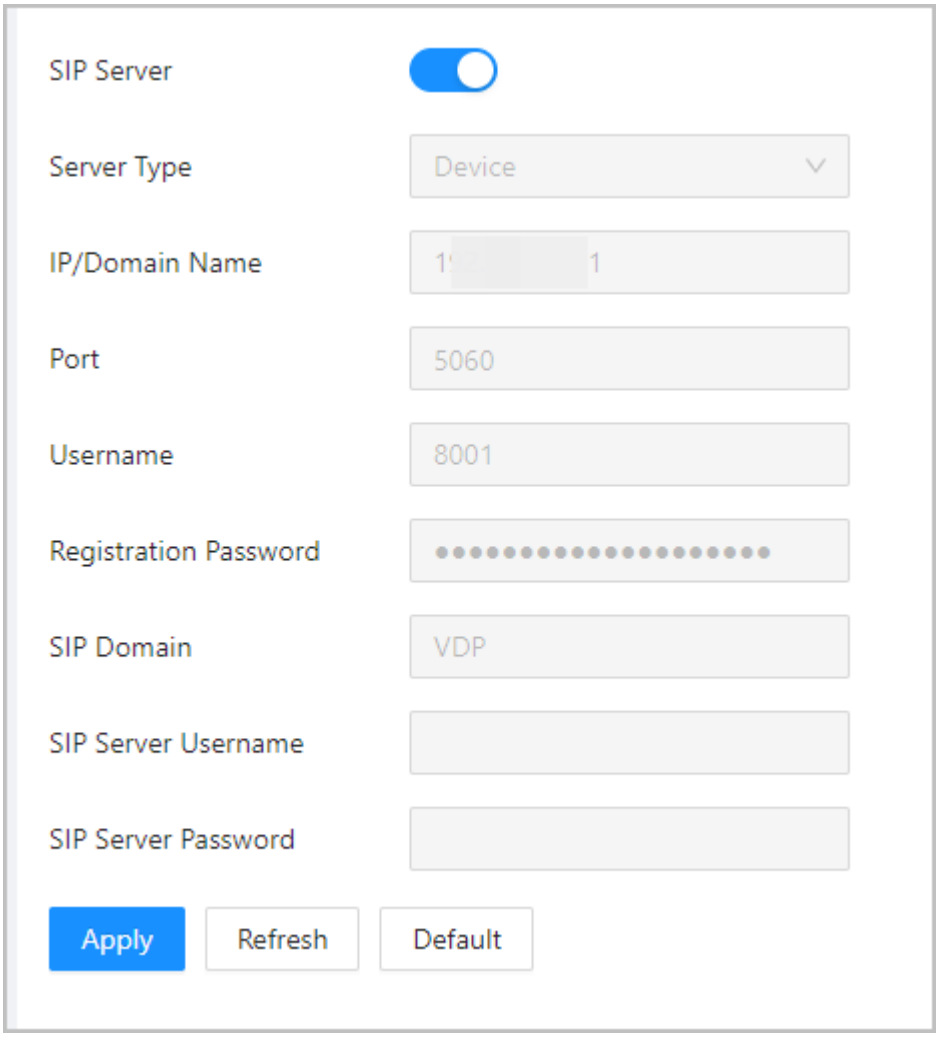
Procedimiento

Paso 1 Seleccionar**Configuración de intercomunicador**>**Servidor SIP**.

Paso 2 Encender**Servidor SIP**.

La configuración del dispositivo se restaurará automáticamente a los valores predeterminados de fábrica si cambia el estado del servidor SIP.

Figura 3-21 Utilice el dispositivo como servidor SIP



Paso 3 Hacer clic**Aplicar**.

3.7.1.2 Configuración de parámetros locales

Cuando el Dispositivo funcione como servidor SIP, configure los parámetros del Dispositivo.

Procedimiento

Paso 1 Seleccionar**Configuración de intercomunicador**>**Configuración del**

Paso 2 **dispositivo local**. Configure los parámetros.

Figura 3-22 Parámetros básicos

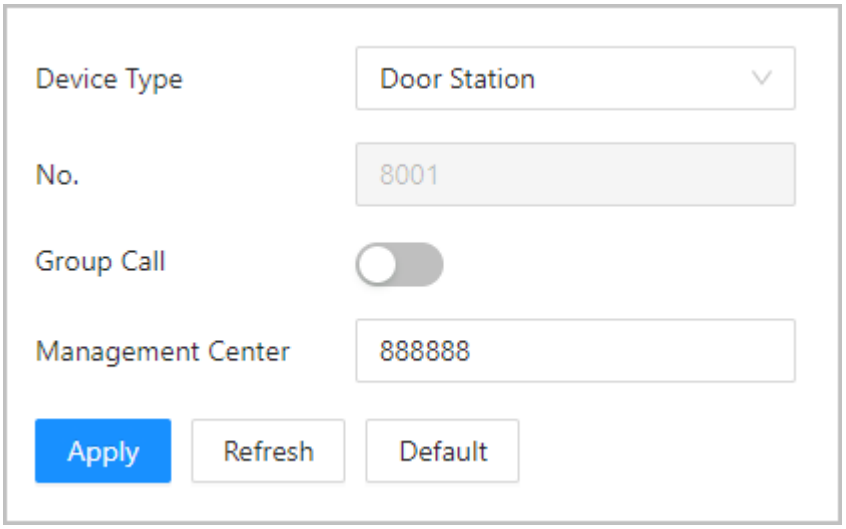


Tabla 3-12 Descripción de los parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccionar**Estación de puerta**.
No.	No se puede configurar.
Llamada grupal	Cuando activa la función de llamada grupal, la estación de puerta llama al VTH principal y a las extensiones al mismo tiempo. La configuración es efectiva después de que se reinicia la estación de puerta.
Centro de Gestión	El número de llamada predeterminado del centro de gestión es 888888+VTS No. Para el VTS No, vaya a la**Configuración del proyecto**>**General**del centro directivo.

Paso 3 Hacer clic**Aplicar**.

3.7.1.3 Agregar la estación de puerta

Cuando el dispositivo funciona como servidor SIP, debe agregar una estación de puerta al servidor SIP para asegurarse de que puedan llamarse entre sí.

Procedimiento

Paso 1 En la página web del Dispositivo, seleccione**Configuración de intercomunicador**>**Configuración del**

Paso 2 **dispositivo**. Hacer clic**Agregar**y luego configure la estación de puerta.

Figura 3-23 Agregar estación de puerta

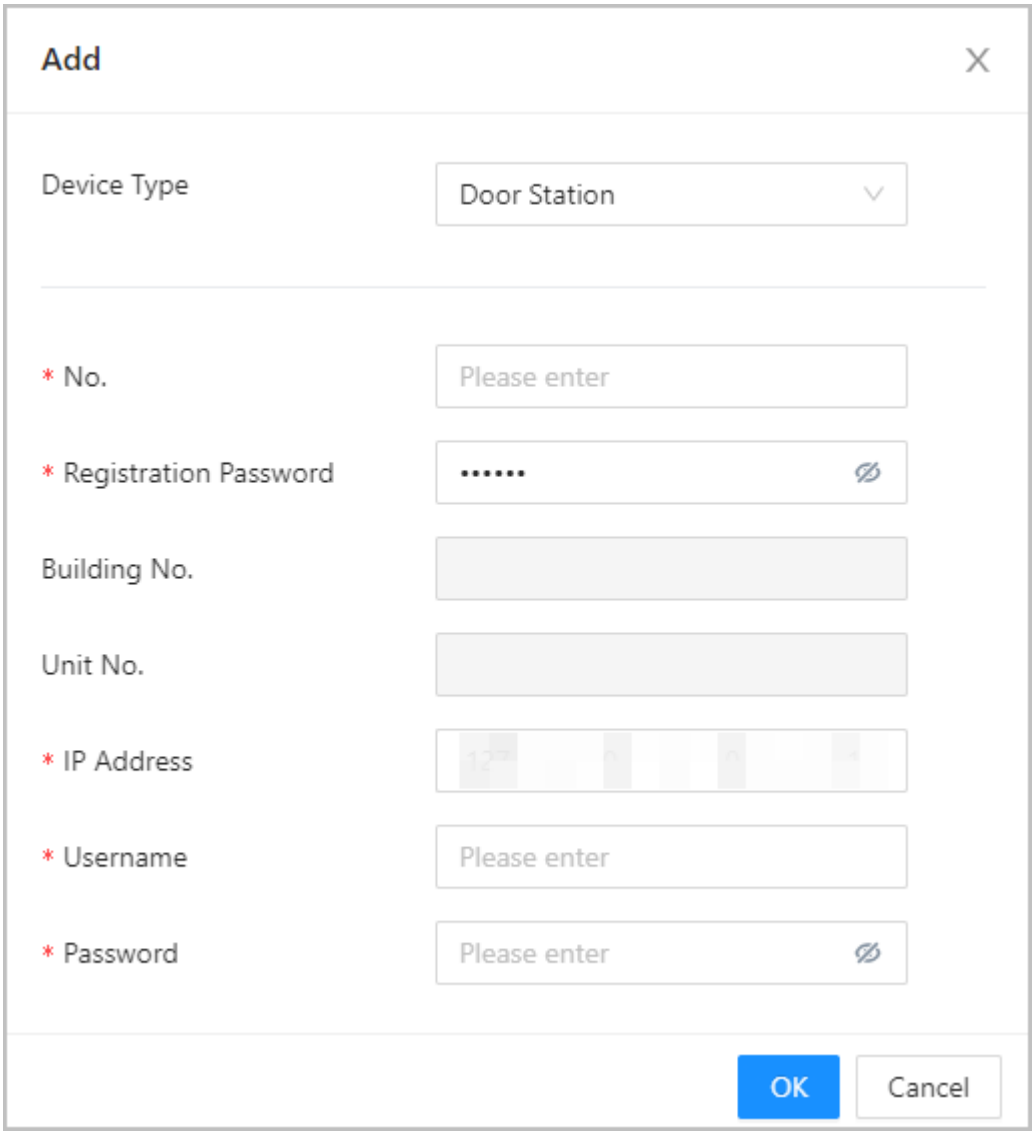


Tabla 3-13 Agregar configuración de VTO

Parámetro	Descripción
Tipo de dispositivo	Seleccionar**Estación de puerta**.
No.	Para ver el número de la estación de puerta, vaya a la**Dispositivo**pantalla de la estación de puerta y luego ingrese el número de la estación de puerta en esta página.
Registro Contraseña	Manténgalo predeterminado.
Edificio número.	No se puede configurar.
Numero de unidad.	
Dirección IP	La dirección IP de la estación de puerta agregada.
Nombre de usuario	El nombre de usuario y la contraseña que se utilizan para iniciar sesión en la página web del videoportero agregado.
Contraseña	

Paso 3 Hacer clic**DE ACUERDO**.

3.7.1.4 Agregar el VTH

Cuando el dispositivo funciona como servidor SIP, puede agregar todos los VTH de la misma unidad al servidor SIP para asegurarse de que puedan llamarse entre sí.

Información de contexto

- Cuando hay VTH principal y una extensión, primero debe activar la función de llamada grupal y luego agregar el VTH principal y la extensión en el**Gestión VTH**página. Para saber cómo activar la función de llamada de grupo, consulte "3.7.1.2 Configuración de parámetros locales".
- No se puede agregar extensión cuando no se agregan los VTH principales.

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración de intercomunicador**>**Configuración del dispositivo**.

Paso 2 Agregue el VTH.

- Agrega uno por uno.

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

Figura 3-24 Agregar uno por uno

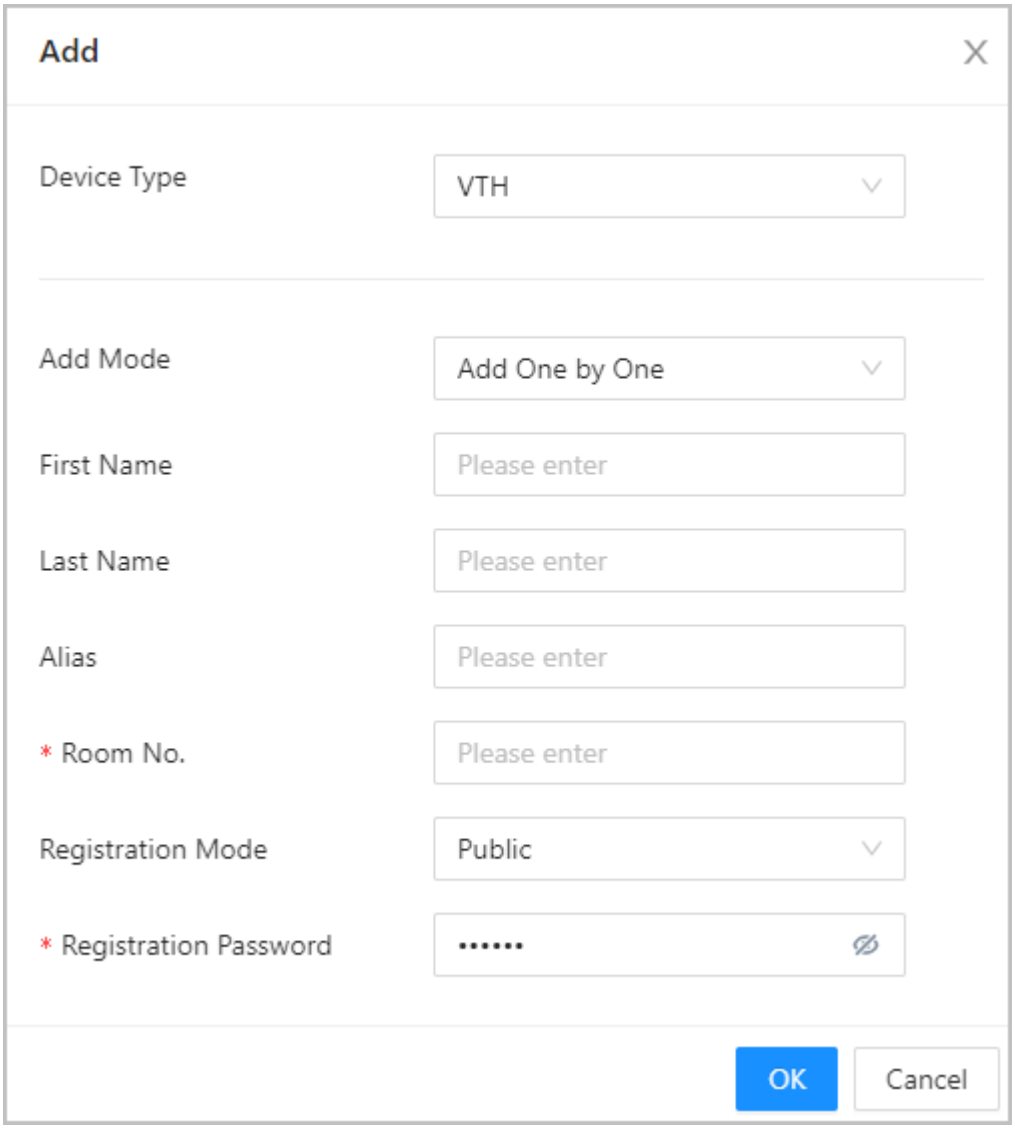


Tabla 3-14 Información de la habitación

Parámetro	Descripción
Nombre de pila	Ingrese el nombre del VTH para ayudarlo a diferenciar los VTH.
Apellido	
Alias	

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

- Agregue en lotes.

  1. Haga clic**Agregar en lotes**.
  2. Configure los parámetros.
  3. Haga clic**Agregar**.

Figura 3-25 Agregar lote

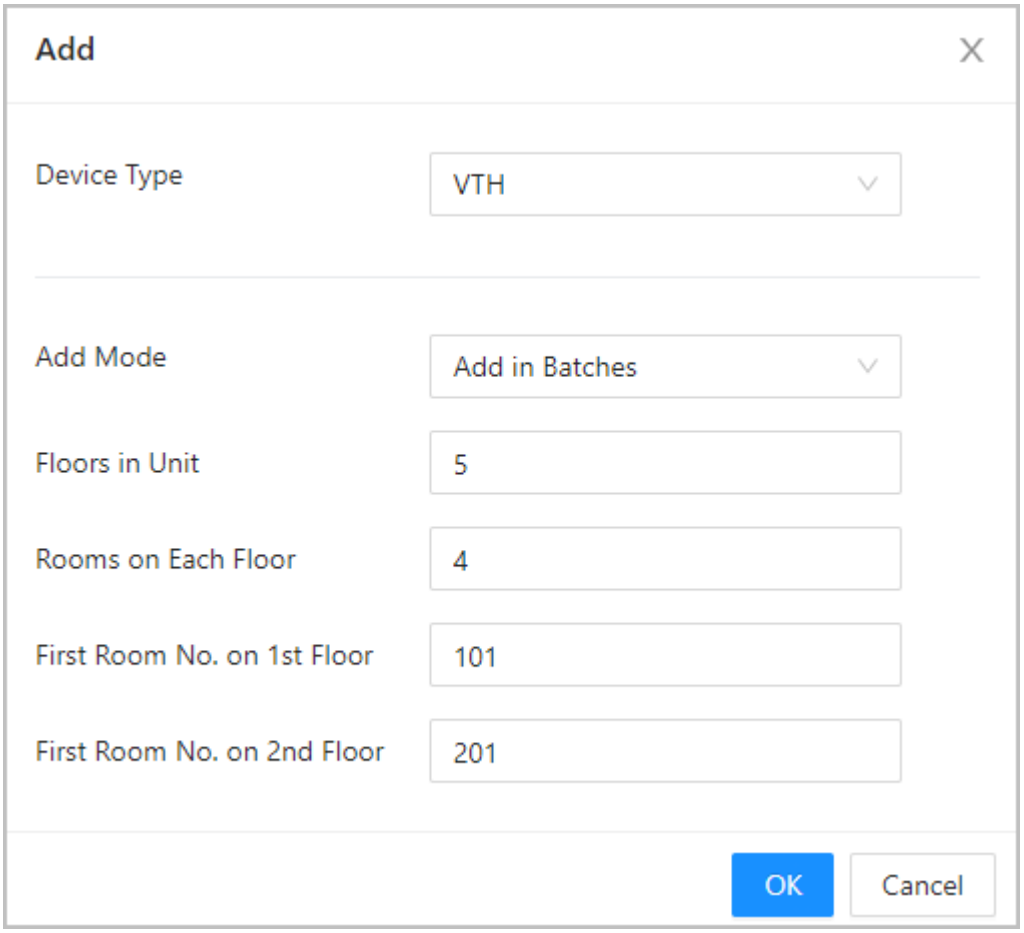


Tabla 3-15 Agregar en lotes

Parámetro	Descripción
Pisos en la unidad	El número de plantas del edificio, que oscila entre 1 y 99.
Habitaciones en cada piso	El número de habitaciones en cada piso, que oscila entre 1 y 99.
Primera Habitación No. en 1er Piso	La primera habitación en el primer piso.
Primera Habitación No. en 2do Piso	El número de la primera habitación en el segundo piso = El primer dígito del número de la primera habitación en el primer piso más 1. Por ejemplo, si el número de la primera habitación en el primer piso es 101, el número de la primera habitación en el segundo piso debe ser 201 .

3.7.1.5 Agregar el VTS

Cuando el dispositivo 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 intercomunicador**>**Configuración del dispositivo**.

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

Figura 3-26 Gestión de VTS

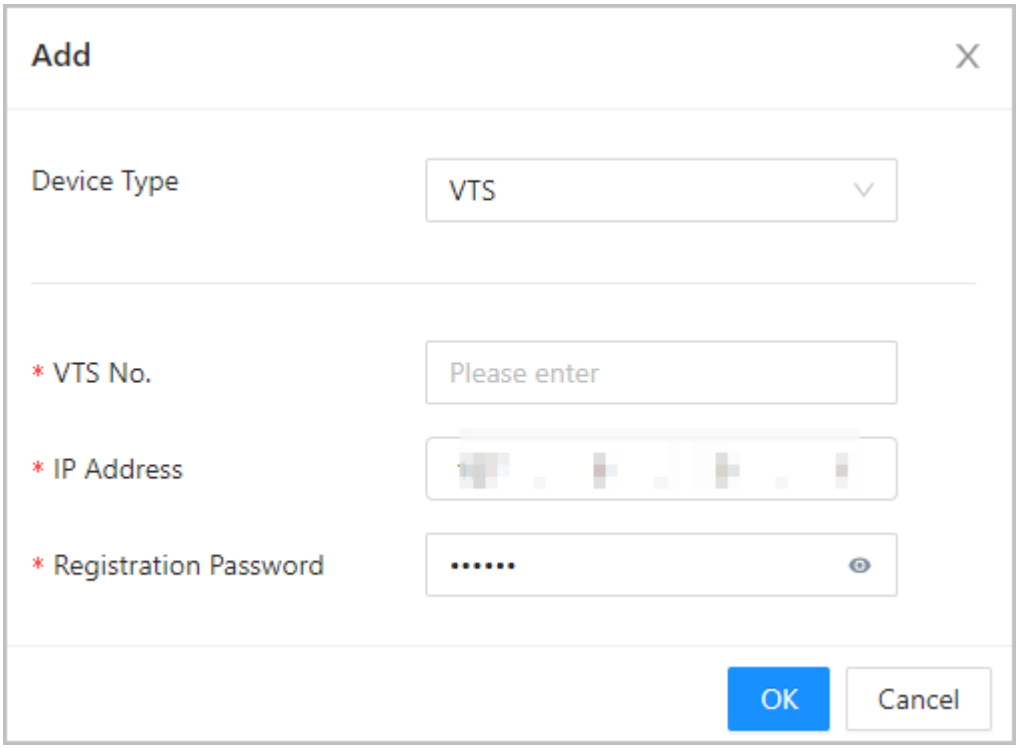


Tabla 3-16 Parámetros VTS

Parámetro	Descripción
VTS No.	Ingrese 888888+ VTS No, que puede incluir hasta 9 dígitos. Para el VTS No, vaya a**Dispositivo**pantalla en el VTS.
Dirección IP	La dirección IP del VTS.
Contraseña de registro	Mantenlo como predeterminado.

Paso 3 Hacer clic**DE ACUERDO**.

3.7.2 Uso de VTO como servidor SIP

3.7.2.1 Configurar el servidor SIP

Utilice otro VTO como servidor SIP.

Procedimiento

Paso 1 Seleccionar**Configuración de intercomunicador**>**Servidor**

Paso 2 **SIP**. Seleccionar**Dispositivo**desde el**Tipo de servidor**.

No active**servidor SIP**.

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

Figura 3-27 Utilice VTO como servidor SIP

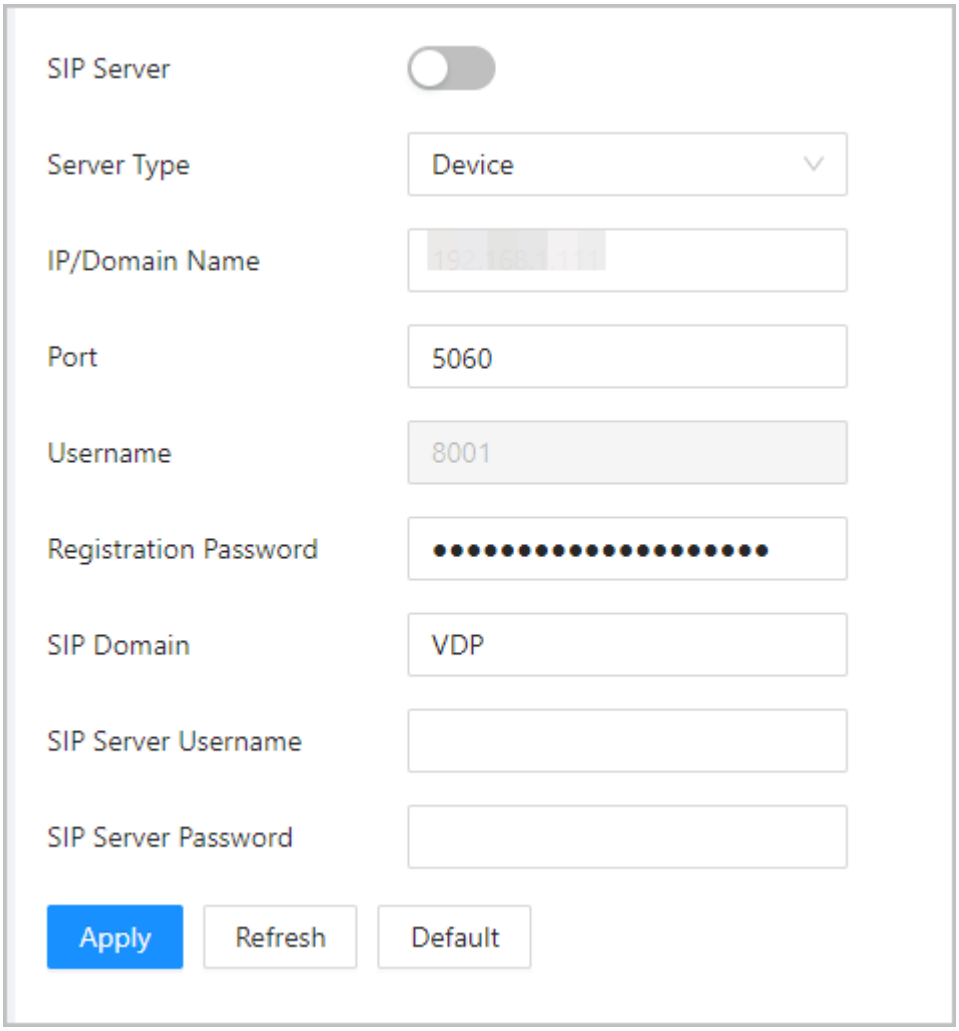


Tabla 3-17 Configuración del servidor SIP

Parámetro	Descripción
IP/Nombre de dominio	Dirección IP o nombre de dominio de la VTO.
Puerto	5060 de forma predeterminada cuando VTO funciona como servidor SIP.
Nombre de usuario	Déjalos como predeterminados.
Contraseña de registro	
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	

Etapa 4 Hacer clic**Aplicar**.

3.7.2.2 Configuración de parámetros locales

Configure los parámetros del dispositivo cuando utilice otro VTO como servidor SIP.

Procedimiento

Paso 1 Seleccionar**Configuración de intercomunicador**>**Configuración del**

Paso 2 **dispositivo local**. Configure los parámetros.

Figura 3-28 Configurar los parámetros

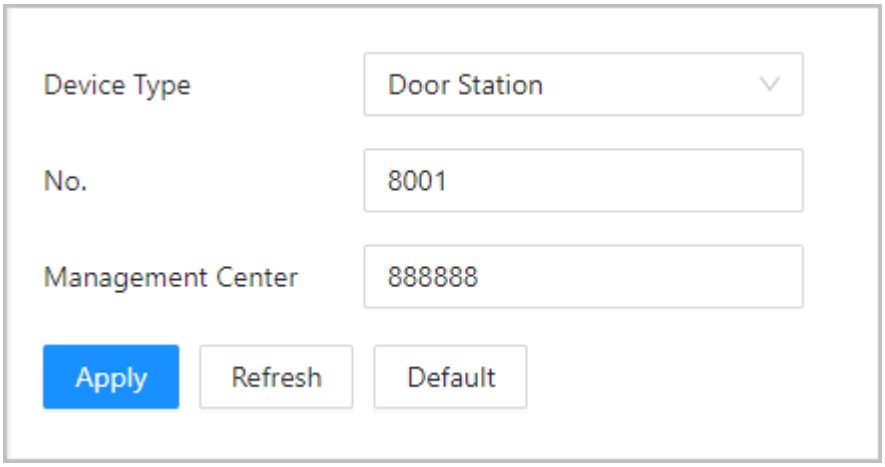


Tabla 3-18 Descripción de parámetros

Parámetro	Descripción
Tipo de dispositivo	Seleccionar**Estación de puerta**.
No.	El número de la VTO. ● El número debe tener 4 dígitos. Los primeros 2 dígitos deben ser 80 y los 2 últimos dígitos deben comenzar desde 01. Por ejemplo, 8001. ● Si existen varios VTO en una unidad, el número de VTO no se puede repetir.
Centro de Gestión	El número de teléfono del centro de gestión es 888888. Manténgalo como predeterminado.

Paso 3 Hacer clic**Aplicar**.

3.7.3 Uso de la plataforma como servidor SIP

3.7.3.1 Configurar el servidor SIP

La plataforma de gestión se utiliza como servidor SIP.

Procedimiento

Paso 1 Seleccionar**Configuración de intercomunicador**>**Servidor SIP**.

Paso 2 Seleccionar**Servidor SIP privado**desde el**Tipo de servidor**.

No actives**Servidor SIP**.

Figura 3-29 Utilice la plataforma de gestión como servidor SIP

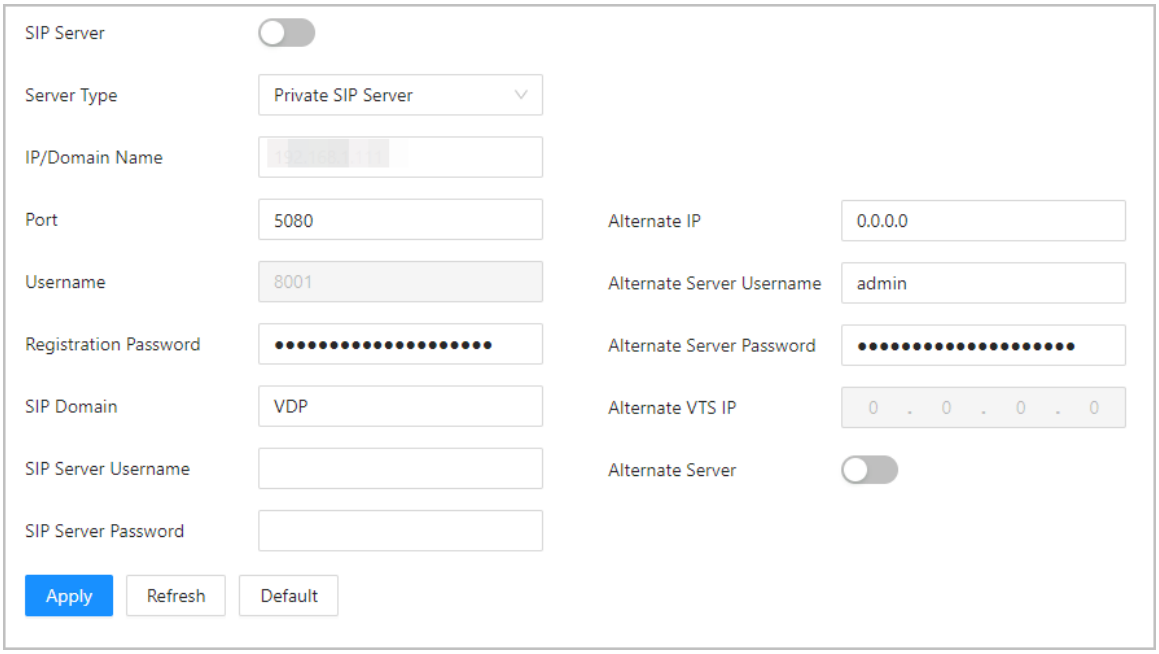


Tabla 3-19 Configuración del servidor SIP

Parámetro	Descripción
IP/Nombre de dominio	Dirección IP o nombre de dominio de la plataforma.
Puerto	5080 por defecto cuando la plataforma funciona como servidor SIP.
Nombre de usuario	Déjalos como predeterminados.
Contraseña de registro	
Dominio SIP	Déjalo por defecto.
Nombre de usuario del servidor SIP	El nombre de usuario y contraseña de inicio de sesión de la plataforma.
Contraseña del servidor SIP	
IP alternativa	El servidor alternativo se utilizará como servidor SIP cuando la plataforma no responda. ● Si enciendes el**Servidor alternativo**función, configurará el dispositivo como 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 actives **Servidor alternativo**en este caso. ● Le recomendamos configurar el VTO principal como servidor alternativo.

Parámetro	Descripción
Servidor alternativo Nombre de usuario	Después de configurar el servidor alternativo, cuando la plataforma de administración no responde, el servidor alternativo se activará para garantizar que VTO y VTH puedan comunicarse entre sí. ● Si**Servidor alternativo**está habilitado, el dispositivo se configura como servidor alternativo. ● Si**Servidor alternativo**no está habilitado, ingrese la IP del servidor alternativo, su nombre de usuario y contraseña para configurar VTO como el servidor alternativo. Le recomendamos configurar el VTO principal como servidor alternativo.
Servidor alternativo Contraseña	
Servidor alternativo	
IP VTS alternativa	Ingrese la dirección IP del VTS alternativo. Cuando la plataforma de gestión no responde, se activará el VTS alternativo para garantizar que VTO, VTH y VTS puedan comunicarse entre sí.

Paso 3 Hacer clic**Aplicar**.

3.7.3.2 Configuración de parámetros locales

Configure los parámetros del Dispositivo cuando la plataforma se utilice como servidor SIP.

Procedimiento

Paso 1 Seleccionar**Configuración de intercomunicador**>**Configuración del**

Paso 2 **dispositivo local**. Configure los parámetros.

Figura 3-30 Parámetro básico

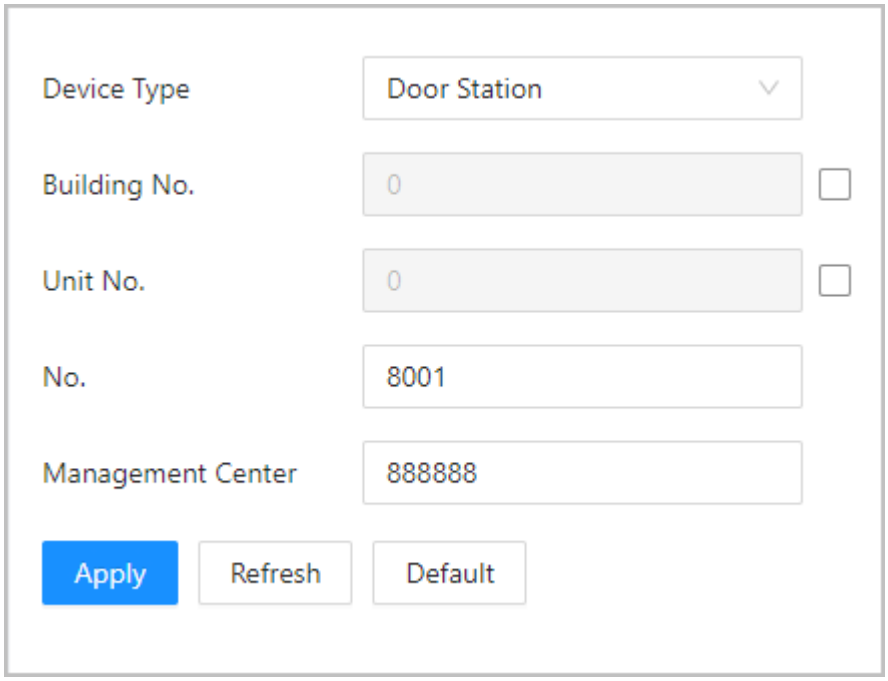


Tabla 3-20 Descripción de parámetros

Parámetro	Descripción
Tipo de dispositivo	Seleccione la estación de cerca o la estación de puerta según su sitio de instalación.

