Controlador de acceso con reconocimiento facial

Manual del usuario

Versión 1.0.0

Prefacio

General

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

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

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

Historial de revisiones

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

Aviso de protección de la privacidad

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

Acerca del manual

- El manual es solo de referencia. Pueden existir ligeras diferencias entre el manual y el producto.
- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas que no cumplan con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Pueden encontrarse ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y software están sujetos a cambios sin previo aviso por escrito. Actualizaciones de productos

Es posible que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.

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

Medidas de seguridad y advertencias importantes

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

Requerimientos de transporte

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

Requisito de almacenamiento

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

Requisitos de instalación

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

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

Requisitos de funcionamiento

- Compruebe si la fuente de alimentación es correcta antes de usarlo.

- No desconecte el cable de alimentación del costado del controlador de acceso mientras el adaptador esté encendido.

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

Tabla de contenido

1 Descripción general

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

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

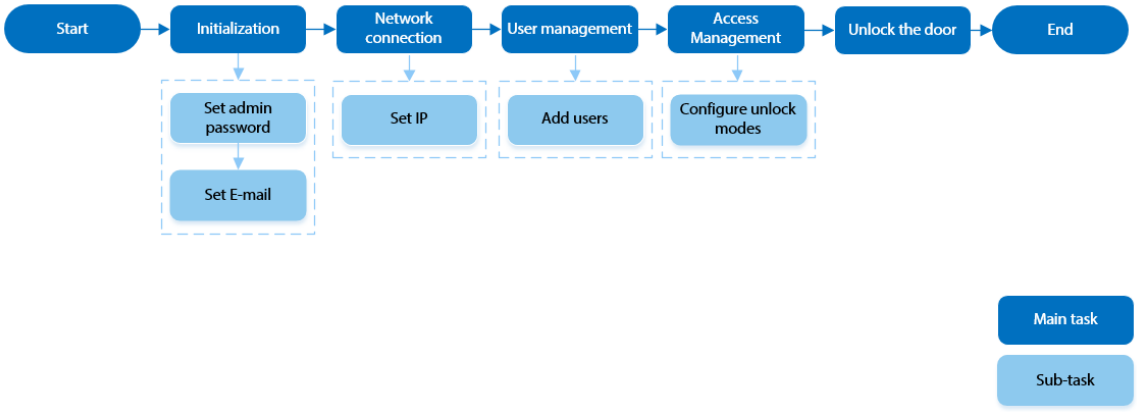
- Las configuraciones pueden variar según los modelos del producto, consulte el producto real.
- Los dispositivos que no tienen pantalla táctil deben conectarse a un mouse para realizar configuraciones. Este manual utiliza el dispositivo con pantalla táctil como ejemplo.
- Algunos modelos admiten la conexión de módulos de extensión, como el módulo de código QR, el módulo de huella dactilar, etc. El tipo de módulos de extensión que admite el controlador de acceso puede variar; consulte el producto real.

2 Operaciones locales

- Las configuraciones pueden variar según el producto real.
- Los modelos sin pantalla táctil necesitan conectar un mouse USB con cable. En esta sección se utilizan los modelos con pantalla táctil como ejemplo.
- Los módulos de expansión externos solo están disponibles en modelos seleccionados.
- Es posible que algunos textos de la interfaz de usuario no se muestren 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 los iconos

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

2.3 Pantalla de espera

Puede desbloquear la puerta mediante reconocimiento facial, tarjeta, contraseñas y código QR. También puede realizar llamadas a través de la función de intercomunicador. Los métodos de desbloqueo pueden variar según los modelos del producto.

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

Figura 2-2 Pantalla de espera

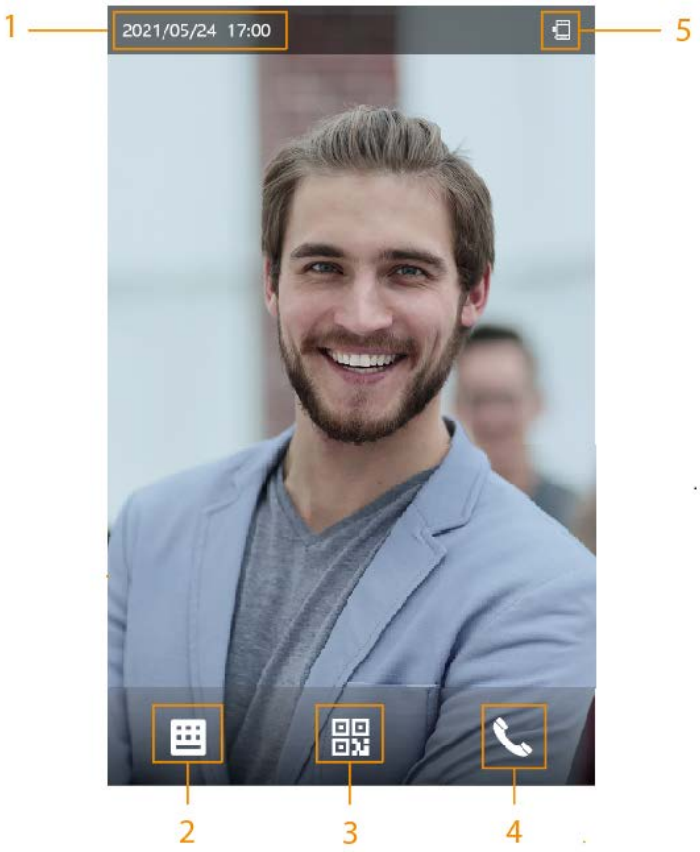


Tabla 2-2 Descripción de la pantalla de inicio

No.	Nombre	Descripción
1	Fecha y hora	Fecha y hora actual.
2	Contraseña	Ingrese la contraseña de usuario o la contraseña de administrador o la contraseña temporal para desbloquear la puerta.

No.	Nombre	Descripción
3	Código QR	Toque el ícono del código QR y escanee el código QR para desbloquear la puerta. Para los modelos que tienen un módulo de código QR independiente o que conectan un módulo de expansión QR, el ícono no se mostrará. Simplemente puede colocar su código OR frente a la lente del controlador de acceso o el módulo de expansión y se escaneará automáticamente.
4	Intercomunicador	● Cuando el controlador de acceso funciona como servidor, puede llamar al VTO y al VTH. ● Cuando la plataforma de gestión funciona como servidor, el controlador de acceso puede llamar al VTO, al VTS y a la plataforma de gestión. ● Cuando funciona con DMSS, puede llamar a DMSS.
5	Visualización de estado	Muestra el estado de Wi-Fi, red, módulo de extensión, USB y más. Wi-Fi y módulos de extensión solo están disponibles en modelos selectos.

2.4 Inicialización

Para el primer uso o después de restaurar los valores predeterminados de fábrica, debe seleccionar un idioma en Access Controller y luego configurar la contraseña y la dirección de correo electrónico para la cuenta de administrador. Puede usar la cuenta de administrador para ingresar al menú principal de Access Controller 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 sean espacios en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &).

2.5 Iniciar sesión

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

Información de contexto

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

Procedimiento

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

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

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

  La función de huella dactilar solo está disponible en modelos seleccionados.
- Perforación de tarjeta: ingrese al menú principal deslizando la tarjeta.
- PWD: Ingrese el ID de usuario y la contraseña de la cuenta de administrador.
- admin: Ingrese la contraseña de administrador para ingresar al menú principal.

2.6 Métodos de desbloqueo

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

2.6.1 Desbloqueo por tarjetas

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

2.6.2 Desbloqueo por reconocimiento facial

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

2.6.3 Desbloqueo por contraseña de usuario

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

Procedimiento

Paso 1 Grifo en la pantalla de espera.

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

Paso 3 **ACUERDO**.

2.6.4 Desbloqueo mediante contraseña de administrador

Ingrese solo la contraseña de administrador para desbloquear la puerta. La puerta se puede desbloquear con la contraseña de administrador, excepto si la puerta está normalmente cerrada. Un dispositivo solo permite una contraseña de administrador.

Prerrequisitos

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

La contraseña de administrador no se puede usar para desbloquear cuando el estado de la puerta está configurado como siempre Estado cerrado.

2.6.5 Desbloqueo mediante código QR

Procedimiento

Paso 1 En la pantalla de espera, toque .

Paso 2 Coloque su código QR frente a la lente.