Parámetro	Descripción
Edificio número.	Seleccione la casilla de verificación y luego ingrese el número del edificio donde está instalada la estación de puerta de la unidad.
Numero de unidad.	Seleccione la casilla de verificación y luego ingrese el número de la unidad donde está instalada la estación de puerta de la unidad.
No.	• El número debe tener 4 dígitos. Los primeros 2 dígitos deben ser 80 y los 2 últimos dígitos deben comenzar desde 01. Por ejemplo, 8001. • Si existen varios VTO en una unidad, el número de VTO no se puede repetir.
Centro de Gestión	El número de teléfono predeterminado es 888888 cuando el VTO llama al VTS. Mantenlo como predeterminado.

Paso 3 Hacer clic**Aplicar**.

Después de la configuración, el nombre de usuario en**Intercomunicador**>**SORBO**La página se actualiza automáticamente. Asegúrese de que el nombre de usuario sea el mismo que el número de llamada cuando agregue el dispositivo a la plataforma de administración.

3.7.3.3 Gestión de Registro

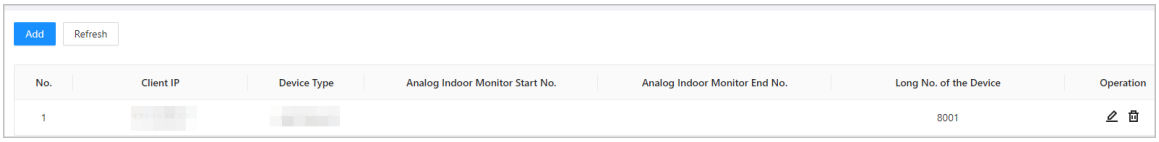
Cuando la plataforma de administración funciona como servidor SIP, puede ver y administrar todos los dispositivos registrados en el servidor SIP.

Procedimiento

Paso 1 Seleccionar**Configuración de intercomunicador**>**Gestión de**

Paso 2 **Registro**. Puede ver y editar los dispositivos.

Figura 3-31 Ver y administrar dispositivos



3.7.4 Modo sencillo

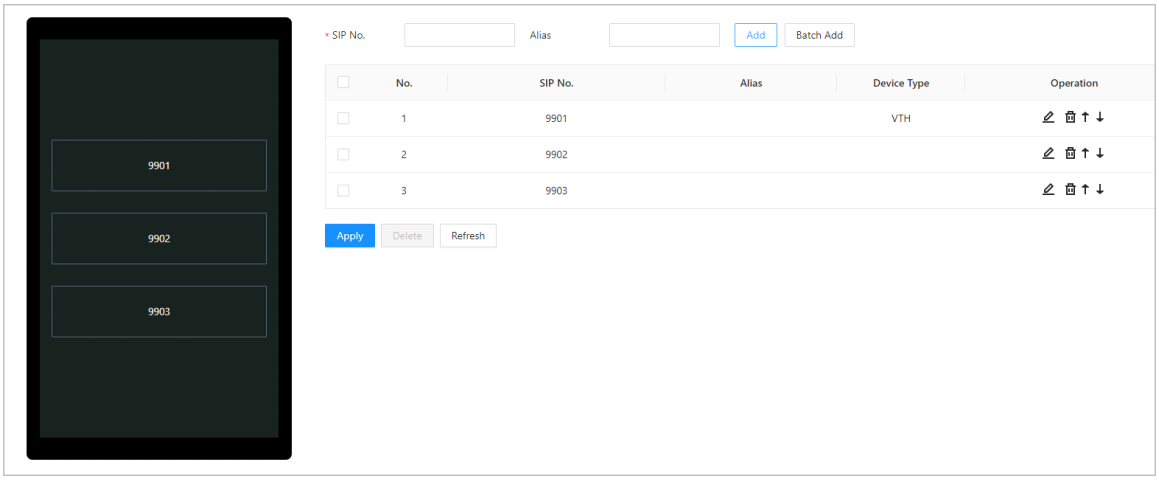
Llamada con un solo toque a VTH o VTS en el Dispositivo.

Procedimiento

Paso 1 En la página web, seleccione**Configuración de intercomunicador**>**Modo simple**.

- La ventana de vista previa de la lista de llamadas es diferente según los modelos del producto.
- El dispositivo de la serie de pantalla horizontal de 4,3 pulgadas no admite la vista previa de la lista de llamadas.
- Solo cuando el dispositivo está configurado como servidor SIP y VTH y VTS se agregan al servidor SIP en el**Configuración del dispositivo**página, se muestra el tipo de dispositivo correspondiente.

Figura 3-32 Modo simple



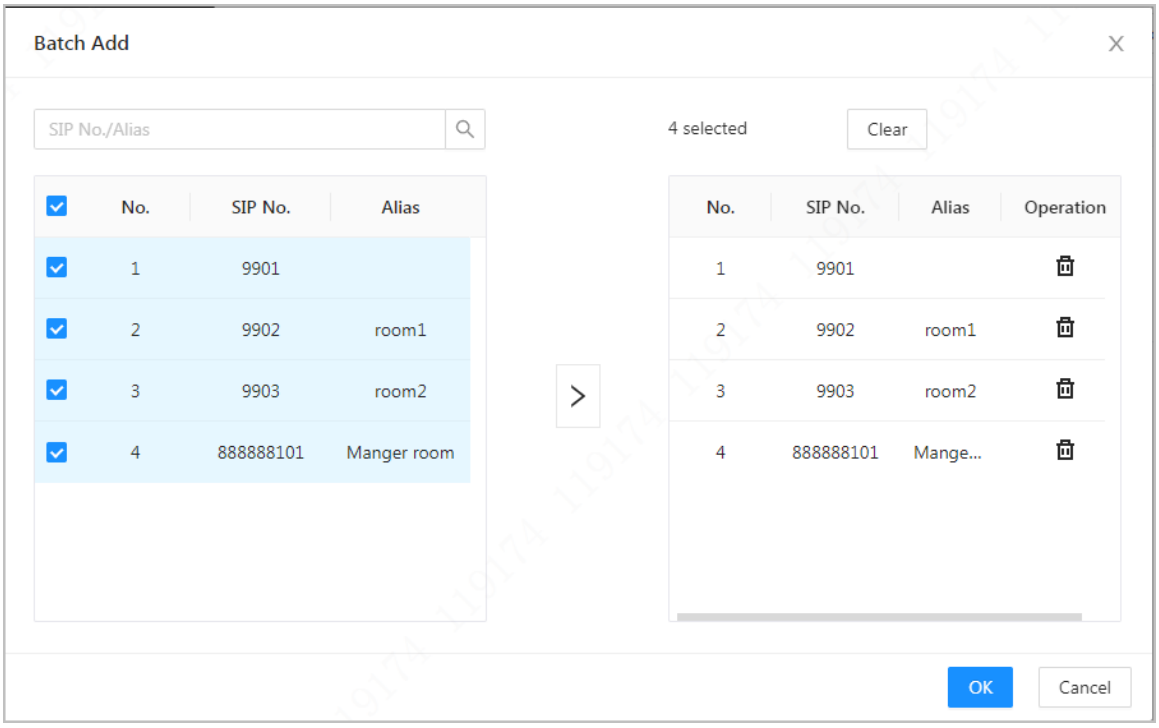
Paso 2 Agregue VTH y VTS uno por uno o en lotes.

Si el VTH tiene extensiones (como 9901-0, 9901-1 y 9901-2) y el número SIP es 9901, entonces puede simplemente llamar al número SIP y a 9901-0, 9901-1 y 9901- Se llamarán 2 al mismo tiempo.

- Agregar uno por uno: ingrese el número SIP y luego haga clic en**Agregar**.
- Agregar en lotes: esta función solo está disponible cuando el dispositivo está configurado como servidor SIP y VTH y VTS se agregan al servidor SIP en el**Configuración del dispositivo**página.

1. Haga clic**Agregar lote**.
2. Seleccione VTS o VTH agregado y luego haga clic en**DE ACUERDO**.

Figura 3-33 Agregar en lotes



Paso 3 (Opcional) Haga clic para ajustar el orden de los dispositivos, o simplemente puede arrastrar los dispositivos en la ventana de vista previa.

Operaciones relacionadas

- Hacer clic para editar el alias del dispositivo. para
- Hacer clic eliminar el dispositivo.

3.8 Configuración de asistencia

Esta función solo está disponible en modelos seleccionados.

3.8.1 Configurar departamentos

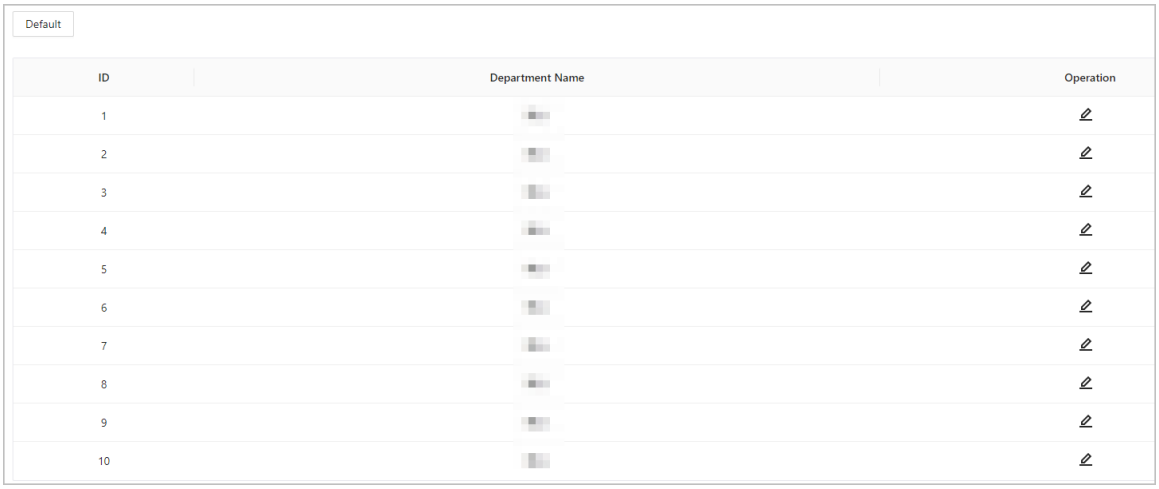
Procedimiento

Paso 1 Seleccionar**Configuración de asistencia**>**Configuración del departamento**.

Paso 2 Haga clic para cambiar el nombre del departamento.

Hay 20 departamentos predeterminados. Le recomendamos cambiarles el nombre.

Figura 3-34 Crear departamentos



Operaciones relacionadas

Puedes hacer clic**Por defecto**para restaurar los departamentos a la configuración predeterminada.

3.8.2 Configurar turnos

Configure turnos para definir reglas de tiempo de asistencia. Los empleados deben trabajar a la hora prevista para el inicio de su turno y salir a la hora de finalización, excepto cuando opten por trabajar horas extras.

Procedimiento

Paso 1 Seleccionar**Configuración de asistencia**>**Configuración de**

Paso 2 **turnos**. Haga clic para configurar el turno.

Figura 3-35 Crear turnos

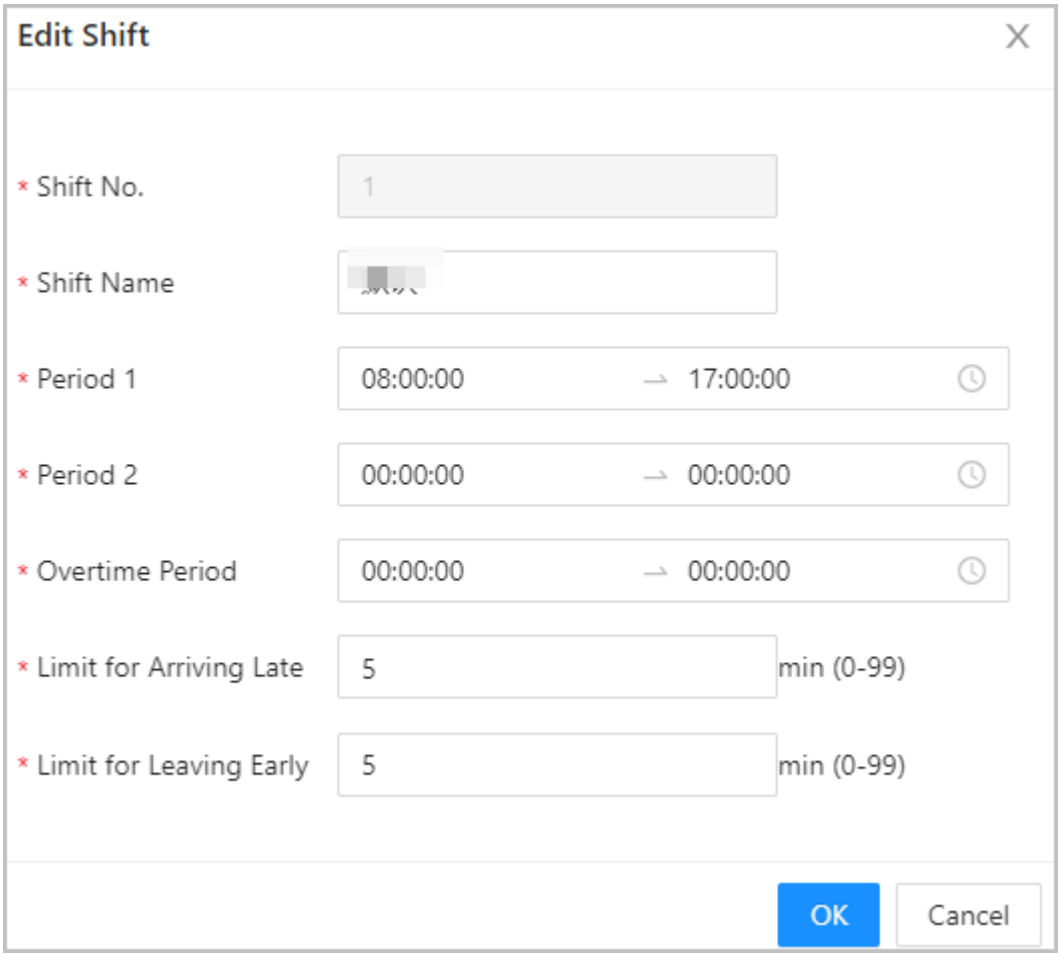
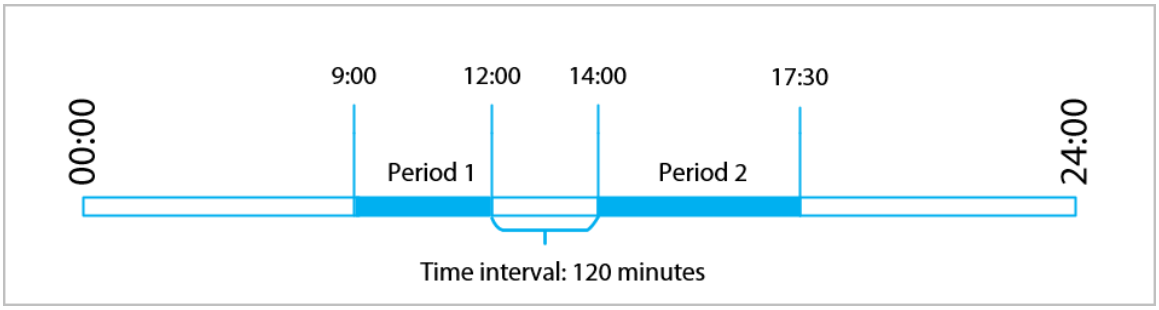


Tabla 3-21 Descripción de los parámetros de cambio

Parámetro	Descripción
Nombre del turno	Ingrese el nombre del turno.
Periodo 1	Especifique un rango de tiempo en el que las personas pueden registrar la entrada y la salida de la jornada laboral. Si solo establece un período de asistencia, los empleados deben registrar su entrada y salida en los horarios designados para evitar que aparezca una anomalía en su registro de asistencia. Por ejemplo, si configura de 08:00 a 17:00, los empleados deben registrar su entrada antes de las 08:00 y su salida a partir de las 17:00. Si establece 2 períodos de asistencia, los 2 períodos no pueden superponerse. Los empleados deben registrar su entrada y salida en ambos períodos.
Periodo 2	
Periodo de horas extras	Se considerará que los empleados que registren su entrada o salida durante el período definido trabajan más allá de su horario normal de trabajo.
Límite por llegar tarde (min)	Se puede conceder una cierta cantidad de tiempo a los empleados para que puedan registrar su entrada un poco tarde y su salida un poco antes. Por ejemplo, si la hora habitual para registrar la entrada es a las 08:00, el período de tolerancia se puede establecer en 5 minutos para que los empleados que lleguen antes de las 08:05 no se consideren retrasados.
Límite de salida anticipada (min)	

- Cuando el intervalo de tiempo entre 2 periodos es un número par, puedes dividir el intervalo de tiempo entre 2 y asignar la primera mitad del intervalo al primer periodo, que será el tiempo de salida. La segunda mitad del intervalo debe asignarse al segundo período como cronómetro.

Figura 3-36 Intervalo de tiempo (número par)

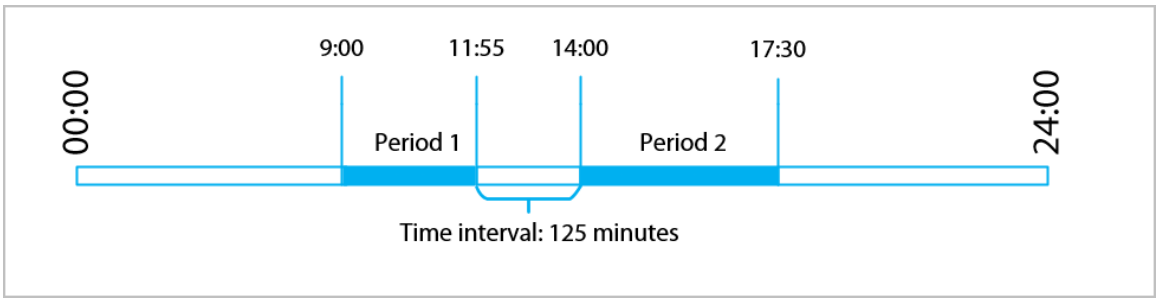


Por ejemplo: si el intervalo es de 120 minutos, entonces la hora de salida para el período 1 es de 12:00 a 12:59, y la hora de entrada para el período 2 es de 13:00 a 14:00.

Si una persona registra su salida varias veces durante el período 1, la última hora será válida, y si registra su entrada varias veces durante el período 2, la hora más temprana será válida.

- Cuando el intervalo de tiempo entre 2 períodos sea un número impar, la porción más pequeña del intervalo se asignará al primer período, que será el tiempo de salida. La mayor parte del intervalo se asignará al segundo período como el reloj en el tiempo.

Figura 3-37 Intervalo de tiempo (número par)



Por ejemplo: si el intervalo es de 125 minutos, entonces la hora de salida para el período 1 es de 11:55 a 12:57, y la hora de entrada para el período 2 es de 12:58 a 14:00. El período 1 tiene 62 minutos y el período 2 tiene 63 minutos.

Si una persona registra su salida varias veces durante el período 1, la última hora será válida, y si registra su entrada varias veces durante el período 2, la hora más temprana será válida.

Todos los tiempos de asistencia son precisos al segundo. Por ejemplo, si la hora normal de entrada se establece en las 8:05 a. m., el empleado que registre su entrada a las 8:05:59 a. m. no se considerará que llega tarde. Sin embargo, el empleado que llegue a las 8:06 a. m. se marcará como retrasado por 1 minuto.

Paso 3 Hacer clic**DE ACUERDO**.

Operaciones relacionadas

Puedes hacer clic**Por defecto**para restaurar los cambios a los valores predeterminados de fábrica.

3.8.3 Configurar vacaciones

Configure planes de vacaciones para establecer períodos en los que no se realizará un seguimiento de la asistencia.

Procedimiento

Paso 1 Seleccionar**Configuración de asistencia**>**Configuración de turnos**>**Día festivo**.

Paso 2 Hacer clic**Agregar**para agregar planes de vacaciones. Configure los parámetros.

Paso 3

Figura 3-38 Crear planes de vacaciones

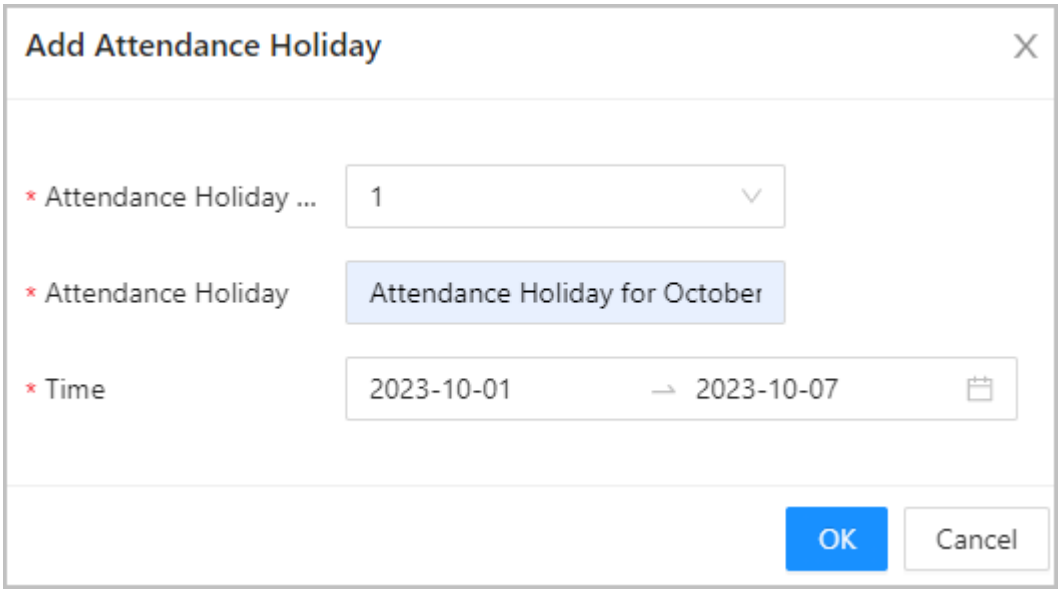


Tabla 3-22 Descripción de parámetros

Parámetro	Descripción
Asistencia Día festivo No.	El número de las vacaciones.
Asistencia vacaciones	El nombre de la festividad.
Hora de inicio	La hora de inicio y finalización de las vacaciones.
Hora de finalización	

Etapa 4 Hacer clic**DE ACUERDO**.

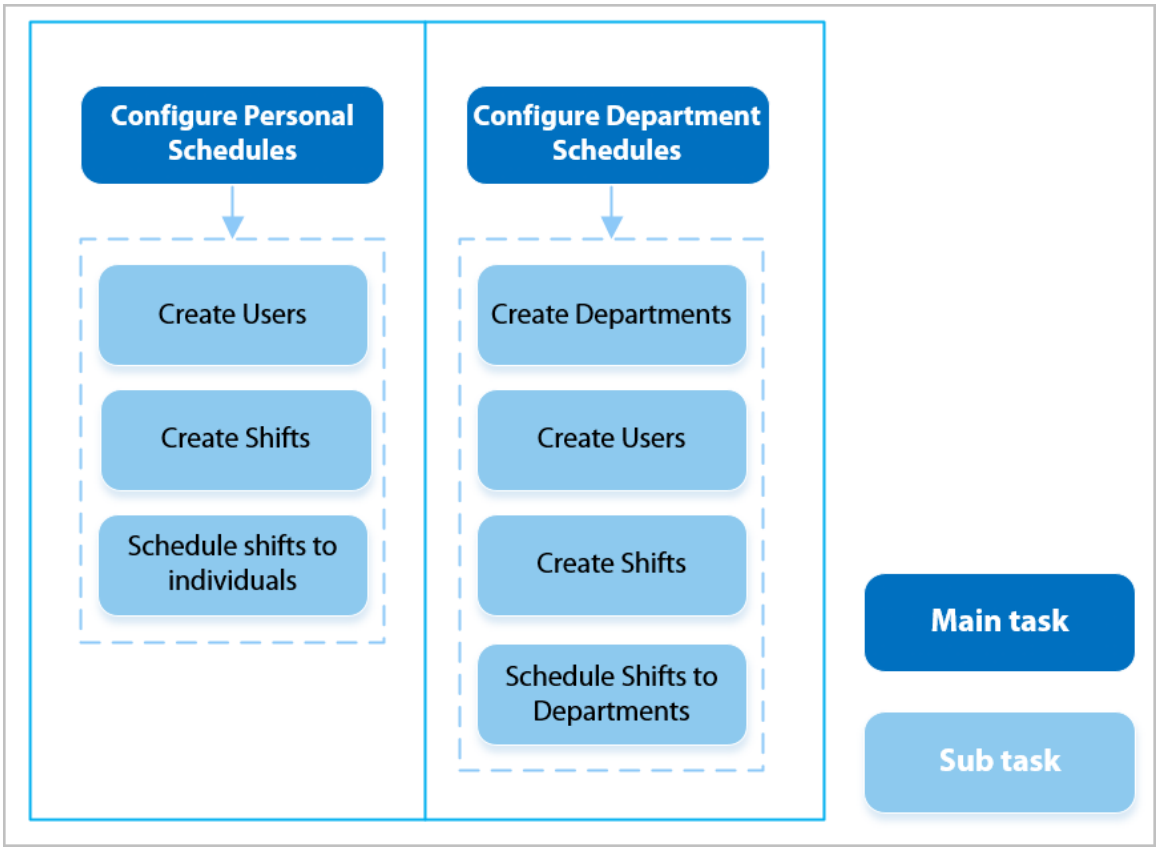
3.8.4 Configurar horarios de trabajo

Un horario de trabajo generalmente se refiere a los días por mes y las horas por día que se espera que un empleado esté en su trabajo. Puede crear diferentes tipos de horarios de trabajo basados en diferentes personas o departamentos, y luego los empleados deben seguir los horarios de trabajo establecidos.

Información de contexto

Consulte el diagrama de flujo para configurar horarios personales o horarios de departamento.

Figura 3-39 Configuración de horarios de trabajo



Procedimiento

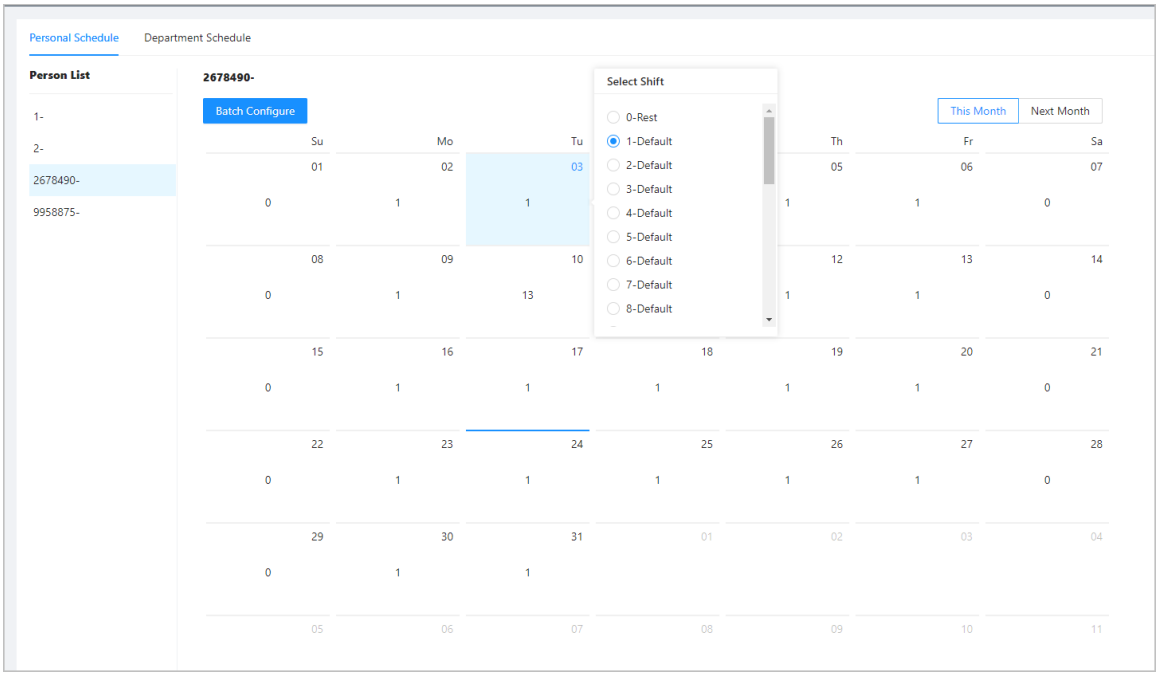
Paso 1 Seleccionar**Configuración de asistencia**>**Programar configuración**.

Paso 2 Establecer horarios de trabajo para individuos.

1. Haga clic**Horario personal**.
2. Seleccione una persona en la lista de personas.
3. En el calendario, seleccione un día y luego seleccione un turno.

También puedes hacer clic**Configurar por lotes**para programar turnos a varios días.

Figura 3-40 Horario personal



Solo puede establecer horarios de trabajo para el mes actual y el mes siguiente.

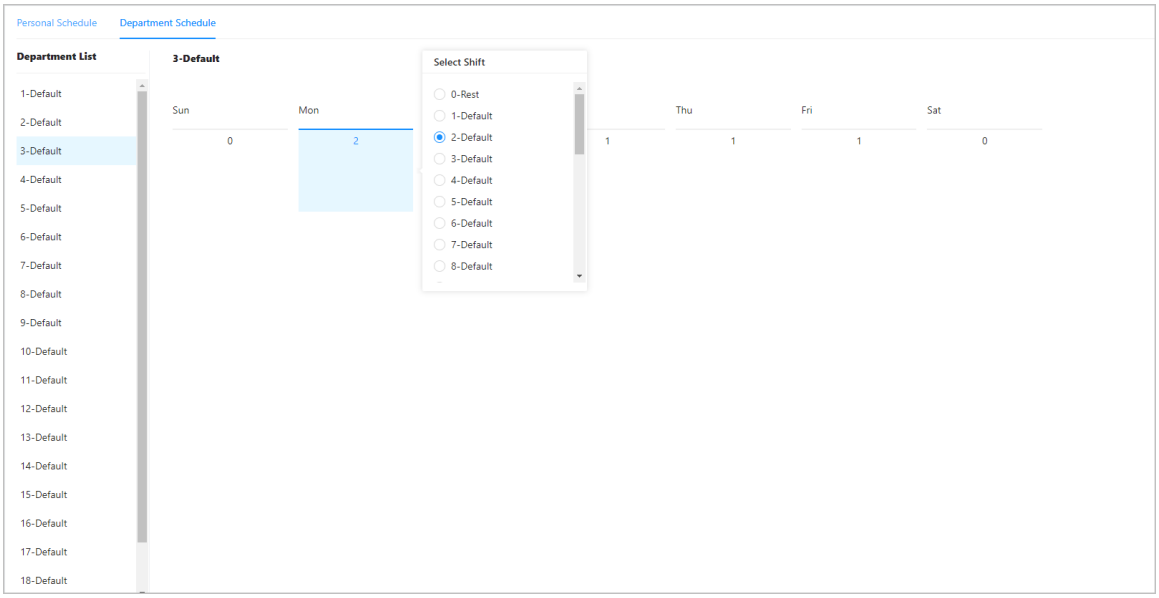
- 0 indica ruptura.
- Del 1 al 24 indica el número de turnos definidos. Para saber cómo configurar turnos, consulte "2.10.2 Configuración de turnos".
- 25 indica viaje de negocios.
- 26 indica excedencia.

Paso 3 Establecer horarios de trabajo para los departamentos.

1. Haga clic**Horario del departamento**.
2. Seleccione un departamento en la lista de departamentos.
3. En el calendario, seleccione un día y luego seleccione un turno.

- 0 indica descanso.
- Del 1 al 24 indica el número de turnos definidos. Para saber cómo configurar turnos, consulte "2.10.2 Configuración de turnos".
- 25 indica viaje de negocios.
- 26 indica excedencia.

Figura 3-41 Horario de turnos a un departamento



El horario de trabajo definido es en un ciclo semanal y se aplicará a todos los empleados del departamento.

3.8.5 Configurar modos de asistencia

Procedimiento

Paso 1 Seleccionar**Configuración de asistencia**>**Configuración de asistencia**.

Paso 2 Ingrese el intervalo de verificación.

Cuando un empleado registra su entrada y salida varias veces dentro de un intervalo establecido, la hora más temprana será válida.

Paso 3 Permitir**Local o Remoto**y luego configure el modo de asistencia.

Etapa 4 Configurar modos de asistencia.