2.6.6 Desbloqueo por huella dactilar

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

2.6.7 Desbloqueo mediante contraseña temporal

Desbloquee la puerta con la contraseña temporal.

Procedimiento

Paso 1 Agregue el controlador de acceso a DMSS.

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

Paso 2 En la pantalla de inicio, toque y luego toque**Desbloqueo con contraseña temporal**.

Paso 3 Ingrese la contraseña temporal y luego toque

2.7 Gestión de usuarios

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

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

2.7.1 Agregar usuarios

Procedimiento

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

Paso 2 . Configure los parámetros en la interfaz.

Figura 2-3 Agregar nuevo usuario

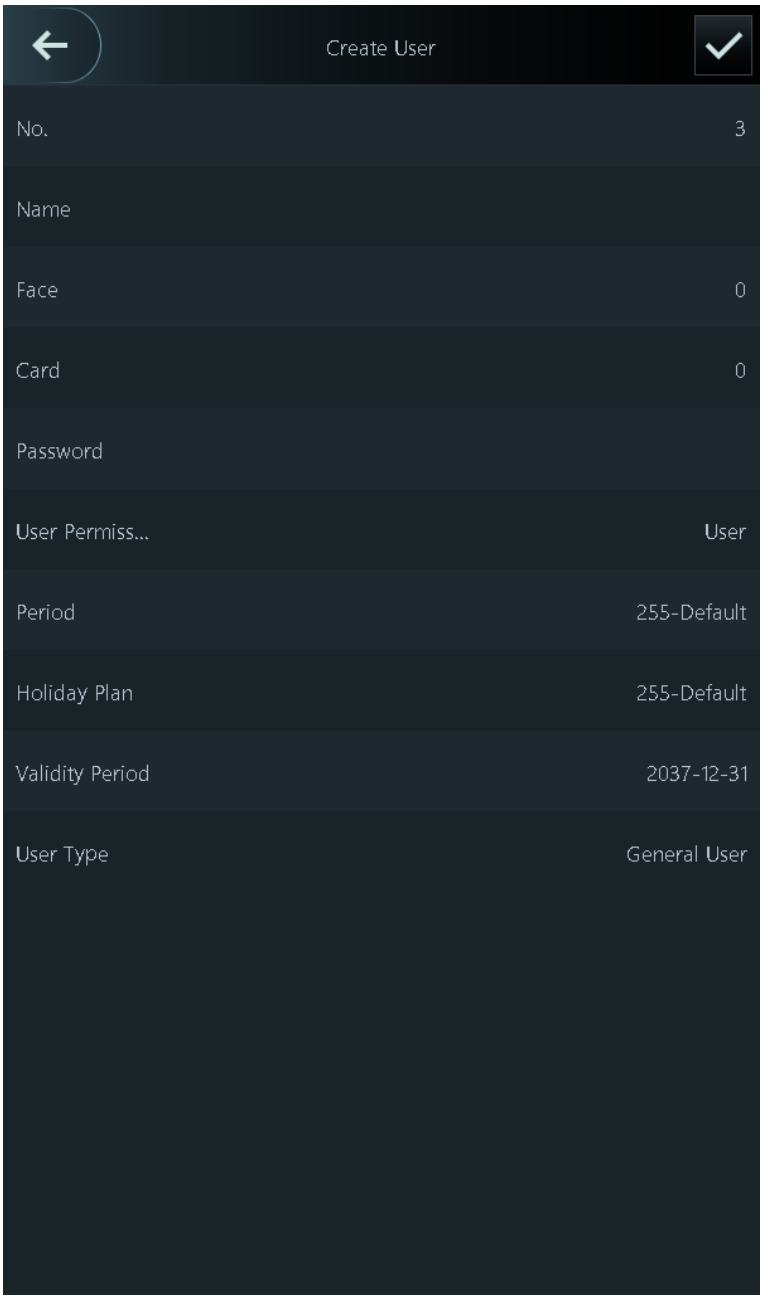


Tabla 2-3 Descripción de parámetros

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

Parámetro	Descripción
FP	Registrar huellas dactilares. Un usuario puede registrar hasta 3 huellas dactilares y puede configurar una huella dactilar como huella de coacción. Se activará una alarma cuando se use la huella dactilar de coacción para desbloquear la puerta.  ● La función de huella dactilar solo está disponible en algunos modelos modelos. ● No recomendamos que configure la primera huella digital como huella digital de coacción. ● Un usuario sólo puede configurar una huella digital de coacción. ● La función de huella dactilar está disponible si el controlador de acceso admite la conexión de un módulo de extensión de huella dactilar.
Rostro	Coloque su rostro dentro del marco y se capturará automáticamente una imagen de su 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 deslícela y luego el controlador de acceso leerá la información de la tarjeta. Puedes habilitar el**Tarjeta de coacción**Función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta.  Un usuario sólo puede configurar una tarjeta de coacción.
Contraseña	Introduzca 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.
Permiso de usuario	● **Usuario**:Los usuarios solo tienen permisos de acceso a puertas o de control de asistencia. ● **Administración**:Los administradores pueden configurar el controlador de acceso además del acceso a la puerta y los permisos de asistencia.
Período	Las personas pueden desbloquear la puerta o tomar asistencia durante el período definido. Para obtener más información sobre cómo configurar períodos, consulte "3.7.8.1 Configuración de períodos de tiempo".
Plan de vacaciones	Las personas pueden desbloquear la puerta o pasar lista durante los días festivos definidos. Para obtener más información sobre cómo configurar los períodos, consulte "3.7.8.2 Configuración de planes de vacaciones".
Periodo de validez	Establecer una fecha en la que caducarán los permisos de acceso a la puerta y de asistencia de la persona.

Parámetro	Descripción
Tipo de usuario	● **Usuario general**:Los usuarios generales pueden desbloquear la puerta. ● **Usuario de la lista negra**: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 que expire el período definido o se agote el tiempo de desbloqueo, no podrán desbloquear la puerta. ● **Usuario de patrulla**:Los usuarios de patrulla pueden tomar asistencia en el controlador de acceso, pero no tienen puerta. permisos. ● **Usuario VIP**:Cuando el VIP desbloquee la puerta, el personal de servicio recibirá una notificación. ● **Otro usuario**:Cuando desbloqueen la puerta, ésta permanecerá desbloqueada durante 5 segundos más. ● **Usuario personalizado 1/Usuario personalizado 2**:Lo mismo ocurre con los usuarios generales.
Departamento	Seleccione departamentos, lo cual resulta útil al configurar los cronogramas de los departamentos. Para obtener información sobre cómo crear departamentos, consulte "2.9.1 Configuración de departamentos". Esta función solo está disponible en modelos seleccionados.
Modo de programación	● Horario de departamento: aplica los horarios de departamento al usuario. ● Horario personal: aplica horarios personales al usuario. Para saber cómo configurar horarios personales o departamentales, consulte "2.9.4 Configuración de horarios de trabajo". ◇ Esta función solo está disponible en modelos seleccionados. ◇ Si configura el modo de programación en departamento agenda aquí, la agenda personal que tienes configurado para el usuario en**Asistencia**>**Configuración de programación**>**Horario personal**se vuelve inválido.

Paso 3 Grifo .

2.7.2 Visualización de la información del usuario

Procedimiento

Paso 1 En el**Menú principal**, seleccionar**Gestión de personas**>**Lista de usuarios**, o seleccione**Usuario**>**Lista de administradores**. Ver todos los

Paso 2 usuarios y cuentas de administrador agregados.

- :Desbloqueo mediante contraseña.
- :Desbloqueo mediante pase de tarjeta.

- : Desbloqueo mediante reconocimiento facial.
- : Desbloqueo mediante huella dactilar.

Operaciones relacionadas

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

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

2.7.3 Configuración de la contraseña de desbloqueo del administrador

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

Procedimiento

Paso 1 En el**Menú principal**pantalla, seleccionar**Usuario**>**Contraseña de desbloqueo de administrador**. Grifo

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

Paso 3 desbloqueo de administrador.

2.8 Gestión de acceso

Puede configurar ajustes para puertas como el modo de desbloqueo, la conexión de alarmas y los horarios de las puertas. Los modos de desbloqueo disponibles pueden variar según el modelo del producto.

2.8.1 Configuración de combinaciones de desbloqueo

Utilice la tarjeta, la huella dactilar, el reconocimiento facial o la contraseña o sus combinaciones para desbloquear la puerta. Los modos de desbloqueo disponibles pueden variar según el modelo del producto.

Procedimiento

Paso 1 Seleccionar**Gestión de control de acceso**>**Desbloquear combinación**. Seleccione

Paso 2 métodos de desbloqueo.

Para cancelar su selección, toque nuevamente el método seleccionado.

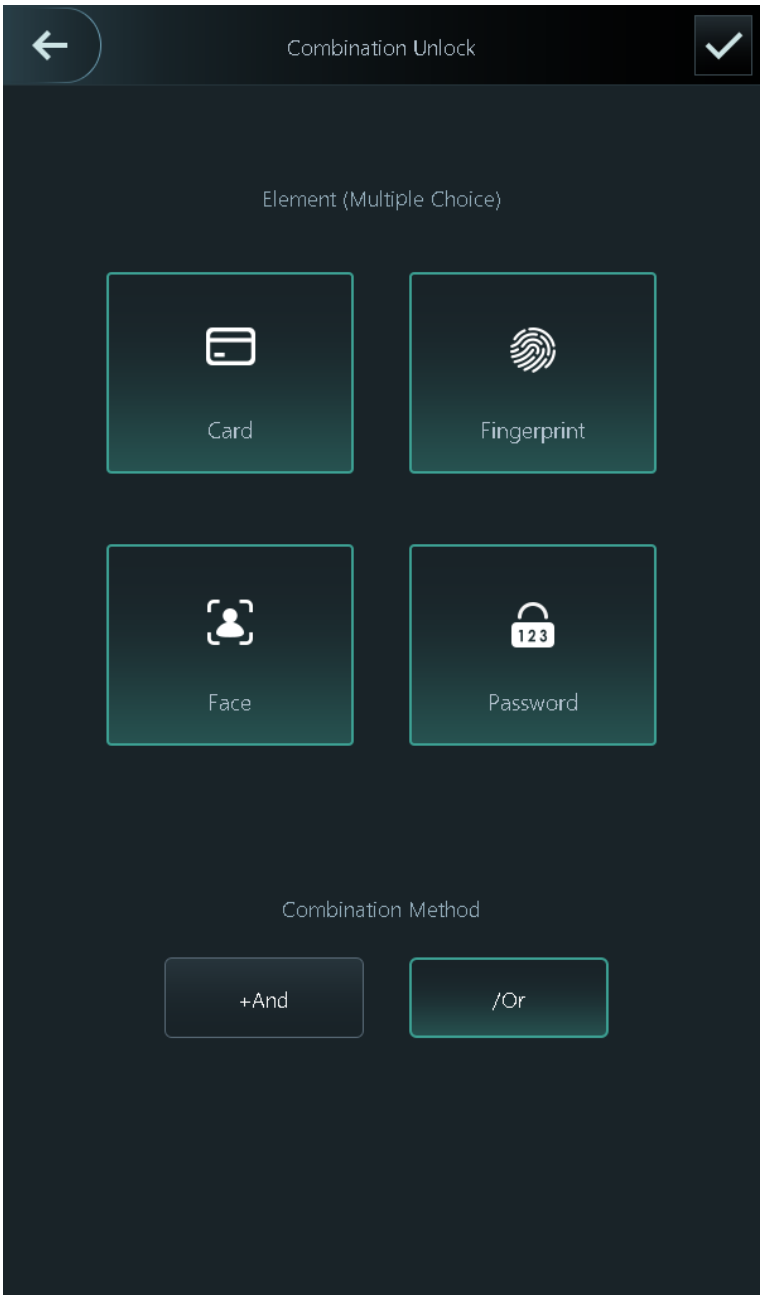
Paso 3 Toca +**Y**o**/O**para configurar combinaciones.

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

  Las personas tienen que 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.

Figura 2-4 Elemento (opción múltiple)



Paso 4 Grifo para guardar los cambios.

2.8.2 Configuración de alarmas

Se activará una alarma cuando se acceda anormalmente a la entrada o salida.

Procedimiento

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

Paso 2 Habilitar el tipo de alarma.

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

Figura 2-5 Alarma

Tabla 2-4 Descripción de los parámetros de alarma

Parámetro	Descripción
Anti-passback	Los usuarios deben verificar su identidad tanto para entrar como para salir; de lo contrario, se activará una alarma. Esto ayuda a evitar que los titulares de tarjetas puedan entregar su tarjeta a otras personas para permitirles el acceso. Cuando se activa la función anti-passback, el titular de la tarjeta debe abandonar el área protegida a través de un lector de salida antes de que el sistema le conceda el 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. Siempre que la secuencia sea "entrada, salida, entrada, salida, etc.", el sistema funcionará bien. ● 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 controlador de acceso solo puede conectar una cerradura, verifique en la Controlador de acceso significa una dirección de "entrada" y la verificación en el lector de tarjetas externo significa una dirección de "salida" de manera predeterminada. Puede modificar la configuraciones en la plataforma de administración.
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
Intrusión	Cuando el sensor de puerta está habilitado, se activará una alarma de intrusión si la puerta se abre de forma anormal.
Puerta agotada	Se activará una alarma cuando la puerta permanezca desbloqueada durante más tiempo del definido. Varía entre 1 y 9999 segundos.

2.8.3 Configuración del estado de la puerta

Procedimiento

Paso 1 En el**Menú principal**pantalla, seleccionar**Gestión de control de acceso**>**Configuración del estado de bloqueo**. Establecer el estado

Paso 2 de la puerta.

Figura 2-6 Estado de bloqueo

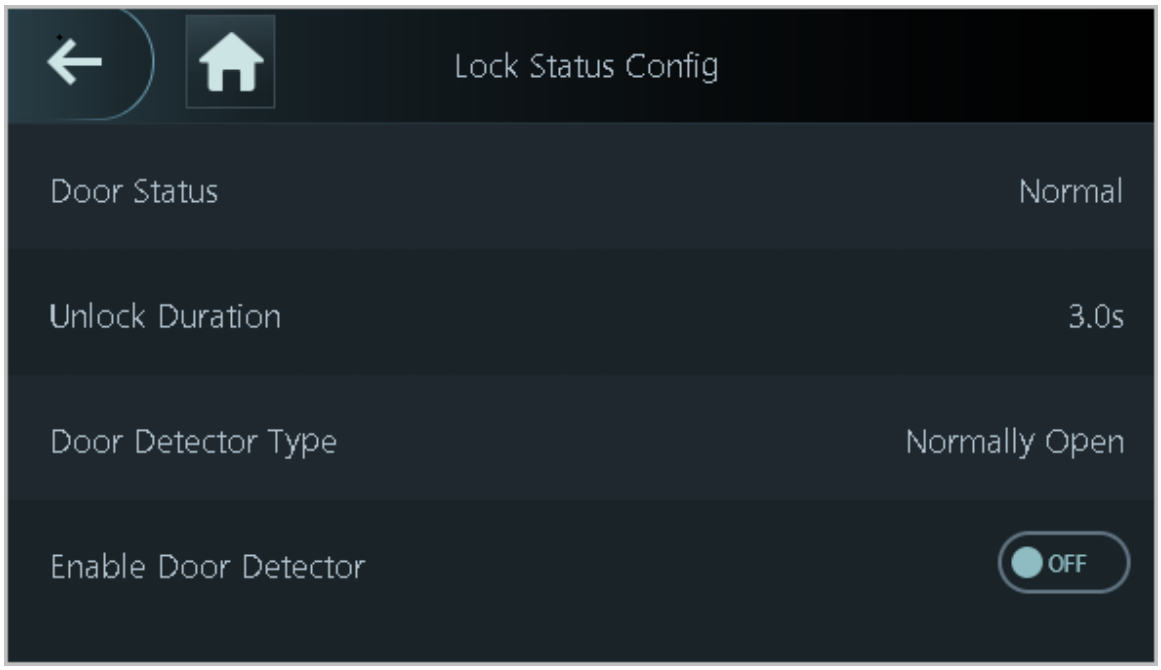


Tabla 2-5 Descripción de parámetros

Parámetro	Descripción
Estado de la puerta	● **Normalmente abierto**:La puerta permanece desbloqueada todo el tiempo. ● **Normalmente cerrado**:La puerta permanece cerrada todo el tiempo. ● **Normal**: Si**Normal**Si se selecciona, la puerta se bloqueará y desbloqueará según su configuración.
Duración del desbloqueo	Después de que a una persona se le concede el acceso, la puerta permanecerá desbloqueada durante un tiempo definido para que pueda pasar.
Tipo de detector de puerta	Con el detector de puerta conectado a su dispositivo, se pueden activar alarmas 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.