Figura 3-42 Modos de asistencia

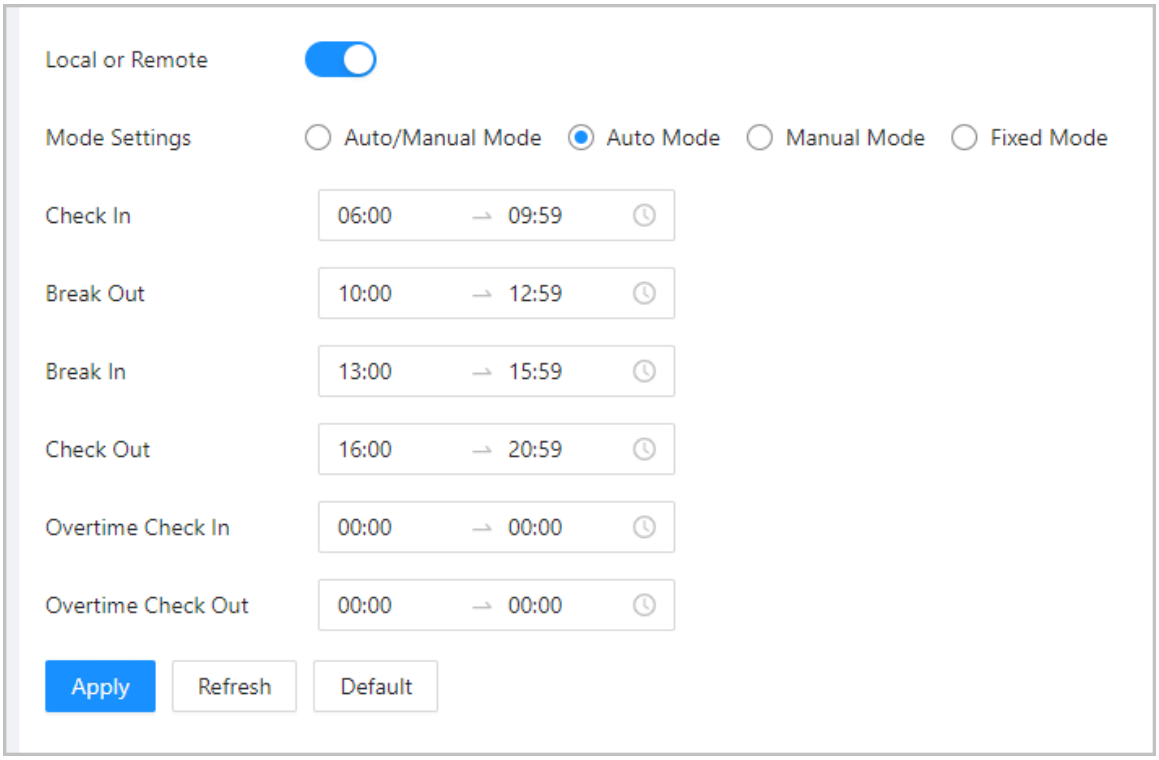


Tabla 3-23 Modo de asistencia

Parámetro	Descripción
Modo automático/manual	La pantalla muestra el estado de asistencia automáticamente después de registrar su entrada o salida, pero también puede cambiar manualmente su estado de asistencia. ● Registro: regístrese cuando comience su jornada laboral normal. ● Break Out: registre cuándo comienza su descanso. ● Break In: registre cuando finalice su descanso. ● Salida: registre la salida cuando comience su jornada laboral normal. ● Registro de horas extras: Regístrese cuando comience su período de horas extras. ● Salida de horas extras: marque cuando finalice su período de horas extras.
Modo automático	La pantalla muestra su estado de asistencia automáticamente después de registrar su entrada o salida. ● Registro: regístrese cuando comience su jornada laboral normal. ● Break Out: registre cuándo comienza su descanso. ● Break In: registre cuando finalice su descanso. ● Salida: registre la salida cuando comience su jornada laboral normal. ● Registro de horas extras: Regístrese cuando comience su período de horas extras. ● Salida de horas extras: marque cuando finalice su período de horas extras.
Modo manual	Seleccione manualmente su estado de asistencia cuando registre su entrada o salida.
Modo fijo	Cuando registre su entrada o salida, la pantalla mostrará el estado de asistencia definido todo el tiempo.

Paso 5 Hacer clic**Aplicar**.

Operaciones relacionadas

- Actualizar: si no desea guardar los cambios actuales, haga clic en**Actualizar**para cancelar los cambios y restaurarlos a la configuración anterior.
- Predeterminado: Restaura la configuración de asistencia a los valores predeterminados de fábrica.

3.9 Configuración de audio y vídeo

3.9.1 Configuración de vídeo

En la página de inicio, seleccione**Configuración de audio y vídeo**>**Video**y luego configure los parámetros de vídeo.

Información de contexto

- Canal No.: El canal 1 es para configuraciones de imagen de luz visible. El canal 2 es para configuraciones de imagen de luz infrarroja.
- Predeterminado: restaurar la configuración predeterminada.
- Capturar: tome una instantánea de la imagen actual.

3.9.1.1 Configuración del canal 1

Procedimiento

Paso 1 Seleccionar**Configuración de audio y vídeo**>**Video**.

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

Paso 3 velocidad de bits.

Figura 3-43 Tarifa de fecha

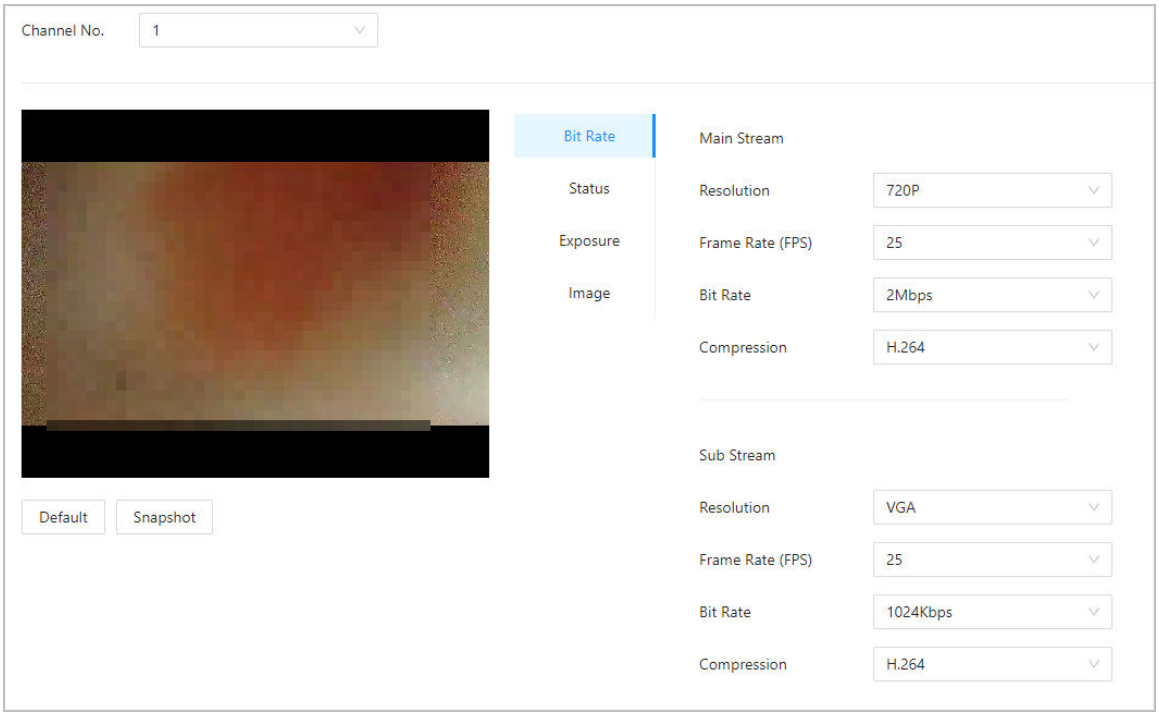


Tabla 3-24 Descripción de la velocidad de bits

Parámetro		Descripción
Formato principal	Resolución	Cuando el dispositivo funciona como VTO y conecta el VTH, el límite de transmisión adquirida de VTH es 720p. Cuando la resolución se cambia a 1080p, la función de llamada y monitoreo podría verse afectada.
	Velocidad de fotogramas (FPS)	El número de fotogramas (o imágenes) por segundo.
	Tasa de bits	La cantidad de datos transmitidos a través de una conexión a Internet en un período de tiempo determinado. Seleccione un ancho de banda adecuado según la velocidad de su red.
	Compresión	Estándar de compresión de vídeo para ofrecer buena calidad de vídeo a velocidades de bits más bajas.
Sub corriente	Resolución	La subtransmisión admite D1, VGA y QVGA.
	Velocidad de fotogramas (FPS)	El número de fotogramas (o imágenes) por segundo.
	Tasa de bits	Indica la cantidad de datos transmitidos a través de una conexión a Internet en un período de tiempo determinado.
	Compresión	Estándar de compresión de vídeo para ofrecer buena calidad de vídeo a velocidades de bits más bajas.

Etapa 4 Configurar el estado.

Figura 3-44 Estado

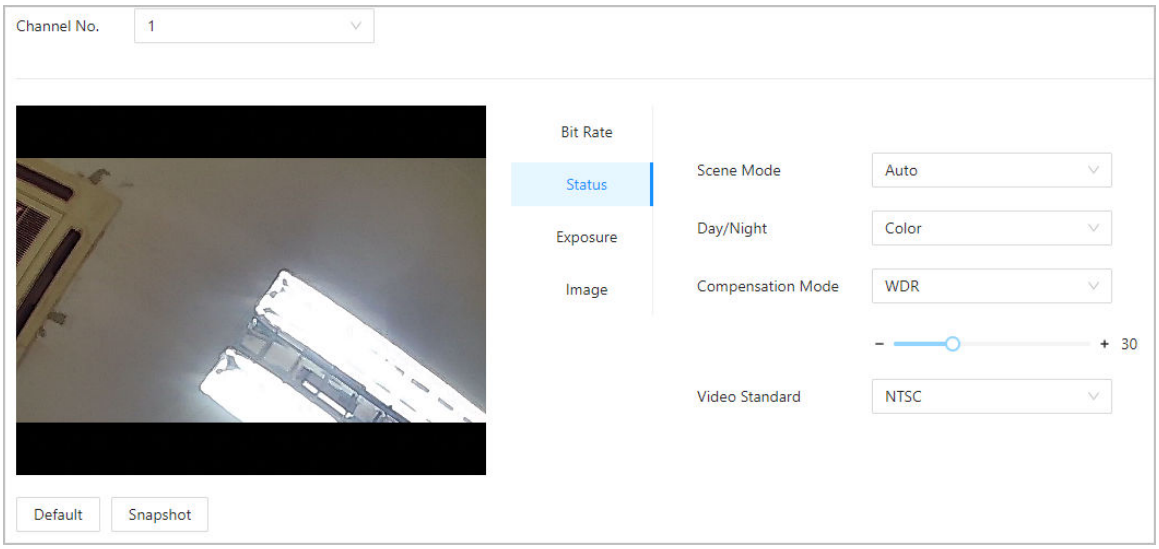


Tabla 3-25 Descripción de parámetros de estado

Parámetro	Descripción
Modo escena	El tono de la imagen es diferente en diferentes modos de escena. ● **Cerca**:La función del modo de escena está desactivada. ● **Auto**:El sistema ajusta automáticamente el modo de escena según la sensibilidad fotográfica. ● **Soleado**:En este modo, se reducirá el tono de la imagen. ● **Noche**:En este modo, se aumentará el tono de la imagen.
Día/Noche	El modo Día/Noche afecta la compensación de luz en diferentes situaciones. ● **Auto**:El sistema ajusta automáticamente el modo día/noche según la sensibilidad fotográfica. ● **Vistoso**:En este modo, las imágenes son coloridas. ● **En blanco y negro**:En este modo, las imágenes están en blanco y negro.
Modo de compensación	● **Desactivar**:La compensación está desactivada. ● **BLC**:La compensación de contraluz aporta automáticamente más luz a las áreas más oscuras de una imagen cuando la luz brillante que brilla desde atrás las oscurece. ● **WDR**:El sistema atenúa las áreas brillantes y compensa las áreas oscuras para crear un equilibrio que mejore la calidad general de la imagen. ● **CHL**:La compensación de altas luces (HLC) es una tecnología utilizada en las cámaras de seguridad CCTV/IP para tratar imágenes expuestas a luces como faros o focos. El sensor de imagen de la cámara detecta luces intensas en el vídeo y reduce la exposición en estos puntos para mejorar la calidad general de la imagen.

Paso 5 Configure los parámetros de exposición.

Figura 3-45 Exposición

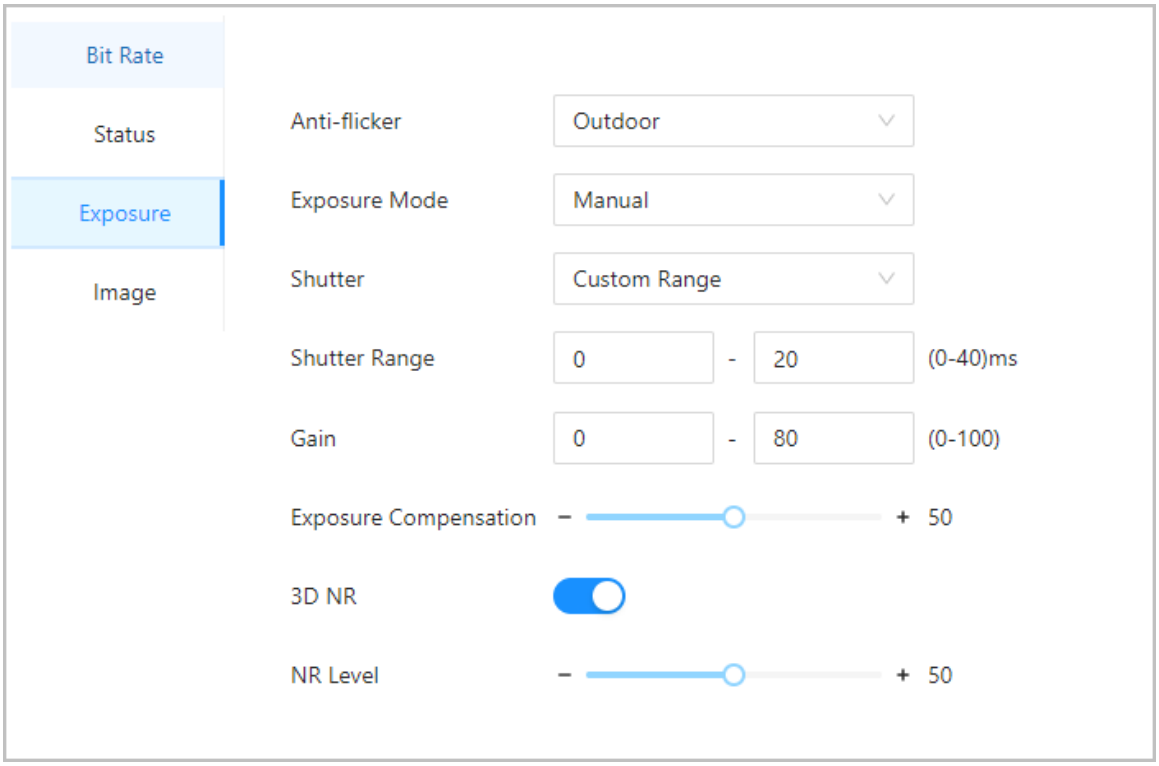


Tabla 3-26 Descripción del parámetro de exposición

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

Parámetro	Descripción
Modo de exposición	Puede configurar la exposición para ajustar el brillo de la imagen. ● **Auto**:El dispositivo ajusta automáticamente el brillo de las imágenes según el entorno. ● **Prioridad de obturador**:El dispositivo ajusta el brillo de la imagen de acuerdo con el rango establecido del obturador. Si la imagen no es lo suficientemente brillante pero el valor del obturador ha alcanzado su límite superior o inferior, el dispositivo ajustará automáticamente el valor de ganancia para obtener el nivel de brillo ideal. ● **Manual**:Puede ajustar manualmente la ganancia y el valor del obturador para ajustar el brillo de la imagen. ◇ Cuando seleccionas**Exterior**desde el**Contra parpadeo**lista, puede seleccionar**Prioridad de obturador**como modo de exposición. ◇ El modo de exposición puede diferir según los modelos de dispositivo.
Obturador	La persiana es un componente que deja pasar la luz durante un período determinado. Cuanto mayor sea la velocidad de obturación, más corto será el tiempo de exposición y más oscura será la imagen. Puede seleccionar un rango de obturación o agregar un rango personalizado.
Ganar	Cuando se establece el rango del valor de ganancia, se mejorará la calidad del video.
Exposición Compensación	El vídeo será más brillante ajustando el valor de compensación de exposición.
Reducción de ruido 3D	Cuando la Reducción de ruido 3D (RD) está activada, el ruido del video se puede reducir para garantizar una mayor definición de los videos.
Nivel NR	Puede establecer su calificación cuando esta función está activada. Un grado más alto significa una imagen más clara.

Paso 6 Configura la imagen.

Figura 3-46 Imagen

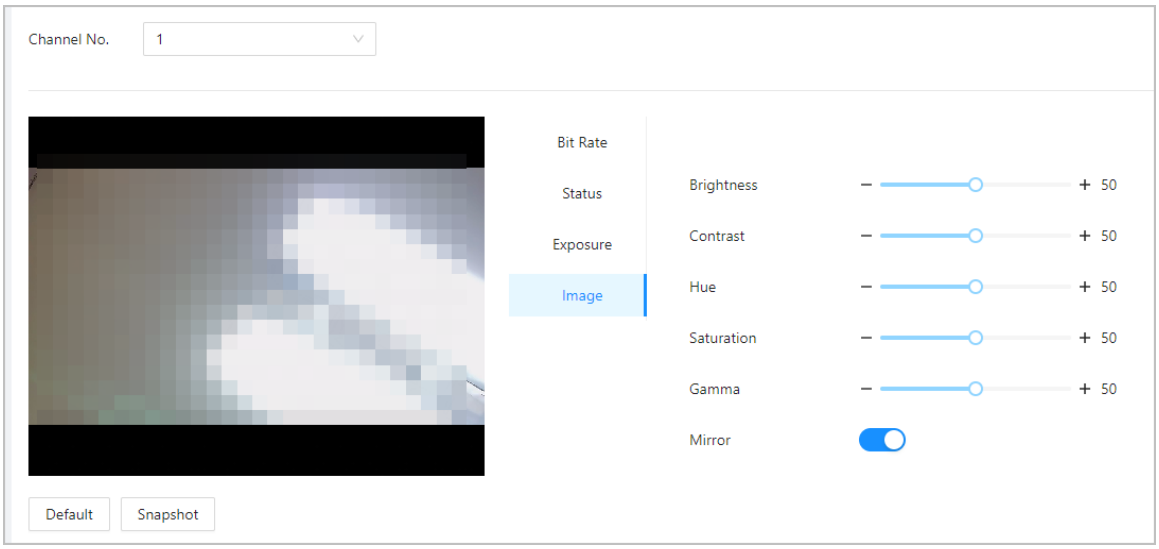


Tabla 3-27 Descripción de la imagen

Parámetro	Descripción
Brillo	El brillo de la imagen. Un valor más alto significa imágenes más brillantes.
Contraste	El contraste es la diferencia de luminancia o color que hace que un objeto sea distinguible. Cuanto mayor sea el valor de contraste, mayor será el contraste de color.
Matiz	Se refiere a la fuerza o saturación de un color. Describe la intensidad del color o su pureza.
Saturación	La saturación de color indica la intensidad del color en una imagen. A medida que aumenta la saturación, aparecen más fuertes, por ejemplo más rojos o más azules. El valor de saturación no cambia el brillo de la imagen.
Espejo	Cuando la función está activada, las imágenes se mostrarán con los lados izquierdo y derecho invertidos.

3.9.1.2 Configuración del canal 2

Procedimiento

Paso 1 Seleccionar**Configuración de audio y vídeo**>**Video**.

Paso 2 Seleccionar**2**desde el**Canal No.**lista. Configura el

Paso 3 estado del vídeo.

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

Figura 3-47 Configurar estado

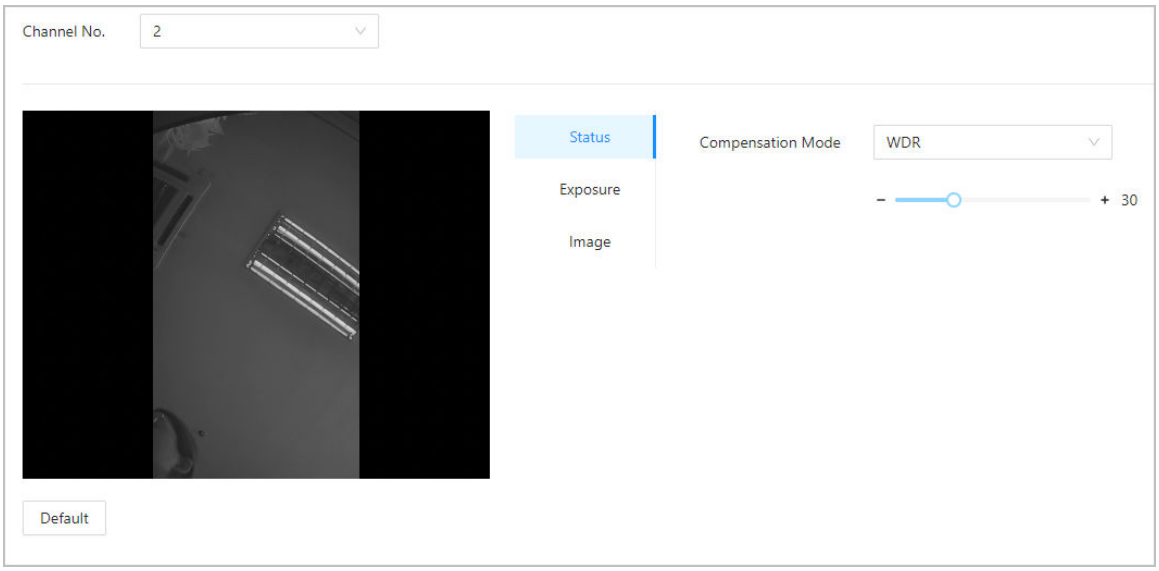


Tabla 3-28 Descripción del estado

Parámetro	Descripción
Modo de compensación	• **Desactivar**:La compensación está desactivada. • **BLC**:La compensación de contraluz aporta automáticamente más luz a las áreas más oscuras de una imagen cuando la luz brillante que brilla desde atrás las oscurece. • **WDR**:El sistema atenúa las áreas brillantes y compensa las áreas oscuras para crear un equilibrio que mejore la calidad general de la imagen. • **CHL**:La compensación de altas luces (HLC) es una tecnología utilizada en las cámaras de seguridad CCTV/IP para tratar imágenes expuestas a luces como faros o focos. El sensor de imagen de la cámara detecta luces intensas en el vídeo y reduce la exposición en estos puntos para mejorar la calidad general de la imagen.

Etapa 4 Configure los parámetros de exposición.

Figura 3-48 Parámetro de exposición

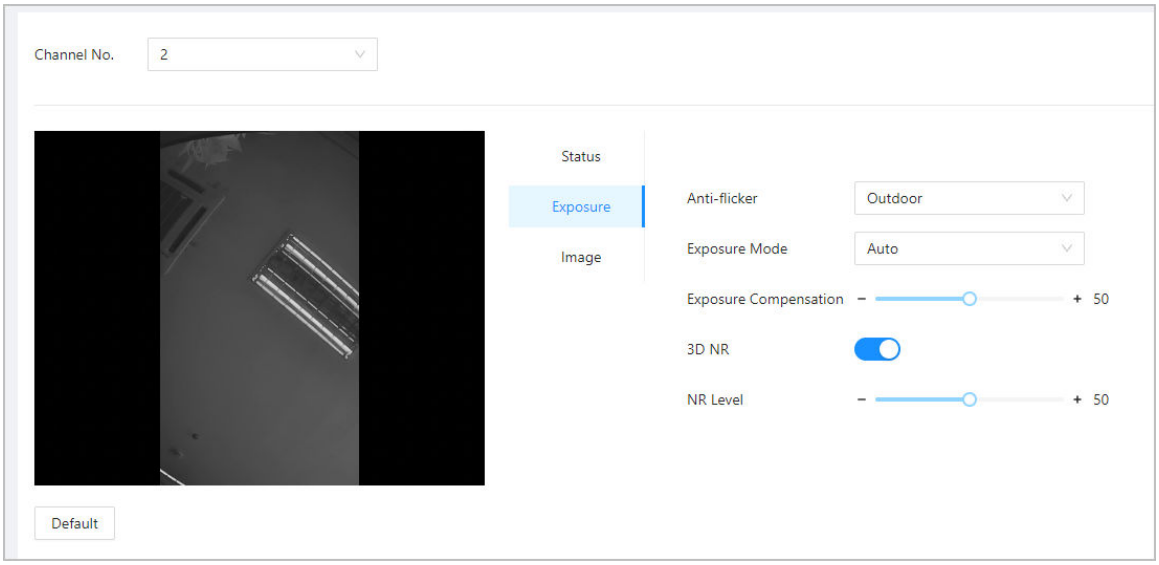


Tabla 3-29 Descripción del parámetro de exposición

Parámetro	Descripción
Contra parpadeo	Configure el antiparpadeo para reducir el parpadeo y disminuir o reducir los colores o la exposición desiguales. • **50Hz**:Cuando la red eléctrica es de 50 Hz, la exposición se ajusta automáticamente en función del brillo del entorno para evitar la aparición de líneas horizontales. • **60Hz**:Cuando la red eléctrica es de 60 Hz, la exposición se ajusta automáticamente en función del brillo del entorno para reducir la aparición de líneas horizontales. • **Exterior**:Cuando**Exterior**Cuando se selecciona, se puede cambiar el modo de exposición.

Parámetro	Descripción
Modo de exposición	Puede configurar la exposición para ajustar el brillo de la imagen. ● **Auto**:El dispositivo ajusta automáticamente el brillo de las imágenes según el entorno. ● **Prioridad de obturador**:El dispositivo ajusta el brillo de la imagen de acuerdo con el rango establecido del obturador. Si la imagen no es lo suficientemente brillante pero el valor del obturador ha alcanzado su límite superior o inferior, el dispositivo ajustará automáticamente el valor de ganancia para obtener el nivel de brillo ideal. ● **Manual**:Puede ajustar manualmente la ganancia y el valor del obturador para ajustar el brillo de la imagen. ◇ Cuando seleccionas**Exterior**desde el**Contra parpadeo**lista, puede seleccionar**Prioridad de obturador**como modo de exposición. ◇ El modo de exposición puede diferir según los modelos de dispositivo.
Exposición Compensación	El vídeo será más brillante ajustando el valor de compensación de exposición.
Reducción de ruido 3D	Cuando la Reducción de ruido 3D (RD) está activada, el ruido del video se puede reducir para garantizar una mayor definición de los videos.
Nivel NR	Puede establecer su calificación cuando esta función está activada. Un grado más alto significa una imagen más clara.

Paso 5 Configure los parámetros de la imagen.

Figura 3-49 Parámetros de imagen

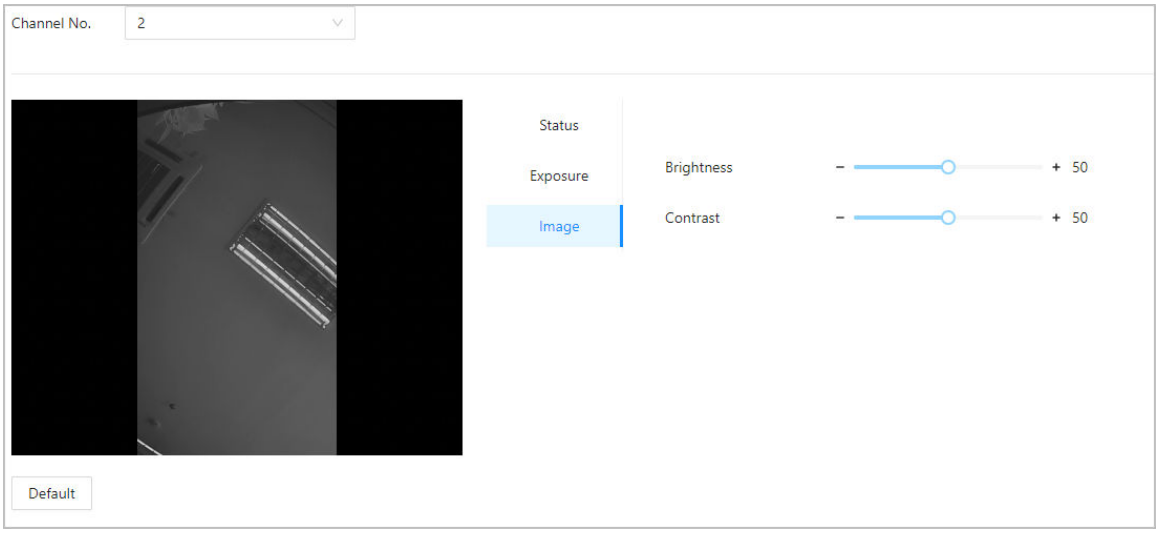


Tabla 3-30 Descripción de la imagen

Parámetro	Descripción
Brillo	El brillo de la imagen. Un valor más alto significa imágenes más brillantes.
Contraste	El contraste es la diferencia de luminancia o color que hace que un objeto sea distinguible. Cuanto mayor sea el valor de contraste, mayor será el contraste de color.

3.9.2 Configuración de mensajes de audio

Configure indicaciones de audio durante la verificación de identidad.

Procedimiento

Paso 1 Seleccionar**Configuración de audio y vídeo**>**Audio**.

Paso 2 Configura los parámetros de audio.

Figura 3-50 Configurar parámetros de audio

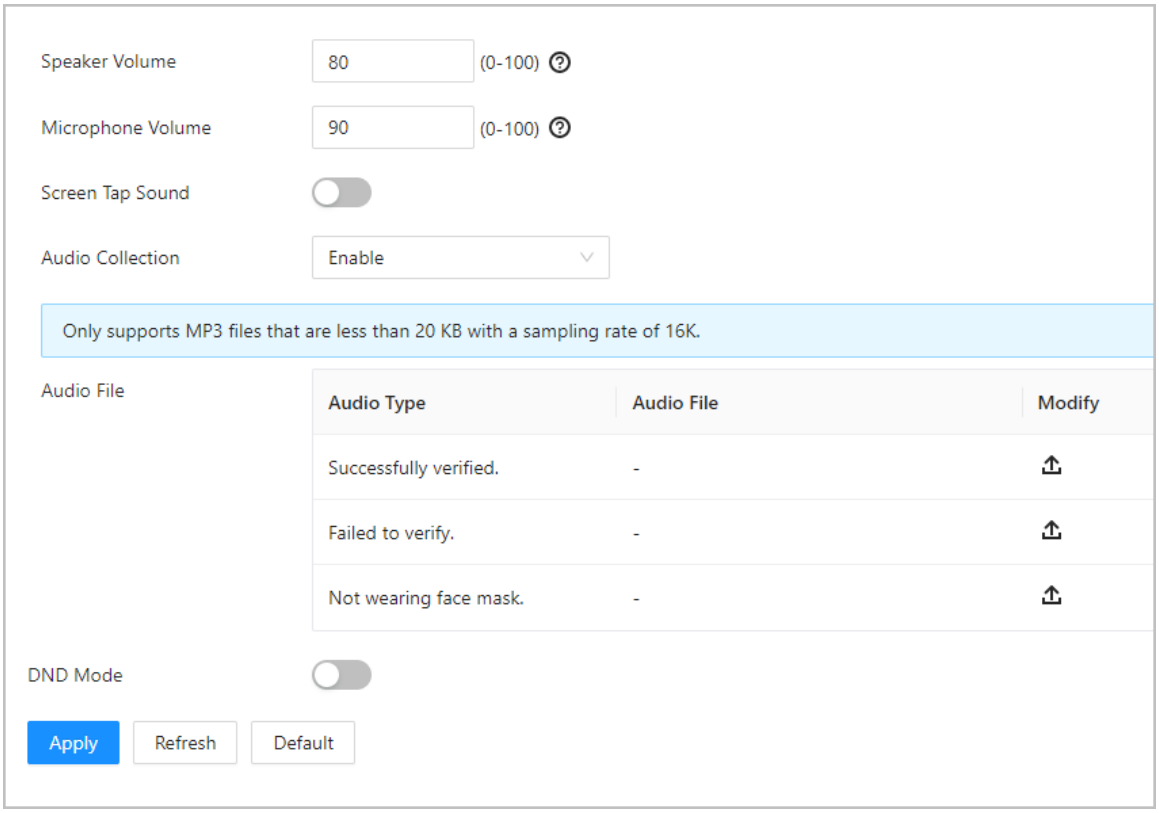


Tabla 3-31 Descripción de los parámetros

Parámetros	Descripción
Vocero	Configure el volumen del altavoz.
Volumen del micrófono	Configura el volumen del micrófono.
Sonido de toque de pantalla	Cuando esta función está habilitada, los dispositivos con pantalla táctil producirán un sonido de toque y los dispositivos sin pantalla táctil producirán un sonido de clic del mouse.
Colección de audios	El audio no se grabará durante la conversación por video cuando esta función no esté habilitada.
Archivo de audio	Haga clic en Cargar archivos de audio a la plataforma.
Modo No Molestar	No hay mensajes de voz durante el tiempo establecido cuando verifica su identidad en el Dispositivo. Puede configurar hasta 4 períodos.

Paso 3 Hacer clic para cargar archivos de audio a la plataforma para cada tipo de audio.

Solo admite archivos MP3 de menos de 20 KB con una frecuencia de muestreo de 16 K.

Etapa 4 Hacer clic**Aplicar**.

3.9.3 Configurar la detección de movimiento

Cuando se detecten objetos en movimiento y se alcance el umbral establecido, la pantalla se despertará.

Información de contexto

Esta función solo está disponible en modelos seleccionados.

Procedimiento

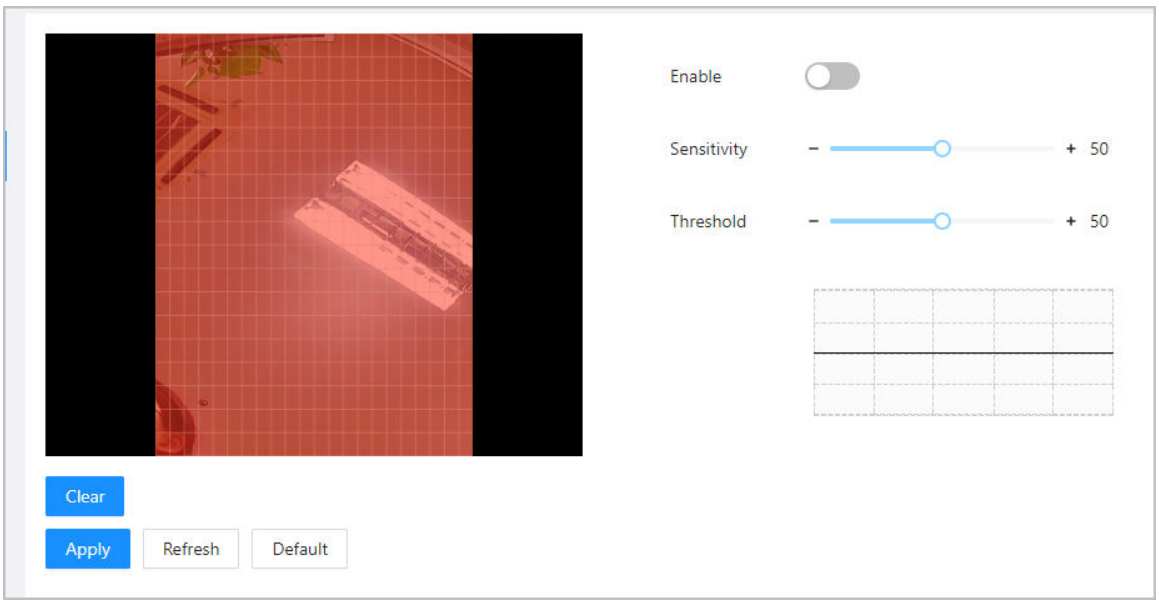
Paso 1 Seleccionar**Configuración de audio y vídeo**>**Configuración de detección de movimiento**

Paso 2 . Habilite la función de detección de movimiento.