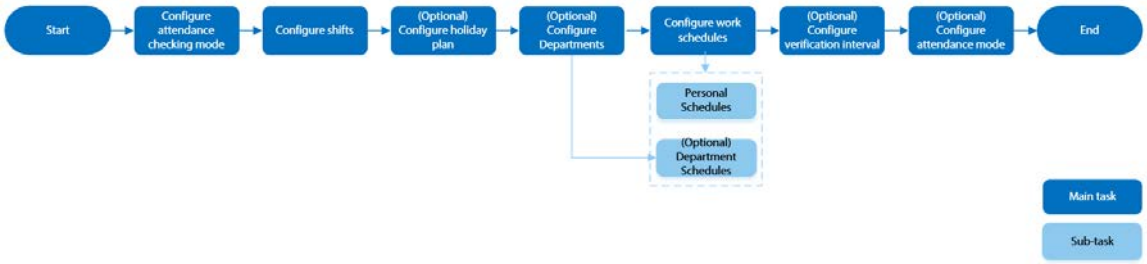
Parámetro	Descripción
Habilitar detector de puerta	Las alarmas de intrusión y de tiempo de espera de puerta tendrán efecto solo después de habilitar esta función.

2.9 Gestión de asistencia

El control de asistencia permite la gestión de asistencia tanto en el dispositivo local como en Smart PSS Lite. En esta sección, solo se utiliza la configuración de asistencia en el dispositivo local como ejemplo.

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

Figura 2-7 Diagrama de flujo de configuración del control de asistencia



2.9.1 Configuración de departamentos

Procedimiento

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

Paso 2 Seleccione un departamento y luego cámbiele el nombre.

Hay 20 departamentos predeterminados. Te recomendamos cambiarles el nombre.

Figura 2-8 Crear departamentos

Paso 3 Grifo .

2.9.2 Configuración de turnos

Configurar turnos para definir reglas de control de asistencia. Los empleados deben presentarse a trabajar a la hora programada para el inicio de su turno y retirarse a la hora de finalización, excepto cuando elijan trabajar horas extra.

Procedimiento

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

Paso 2 Seleccione un turno.

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

Paso 3 Configura los parámetros del turno.

Figura 2-9 Crear turnos

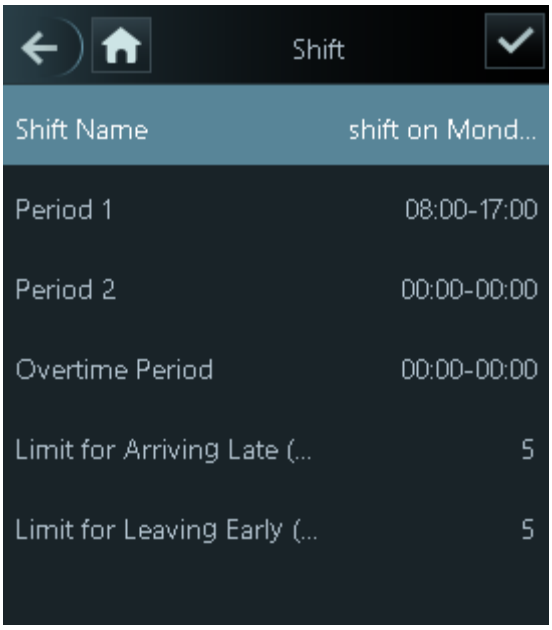
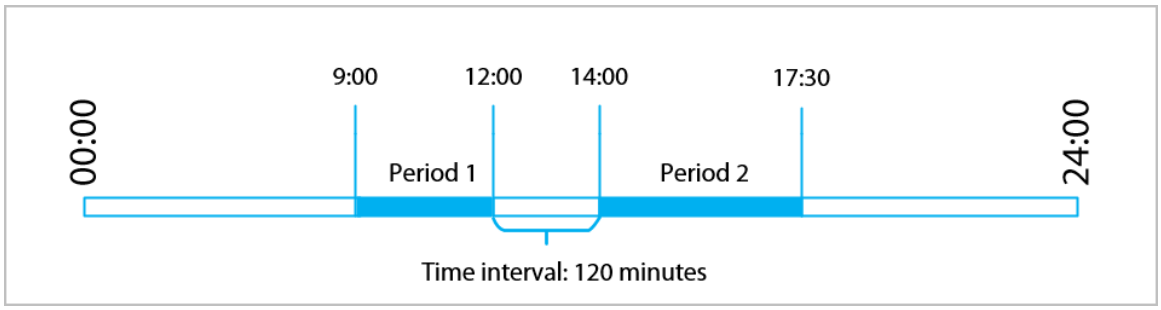


Tabla 2-6 Descripción de los parámetros de cambio

Parámetro	Descripción
Nombre del turno	Introduzca el nombre del turno.
Periodo 1	Especifique un rango de tiempo en el que las personas pueden registrar su entrada y salida durante la jornada laboral. Si solo establece un período de asistencia, los empleados deben registrar su entrada y salida a las horas designadas para evitar que aparezca una anomalía en su registro de asistencia. Por ejemplo, si establece de 08:00 a 17:00, los empleados deben registrar su entrada a las 08:00 y su salida a partir de las 17:00. Si establece 2 períodos de asistencia, estos no pueden superponerse. Los empleados deben registrar su entrada y salida en ambos períodos.
Periodo 2	
Período de horas extras	Los empleados que registren su entrada o salida durante el período definido serán considerados como si estuvieran trabajando más allá de sus horas normales de trabajo.
Límite de llegada tardía (min)	Se puede conceder a los empleados una cierta cantidad de tiempo para que puedan fichar su entrada un poco más tarde y su salida un poco más temprano. Por ejemplo, si la hora habitual de fichar su entrada es las 08:00, el período de tolerancia se puede establecer en 5 minutos para que los empleados que lleguen a las 08:05 no se consideren retrasados.
Límite para salida anticipada (min)	

- Cuando el intervalo de tiempo entre dos períodos es un número par, se puede dividir el intervalo de tiempo por dos y asignar la primera mitad del intervalo al primer período, que será la hora de salida. La segunda mitad del intervalo se debe asignar al segundo período como hora de entrada.

Figura 2-10 Intervalo de tiempo (número par)

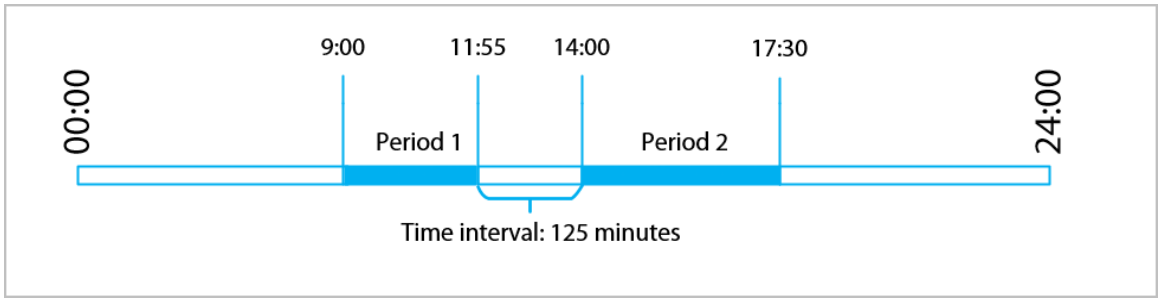


Por ejemplo: si el intervalo es de 120 minutos, entonces la hora de salida para el período 1 es de 12:00 a 12:59, y la hora de entrada para el período 2 es de 13:00 a 14:00.

Si una persona registra su salida varias veces durante el período 1, la última hora será válida y, si se registran varias veces durante el período 2, el horario más temprano será válido.

- Cuando el intervalo de tiempo entre dos períodos es un número impar, la parte más pequeña del intervalo se asignará al primer período, que será el tiempo de salida. La parte más grande del intervalo se asignará al segundo período, que será el tiempo de entrada.

Figura 2-11 Intervalo de tiempo (número par)



Por ejemplo: si el intervalo es de 125 minutos, la hora de salida del período 1 es de 11:55 a 12:57, y la hora de entrada del 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 se registran varias veces durante el período 2, el horario más temprano será válido.

Todos los horarios de asistencia son precisos hasta el segundo. Por ejemplo, si el registro de entrada normal La hora se establece a las 8:05 AM, el empleado que registre su entrada a las 8:05:59 AM no será considerado como Llegando tarde. Pero, el empleado que llegue a las 8:06 AM será marcado como retrasado por 1 minuto.

Paso 4 Grifo .

2.9.3 Configuración de planes de vacaciones

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

Procedimiento

Paso 1 Seleccionar**Asistencia**>**Configuración de cambio**>**Día festivo**Haga

Paso 2 clic para agregar planes de vacaciones.

Paso 3 Configurar los parámetros.

Figura 2-12 Crear planes de vacaciones

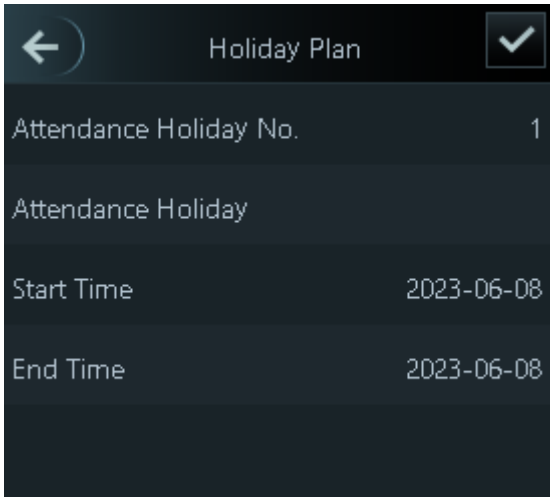


Tabla 2-7 Descripción de parámetros

Parámetro	Descripción
Asistencia Vacaciones No.	El número de la fiesta.
Vacaciones de asistencia	El nombre de la fiesta.
Hora de inicio	La hora de inicio y finalización de las vacaciones.
Fin del tiempo	

Paso 4 Grifo .

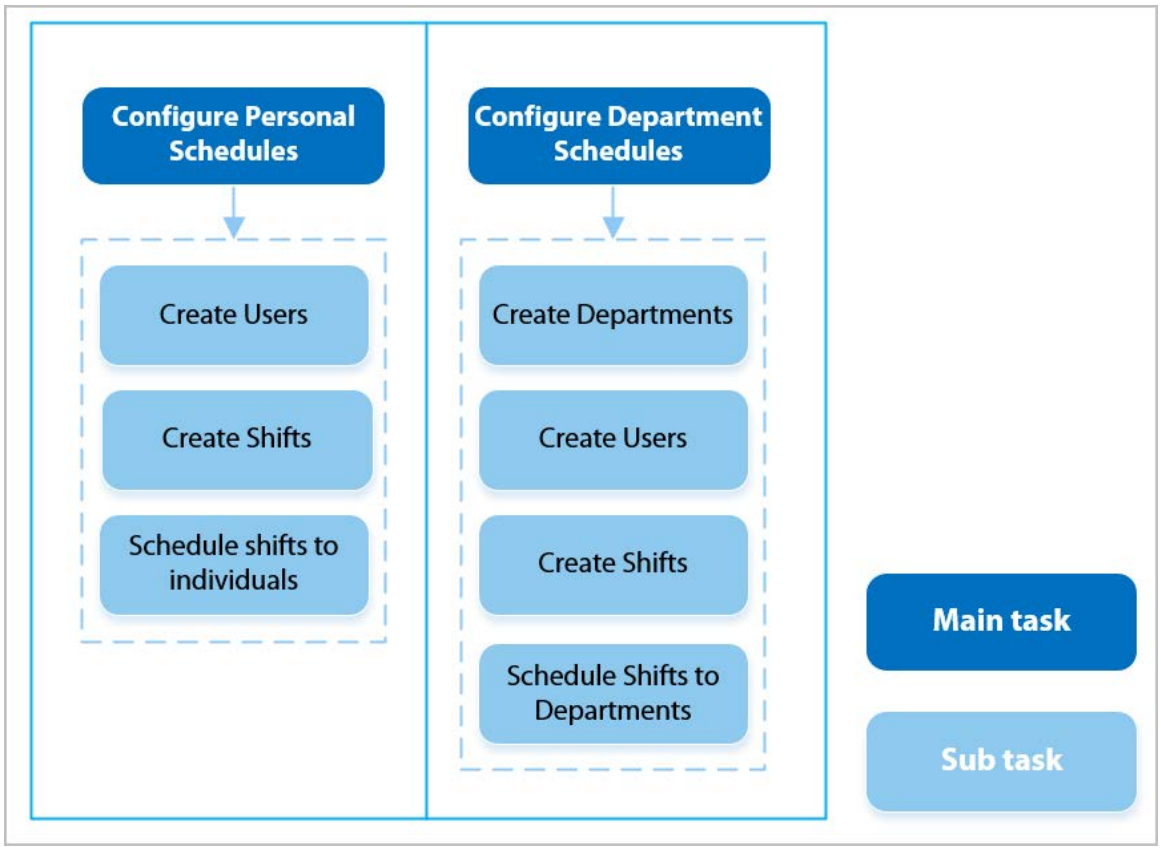
2.9.4 Configuración de horarios de trabajo

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. Puedes crear diferentes tipos de horarios de trabajo según 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 los horarios personales o los horarios departamentales.

Figura 2-13 Configuración de horarios de trabajo



Procedimiento

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

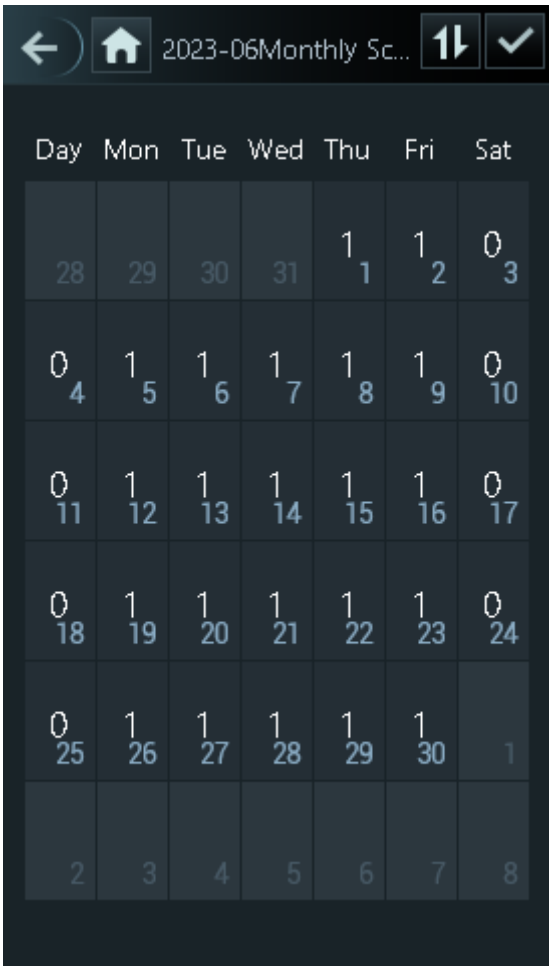
Paso 2 Establecer horarios de trabajo para personas individuales.

1. Toque**Horario personal**.
2. Ingrese el ID de usuario y luego toque ✔
3. En el calendario, seleccione un día y, a continuación, seleccione un turno. El turno queda programado para ese día.

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

- 0 indica ruptura.
- Del 1 al 24 se indica el número de turnos definidos previamente. Para saber cómo configurar los turnos, ver "2.9.2 Configuración de turnos".
- 25 indica viaje de negocios.
- 26 indica licencia por ausencia.