Paso 3 Mantenga presionado el botón izquierdo del mouse y luego dibuje un área de detección en el área roja.

- El área de detección de movimiento se muestra en rojo.
- Para eliminar el área de detección de movimiento existente, haga clic en**Claro**.
- El área de detección de movimiento que dibujes será un área sin detección de movimiento si dibujas en el área de detección de movimiento predeterminada.

Figura 3-51 Área de detección de movimiento



Etapa 4 Configure los parámetros.

- Sensibilidad: El sensible al entorno. Una mayor sensibilidad significa que es más fácil activar las alarmas.
- Umbral: el porcentaje del área del objeto en movimiento en el área de detección de movimiento. Un umbral más alto significa que es más fácil activar las alarmas.

Paso 5 Hacer clic**Aplicar**.

La detección de movimiento se activa cuando se muestran las líneas rojas; Las líneas verdes se muestran cuando no se activa.

3.9.4 Configuración de codificación local

Configure el área de visualización en la charla en video y la vista previa.

Información de contexto

- Esta función solo está disponible en modelos seleccionados.
- Esta función está habilitada por defecto cuando trabaja con un VTH. Es posible que no se pueda acceder a la vista previa cuando esta función está desactivada.

Procedimiento

Paso 1 Inicie sesión en la página web.

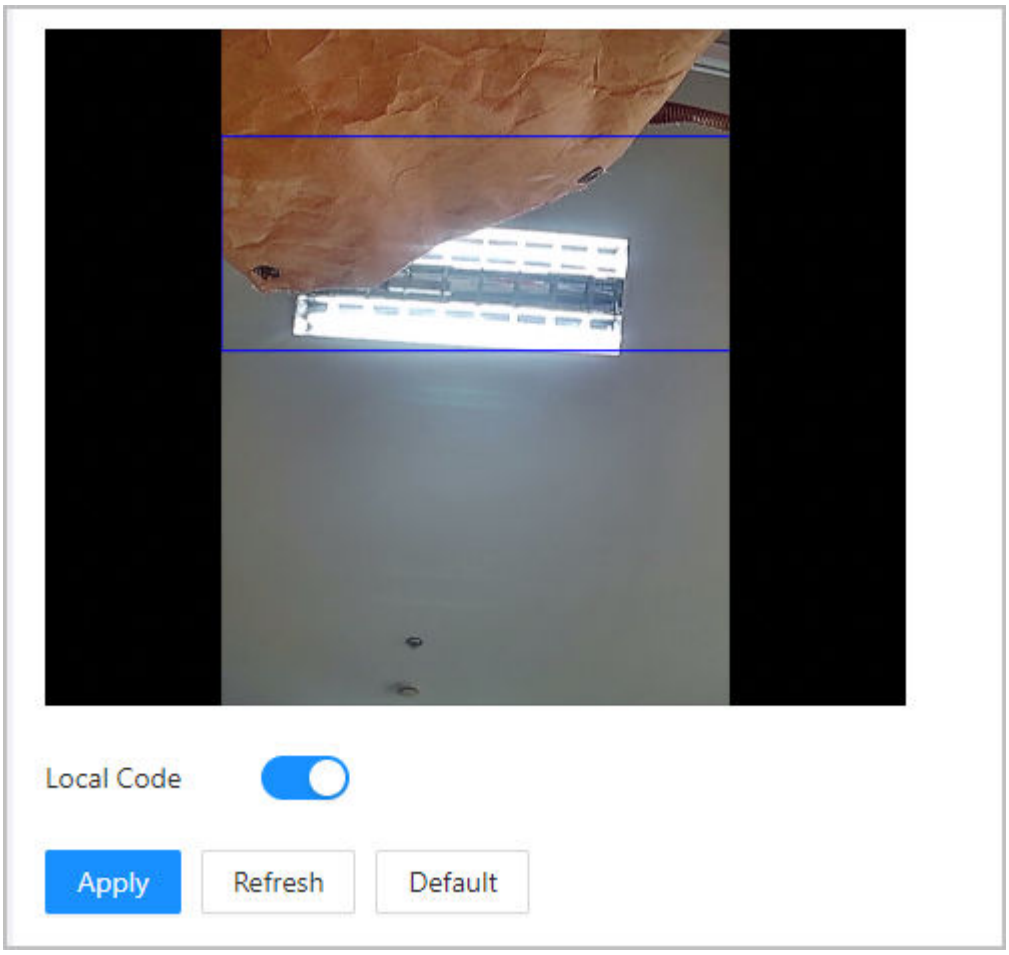
Paso 2 Seleccionar**Configuración de audio y vídeo**>**Código**

Paso 3 **Local**. Seleccionar**Permitir**para activar la función. Arrastre

Etapa 4 el cuadro a una posición designada.

El cuadro indica el área de vista previa durante la charla en video.

Figura 3-52 Codificación local



Paso 5 Hacer clic**Aplicar**.

3.10 Configuración de comunicación

3.10.1 Configuración de red

3.10.1.1 Configuración de TCP/IP

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

Procedimiento

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

Paso 2 Configure los parámetros.

Figura 3-53 TCP/IP

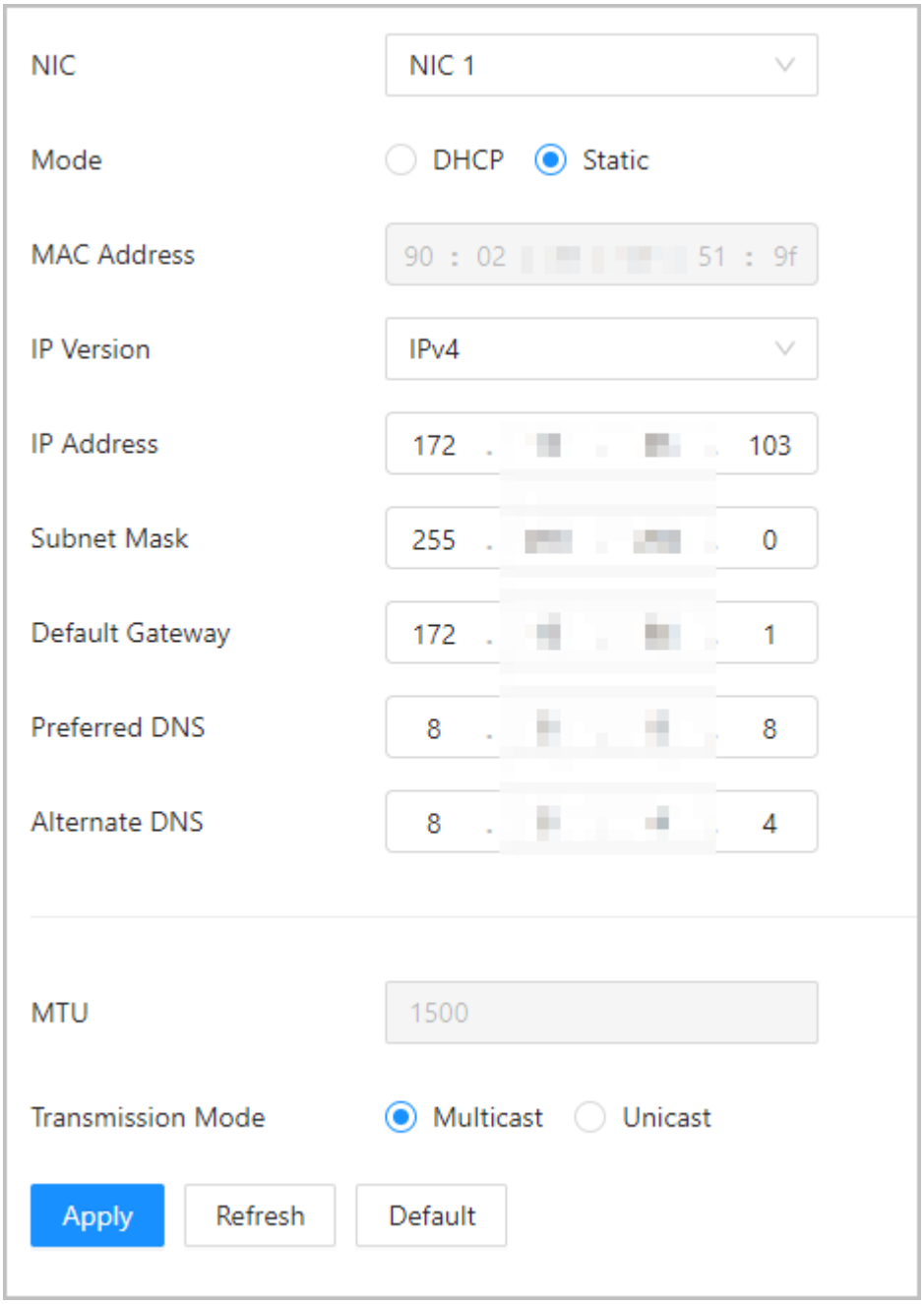


Tabla 3-32 Descripción de TCP/IP

Parámetro	Descripción
Modo	• Estático: ingrese manualmente la dirección IP, la máscara de subred y la puerta de enlace. • DHCP: Significa Protocolo de configuración dinámica de host. Cuando DHCP está activado, al dispositivo se le asignará automáticamente la dirección IP, la máscara de subred y la puerta de enlace.
Dirección MAC	Dirección MAC del Dispositivo.
Versión IP	IPv4 o IPv6.

Parámetro	Descripción
Dirección IP	Si configura el modo en**Estático**, configure la dirección IP, la máscara de subred y la puerta de enlace.  ● La dirección IPv6 se representa en hexadecimal. ● La versión IPv6 no requiere la configuración de máscaras de subred. ● La dirección IP y la puerta de enlace predeterminada 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	Establezca la dirección IP del servidor DNS alternativo.
MTU	MTU (Unidad de transmisión máxima) se refiere al tamaño máximo de datos que se pueden transmitir en un solo paquete de red en redes informáticas. Un valor de MTU mayor puede mejorar la eficiencia de transmisión de la red al reducir la cantidad de paquetes y la sobrecarga de red asociada. Si un dispositivo a lo largo de la ruta de la red no puede manejar paquetes de un tamaño específico, puede provocar fragmentación de paquetes o errores de transmisión. En las redes Ethernet, el valor MTU común es 1500 bytes. Sin embargo, en ciertos casos, como el uso de PPPoE o VPN, es posible que se requieran valores de MTU más pequeños para adaptarse a los requisitos de protocolos o servicios de red específicos. Los siguientes son valores de MTU recomendados como referencia: ● 1500: Valor máximo para paquetes Ethernet, también el valor predeterminado. Esta es una configuración típica para conexiones de red sin PPPoE ni VPN, algunos enrutadores, adaptadores de red y conmutadores. ● 1492: valor óptimo para PPPoE ● 1468: Valor óptimo para DHCP. ● 1450: valor óptimo para VPN.
Modo de transmisión	● Multidifusión: Ideal para videoconferencias. ● Unicast: Ideal para llamadas grupales.

Paso 3 Hacer clic**DE ACUERDO**.

3.10.1.2 Configuración de Wi-Fi

Procedimiento

Paso 1 Seleccionar**Configuración de comunicación**>**Configuración de red**>**Wifi**.

Paso 2 Enciende el wifi.

Se muestran todas las redes Wi-Fi disponibles.

Figura 3-54 Wi-Fi

- Wi-Fi y Wi-Fi AP no se pueden habilitar al mismo tiempo.
- La función Wi-Fi solo está disponible en modelos seleccionados.

Paso 3 Grifo + y luego ingrese la contraseña de Wi-Fi.

El wifi está conectado.

Operaciones relacionadas

- DHCP: Habilite esta función y haga clic en**Aplicar**, al dispositivo se le asignará automáticamente una dirección Wi-Fi.
- Estático: habilite esta función, ingrese manualmente una dirección Wi-Fi y luego haga clic en**Aplicar**, el dispositivo se conectará a la red Wi-Fi.

3.10.1.3 Configuración del puerto

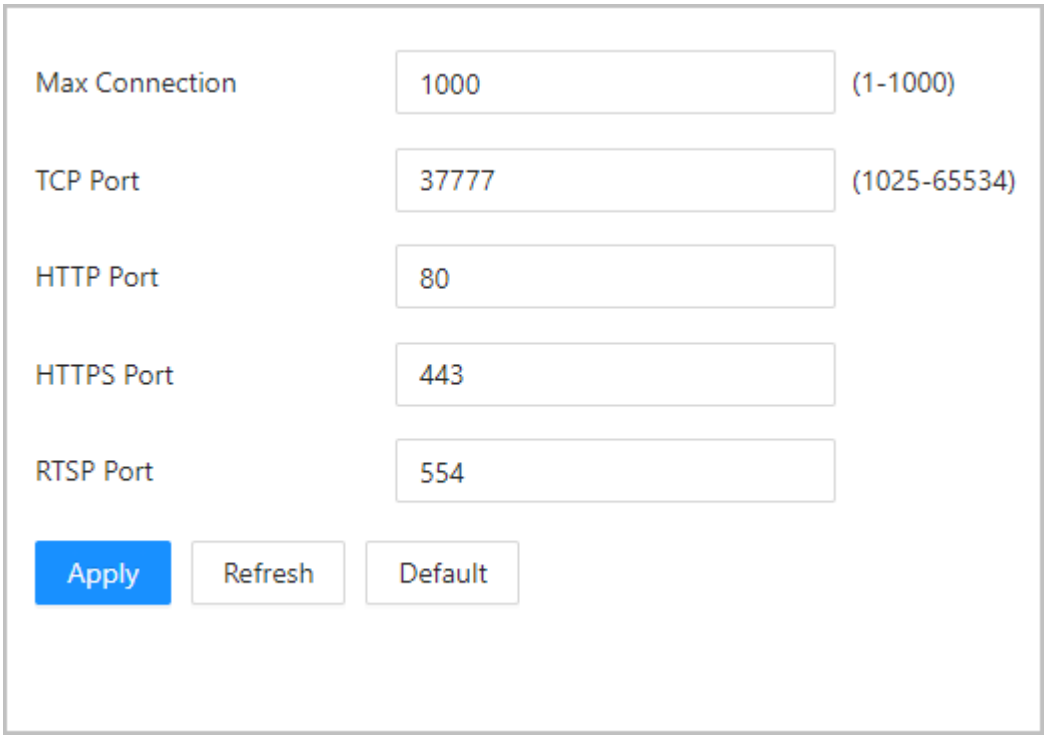
Puede limitar el acceso al Dispositivo al mismo tiempo a través de la página web, el cliente de escritorio y el cliente móvil.

Procedimiento

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

Paso 2 Configure los puertos.

Figura 3-55 Configurar puertos



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

Tabla 3-33 Descripción de puertos

Parámetro	Descripción
Conexión máxima	Puede establecer la cantidad máxima de clientes (como página web, cliente de escritorio y cliente móvil) que pueden acceder al dispositivo al mismo tiempo.
Puerto TCP	El valor predeterminado es 37777.
Puerto HTTP	El valor predeterminado es 80. Si ha cambiado el número de puerto, agréguelo después de la dirección IP cuando acceda a la página web.
Puerto HTTPS	El valor predeterminado es 443.
Puerto RTSP	El valor predeterminado es 554.

Paso 3 Hacer clic**Aplicar**.

3.10.1.4 Configuración del servicio básico

Cuando desee conectar el Dispositivo a una plataforma de terceros, active las funciones CGI y ONVIF.

Procedimiento

Paso 1 Seleccionar**Configuración de comunicación**>**Configuración de la red**>**Servicios basicos**

Paso 2 . Configurar el servicio básico.

Figura 3-56 Servicio básico

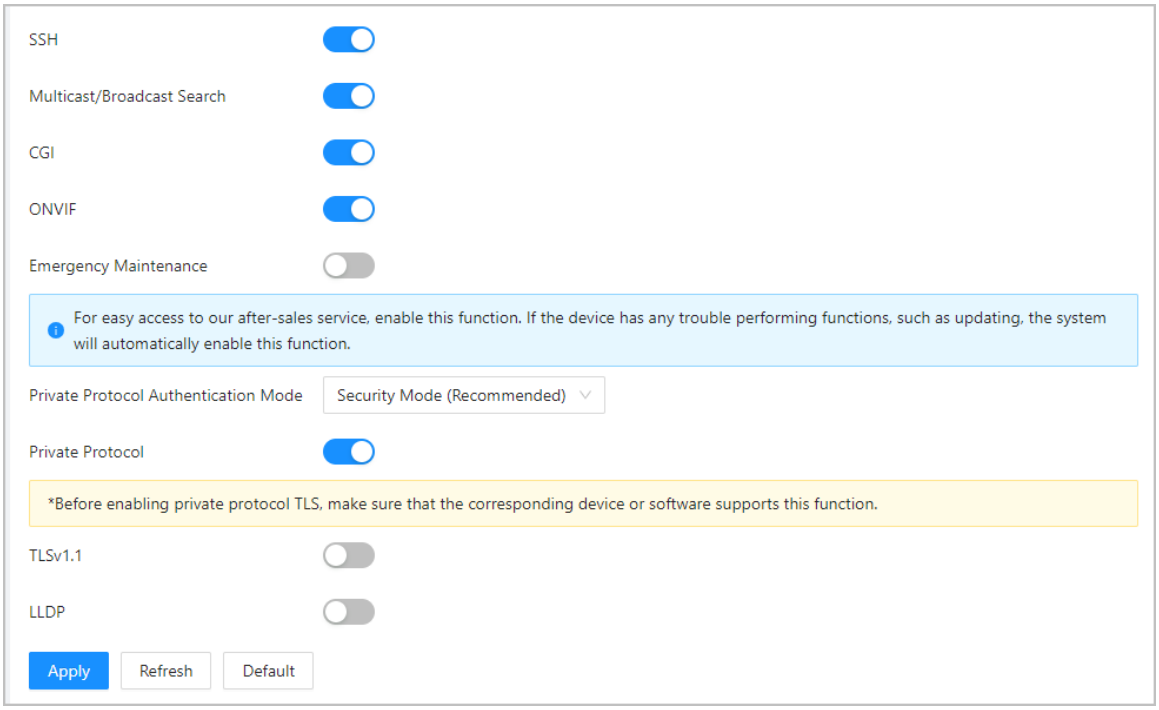


Tabla 3-34 Descripción de los parámetros del servicio básico

Parámetro	Descripción
SSH	SSH, o Secure Shell Protocol, es un protocolo de administración remota que permite a los usuarios acceder, controlar y modificar sus servidores remotos a través de Internet.
Búsqueda de multidifusión/difusión	Busque dispositivos a través de protocolo de multidifusión o transmisión.
CGI	La Common Gateway Interface (CGI) es una intersección entre servidores web a través de la cual es posible el intercambio de datos estandarizado entre aplicaciones y servidores externos.
ONVIF	ONVIF significa Foro de interfaz de vídeo en red abierta. Su objetivo es proporcionar un estándar para la interfaz entre diferentes dispositivos de seguridad basados en IP. Estas especificaciones ONVIF estandarizadas son como un lenguaje común que todos los dispositivos pueden usar para comunicarse.
Mantenimiento de emergencia	Está activado de forma predeterminada.
Modo de autenticación de protocolo privado	Configure el modo de autenticación, incluido el modo seguro y el modo de compatibilidad. Se recomienda elegir**modo de seguridad**. ● Modo de seguridad (recomendado): no admite el acceso al dispositivo a través de métodos de autenticación implícita, DES y de texto sin formato, lo que mejora la seguridad del dispositivo. ● Modo compatible: admite el acceso al dispositivo a través de métodos de autenticación implícita, DES y de texto sin formato, con seguridad reducida.
Protocolo privado	La plataforma agrega dispositivos mediante protocolo privado.

Parámetro	Descripción
TLSv1.1	TLSv1.1 hace referencia a la versión 1.1 de Transport Layer Security. TLS es un protocolo criptográfico diseñado para proporcionar comunicación segura y autenticada a través de una red informática. Es posible que se presenten riesgos de seguridad cuando TLSv1.1 está habilitado. Por favor tenga en cuenta.
LLDP	LLDP es la abreviatura de Link Layer Discovery Protocol, que es un protocolo de capa de enlace de datos. Permite que los dispositivos de red, como conmutadores, enrutadores o servidores, intercambien información sobre sus identidades y capacidades entre sí. El protocolo LLDP ayuda a los administradores de red a comprender mejor la topología de la red y proporciona una forma estandarizada de automatizar el descubrimiento y mapeo de conexiones entre dispositivos de red. Esto facilita la configuración de la red, la resolución de problemas y la optimización del rendimiento.

Paso 3 Hacer clic**Aplicar**.

3.10.1.5 Configuración del servicio en la nube

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

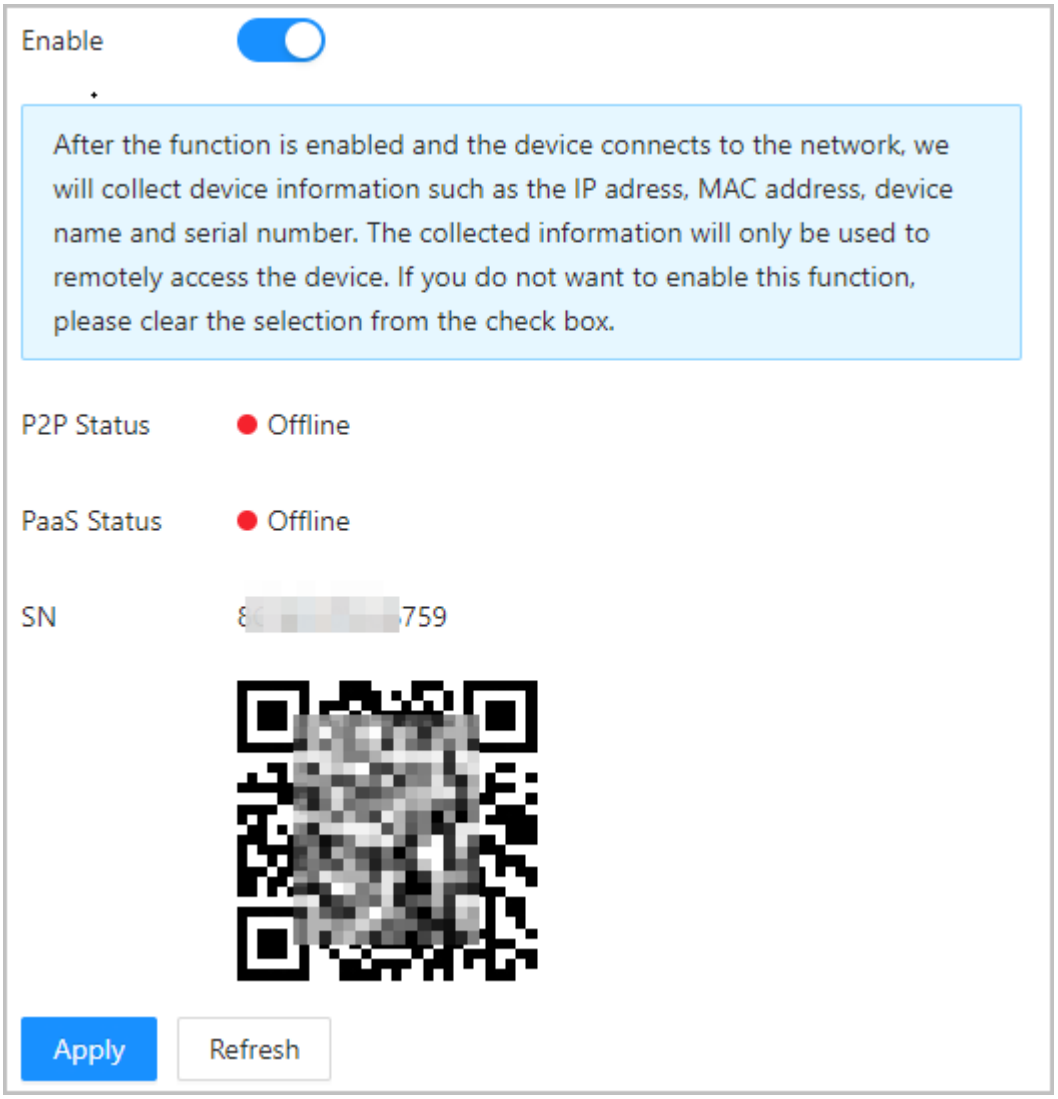
Procedimiento

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

Paso 2 Active la función del servicio en la nube.

El servicio en la nube se conecta en línea si P2P y PaaS están en línea.

Figura 3-57 Servicio en la nube



Paso 3 Hacer clic**Aplicar**.

Etapa 4 Escanee el código QR con DMSS para agregar el dispositivo.

3.10.1.6 Configuración del registro automático

El registro automático permite agregar los dispositivos a la plataforma de administración sin ingresar manualmente la información del dispositivo, como la dirección IP y el puerto.

Información de contexto

El registro automático solo admite SDK.

Procedimiento

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

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

Figura 3-58 Registro automático

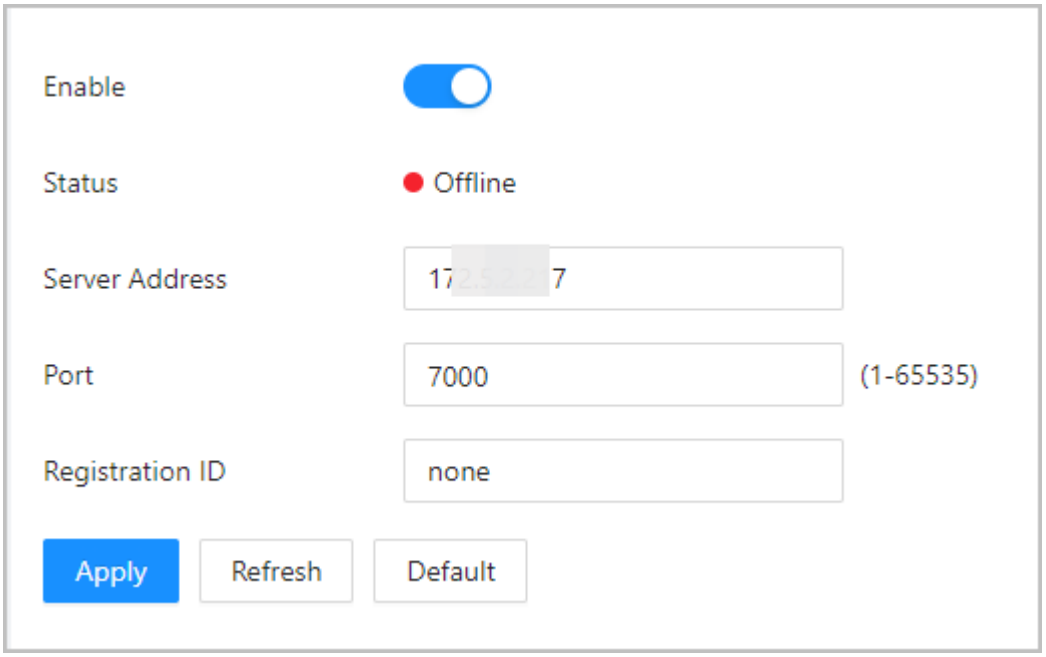


Tabla 3-35 Descripción del registro automático

Parámetro	Descripción
Estado	Muestra el estado de conexión del registro automático.
Dirección del servidor	La dirección IP o el nombre de dominio del servidor.
Puerto	El puerto del servidor que se utiliza para el registro automático.
Identificación de Registro	El ID de registro (definido por el usuario) del dispositivo. Agregar el dispositivo a la gestión ingresando el ID de registro en la plataforma.

Paso 3 Hacer clic**Aplicar**.

3.10.1.7 Configuración de registros activos CGI

Conéctese a una plataforma de terceros a través del protocolo CGI.

Información de contexto

Sólo admite IPv4.

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración de comunicación**>**Configuración de la red**>**CGI se registra activamente**.

Paso 2 Habilite esta función y luego configure los parámetros. Hacer clic

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

Figura 3-59 Registro activo de CGI

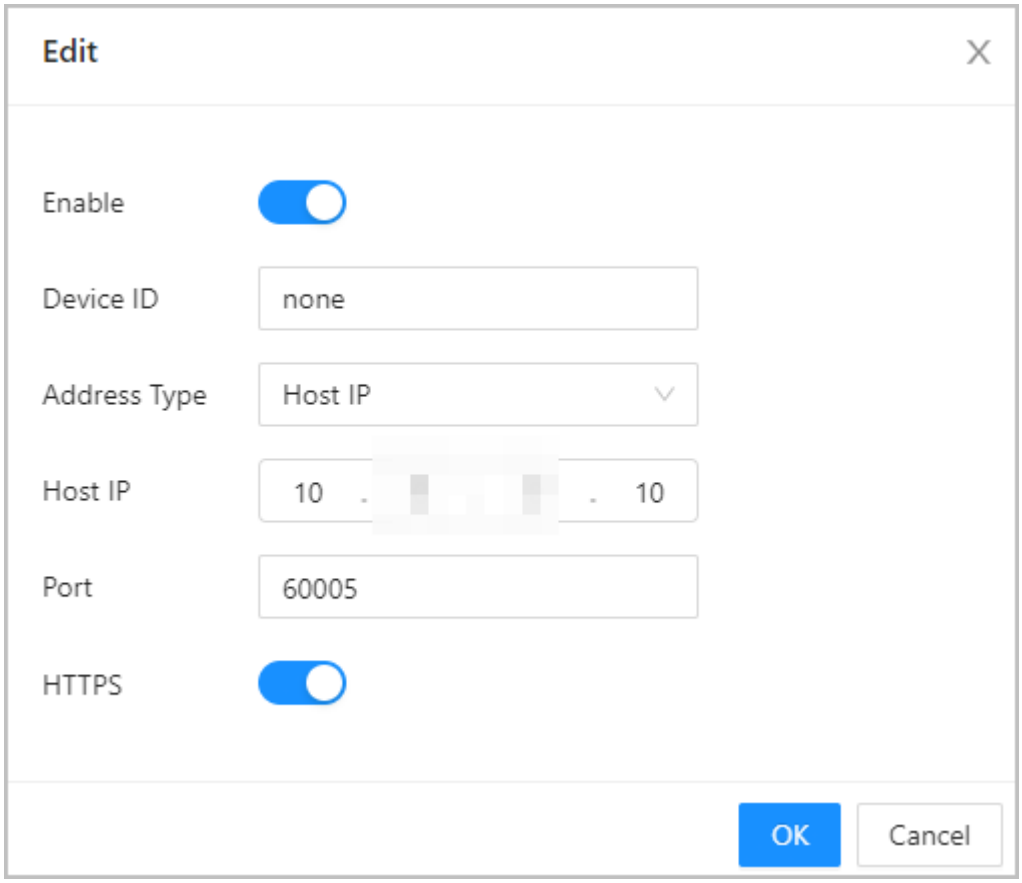


Tabla 3-36 Descripción del registro automático

Parámetro	Descripción
ID del dispositivo	Admite hasta 32 bytes, incluidos chinos, números, letras y caracteres especiales.
Tipo de dirección	Admite 2 métodos para registrarse. ● IP del host: ingrese la dirección IP de la plataforma de terceros. ● Nombre de dominio: ingrese el nombre de dominio de la plataforma de terceros.
IP del host	
Nombre de dominio	
HTTPS	Acceda a la plataforma de terceros a través de HTTPS. HTTPS protege la comunicación a través de una red informática.

Etapa 4 Hacer clic**Aplicar**.

3.10.1.8 Configurar la carga automática

Envíe información de usuario y desbloquee registros a través de la plataforma de gestión.

Procedimiento

Paso 1 En la página de inicio, seleccione**Configuración de comunicación**>**Configuración de la red**>**Carga automática**.

Paso 2 (Opcional) Habilitar**Empujar información de la persona**.

Cuando se actualiza la información del usuario o se agregan nuevos usuarios, el Dispositivo enviará automáticamente la información del usuario a la plataforma de administración.

Paso 3 Habilite el modo de carga HTTP.

Etapa 4 Hacer clic**Agregar**y luego configure los parámetros.

Figura 3-60 Carga automática

Tabla 3-37 Descripción de los parámetros

Parámetro	Descripción
IP/Nombre de dominio	La IP o nombre de dominio de la plataforma de gestión.
Puerto	El puerto de la plataforma de gestión.
HTTPS	Accede a la plataforma de gestión a través de HTTPS. HTTPS protege la comunicación a través de una red informática.
Autenticación	Habilite la autenticación de cuenta cuando acceda a la plataforma de administración. Se requiere nombre de usuario y contraseña de inicio de sesión.
Tipo par	Seleccione el tipo de evento que se enviará a la plataforma de gestión. ● Antes de utilizar esta función, habilite**Empujar información de la persona**. ● La información de la persona solo se puede enviar a una plataforma de administración y los registros de desbloqueo se pueden enviar a múltiples plataformas de administración.

Paso 5 Hacer clic**Aplicar**.

3.10.2 Configuración de RS-485

Configure los parámetros RS-485 si conecta un dispositivo externo al puerto RS-485.

Procedimiento

Paso 1 Seleccionar**Configuración de comunicación**>**Configuración**

Paso 2 **RS-485**. Configure los parámetros.