Figura 2-14 Horarios de turnos para personas individuales



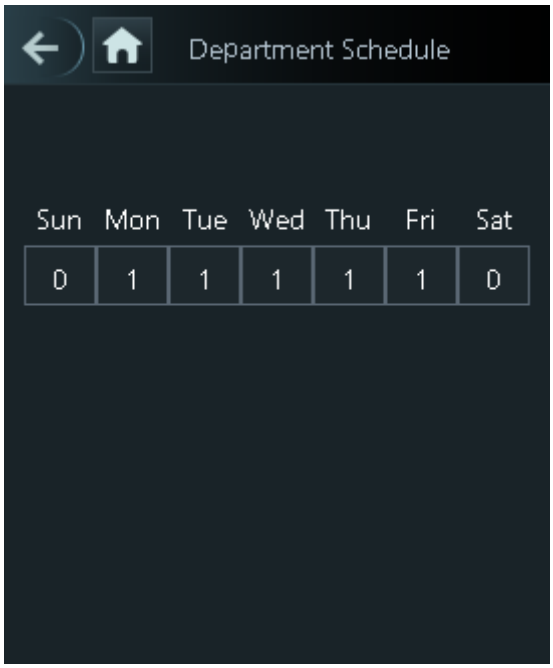
4. Toque

Paso 3 Establecer horarios de trabajo para los departamentos. 1. Toque**Horario del Departamento**.

2. Toque un departamento y luego seleccione los turnos para una semana. Los turnos se programan para la semana.

- 0 indica descanso.
- Del 1 al 24 se indica la cantidad de turnos definidos previamente. Para saber cómo configurar los turnos, consulte "2.9.2 Configuración de turnos".
- 25 indica viaje de negocios.
- 26 indica licencia por ausencia.

Figura 2-15 Programar turnos para un departamento



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

Paso 4 Grifo .

2.9.5 Configuración del intervalo de tiempo de verificación

Cuando un empleado registra su entrada y salida varias veces dentro de un período determinado, el horario más antiguo será válido.

Procedimiento

Paso 1 Seleccionar**Asistencia**>**Intervalo de verificación (seg.)**

Paso 2 Ingrese el intervalo de tiempo y luego toqu

2.9.6 Configuración de modos de asistencia

Al registrar 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, seleccione**Asistencia**>**Configuración de**

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

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

Figura 2-16 Modo de asistencia

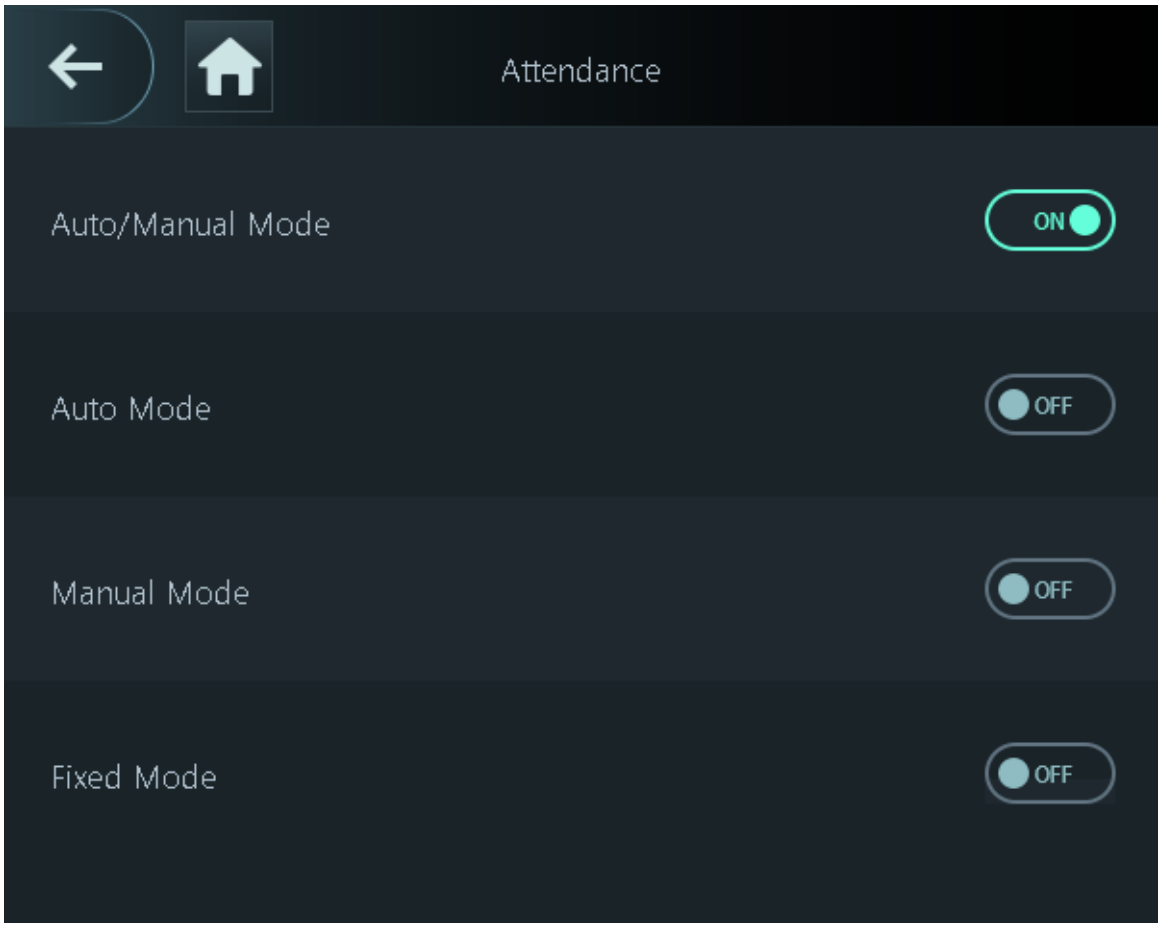


Tabla 2-8 Modalidad de asistencia

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 al registrar su entrada o salida.
Modo fijo	Al registrar su entrada o salida, la pantalla mostrará el estado de asistencia definido previamente en todo momento.

Paso 3 Seleccione un modo de asistencia.

Paso 4 Configure los parámetros para el modo de asistencia.

Figura 2-17 Modo automático/modo manual

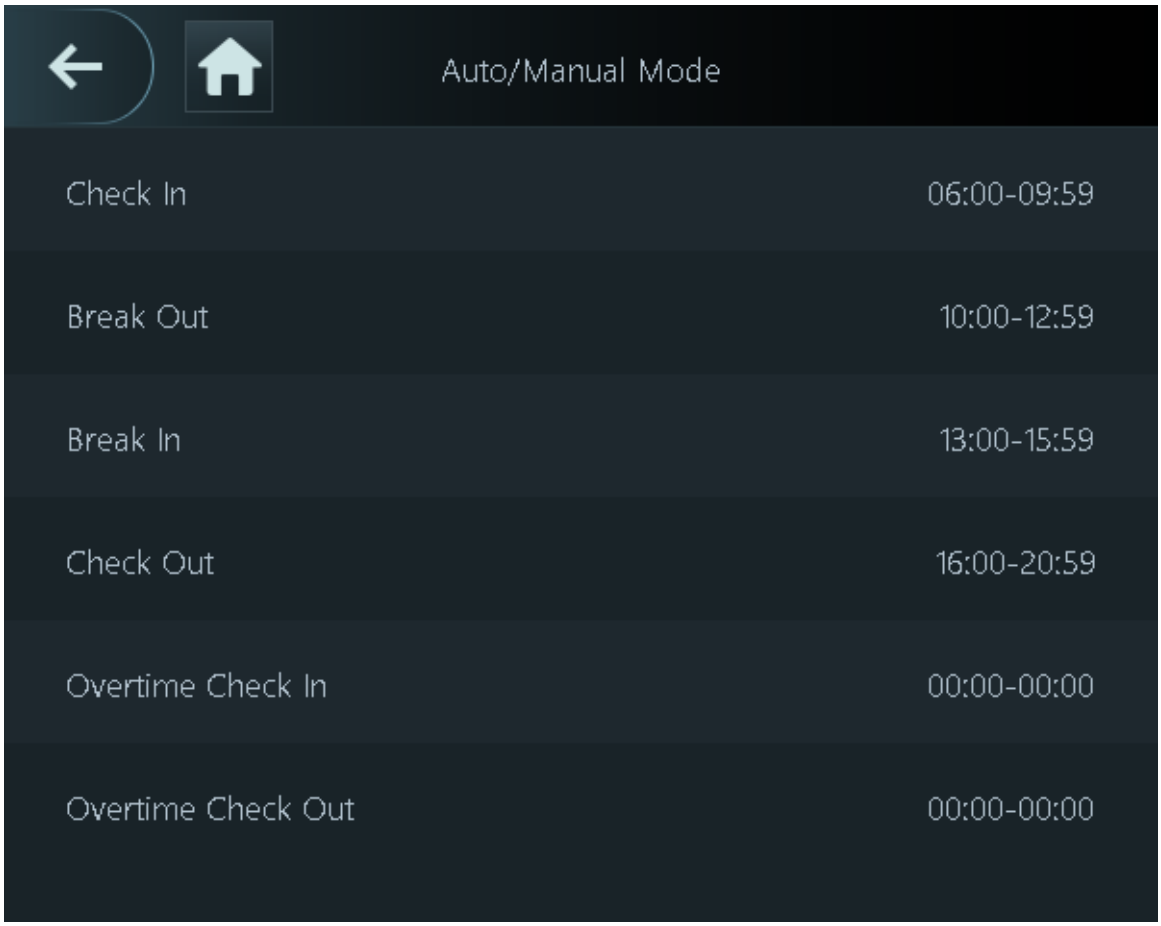


Figura 2-18 Modo fijo

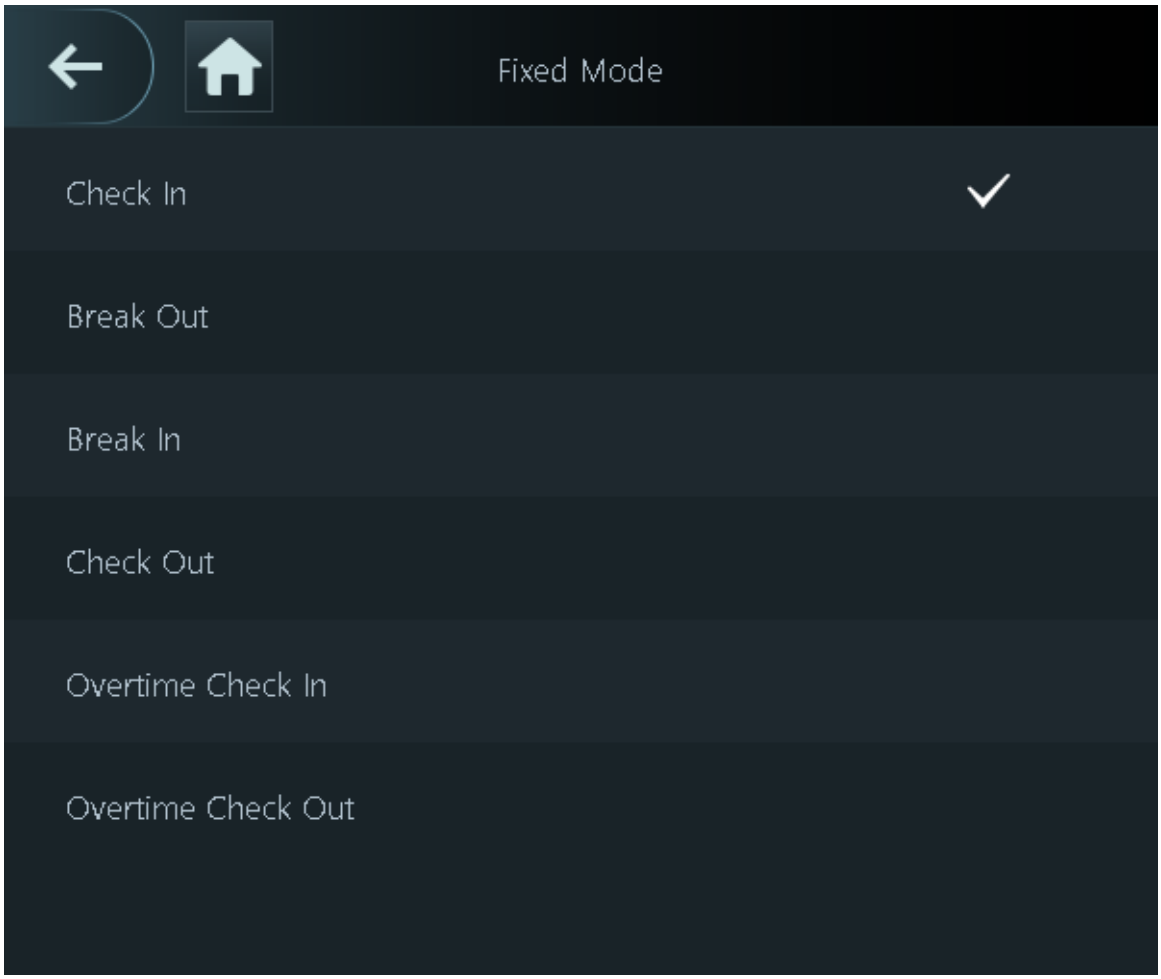


Tabla 2-9 Parámetros del modo de asistencia

Parámetros	Descripción
Registrarse	Fiche su entrada cuando comience su jornada laboral normal.
Fugarse	Marque su salida cuando comience su descanso.
Interrumpir	Ficha el momento en que finaliza tu descanso.
Verificar	Marque su salida cuando comience su jornada laboral normal.
Registro de horas extras	Registre el momento en que comienza su período de horas extras.
Salida de horas extras	Marque su salida cuando finalice su período de horas extra.

2.10 Comunicación en red

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

El puerto serie y el puerto wiegand pueden diferir según los modelos de controlador de acceso.

2.10.1 Configuración de la dirección IP

Establezca una dirección IP para el controlador de acceso para conectarlo a la red. Luego, podrá iniciar sesión en la página web y en la plataforma de administración para administrar el controlador de acceso.

Procedimiento

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

Paso 2 la dirección IP.