Figura 3-61 Configurar parámetros

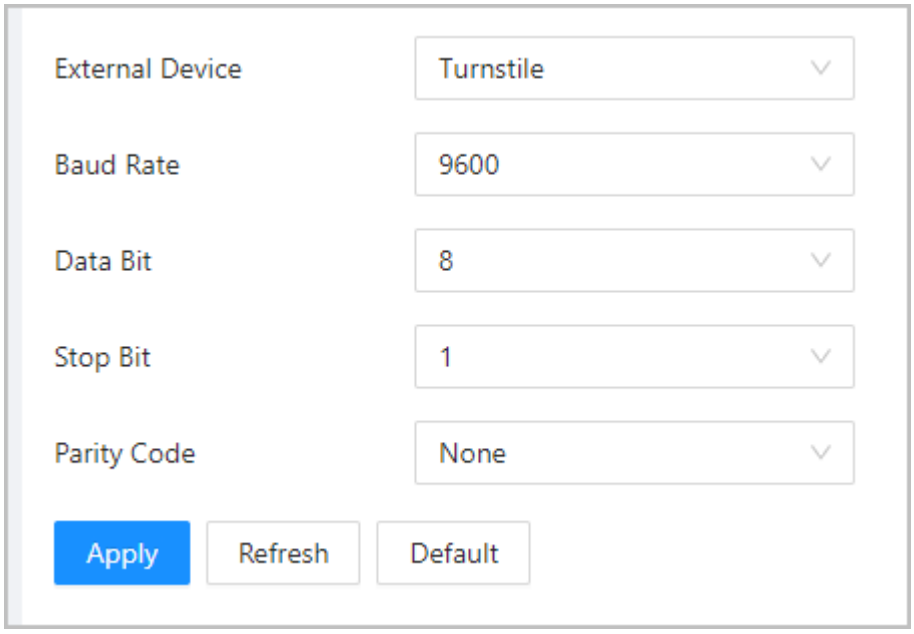


Tabla 3-38 Configurar el formato Wiegand

Parámetro	Descripción
Dispositivo externo	● Controlador de acceso Seleccionar**Controlador de acceso**cuando el Dispositivo funciona como un lector de tarjetas y envía datos a otros controladores de acceso externos para controlar el acceso. Tipo de datos de salida: ◇ Número de tarjeta: genera datos basados en el número de tarjeta cuando los usuarios deslizan la tarjeta para desbloquear la puerta; genera datos basados en el primer número de tarjeta del usuario cuando utiliza otros métodos de desbloqueo. ◇ No.: genera datos basados en la identificación del usuario. ● Lector de tarjetas: El Dispositivo funciona como un controlador de acceso y se conecta a un lector de tarjetas externo. ● Lector (OSDP): El Dispositivo está conectado a un lector de tarjetas basado en el protocolo OSDP. ● Módulo de seguridad de control de puerta: el botón de salida de la puerta, la cerradura y el enlace contra incendios no son efectivos una vez que se habilita el módulo de seguridad. ● Torniquete: cuando el Dispositivo se conecta a un torniquete y la placa controladora de acceso del torniquete se conecta a un módulo de código QR externo o módulo de deslizamiento de tarjeta, la placa transmitirá los datos de verificación al torniquete.
Bit de datos	El número de bits utilizados para transmitir los datos reales en una comunicación en serie. Representa los dígitos binarios que transportan la información que se transmite.

Parámetro	Descripción
Bit de parada	Un bit enviado después de los datos y bits de paridad opcionales para indicar el final de una transmisión de datos. Permite que el receptor se prepare para el siguiente byte de datos y proporciona sincronización en el protocolo de comunicación.
Código de paridad	Un bit adicional enviado después de los bits de datos para detectar errores de transmisión. Ayuda a verificar la integridad de los datos transmitidos al garantizar un número específico de bits lógicos altos o bajos.

Paso 3 Hacer clic**Aplicar**.

3.10.3 Configuración de Wiegand

Admite acceso a dispositivos Wiegand. Configure el modo y el modo de transmisión según sus dispositivos reales.

Procedimiento

Paso 1 Seleccionar**Configuración de comunicación**>**Wiegand**. Seleccione

Paso 2 un tipo de Wiegand y luego configure los parámetros.

- Seleccionar**Entrada Wiegand**cuando conecta un lector de tarjetas externo al Dispositivo.

  Cuando el Dispositivo se conecta a un dispositivo de terceros a través del puerto de entrada Wiegand y el número de tarjeta leído por el Dispositivo está en el orden inverso al número de tarjeta real. En este caso, puede activar**Inversión del número de tarjeta**función.
- Seleccionar**Salida Wiegand**cuando el Dispositivo funciona como lector de tarjetas y necesita conectarlo a otro controlador de acceso.

Figura 3-62 Salida Wiegand

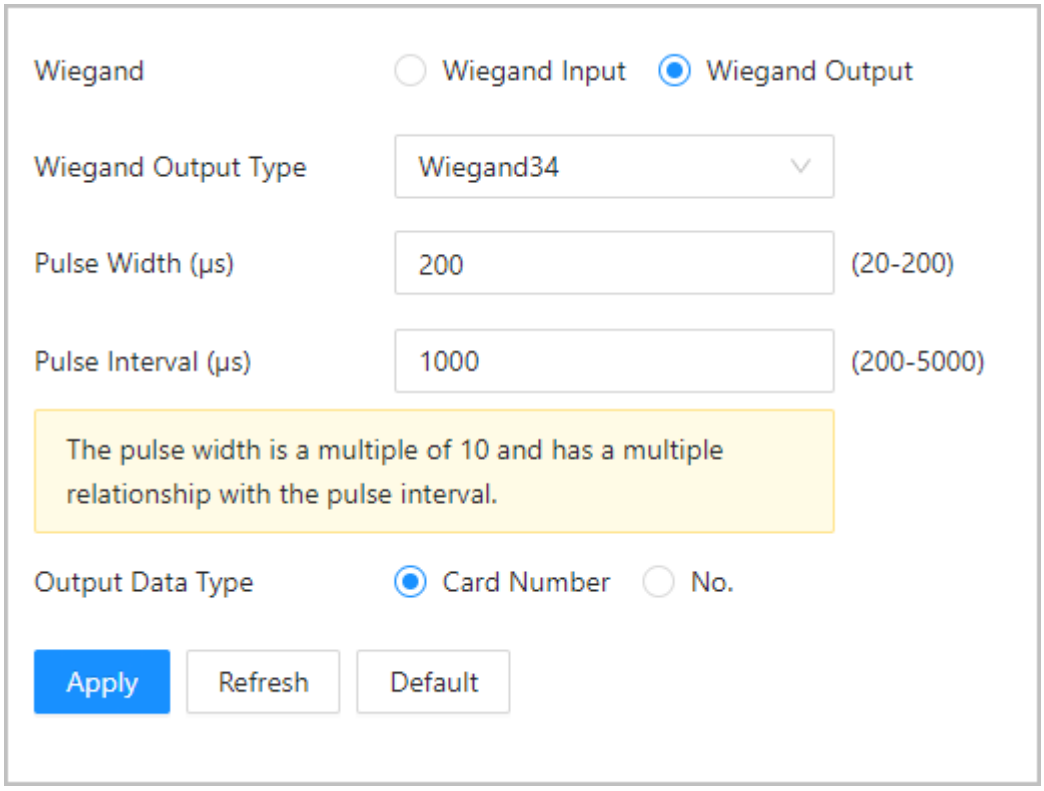


Tabla 3-39 Descripción de la salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	Seleccione un formato Wiegand para leer números de tarjetas o números de identificación. ● **Wiegand26**:Lee 3 bytes o 6 dígitos. ● **Wiegand34**:Lee 4 bytes u 8 dígitos. ● **Wiegand66**:Lee 8 bytes o 16 dígitos.
Ancho de pulso	Ingrese el ancho del pulso y el intervalo de pulso de la salida Wiegand.
Intervalo de pulso	
Tipo de datos de salida	Seleccione el tipo de datos de salida. ● **No.**:Genera datos basados en la identificación del usuario. El formato de datos es hexadecimal o decimal. ● **Número de tarjeta**:Genera datos basados en el primer número de tarjeta del usuario.

Paso 3 Hacer clic**Aplicar**.

3.11 Configurando el sistema

3.11.1 Gestión de usuarios

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

3.11.1.1 Agregar administradores

Puede agregar nuevas cuentas de administrador y luego podrán iniciar sesión en la página web del Dispositivo.

Procedimiento

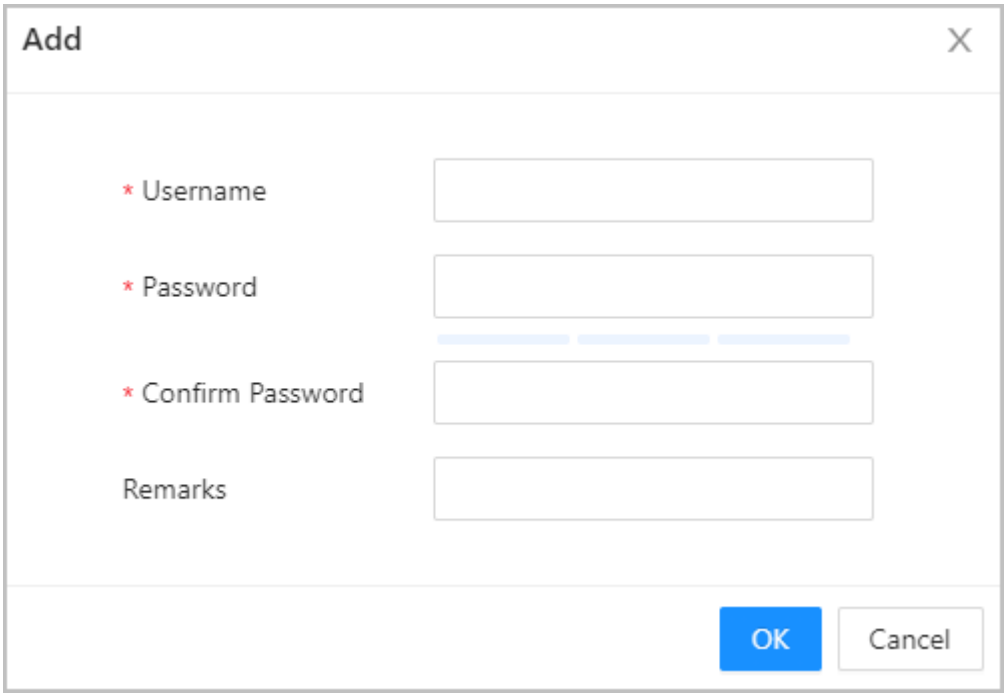
Paso 1 En la página de inicio, seleccione**Sistema**>**Cuenta**. Hacer

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

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

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

Figura 3-63 Agregar administradores



Paso 3 Hacer clic**DE ACUERDO**.

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

3.11.1.2 Agregar usuarios ONVIF

Información de contexto

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

Procedimiento

Paso 1 En la página de inicio, seleccione**Sistema**>**Cuenta**>**Usuario ONVIF**. Hacer

Paso 2 clic**Agregar**y luego configure los parámetros.

Figura 3-64 Agregar usuario ONVIF

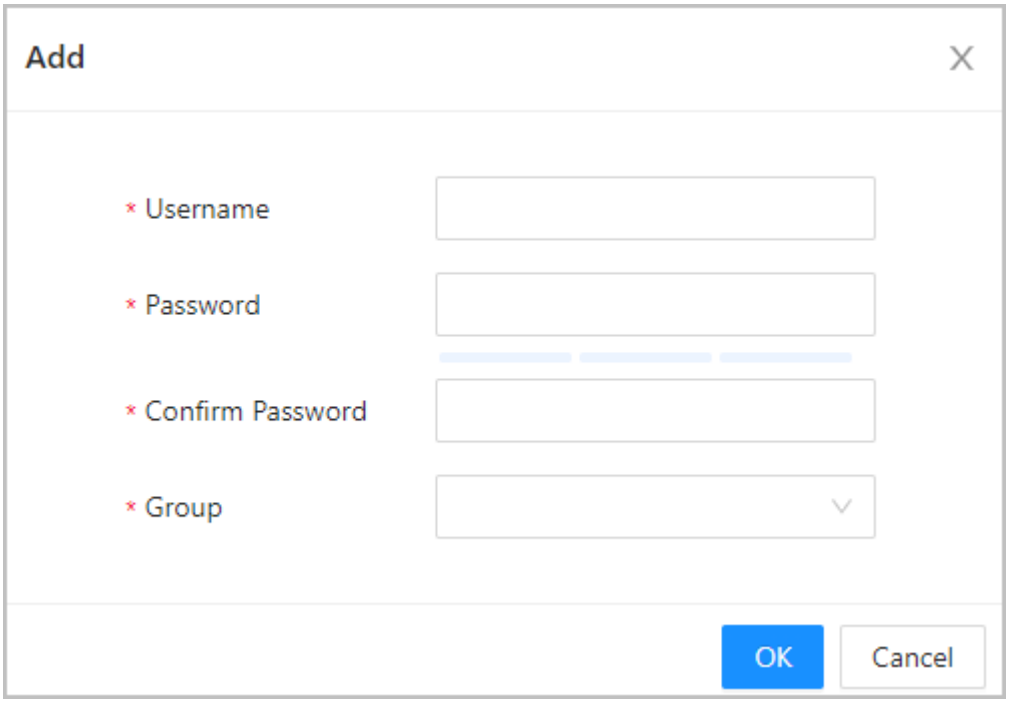


Tabla 3-40 Descripción de usuario de ONVIF

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 medias, puntos o @.
Contraseña	La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excluidos ' " ; : &).
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 ni registros del sistema en el Administrador de dispositivos ONVIF.

Paso 3 Hacer clic**DE ACUERDO**.

3.11.1.3 Restablecer la contraseña

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

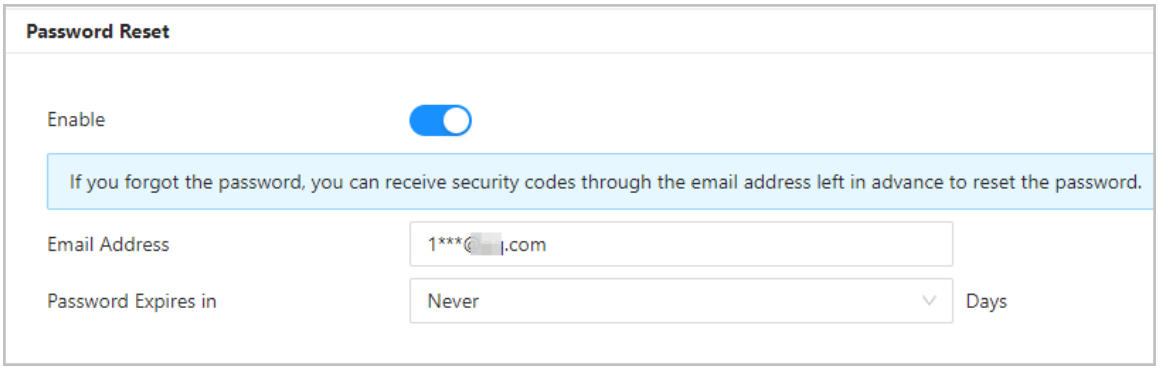
Procedimiento

Paso 1 Seleccionar**Sistema**>**Cuenta**.

Paso 2 Ingrese la dirección de correo electrónico y establezca el tiempo de vencimiento de la

Paso 3 contraseña. Active la función de restablecimiento de contraseña.

Figura 3-65 Restablecer contraseña



Si olvidó la contraseña, puede recibir códigos de seguridad a través de la dirección de correo electrónico vinculada para restablecer la contraseña.

Etapa 4 Hacer clic**Aplicar**.

3.11.1.4 Visualización de usuarios en línea

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

3.11.2 Configurar la hora

Procedimiento

Paso 1 En la página de inicio, seleccione**Sistema**>

Paso 2 **Tiempo**. Configurar la hora de la Plataforma.

Figura 3-66 Configuración de fecha

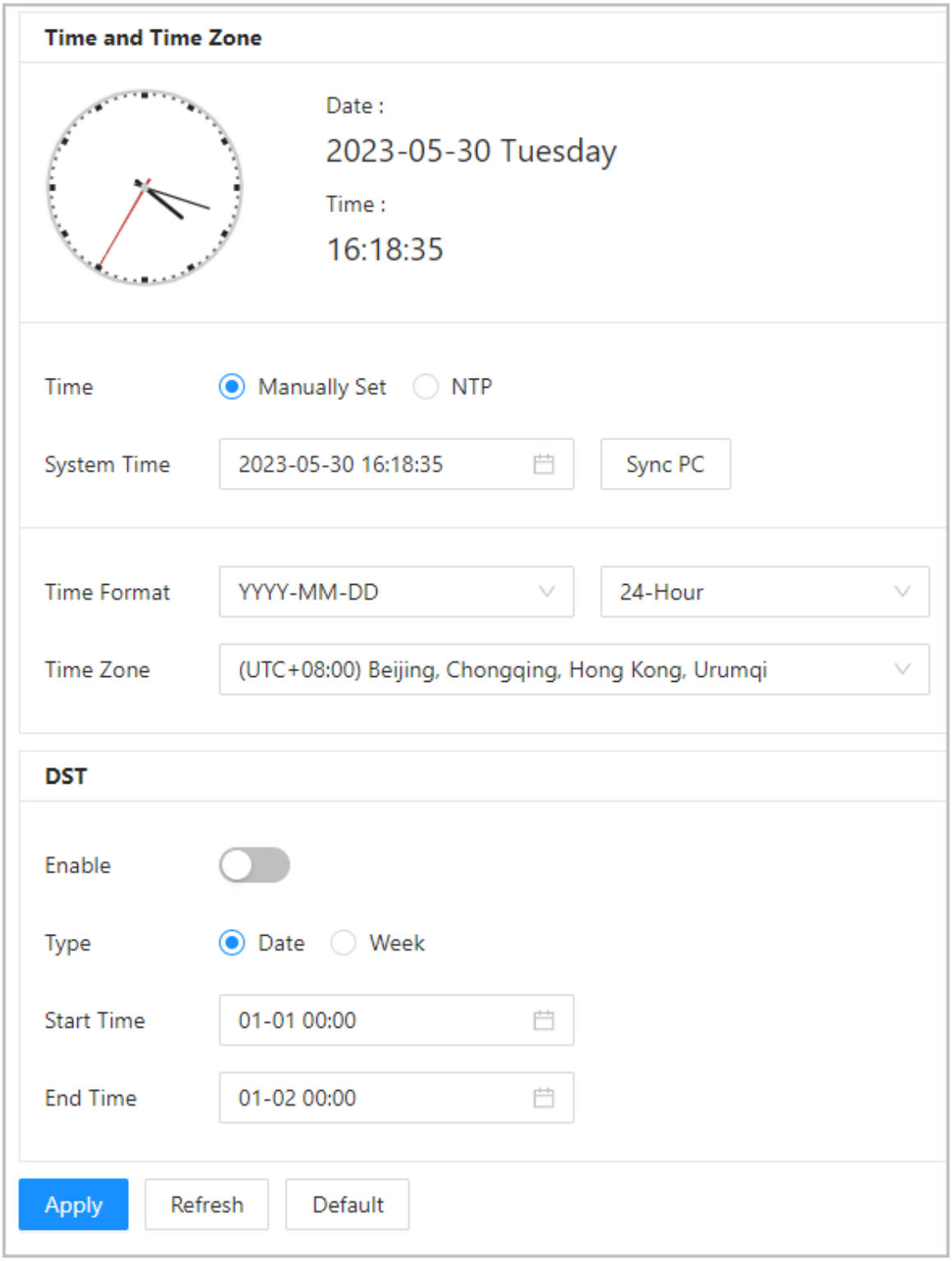


Tabla 3-41 Descripción de la configuración de hora

Parámetro	Descripción
Tiempo	● Configuración manual: ingrese manualmente la hora o puede hacer clic en**Hora de sincronización**para sincronizar la hora con la computadora. ● NTP: el dispositivo sincronizará automáticamente la hora con el servidor NTP. ◇ **Servidor**:Ingrese el dominio del servidor NTP. ◇ **Puerto**:Ingrese el puerto del servidor NTP. ◇ **Intervalo**:Ingrese su hora con el intervalo de sincronización.
Formato de tiempo	Seleccione el formato de hora.
Zona horaria	Ingrese la zona horaria.
horario de verano	1. (Opcional) Habilite el horario de verano. 2. Seleccione**Fecha**o**Semana**desde el**Tipo**. 3. Configure la hora de inicio y finalización del horario de verano.

Paso 3 Hacer clic**Aplicar**.

3.11.3 Configurar los accesos directos

Procedimiento

Paso 1 En la página web, seleccione**Sistema**>**Configuración de acceso directo**.

Paso 2 Configure los parámetros del acceso directo.

Figura 3-67 Configuración de accesos directos

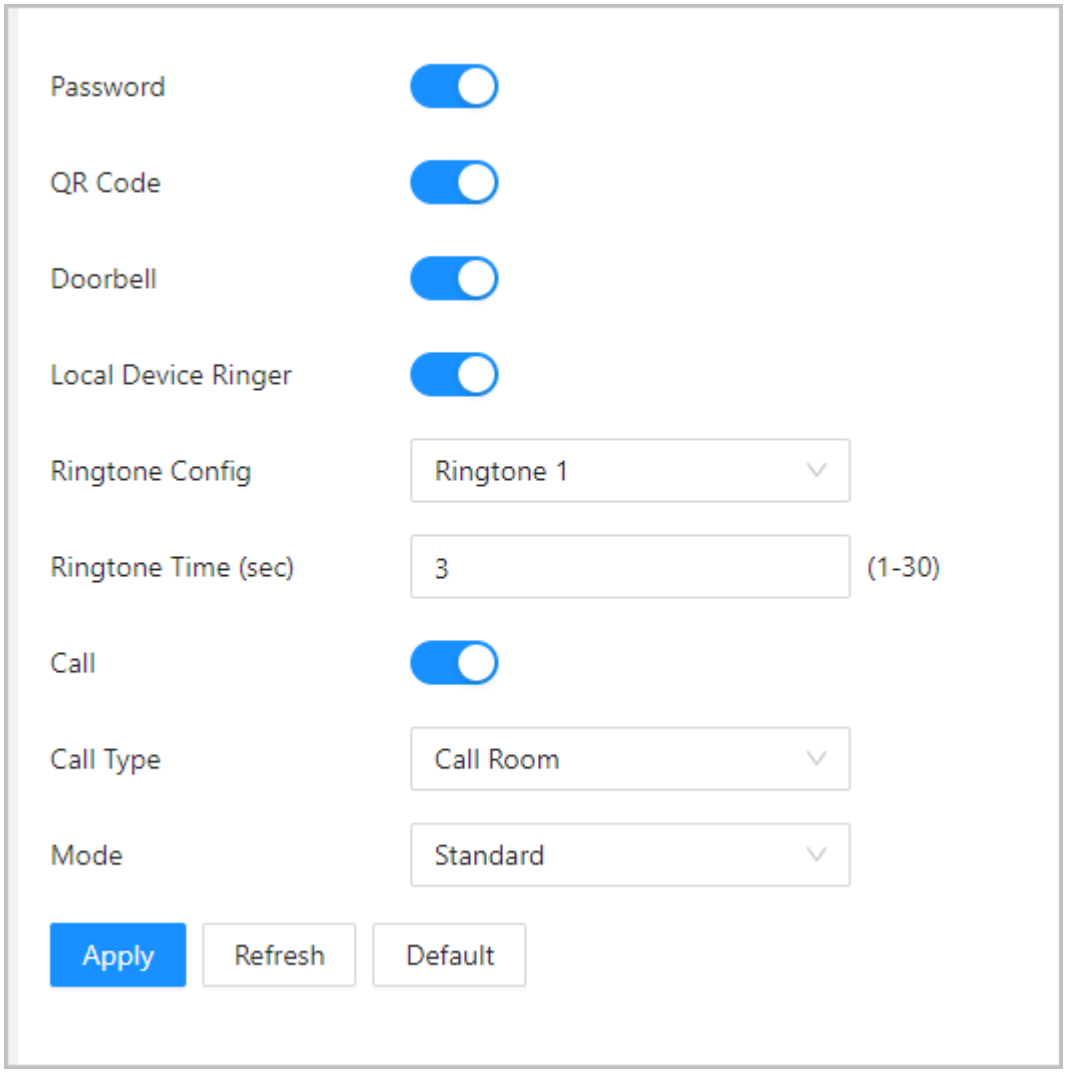


Tabla 3-42 Descripción de parámetros

Parámetro	Descripción
Contraseña	El icono del método de desbloqueo de contraseña se muestra en la pantalla de espera.
Código QR	El icono del código QR se muestra en la pantalla de espera. Esta función no está disponible para dispositivos con un módulo de código QR independiente.
Timbre de la puerta	Después de activar la función de timbre, el icono del timbre aparece en la pantalla de espera. ● Timbre del dispositivo local: toque el ícono de campana en la pantalla de espera y el dispositivo sonará. ● Configuración de tono de llamada: seleccione un tono de llamada ● Tiempo del tono de llamada (seg): establece el tiempo de timbre (1-30 segundos). El valor predeterminado es 3. Esta función solo está disponible en modelos seleccionados.
Llamar	El icono de llamada se muestra en la pantalla de espera.

Parámetro	Descripción
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: ingrese el número de la habitación y luego podrá tocar el ícono de llamada en la pantalla de espera para llamar al número de habitación predefinido. Puede llamar a DMSS solo en este tipo de llamada.

3.12 Personalización

Configure temas y agregue recursos de video o imágenes al Dispositivo.

3.12.1 Agregar recursos

Agregue imágenes o videos para que se muestren en la pantalla de espera del Dispositivo.

Información de contexto

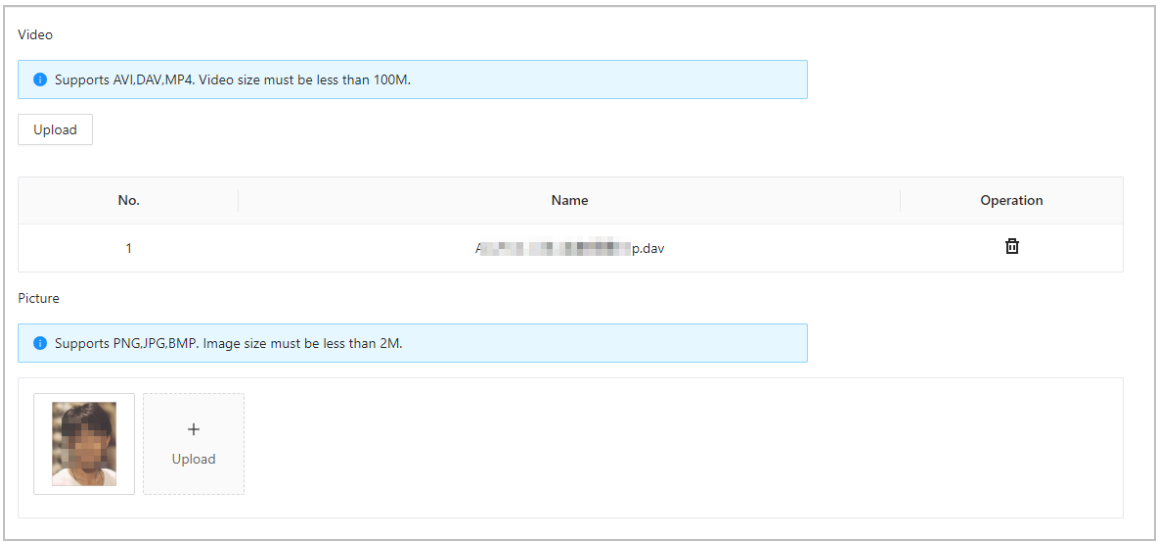
Esta función solo está disponible en modelos seleccionados.

Procedimiento

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

Paso 2 vídeos o imágenes.

Figura 3-68 Agregar videos o imágenes



- Añade vídeos.

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

     El video se carga automáticamente a la plataforma después de la transcodificación.

- Puede cargar hasta 5 archivos de video.
- Soporta DAV, AVI, MP4. El tamaño del vídeo debe ser inferior a 100 M.
- Solo admite la última versión de Firefox y Chrome para cargar archivos de video.

- Añadir imágenes.

  1. Haga clic en .
  2. Seleccione la imagen del local y cárguela.

  Admite PNG, JPG, BMP. El tamaño de la imagen debe ser inferior a 2 M.

Operaciones relacionadas

Hacer clic para eliminar imágenes o videos cargados.

Los vídeos e imágenes en uso no se pueden eliminar.

3.12.2 Configurar temas

Información de contexto

Esta función solo está disponible en modelos seleccionados.

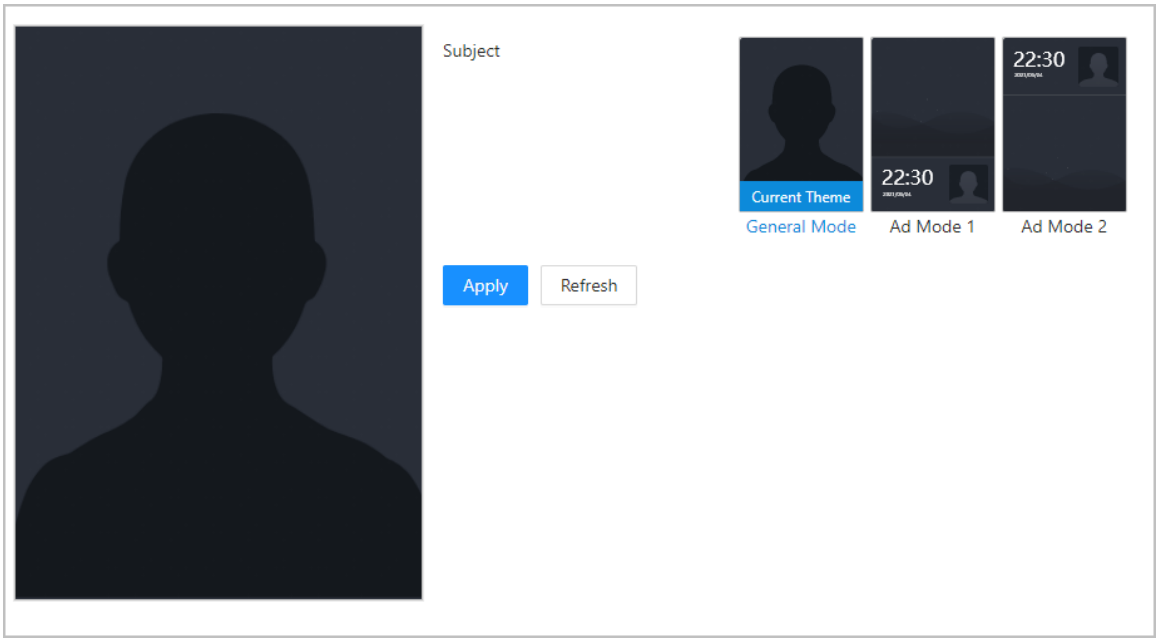
Procedimiento

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

Paso 2 Seleccione el tema.

- Tema general: muestra la imagen de la cara 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 rostros.
- Modo de publicidad 2: el área superior muestra la hora y el cuadro de detección de rostros, y el área inferior muestra los anuncios.

Figura 3-69 Tema

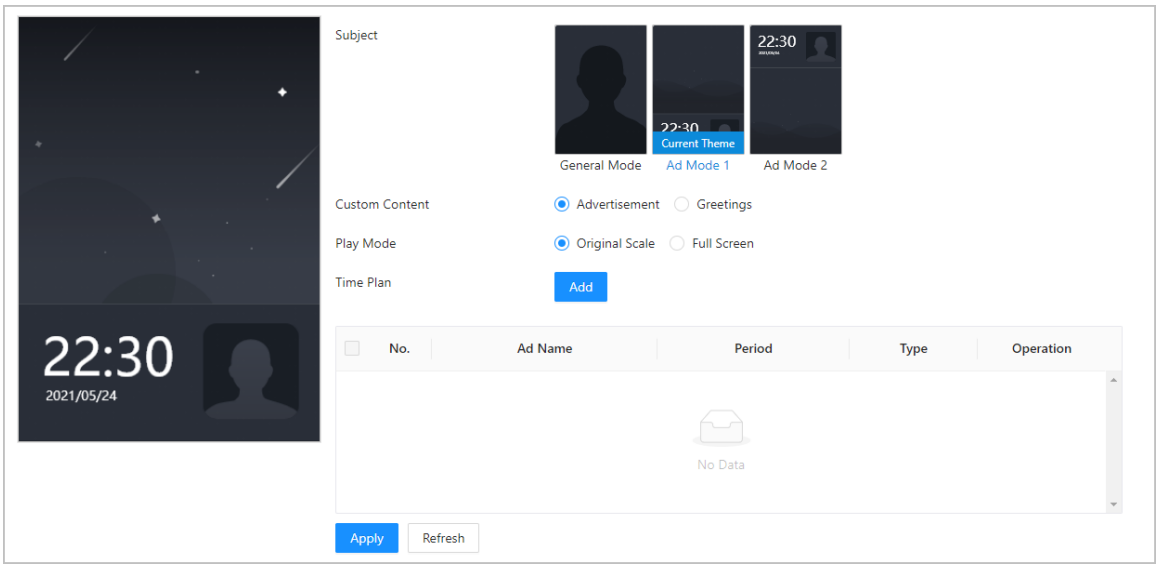


Paso 3 Seleccione el mensaje de voz para una verificación de identidad exitosa.

Etapa 4 Establecer visualización de anuncios.

1. Seleccione Modo de anuncio 1 o Modo de anuncio 2 y luego seleccione**Anuncio**.

Figura 3-70 Modo de publicidad



2. Seleccione el modo de visualización.

- Escala 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.

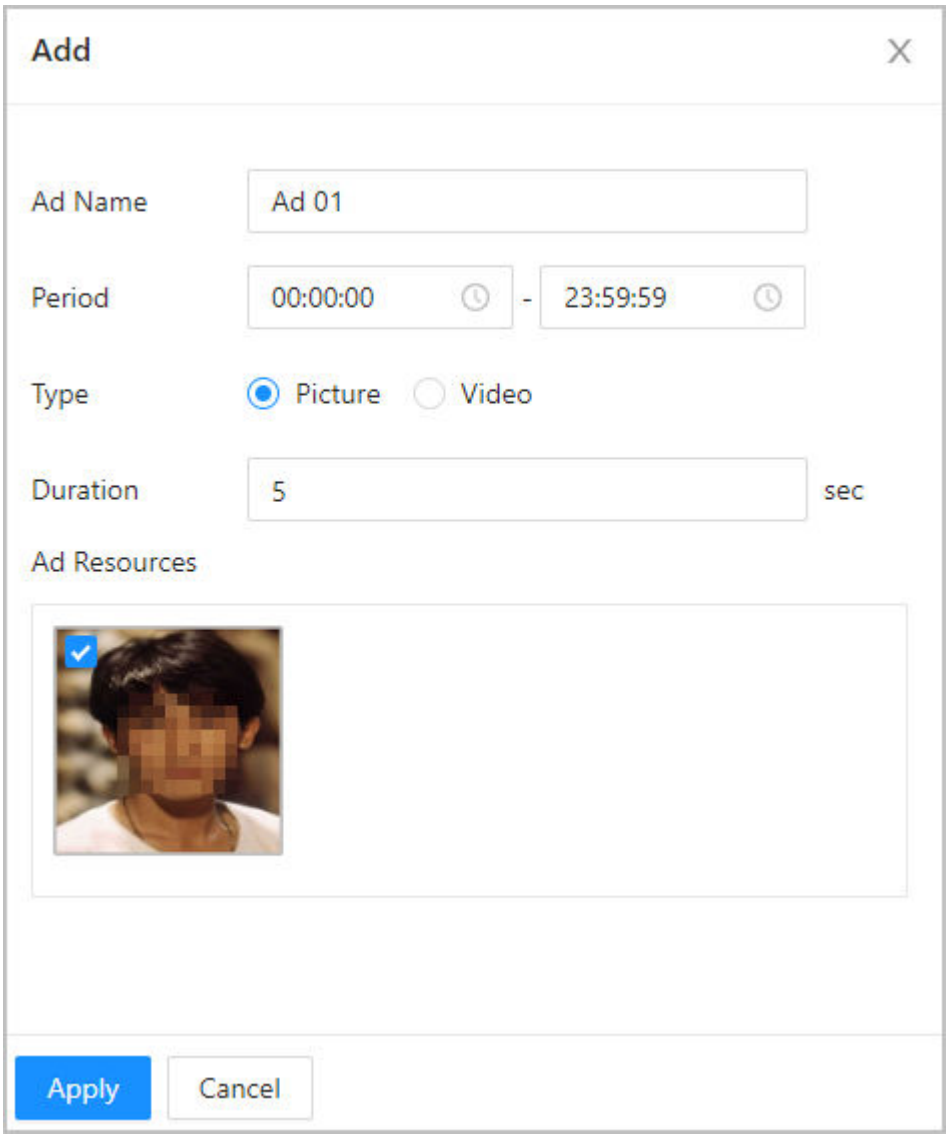
4. Introduzca el nombre del anuncio.

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

6. Introduzca la duración y luego haga clic en**Aplicar**.

Establezca la duración de una sola imagen cuando las imágenes se reproducen en bucle. La duración oscila entre 1 sa 20 sy es de 5 s por defecto.

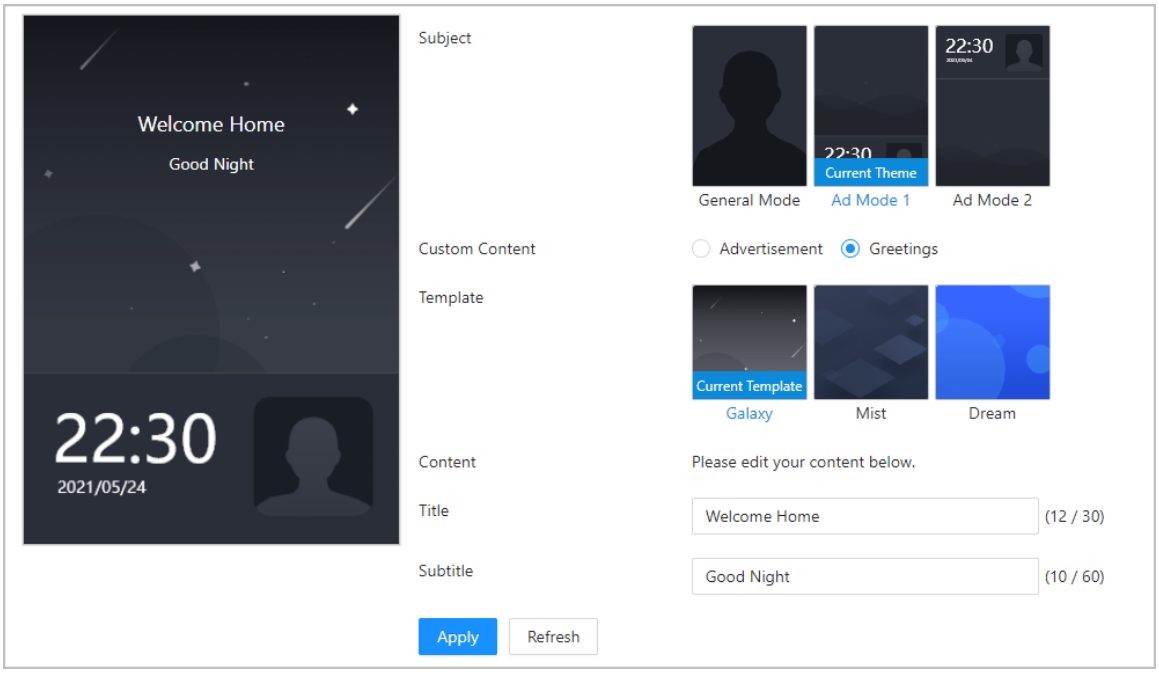
Figura 3-71 Agregar horarios



Paso 5 Configurar saludos.

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

Figura 3-72 Saludos



4. Haga clic**Aplicar**.

3.13 Centro de Gestión

3.13.1 Diagnóstico con un clic

El sistema diagnostica automáticamente las configuraciones y el estado del dispositivo para mejorar su rendimiento.

Procedimiento

Paso 1 En la página de inicio, seleccione**Centro de mantenimiento**>**Diagnóstico con un clic**. Hacer

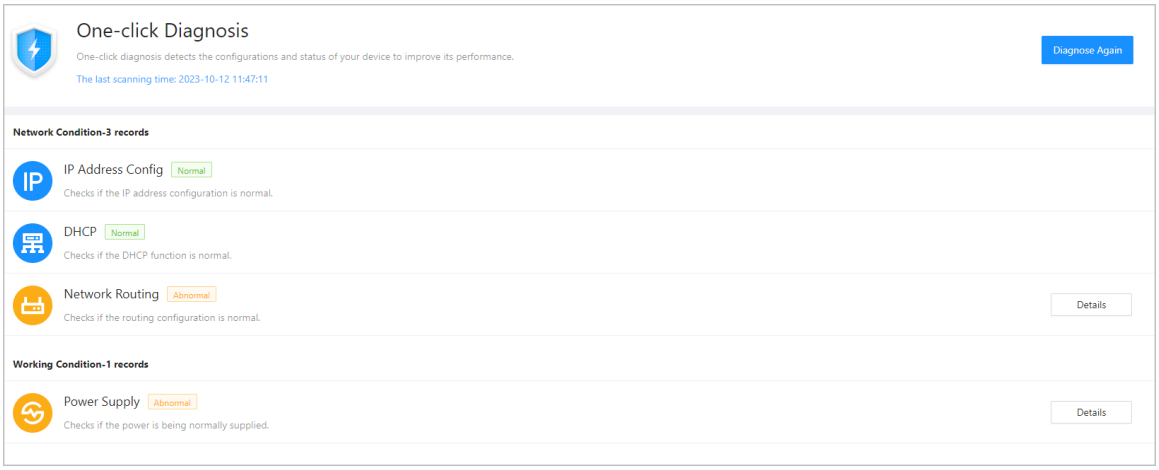
Paso 2 clic**Diagnosticar**.

El sistema diagnostica automáticamente las configuraciones y el estado del dispositivo y muestra los resultados del diagnóstico una vez completado.

Paso 3 (Opcional) Haga clic**Detalles**para ver detalles de elementos anormales.

Puede ignorar la anomalía u optimizarla. También puedes hacer clic**Diagnosticar de nuevo**para volver a realizar el diagnóstico automático.

Figura 3-73 Diagnóstico con un clic



3.13.2 Información del sistema

3.13.2.1 Ver información de la versión

En la página web, seleccione**Sistema**>**Versión**y podrá ver la información de la versión del dispositivo.

3.13.2.2 Ver información legal

En la página de inicio, seleccione**Sistema**>**Información legal**y podrá ver el acuerdo de licencia de software, la política de privacidad y el aviso de software de código abierto.

3.13.3 Capacidad de datos

Puede ver cuántos usuarios, tarjetas e imágenes de rostros puede almacenar el Dispositivo. Inicie

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

3.13.4 Ver registros

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

3.13.4.1 Registros del sistema

Ver y buscar registros del sistema.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Registro**>**Registro**.

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

Operaciones relacionadas

- hacer clic**Exportar**para exportar los registros buscados a su computadora local.

- Hacer clic**Cifrar copia de seguridad de registros**y luego ingrese una contraseña. El archivo exportado se puede abrir solo después de ingresar la contraseña.
- Haga clic para ver los detalles de un registro.

3.13.4.2 Desbloquear registros

Busque registros de desbloqueo y expórtelos.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccionar

Paso 2 **Registro**>**Desbloquear registros**.

Paso 3 Seleccione el rango de tiempo y el tipo, y luego haga clic en**Buscar**.

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

3.13.4.3 Historial de llamadas

Ver registros de llamadas.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccionar

Paso 2 **Registro**>**Historial de llamadas**.

3.13.4.4 Registros de alarmas

Ver registros de alarmas.

Procedimiento

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

Paso 2 **Registro de alarmas**. Seleccione el tipo y el rango de

Paso 3 tiempo. Introduzca el ID de administrador y luego haga clic

Etapa 4 en**Buscar**.

3.13.4.5 Registros de administración

Busque registros de administrador utilizando el ID de administrador.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccionar

Paso 2 **Registro**>**Registro de administrador**.

Paso 3 Introduzca el ID de administrador y luego haga clic en**Buscar**.

Hacer clic**Exportar**para exportar registros de administración.

3.13.4.6 Gestión de USB

Exportar información del usuario desde/hacia USB.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Centro de mantenimiento**>**Registro**>**Gestión de USB**.

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

Paso 3 Seleccione un tipo de datos y luego haga clic en**Importación USB**o**Exportación USB**para importar o exportar los datos.

3.13.5 Gestión de configuración

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

3.13.5.1 Exportación e importación de archivos de configuración

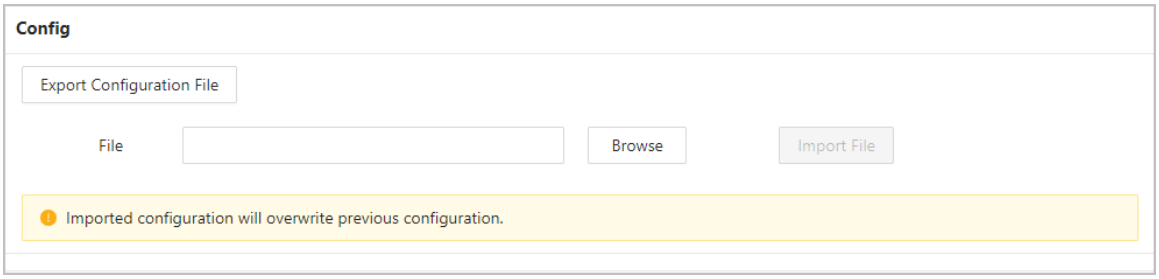
Puede importar y exportar el archivo de configuración del dispositivo. Cuando desee aplicar las mismas configuraciones a varios dispositivos, puede importarles el archivo de configuración.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Sistema**>**configuración**.

Figura 3-74 Gestión de configuración



Paso 3 Exportar o importar archivos de configuración.

- Exporte el archivo de configuración.

  Hacer clic**Exportar archivo de configuración**para descargar el archivo a la computadora local.

  La IP no se exportará.

- Importe el archivo de configuración.

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

     Los archivos de configuración solo se pueden importar a dispositivos que tengan el mismo modelo.

3.13.5.2 Restauración de la configuración predeterminada de fábrica

Procedimiento

Paso 1 Seleccionar**Sistema**>**configuración**.

Restaurando el**Dispositivo**a sus configuraciones predeterminadas resultará en la pérdida de datos. Por favor tenga en cuenta.

Paso 2 Restaure la configuración predeterminada de fábrica si es necesario.

- **Fallas de fábrica**:Restablece todas las configuraciones del Dispositivo y elimina todos los datos.
- **Restaurar a los valores predeterminados (excepto información de usuario y registros)**:Restablece las configuraciones del Dispositivo y elimina todos los datos excepto la información del usuario y los registros.

3.13.6 Mantenimiento

Reinicie periódicamente el Dispositivo durante su tiempo de inactividad para mejorar su rendimiento.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccionar

Paso 2 **Sistema**>**Mantenimiento**. Establezca la hora

Paso 3 y luego haga clic**Aplicar**.

El dispositivo se reiniciará a la hora programada, o puede hacer clic en**Reanudar**para reiniciarlo inmediatamente.

3.13.7 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, y no reinicie ni apague el dispositivo durante la actualización.

3.13.7.1 Actualización de archivos

Procedimiento

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

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

El archivo de actualización debe ser un archivo .bin.

Paso 3 Hacer clic**Actualizar**.

El dispositivo se reiniciará una vez finalizada la actualización.

3.13.7.2 Actualización en línea

Procedimiento

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

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

- Seleccionar**Comprobación automática de actualizaciones**y el dispositivo buscará automáticamente la última actualización de la versión.

- Seleccionar**Verificación manual**, y podrá comprobar inmediatamente si la última versión está disponible.

Paso 3 (Opcional) Haga clic**Actualizar ahora**para actualizar el dispositivo inmediatamente.

3.13.8 Mantenimiento avanzado

Adquiera información del dispositivo y capture paquetes para facilitar que el personal de mantenimiento realice la resolución de problemas.

3.13.8.1 Exportar

Procedimiento

Paso 1 En la página de inicio, seleccione**Centro de mantenimiento**>**Mantenimiento avanzado**>**Exportar**.

Paso 2 Hacer clic**Exportar**para exportar el número de serie, la versión del firmware, los registros de funcionamiento del dispositivo y la información de configuración.

3.13.8.2 Captura de paquetes

Procedimiento

Paso 1 En la página de inicio, seleccione**Centro de mantenimiento**>**Mantenimiento avanzado**>**Captura de paquetes**.

Figura 3-75 Captura de paquetes

Paso 2 Ingrese la dirección IP, haga clic en .

cambios a .

Paso 3 Después de adquirir suficientes datos, haga clic en .

Los paquetes capturados se descargan automáticamente a su computadora local.

3.14 Configuración de seguridad (opcional)

3.14.1 Estado de seguridad

Escanee los módulos de usuarios, servicios y seguridad para verificar el estado de seguridad del Dispositivo.

Información de contexto

- Detección de usuarios y servicios: compruebe si la configuración actual cumple con la recomendación.
- Escaneo de módulos de seguridad: escanea el estado de ejecución de los módulos de seguridad, como la transmisión de audio y video, la protección confiable, la advertencia de seguridad y la defensa contra ataques, sin detectar si están habilitados.

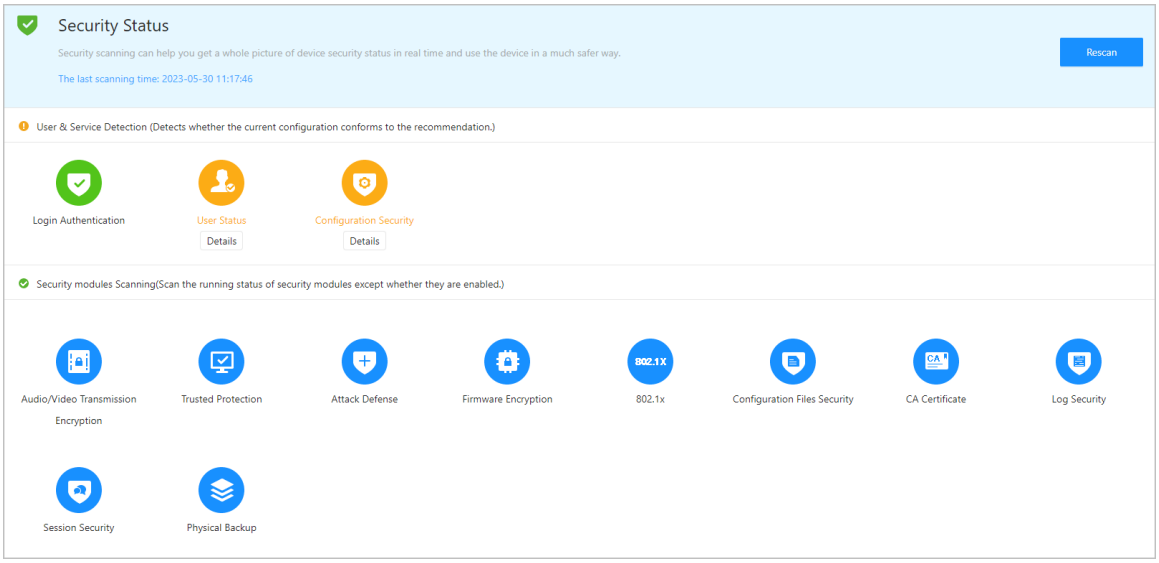
Procedimiento

Paso 1 Seleccionar > **Estado de seguridad**.

Paso 2 Hacer clic**Volver a escanear**para realizar un análisis de seguridad del dispositivo.

Pase el cursor sobre los íconos de los módulos de seguridad para ver su estado de ejecución.

Figura 3-76 Estado de seguridad



Operaciones relacionadas

Después de realizar el escaneo, los resultados se mostrarán en diferentes colores. El amarillo indica que los módulos de seguridad son anormales y el verde indica que los módulos de seguridad son normales.

- Hacer clic**Detalles**para ver los detalles de los resultados del análisis.
- Hacer clic**Ignorar**para ignorar la anomalía y no será escaneada. La anomalía que se ignoró se resaltará en gris.
- Hacer clic**Optimizar**para solucionar la anomalía.

3.14.2 Configurar HTTPS

Cree un certificado o cargue un certificado autenticado y luego podrá iniciar sesión en la página web a través de HTTPS en su computadora. HTTPS protege la comunicación a través de una red informática.

Procedimiento

Paso 1 Seleccionar > **Servicio del sistema**>**HTTPS**.

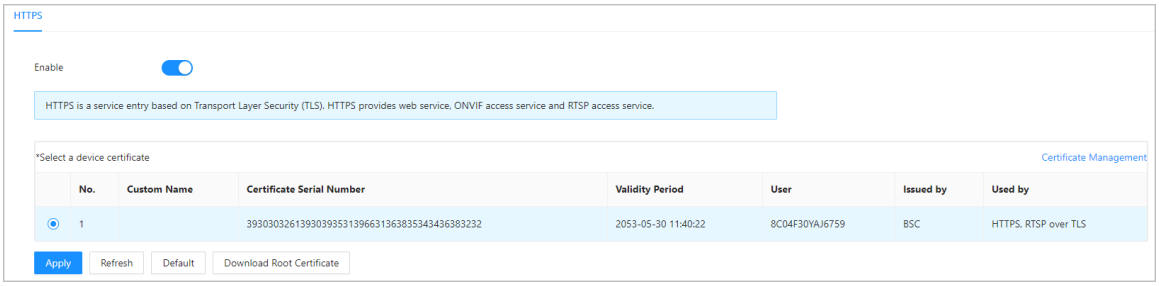
Paso 2 Active el servicio HTTPS.

Si activa la compatibilidad con TLS v1.1 y versiones anteriores, pueden ocurrir riesgos de seguridad. Por favor tenga en cuenta.

Paso 3 Seleccione el certificado.

Si no hay certificados en la lista, haga clic en**Gestión de certificados**para cargar un certificado.

Figura 3-77 HTTPS



Etapa 4 Hacer clic**Aplicar**.

Ingrese “https://*dirección IP.httpsdeporte*" en un navegador web. Si el certificado está instalado, puede iniciar sesión en la página web correctamente. De lo contrario, la página web mostrará el certificado como incorrecto o no confiable.

3.14.3 Defensa de ataque

3.14.3.1 Configuración del cortafuegos

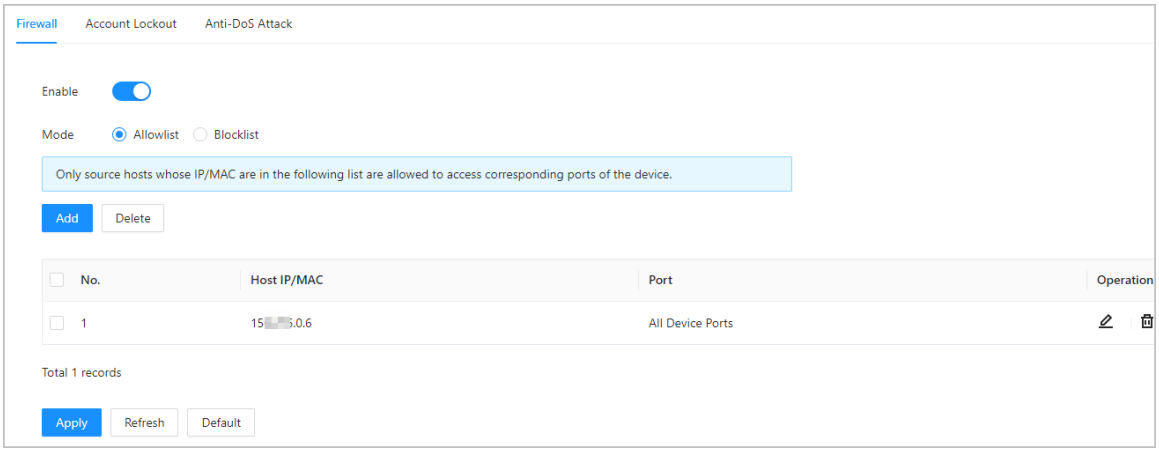
Configure el firewall para limitar el acceso al dispositivo.

Procedimiento

Paso 1 Seleccionar > **Defensa de ataque**>**Cortafuegos**.

Paso 2 Hacer clic para habilitar la función de firewall.

Figura 3-78 Cortafuegos

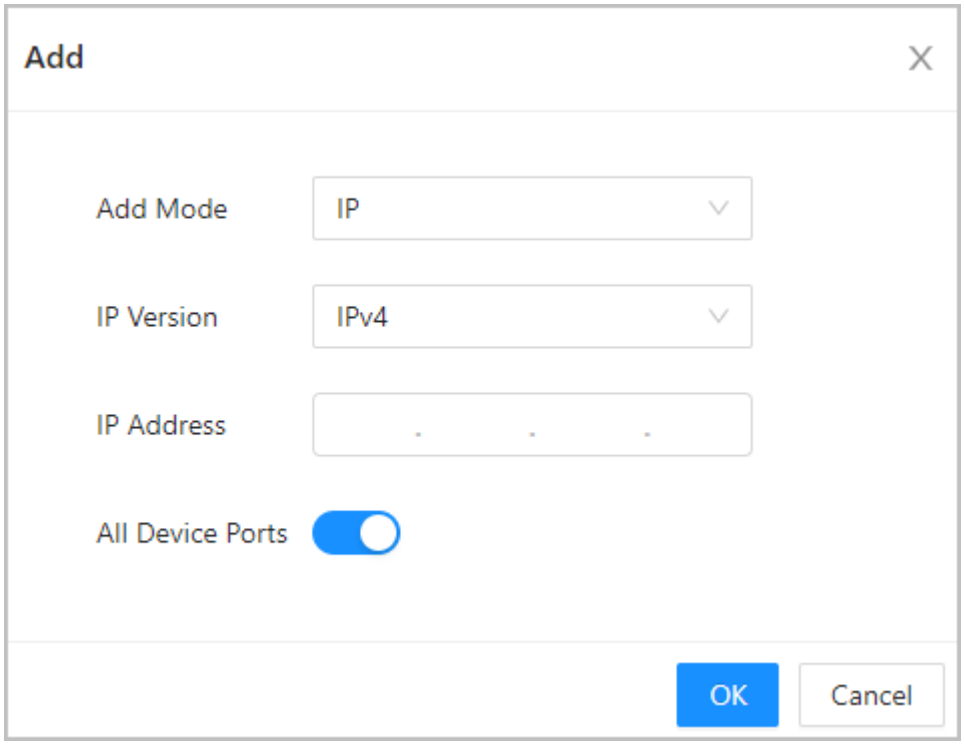


Paso 3 Seleccione el modo:**Lista de permitidos**y**Lista de bloqueos**.

- **Lista de permitidos**:Solo las direcciones IP/MAC en la lista permitida pueden acceder al dispositivo.
- **Lista de bloqueos**:Las direcciones IP/MAC en la lista de bloqueo no pueden acceder al dispositivo.

Etapa 4 Hacer clic**Agregar**para ingresar la información de IP.

Figura 3-79 Agregar información de IP



Paso 5 Hacer clicDE ACUERDO.

Operaciones relacionadas

- Hacer clic para editar la información de IP.
- Hacer clic para eliminar la dirección IP.

3.14.3.2 Configurar el bloqueo de cuenta

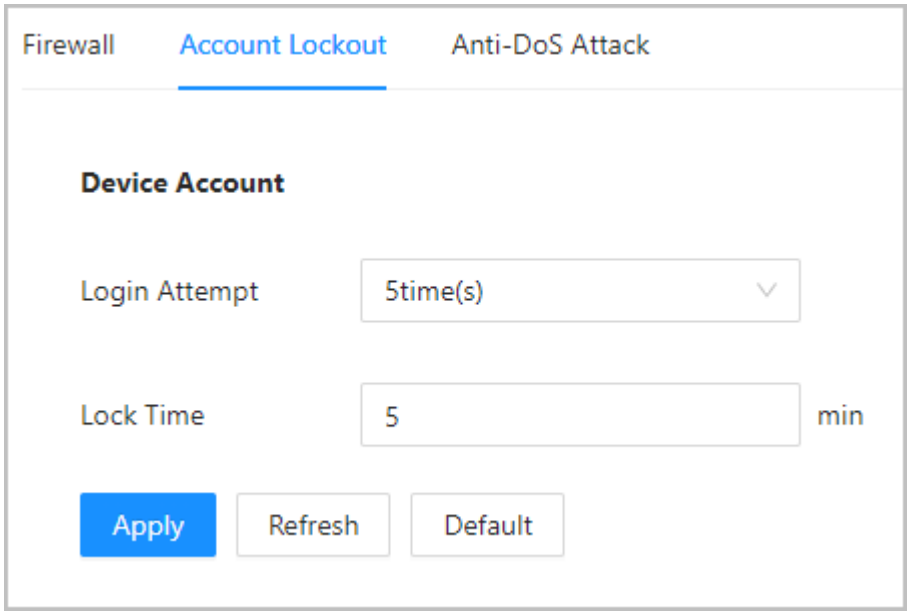
Si se ingresa la contraseña incorrecta una cantidad determinada de veces, la cuenta se bloqueará.

Procedimiento

Paso 1 Seleccionar > **Defensa de ataque**>**Bloqueo de cuenta**.

Paso 2 Ingrese la cantidad de intentos de inicio de sesión y el tiempo durante el cual la cuenta de administrador y el usuario ONVIF estarán bloqueados.

Figura 3-80 Bloqueo de cuenta



- Intento de inicio de sesión: el límite de intentos de inicio de sesión. Si se ingresa la contraseña incorrecta una cantidad determinada de veces, la cuenta se bloqueará.
- Tiempo de bloqueo: el período durante el cual no puede iniciar sesión después de que la cuenta esté bloqueada. Hacer

Paso 3 clic**Aplicar**.

3.14.3.3 Configuración del ataque Anti-DoS

Puedes habilitar**Defensa contra ataques de inundación SYN**y**Defensa contra ataques de inundaciones ICMP**para defender el Dispositivo contra ataques Dos.

Procedimiento

Paso 1 Seleccionar > **Defensa de ataque**>**Ataque anti-DoS**.

Paso 2 Encender**Defensa contra ataques de inundación SYN**o**Defensa contra ataques de inundaciones ICMP**para proteger el dispositivo contra ataques Dos.

Figura 3-81 Ataque Anti-DoS

Paso 3 Hacer clic**Aplicar**.

3.14.4 Instalación del certificado del dispositivo

Cree un certificado o cargue un certificado autenticado y luego podrá iniciar sesión a través de HTTPS en su computadora.

3.14.4.1 Creación de certificado

Cree un certificado para el dispositivo.

Procedimiento

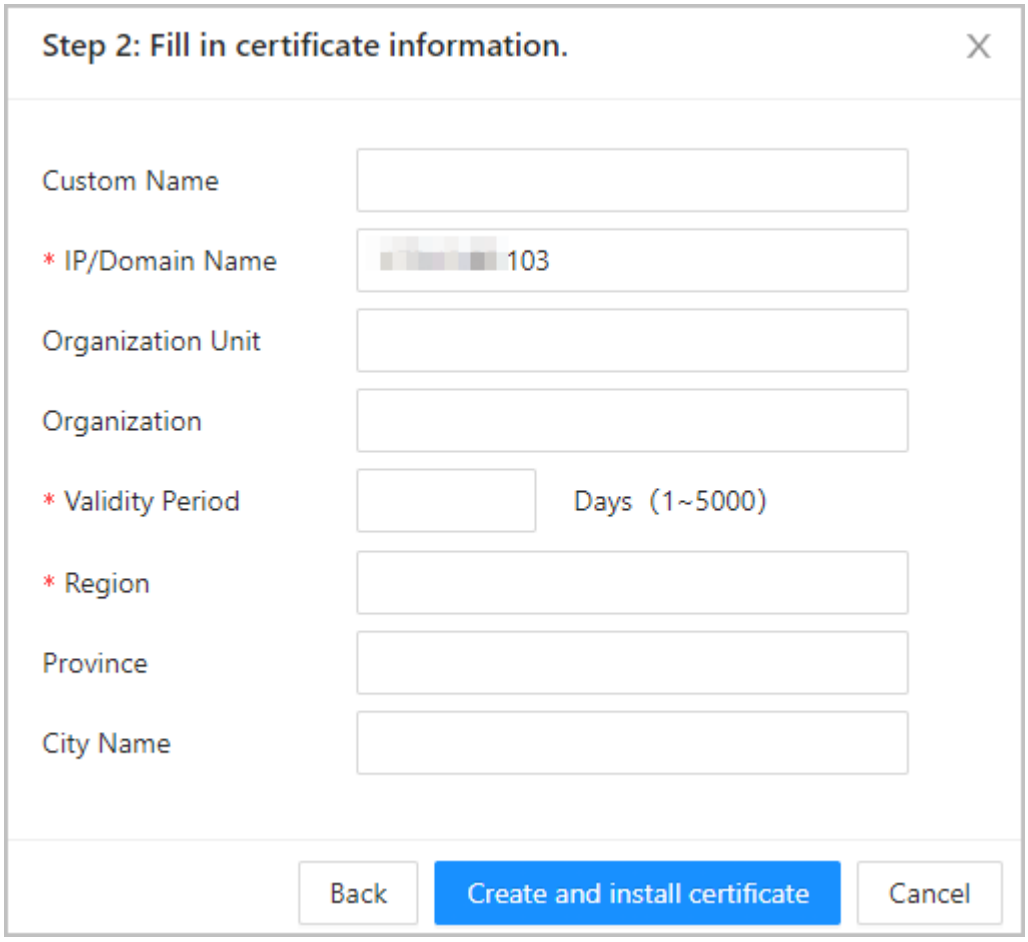
Paso 1 Seleccionar > **Certificado de CA**>**Certificado de dispositivo**.

Paso 2 Seleccionar**Instalar certificado de dispositivo**.

Paso 3 Seleccionar**Crear certificado**,y haga clic**Próximo**.

Etapa 4 Ingrese la información del certificado.

Figura 3-82 Información del certificado



El nombre de la región no puede exceder los 2 caracteres. Recomendamos ingresar la abreviatura del nombre de la región.

Paso 5 Hacer clic**Crear e instalar certificado**.

El certificado recién instalado se muestra en la**Certificado de dispositivo**página después de que el certificado se haya instalado correctamente.

Operaciones relacionadas

- Hacer clic**Ingrese al modo de edición**sobre el**Certificado de dispositivo**página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

3.14.4.2 Solicitud e importación de certificado de CA

Importe el certificado de CA de terceros al dispositivo.

Procedimiento

Paso 1 Seleccionar > **Certificado de CA**>**Certificado de dispositivo**.

Paso 2 Hacer clic**Instalar certificado de dispositivo**.

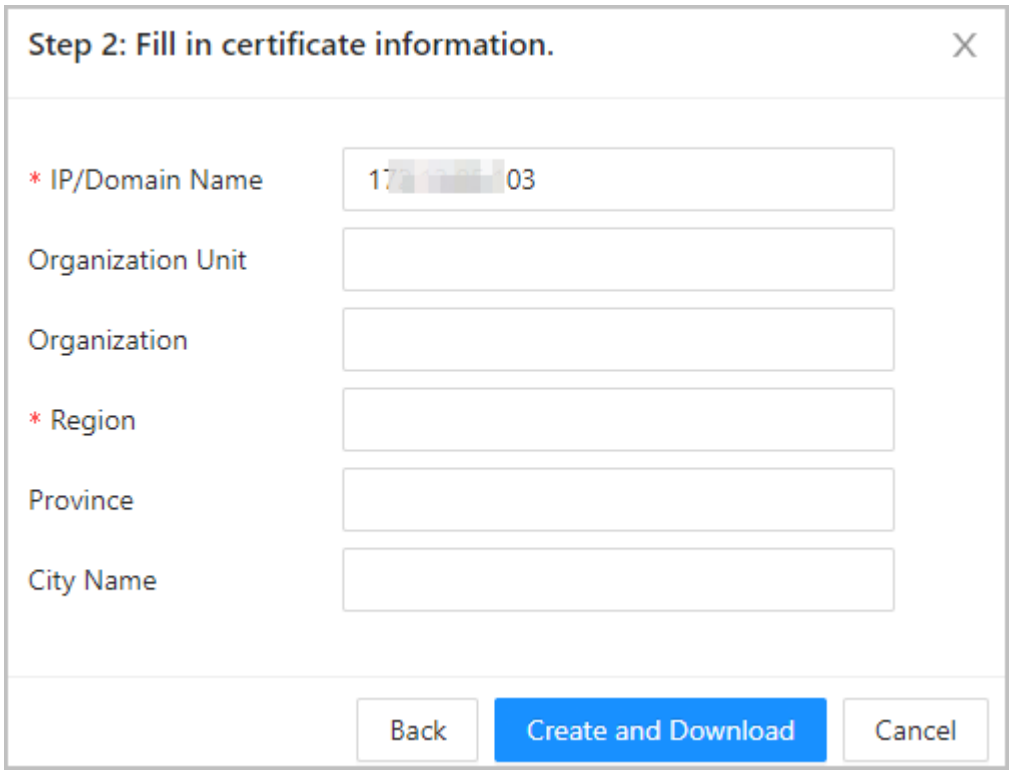
Paso 3 Seleccionar**Solicite certificado de CA e importación (recomendado)**,y haga clic**Próximo**.

Etapa 4 Ingrese la información del certificado.

- IP/Nombre de dominio: la dirección IP o nombre de dominio del Dispositivo.

- Región: el nombre de la región no debe exceder los 3 caracteres. Le recomendamos ingresar la abreviatura del nombre de la región.

Figura 3-83 Información del certificado (2)



Paso 5 Hacer clic**Crear y descargar**.

Guarde el archivo de solicitud en su computadora.

Paso 6 Solicite el certificado a una autoridad de CA de terceros mediante el archivo de solicitud.

Paso 7 Importe el certificado de CA firmado.

1. Guarde el certificado de CA en su computadora.
2. Haga clic**Instalación del certificado del dispositivo**.
3. Haga clic**Navegar**para seleccionar el certificado de CA.
4. Haga clic**Importar e instalar**.

El certificado recién instalado se muestra en la**Certificado de dispositivo**página después de que el certificado se haya instalado correctamente.

- Hacer clic**Recrear**para crear el archivo de solicitud nuevamente.
- Hacer clic**Importar más tarde**importar el certificado en otro momento.

Operaciones relacionadas

- Hacer clic**Ingrese al modo de edición**sobre el**Certificado de dispositivo**página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

3.14.4.3 Instalación del certificado existente

Si ya tiene un certificado y un archivo de clave privada, importe el certificado y el archivo de clave privada.

Procedimiento

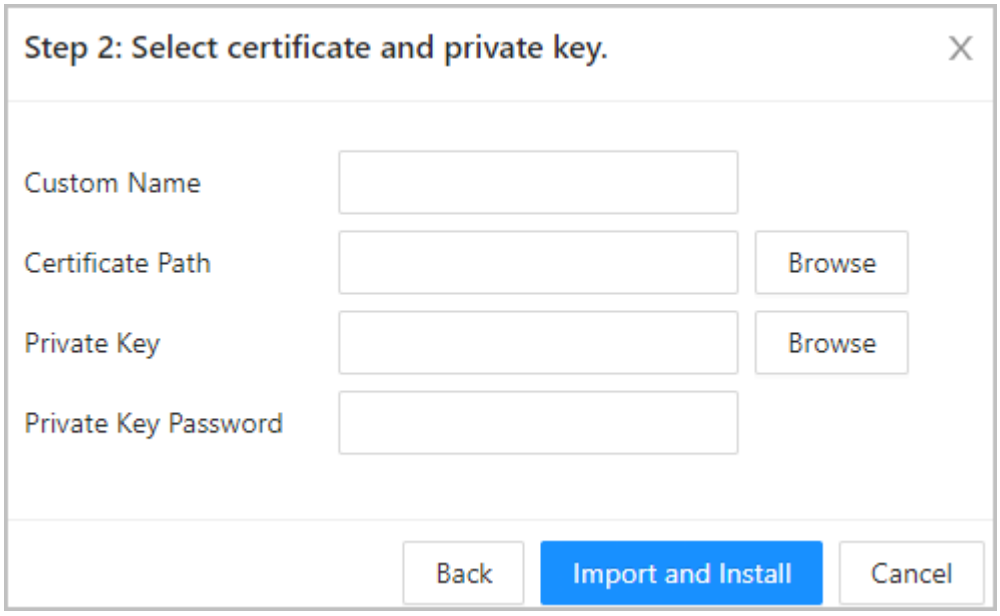
Paso 1 Seleccionar**Seguridad**>**Certificado de CA**>**Certificado de dispositivo**.

Paso 2 Hacer clic**Instalar certificado de dispositivo**.

Paso 3 Seleccionar**Instalar certificado existente**,y haga clic**Próximo**.

Etapa 4 Hacer clic**Navegar**para seleccionar el certificado y el archivo de clave privada, e ingrese la contraseña de clave privada.

Figura 3-84 Certificado y clave privada



Paso 5 Hacer clic**Importar e instalar**.

El certificado recién instalado se muestra en la**Certificado de dispositivo**página después de que el certificado se haya instalado correctamente.

Operaciones relacionadas

- Hacer clic**Ingrese al modo de edición**sobre el**Certificado de dispositivo**página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

3.14.5 Instalación del certificado de CA de confianza

Un certificado de CA confiable es un certificado digital que se utiliza para validar las identidades de sitios web y servidores. Por ejemplo, cuando se utiliza el protocolo 802.1x, se requiere el certificado de CA para los conmutadores para autenticar su identidad.

Información de contexto

802.1X es un protocolo de autenticación de red que abre puertos para el acceso a la red cuando una organización autentica la identidad de un usuario y le autoriza el acceso a la red.

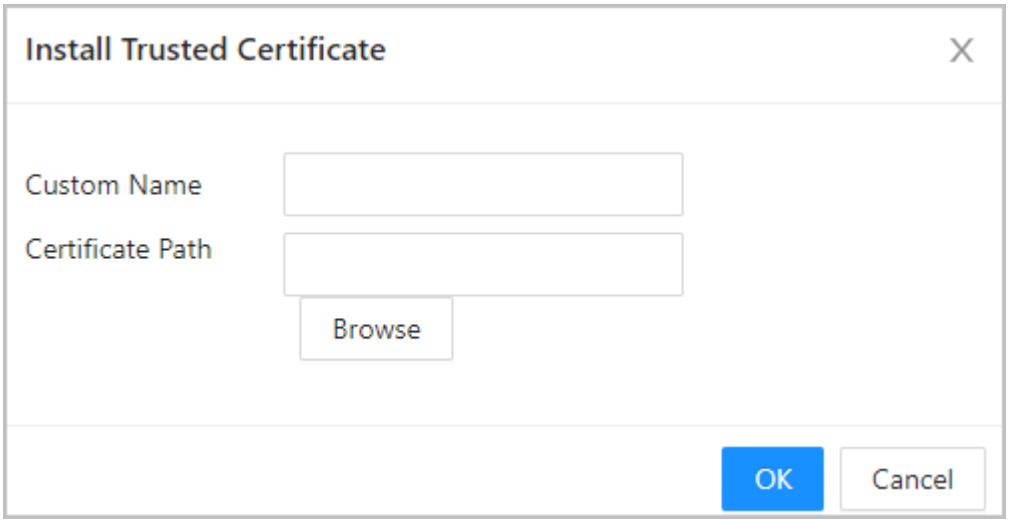
Procedimiento

Paso 1 Seleccionar > **Certificado de CA**>**Certificados de CA confiables**.

Paso 2 Seleccionar**Instalar certificado de confianza**.

Paso 3 Hacer clic**Navegar**para seleccionar el certificado de confianza.

Figura 3-85 Instalar el certificado de confianza



Etapa 4 Hacer clic**DE ACUERDO**.

El certificado recién instalado se muestra en la**Certificados de CA confiables**página después de que el certificado se haya instalado correctamente.

Operaciones relacionadas

- Hacer clic**Ingrese al modo de edición**sobre el**Certificado de dispositivo**página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

3.14.6 Cifrado de datos

Procedimiento

Paso 1 Seleccionar > **Cifrado de datos**.

Paso 2 Configure los parámetros.

Figura 3-86 Cifrado de datos

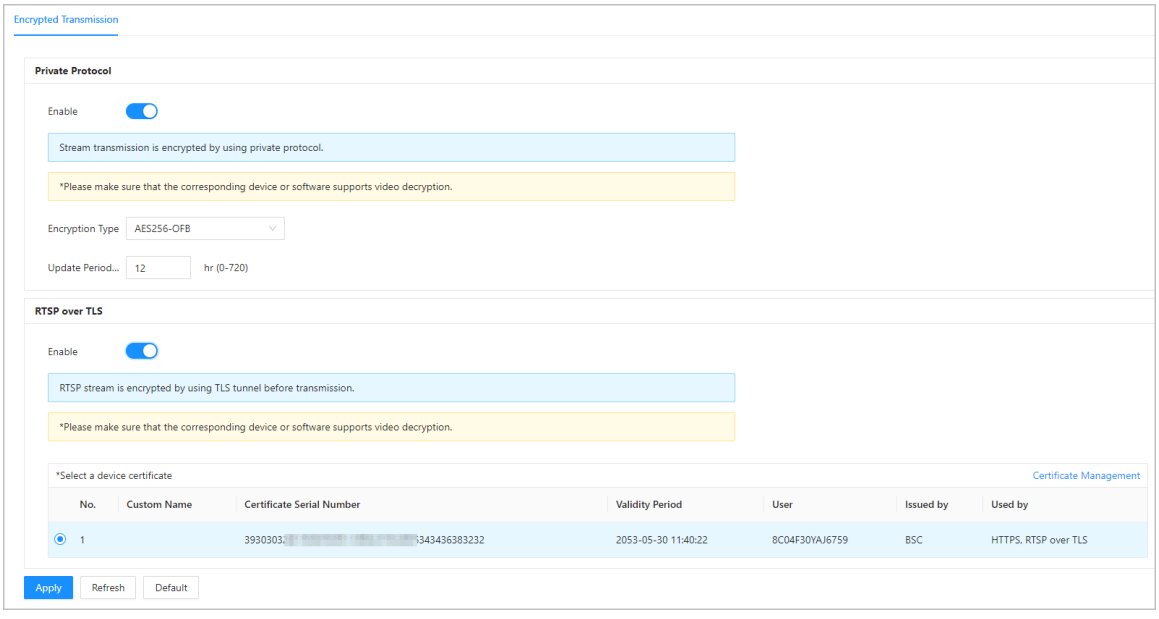


Tabla 3-43 Descripción del cifrado de datos

	Parámetro	Descripción
Protocolo privado	Permitir	Las transmisiones se cifran durante la transmisión a través de un protocolo privado.
	Tipo de cifrado	Mantenlo como predeterminado.
	Período de actualización de la clave secreta	Va desde 0 h -720 h. 0 significa nunca actualizar la clave secreta.
RTSP sobre TLS	Permitir	La transmisión RTSP se cifra durante la transmisión a través del túnel TLS.
	Gestión de certificados	Crear o importar certificado. Para obtener más información, consulte "3.14.4 Instalación del certificado del dispositivo". Los certificados instalados se muestran en la lista.

3.14.7 Advertencia de seguridad

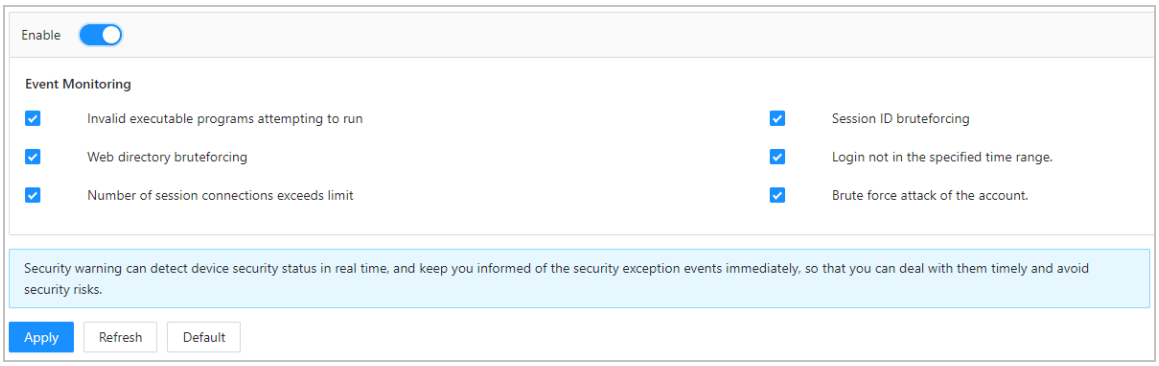
Procedimiento

Paso 1 Seleccionar > **Advertencia de seguridad**.

Paso 2 Habilite la función de advertencia de seguridad.

Paso 3 Seleccione los elementos de seguimiento.

Figura 3-87 Advertencia de seguridad



Etapa 4 Hacer clic**Aplicar**.

3.14.8 Autenticación de seguridad

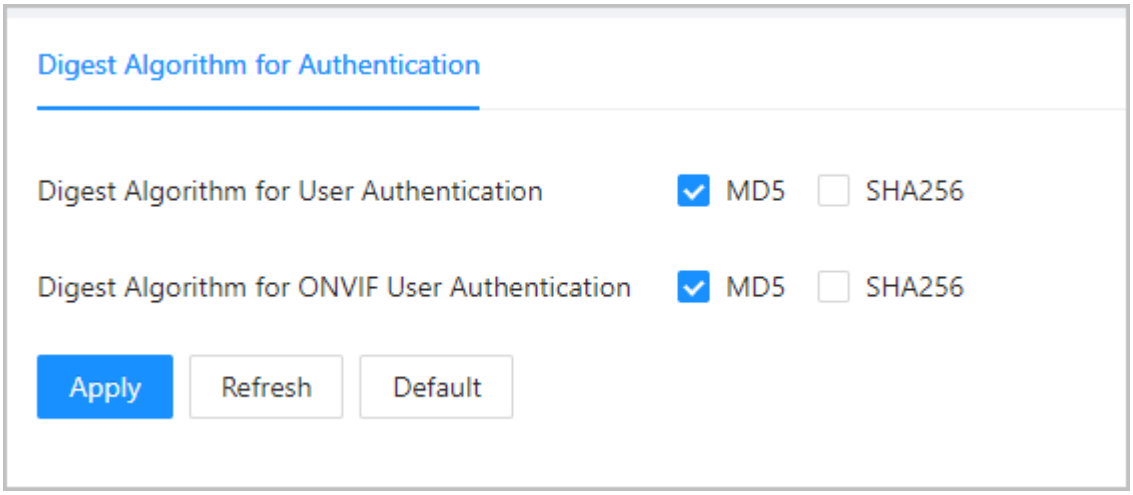
Procedimiento

Paso 1 Seleccionar**Seguridad**>**Autenticación de seguridad**.

Paso 2 Seleccione un algoritmo de resumen de mensajes.

Paso 3 Hacer clic**Aplicar**.

Figura 3-88 Autenticación de seguridad



4 Configuración inteligente de PSS Lite

Esta sección presenta cómo administrar y configurar el dispositivo a través de Smart PSS Lite. Para obtener más información, consulte el manual del usuario de Smart PSS Lite.

4.1 Instalación e inicio de sesión

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

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 contraseña y preguntas de seguridad.

Establezca la contraseña para el primer uso y luego configure preguntas de seguridad para restablecer su contraseña cuando la haya olvidado.

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

4.2 Agregar dispositivos

Debe agregar el dispositivo a Smart PSS Lite. Puedes agregarlos en lotes o individualmente.

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 Sobre el**Administrador de dispositivos**página, haga clic

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

Figura 4-1 Agregar dispositivos

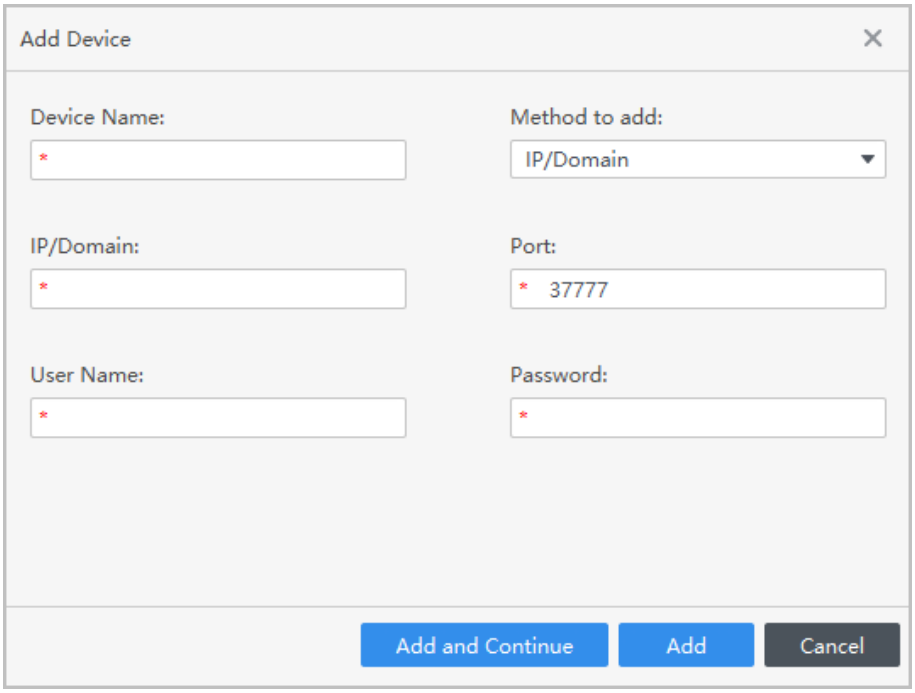


Tabla 4-1 Parámetros de adición de IP

Parámetro	Descripción
Nombre del dispositivo	Le recomendamos nombrar los dispositivos con el área de monitoreo para una fácil identificación.
Método para agregar	Seleccionar**IP/Dominio**. ● IP/Dominio: Introduzca 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 es 37777 de forma predeterminada. El número de puerto real puede diferir según los diferentes modelos.
Nombre de usuario	Ingrese el nombre de usuario del dispositivo.
Contraseña	Ingrese 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 agregar dispositivos mediante la búsqueda automática cuando necesite agregar dispositivos en lotes dentro del mismo segmento de red, o cuando se conozca el segmento de red pero no se conozcan 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

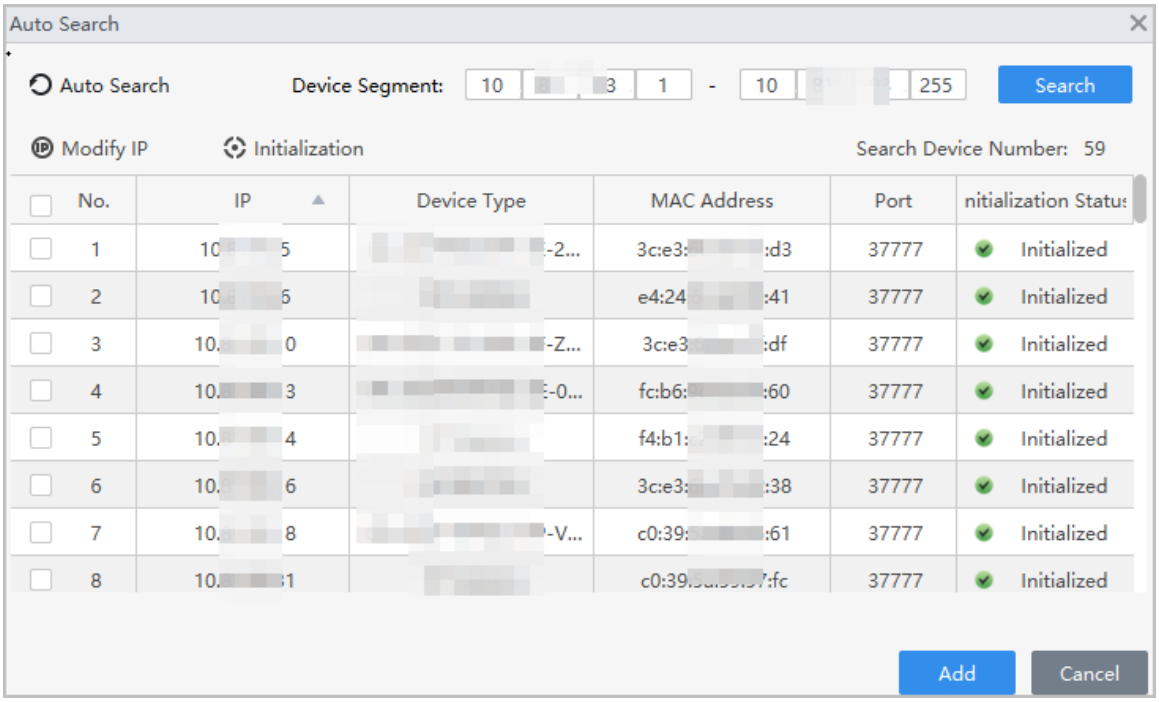
Paso 1 Sobre el**Administrador de dispositivos**página, haga clic**Auto búsqueda**.

Paso 2 Seleccione un método de búsqueda.

- Búsqueda automática: Ingrese el nombre de usuario y la contraseña del dispositivo. El sistema buscará automáticamente dispositivos que estén en la misma red que su computadora.
- Búsqueda de segmento de dispositivo: 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 Buscar dispositivos



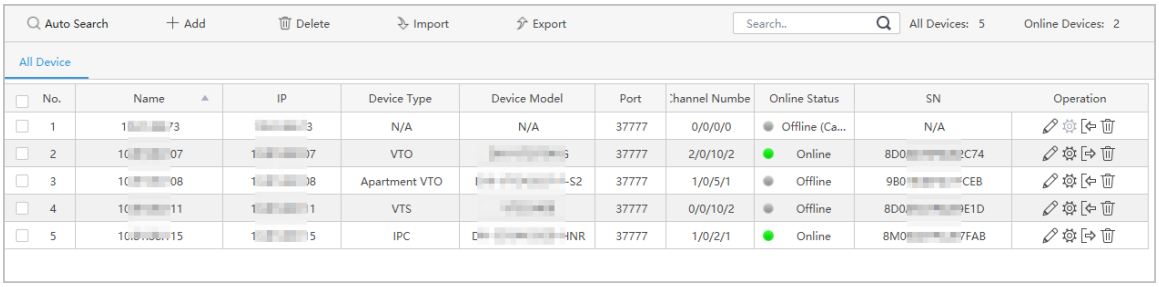
Paso 3 Haga clic en dispositivos y luego haga clic en**Agregar**.

Etapa 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 agregados



4.3 Gestión de usuarios

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

4.3.1 Configurar el tipo de tarjeta

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

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

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

Asegúrese de que el tipo de tarjeta sea el mismo que la tarjeta realmente asignada; de lo contrario, el número de la tarjeta no podrá leerse.

Etapa 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**. Ingrese la

Paso 2 información básica del personal.

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

- El número de tarjeta se puede leer automáticamente o completarse manualmente. Para leer automáticamente el número de tarjeta, seleccione el lector de tarjetas al lado de**Número de tarjeta**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.

- Configurar la clave

  Hacer clic**Agregar**para agregar la contraseña.

- Configurar tarjeta

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

  b. Añade tarjetas.

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

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

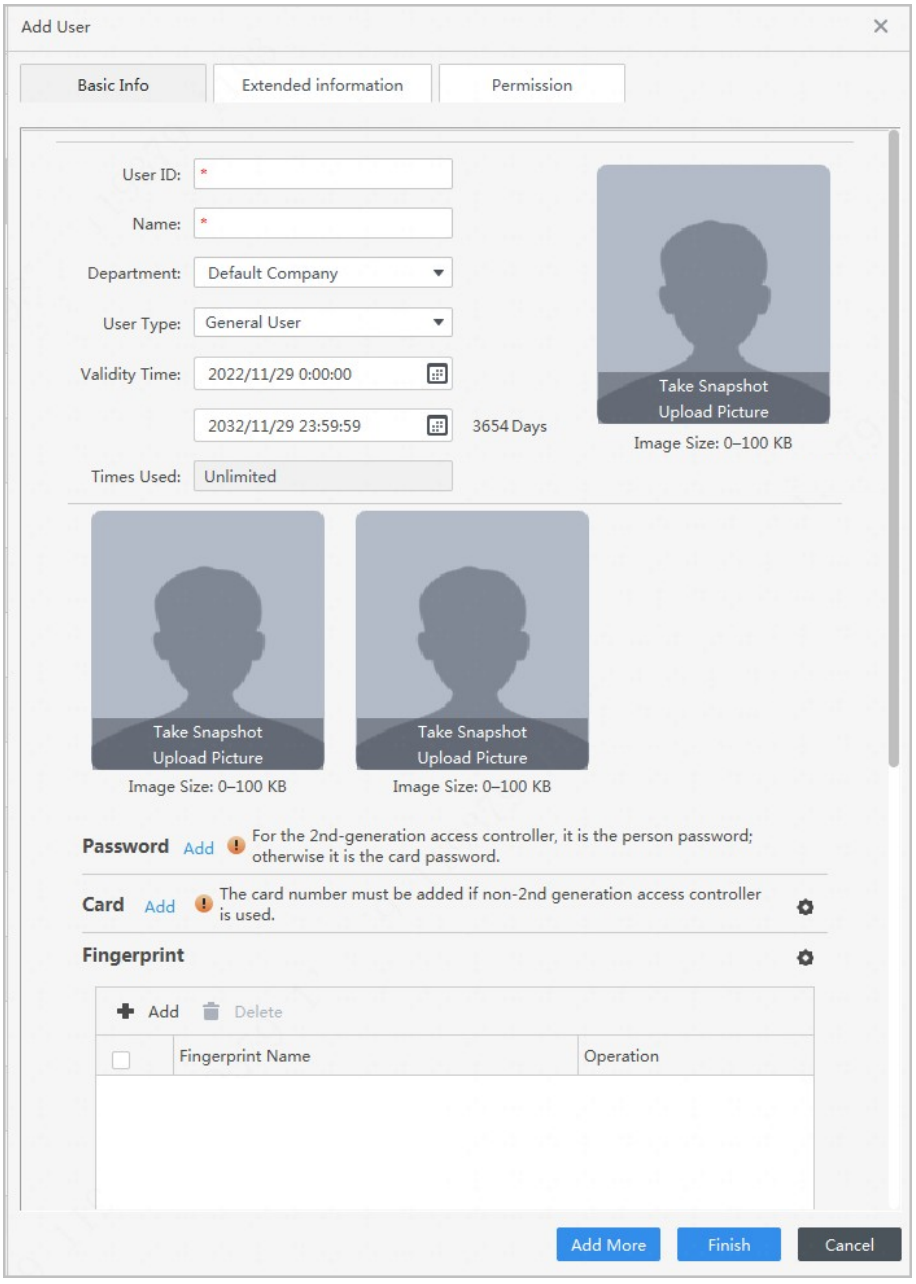
  Solo el número de tarjeta de 8 dígitos en modo hexadecimal puede mostrar el código QR de la tarjeta.

- Configurar huella digital

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

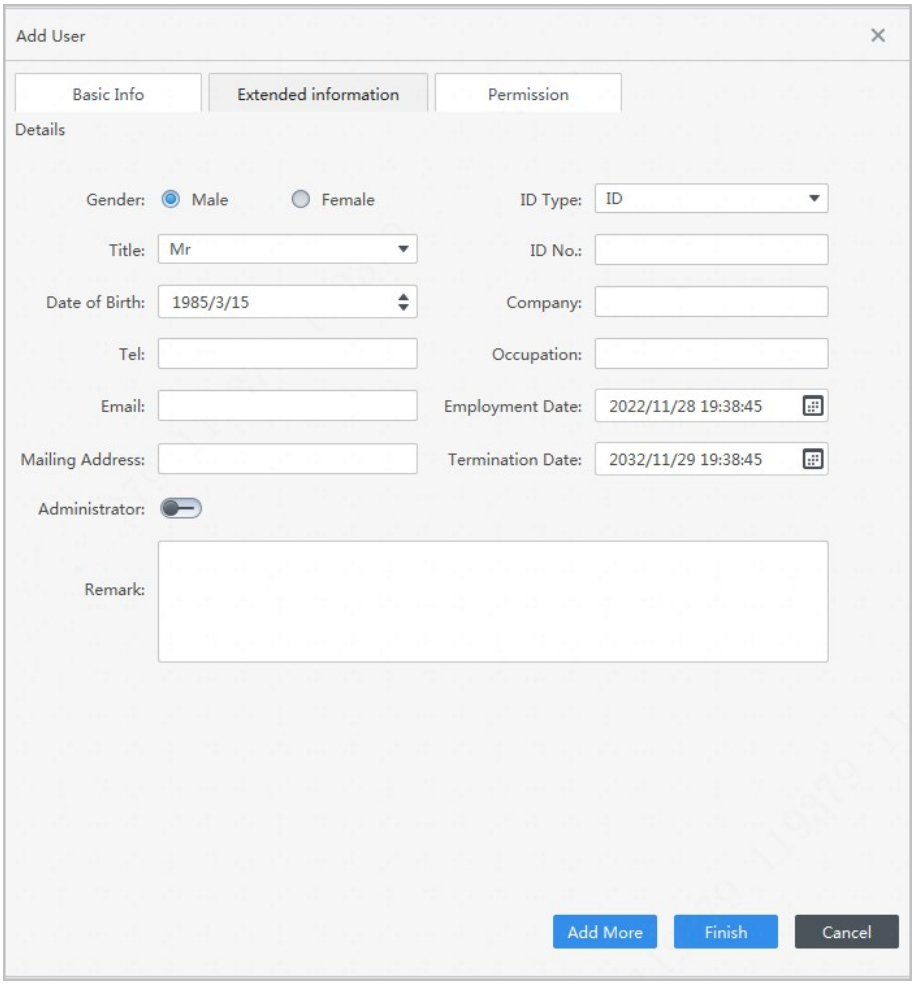
b. Agregar huella digital. Seleccionar**Agregar**>**Agregar huella digital**y luego presione con el dedo el escáner tres veces seguidas.

Figura 4-4 Agregar información básica



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

Figura 4-5 Agregar información extendida



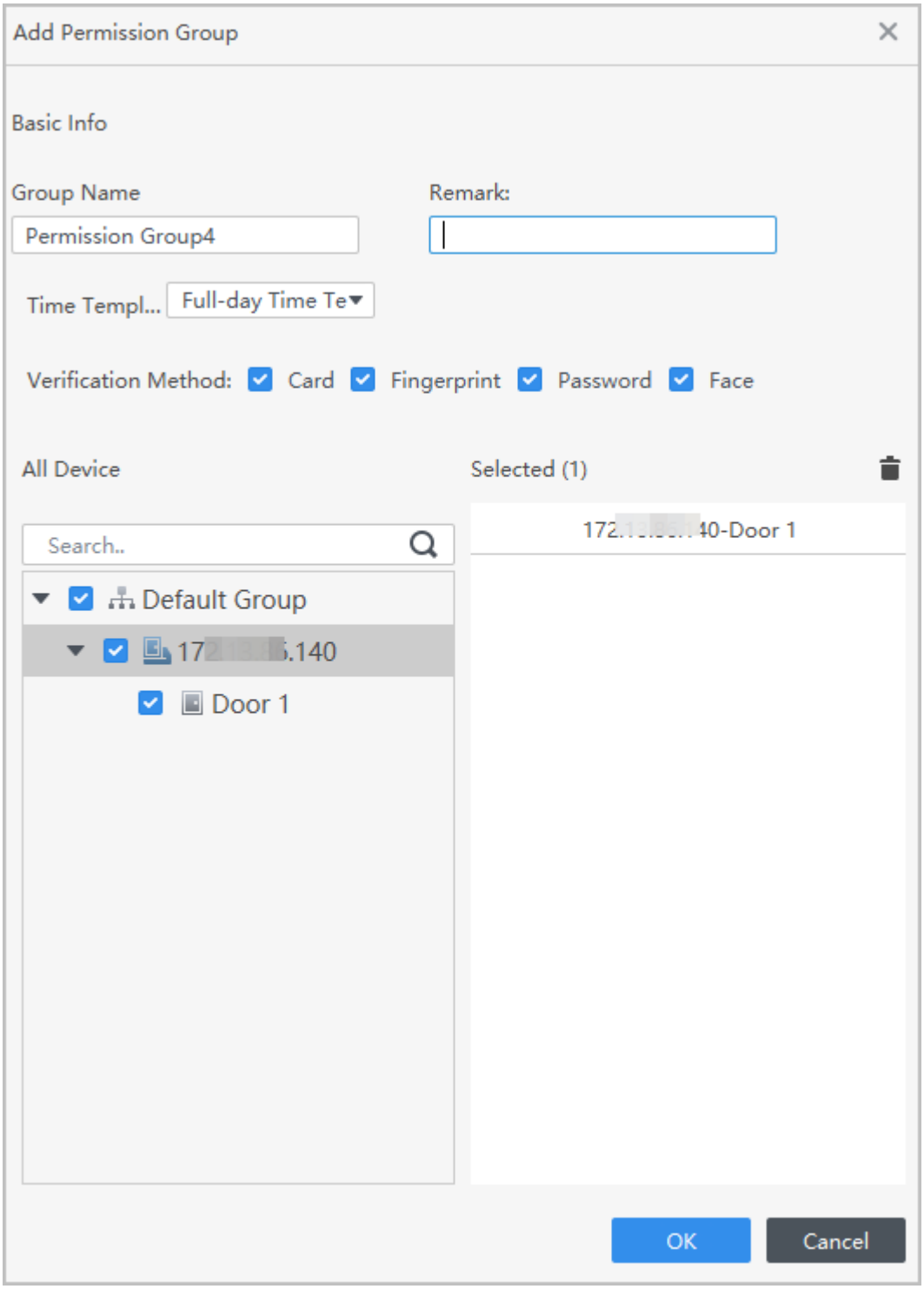
Etapa 4 Configurar permisos.

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

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

1. Seleccione**Grupo**.
2. Ingrese el nombre del grupo, los comentarios (opcional) y seleccione una plantilla de tiempo.
3. Seleccione puertas y métodos de verificación.
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 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 lote**.

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

Figura 4-7 Agregar usuarios en lotes

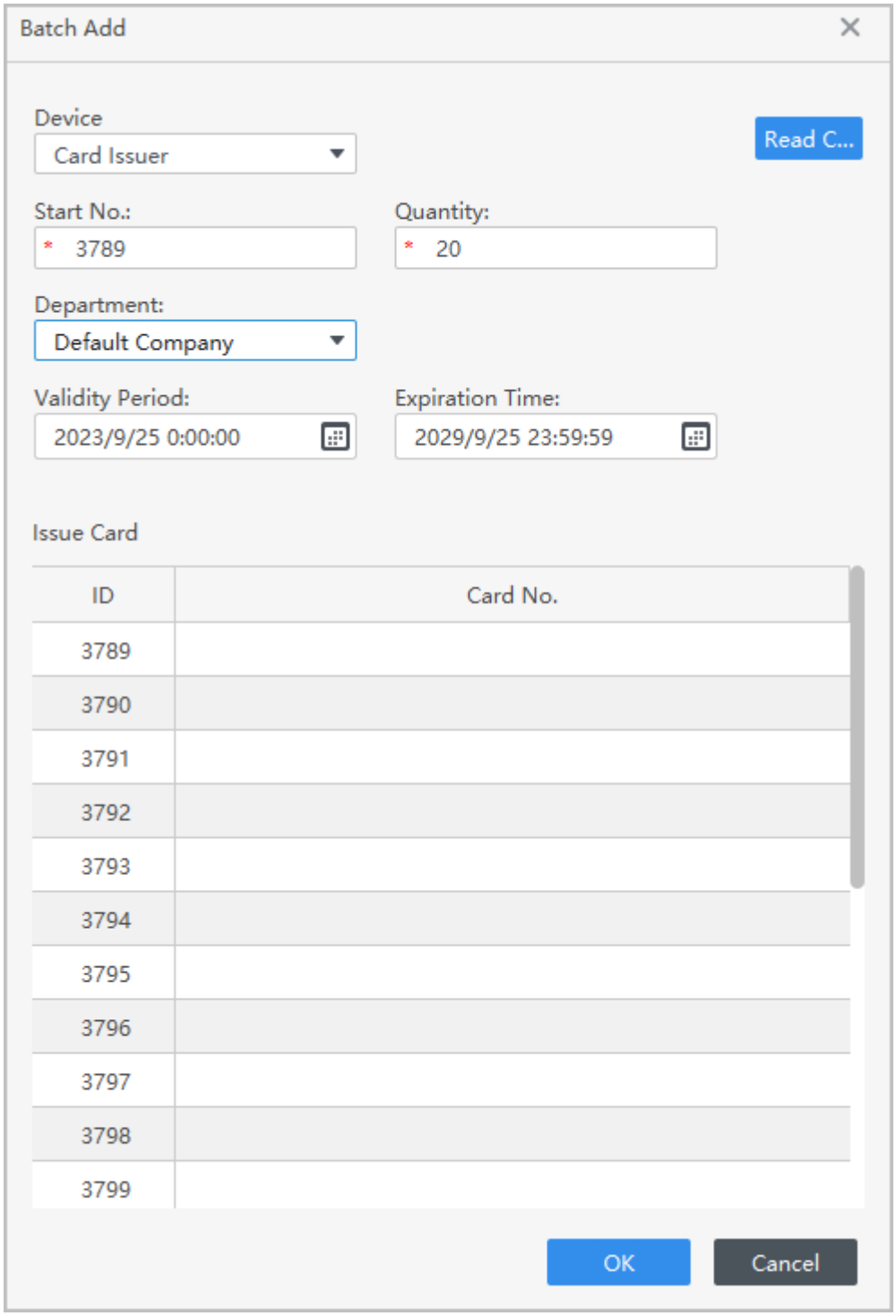


Tabla 4-2 Parámetros para agregar usuarios en lotes

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

Paso 3 Hacer clic**Leer tarjeta No.**y pase las tarjetas en el lector de tarjetas.

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

Etapa 4 **ACUERDO**.

4.3.3 Asignación de permiso de acceso

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

Procedimiento

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

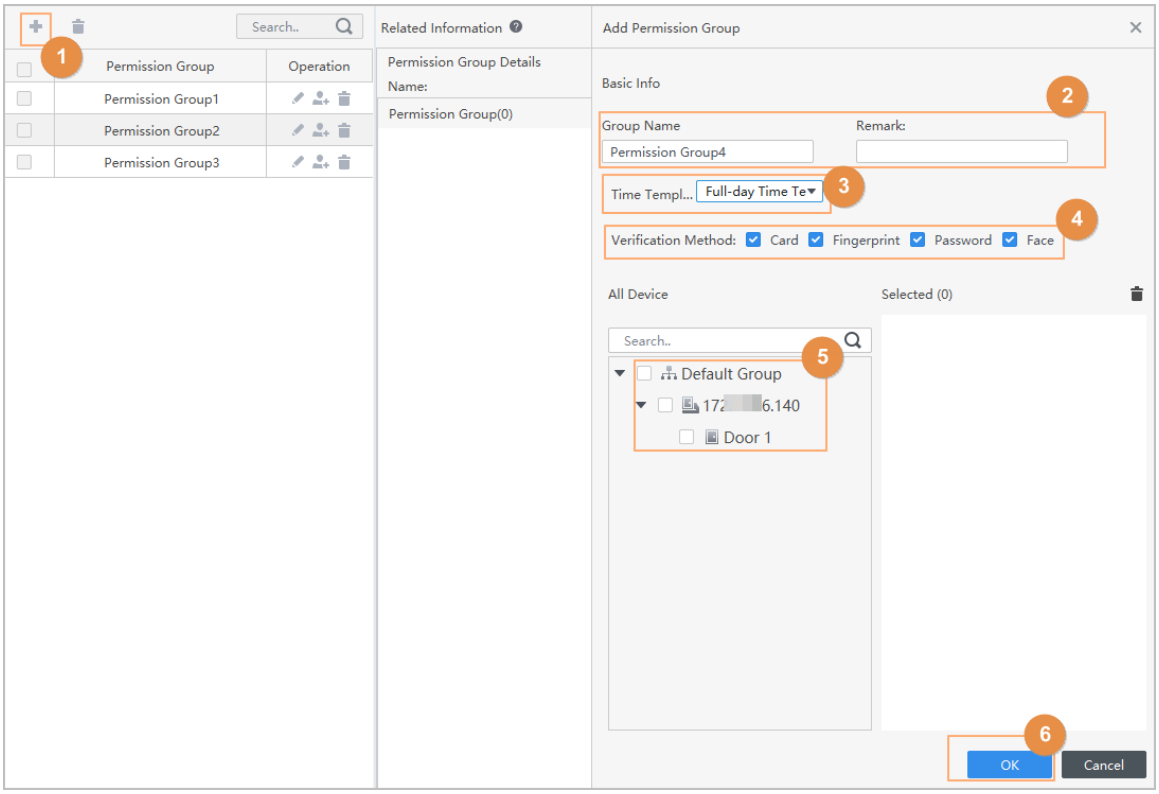
Paso 2 Haga clic.

Paso 3 Ingrese el nombre del grupo, los comentarios (opcional) y seleccione una plantilla de

Etapa 4 tiempo. Seleccione puertas y métodos de verificación.

Paso 5 Hacer clic**DE ACUERDO**.

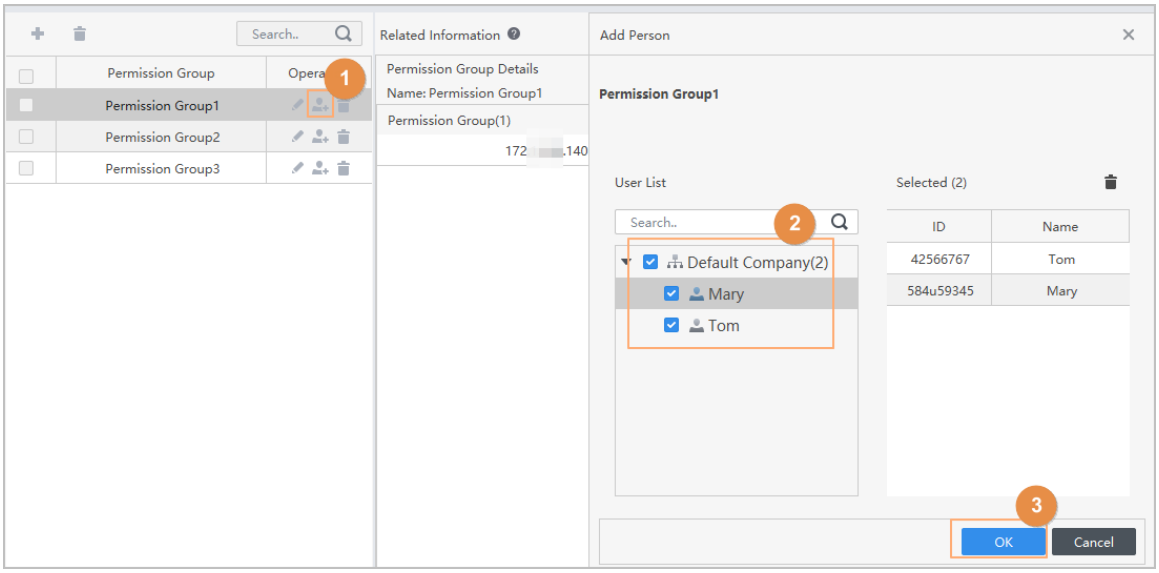
Figura 4-8 Crear un grupo de permisos



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 clicDE ACUERDO.

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

4.3.4 Asignación de permisos de asistencia

Cree un grupo de permisos que sea una colección de permisos de control de asistencia y luego asocie a los empleados con el grupo para que puedan marcar su entrada o salida mediante métodos de verificación definidos.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

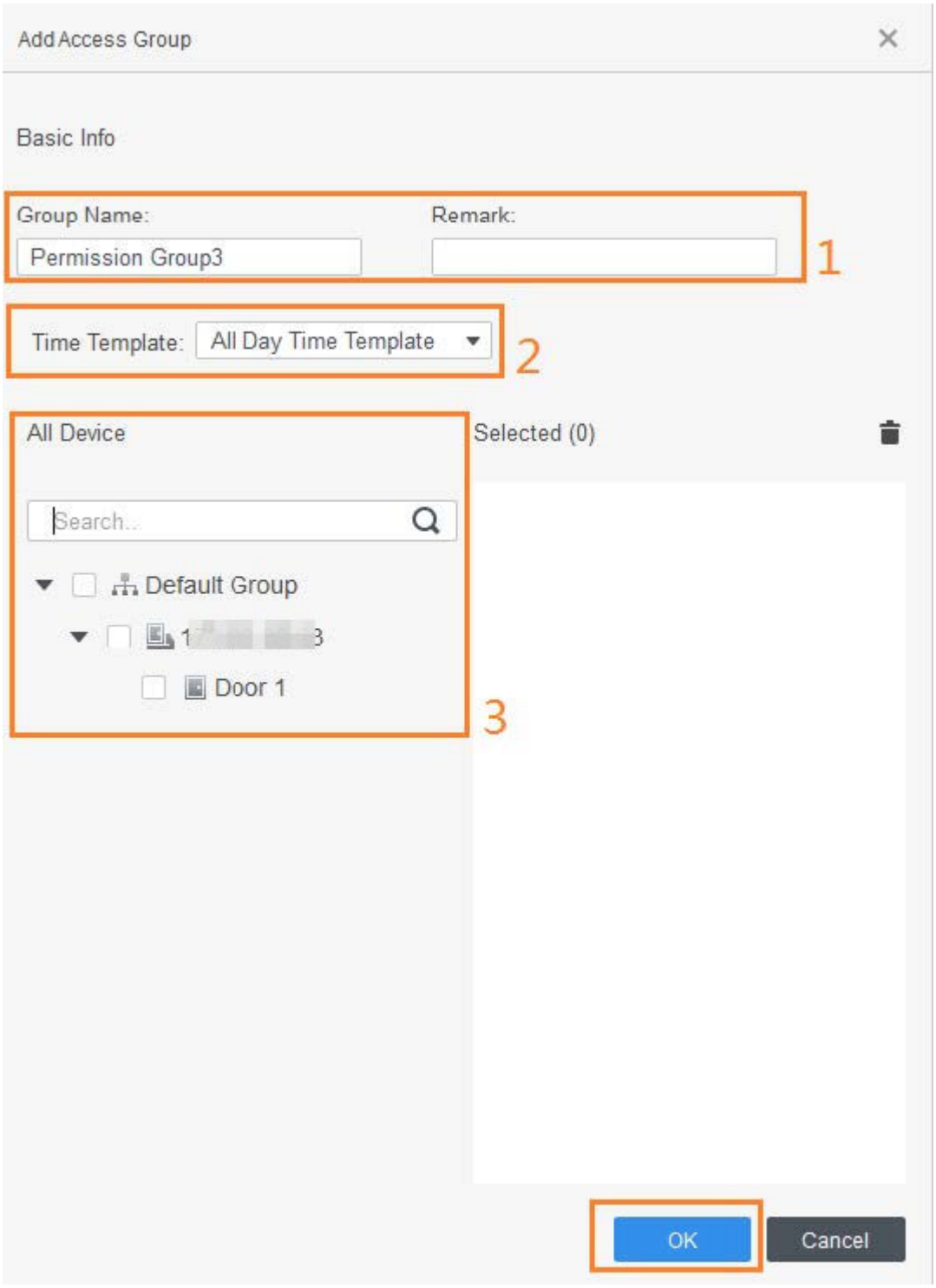
Paso 3 Haga clic.

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

Paso 5 Seleccione el dispositivo de control de acceso.

Paso 6 Hacer clicDE ACUERDO.

Figura 4-10 Crear un grupo de permisos

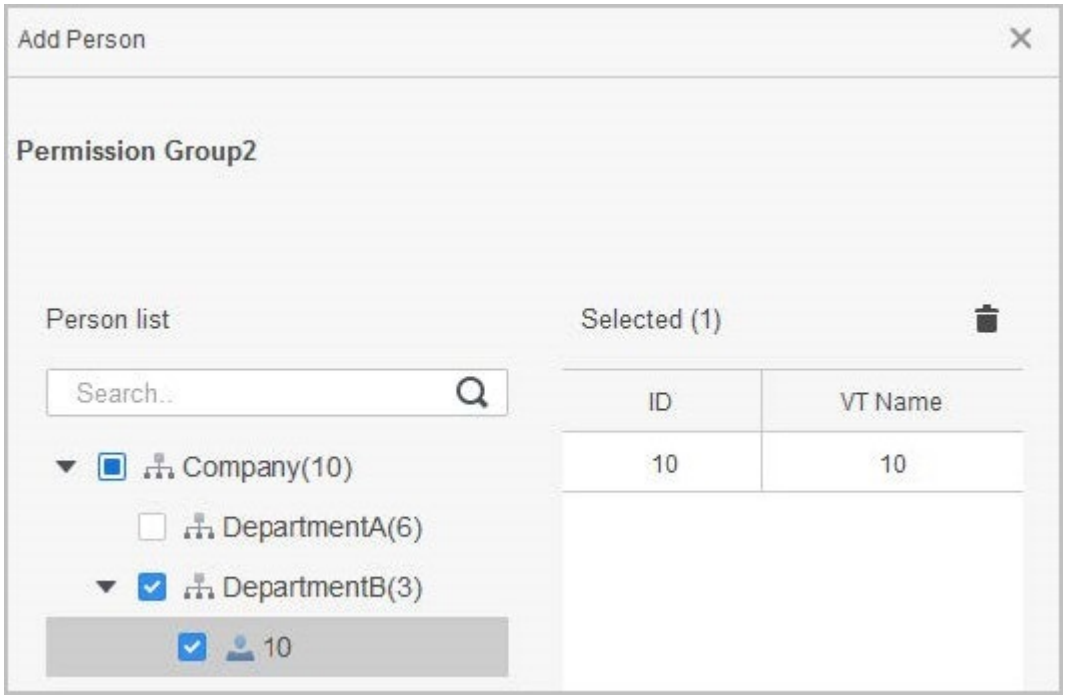


- Time & Attendance admite el registro de entrada/salida mediante contraseña, asistencia facial, asistencia con tarjeta y huellas dactilares.
- La asistencia con tarjetas y huellas dactilares está disponible en modelos selectos.

Paso 7 Hacer clic del grupo de permisos que agregó.

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

Figura 4-11 Agregar usuarios a un grupo de permisos



Paso 9 Hacer clic**DE ACUERDO**.

4.4 Gestión de acceso

4.4.1 Apertura y cierre de puertas de forma remota

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

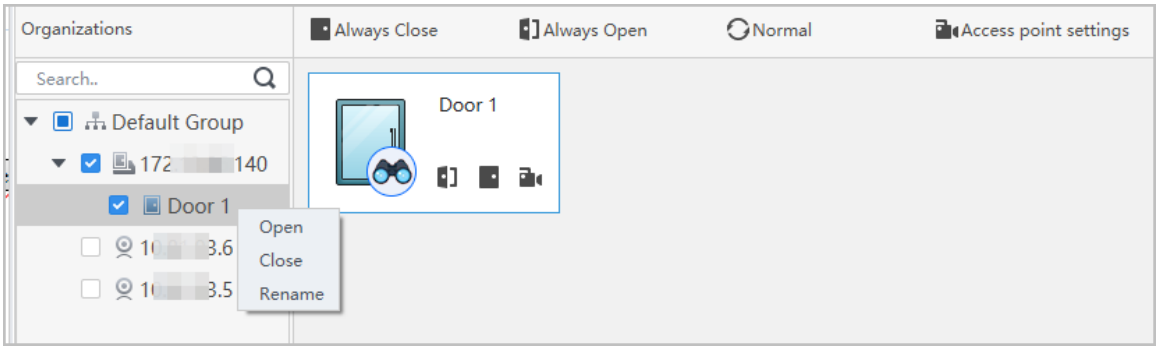
Procedimiento

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

Paso 2 Controla remotamente la puerta.

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

Figura 4-12 Puerta abierta



- : Abra o cierre la puerta.
- : Ver el vídeo 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 luego la lista de eventos dejará de actualizarse. Haga clic para desbloquear.
- Eliminación de eventos: haga clic para borrar todos los eventos en la lista de eventos.

4.4.2 Configuración de Siempre abierto y Siempre cerrado

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

Procedimiento

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

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

Figura 4-13 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

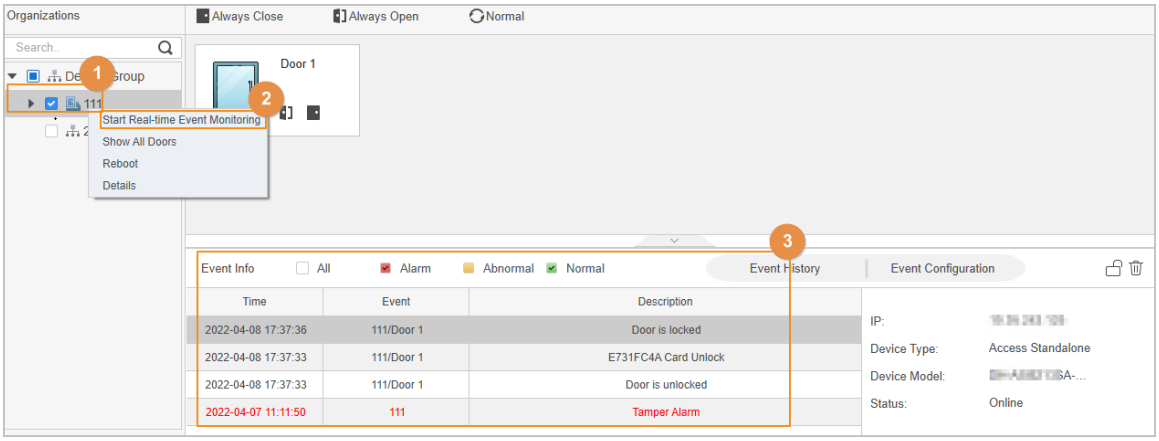
Paso 1 Hacer clic**Solución de acceso**>**Administrador de acceso**en la página de inicio.

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

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

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

Figura 4-14 Monitorear el estado de la puerta



Operaciones relacionadas

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

Apéndice 1 Puntos importantes de cara Registro

Antes del registro

- Las gafas, los sombreros y la barba pueden influir en el rendimiento del reconocimiento facial.
- No te cubras las cejas cuando uses sombreros.
- No cambie mucho el estilo de su 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 afectar el rendimiento del reconocimiento facial del controlador de acceso.

Durante el registro

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

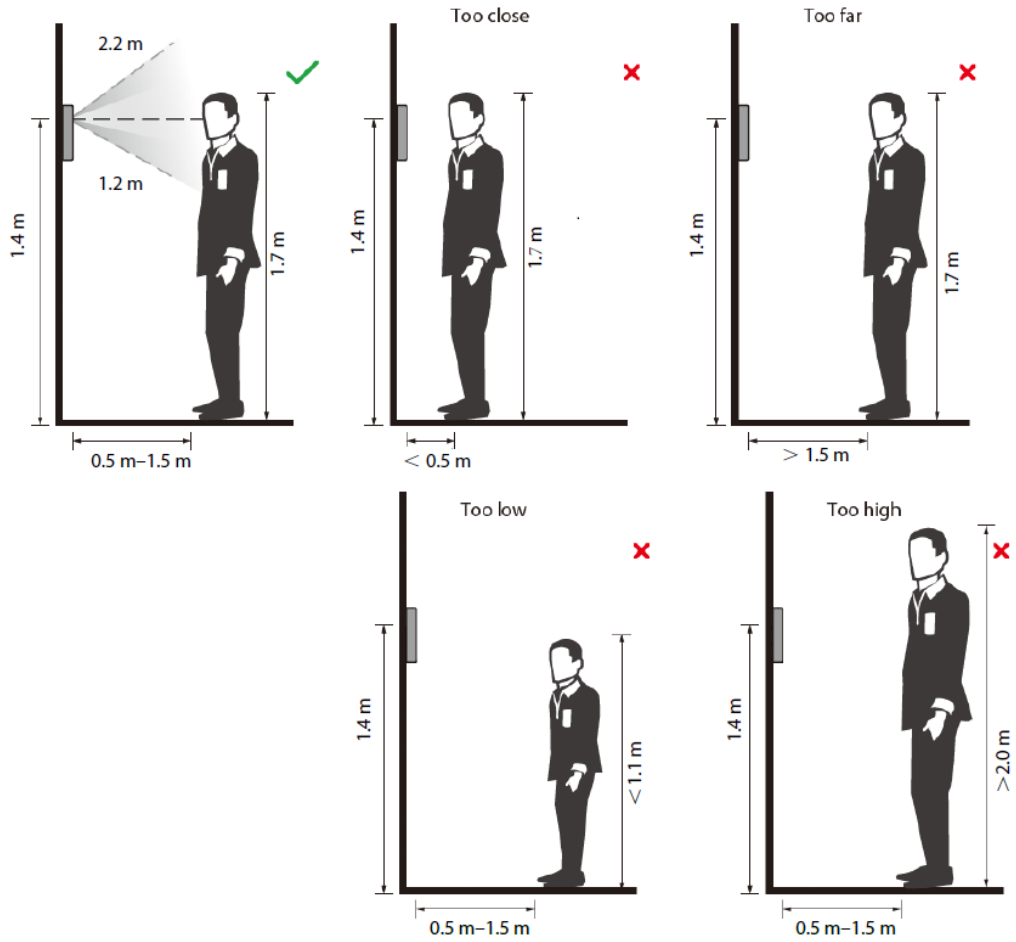
- No sacuda la cabeza ni el cuerpo, de lo contrario el registro podría fallar.
- Evite que aparezcan 2 caras en el marco de captura al mismo tiempo.

Posición de la cara

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

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

Apéndice Figura 1-1 Posición adecuada de la cara



Requisitos de caras

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

Apéndice Figura 1-2 Posición de la cabeza

Apéndice Figura 1-3 Distancia de la cara

- 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 superior a 500 × 500 píxeles, que el tamaño de la imagen sea inferior a 100 KB y que el nombre de la imagen y el ID de la persona sean los mismos.
- Asegúrese de que la cara ocupe más de 1/3 pero no más de 2/3 del área total de la imagen y que la relación de aspecto no supere 1:2.

Apéndice 2 Puntos importantes del intercomunicador

Operación

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

Requisitos previos

La función de intercomunicación se configura en el Dispositivo y VTO.

Procedimiento

Paso 1 En la pantalla de espera, toque . Ingrese al

Paso 2 número de habitación y luego toque .

Apéndice 3 Puntos importantes de las huellas dactilares

Instrucciones de registro

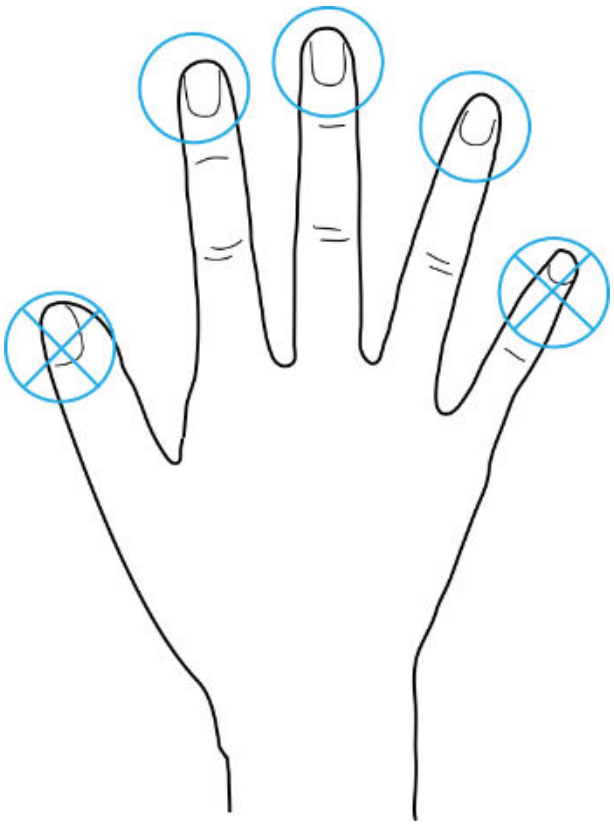
Al registrar la huella digital, preste atención a los siguientes puntos:

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

Dedos recomendados

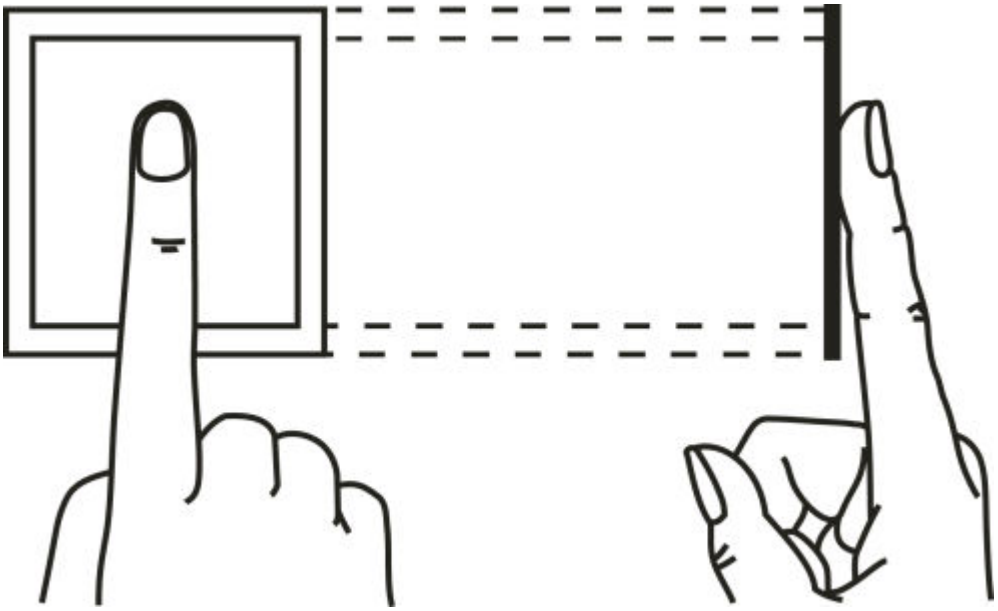
Se recomiendan los dedos índice, medio y anular. Los pulgares y los meñiques no se pueden colocar fácilmente en el centro de grabación.

Apéndice Figura 3-1 Dedos recomendados

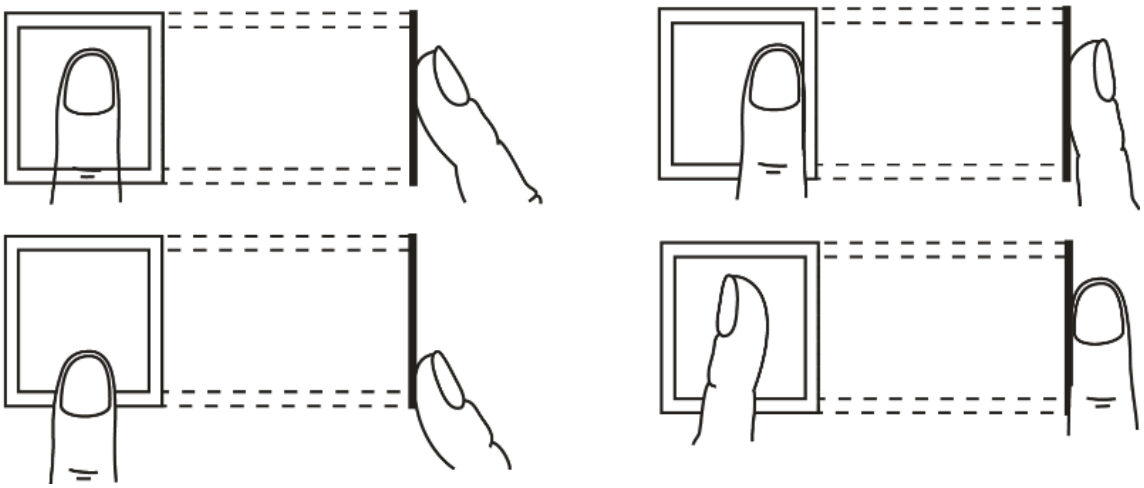


Cómo presionar su huella digital en el escáner

Apéndice Figura 3-2 Colocación correcta



Apéndice Figura 3-3 Ubicación incorrecta



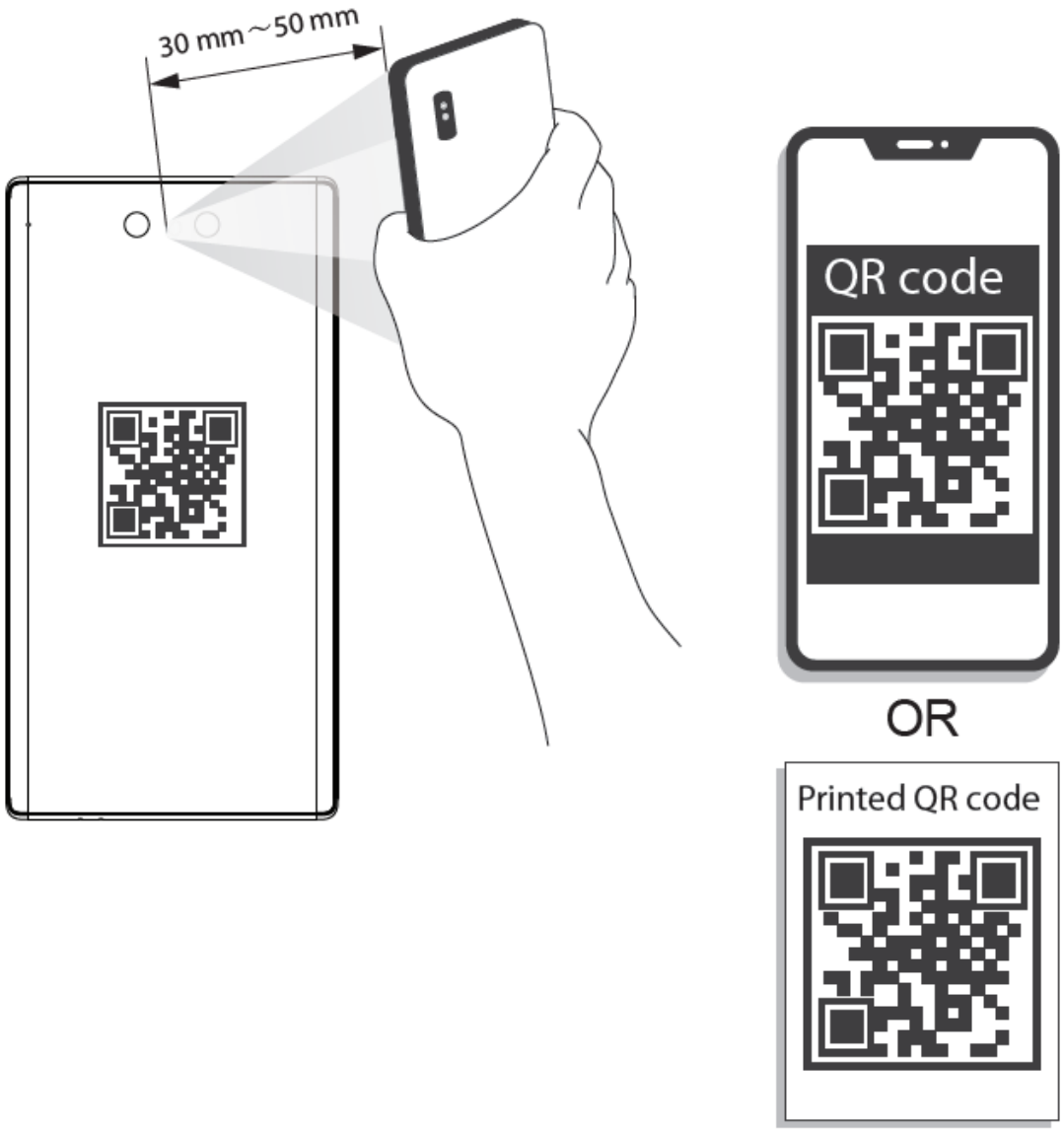
Apéndice 4 Puntos importantes del código QR

Exploración

Coloque el código QR en su teléfono a una distancia de 30 mm a 50 mm de la lente de escaneo de códigos QR. Admite códigos QR de más de 30 mm × 30 mm y 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 4-1 Escaneo de código QR



Apéndice 5 Recomendación de seguridad

Administración de cuentas

1.**Utilice contraseñas complejas**

Consulte las siguientes sugerencias para establecer contraseñas:

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

2.**Cambiar contraseñas periódicamente**

Se recomienda cambiar periódicamente la contraseña del dispositivo para reducir el riesgo de que la adivinen o la descifren.

3.**Asigne cuentas y permisos adecuadamente**

Agregue usuarios adecuadamente 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 mantenerlo habilitado para proteger la seguridad de la cuenta. Después de varios intentos fallidos de contraseña, la cuenta correspondiente y la dirección IP de origen se bloquearán.

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 de amenazas, si hay algún cambio en la información, modifíquelo a tiempo. Al establecer preguntas de seguridad, se recomienda no utilizar respuestas fáciles de adivinar.

Configuración del servicio

1.**Habilitar HTTPS**

Se recomienda habilitar 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 cifrada para reducir el riesgo de que sus datos de audio y video sean interceptados durante la transmisión.

3.**Apague los servicios no esenciales y use el modo seguro**

Si no es necesario, se recomienda desactivar algunos servicios como SSH, SNMP, SMTP, UPnP, punto de acceso AP, 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 buzones.
- 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 que los actores de amenazas lo adivinen.

configuración de la red

1.**Habilitar lista de permitidos**

Se recomienda activar la función de lista de permitidos y solo permitir que IP en la lista de permitidos acceda 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.**Enlace 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.**Construya 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 la intranet desde la red externa;
- Particione la red de acuerdo con las necesidades reales de 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 y lograr el aislamiento de la red;
- Establecer un sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso ilegal de terminales a la red privada.

Auditoría de seguridad

1.**Verificar usuarios en línea**

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

2.**Verificar 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 mucho tiempo, se recomienda habilitar la función de registro de red para garantizar que los registros críticos estén sincronizados con el servidor de registro de red para su seguimiento.

Seguridad del software

1.**Actualice 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 actualización en línea, para obtener la información de actualización del 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 llevar a cabo protección física para los dispositivos (especialmente los dispositivos de almacenamiento), como colocar el dispositivo en una sala de máquinas y un gabinete exclusivos, y tener control de acceso.

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