Figura 2-19 Configuración de la dirección IP

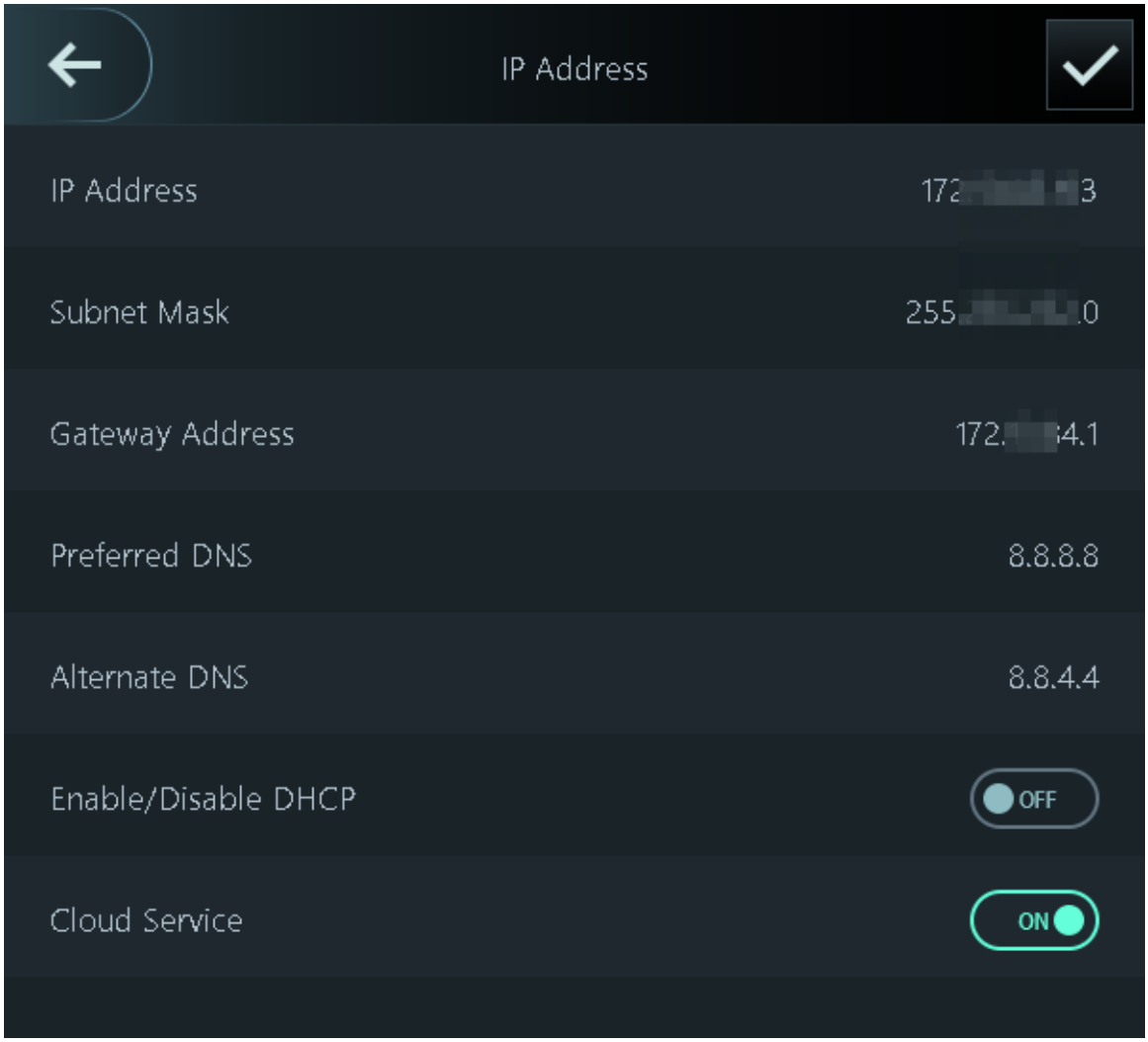


Tabla 2-10 Parámetros de configuración de IP

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

Parámetro	Descripción
Habilitar/Deshabilitar DHCP	Significa Protocolo de configuración dinámica de host. Cuando se activa DHCP, al controlador de acceso se le asignará automáticamente una dirección IP, una máscara de subred y una puerta de enlace.
Servicio en la nube	Administre dispositivos sin solicitar DDNS, configure el mapeo de puertos e implemente servidores de tránsito.

2.10.2 Configuración del registro activo

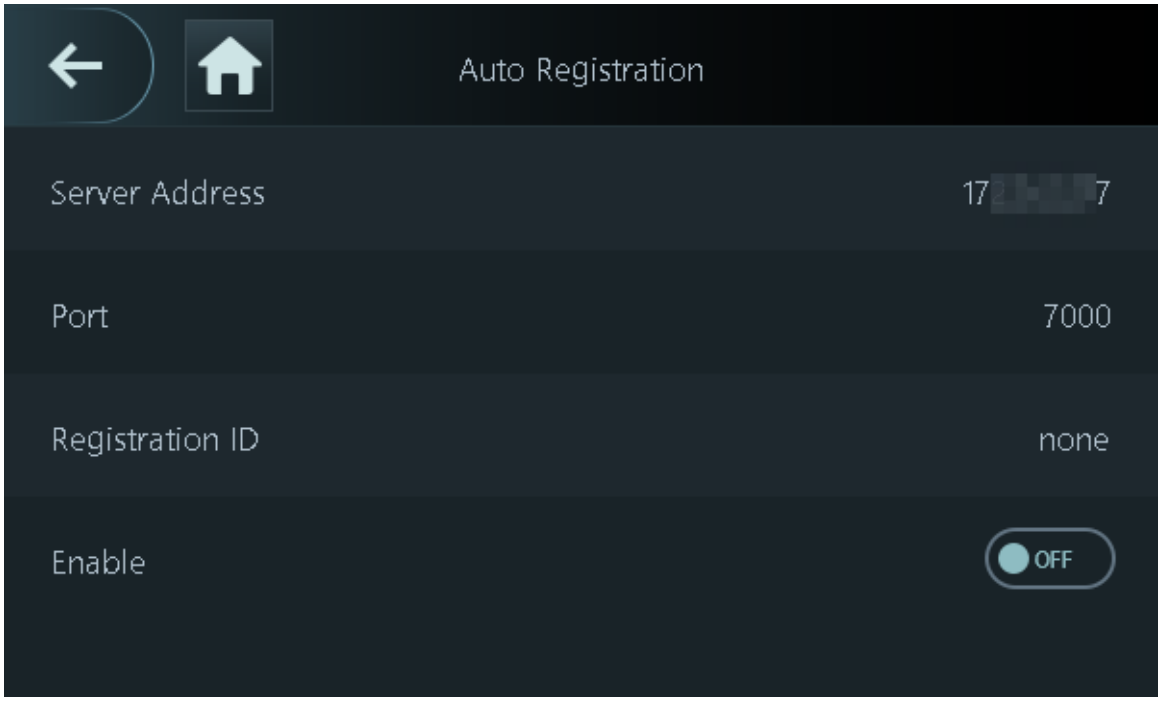
Agregue el dispositivo a una plataforma de administración, para que pueda administrarlo en la plataforma.

Procedimiento

Paso 1 En el**Menú principal**, seleccionar**Comunicación**>**Red**>**Registro automático**.

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

Figura 2-20 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.

Parámetro	Descripción
ID de registro	Introduzca el ID del dispositivo (definido por el usuario). Cuando agrega el controlador de acceso a la plataforma de administración, el ID de registro que ingresa en la plataforma de administración debe coincidir con el ID de registro definido en el controlador de acceso.

Paso 3 Habilitar la función.

2.10.3 Configuración del Wi-Fi

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

Procedimiento

Paso 1 En el**Menú principal**, seleccionar**Comunicación**>**Red**>**Wifi**.

Paso 2 Encienda el Wi-Fi.

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

Paso 3 Grifo para buscar redes inalámbricas disponibles.

Paso 4 Seleccione una red inalámbrica e ingrese la contraseña.

Si el sistema no encuentra una red Wi-Fi, toque**SSID**Para introducir el nombre de la red Wi-Fi,

Paso 5 pulsa

2.10.4 Configuración del puerto serie

Procedimiento

Paso 1 En el**Menú principal**, seleccionar**Configuración de comunicación**>**Puerto serial**. Seleccione un

Paso 2 tipo de puerto.

Tabla 2-12 Descripción del puerto

Dispositivo externo	Descripción
Controlador de acceso	Seleccionar**Controlador de acceso**cuando el controlador de acceso funciona como un lector de tarjetas, y el controlador de acceso enviará datos al controlador de acceso para controlar el acceso. Tipo de datos de salida: ● Número de tarjeta: genera datos basados en el número de tarjeta cuando los usuarios pasan sus tarjetas para desbloquear puertas; genera datos basados en el primer número de tarjeta del usuario cuando los usuarios usan otros métodos de desbloqueo. ● No.: Genera datos en función del ID del usuario.
Lector de tarjetas	El controlador de acceso se conecta a un lector de tarjetas.
Lector (OSDP)	El controlador de acceso está conectado a un lector de tarjetas basado en el protocolo OSDP.

Dispositivo externo	Descripción
Módulo de seguridad para control de puertas	El botón de salida de la puerta, el control de bloqueo y el enlace contra incendios dejan de ser efectivos después de habilitar el módulo de seguridad.
Torniquete	Cuando el controlador de acceso está conectado a un torniquete, y la placa del controlador de acceso del torniquete está conectada a un módulo de código QR externo o un módulo de deslizamiento de tarjeta, la placa transmitirá los datos de verificación al torniquete.

2.10.5 Configuración de Wiegand

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

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

Figura 2-21 Salida Wiegand

Tabla 2-13 Descripción de la salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	Seleccione un formato Wiegand para leer números de tarjeta o números de identificación. ● **Wiegand26**:Lee 3 bytes o 6 dígitos. ● **Wiegand34**:Lee 4 bytes u 8 dígitos. ● **Wiegand66**:Lee 8 bytes o 16 dígitos.
Ancho de pulso	Introduzca el ancho de pulso y el intervalo de pulso de la salida Wiegand.

Parámetro	Descripción
Intervalo de pulso	
Tipo de datos de salida	Seleccione el tipo de datos de salida. ● **No.**:El sistema genera datos en función del ID del usuario. El formato de los datos es hexadecimal o decimal. ● **Número de tarjeta**:El sistema genera datos basados en el primer número de tarjeta del usuario.

Paso 3 Hacer clic**Aplicar**.

2.11 Configuración del sistema

2.11.1 Configuración de la hora

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

Procedimiento

Paso 1 En el**Menú principal**, seleccionar**Configuración del sistema**>**Tiempo**.

Paso 2 Configurar la hora del sistema.

Figura 2-22 Tiempo

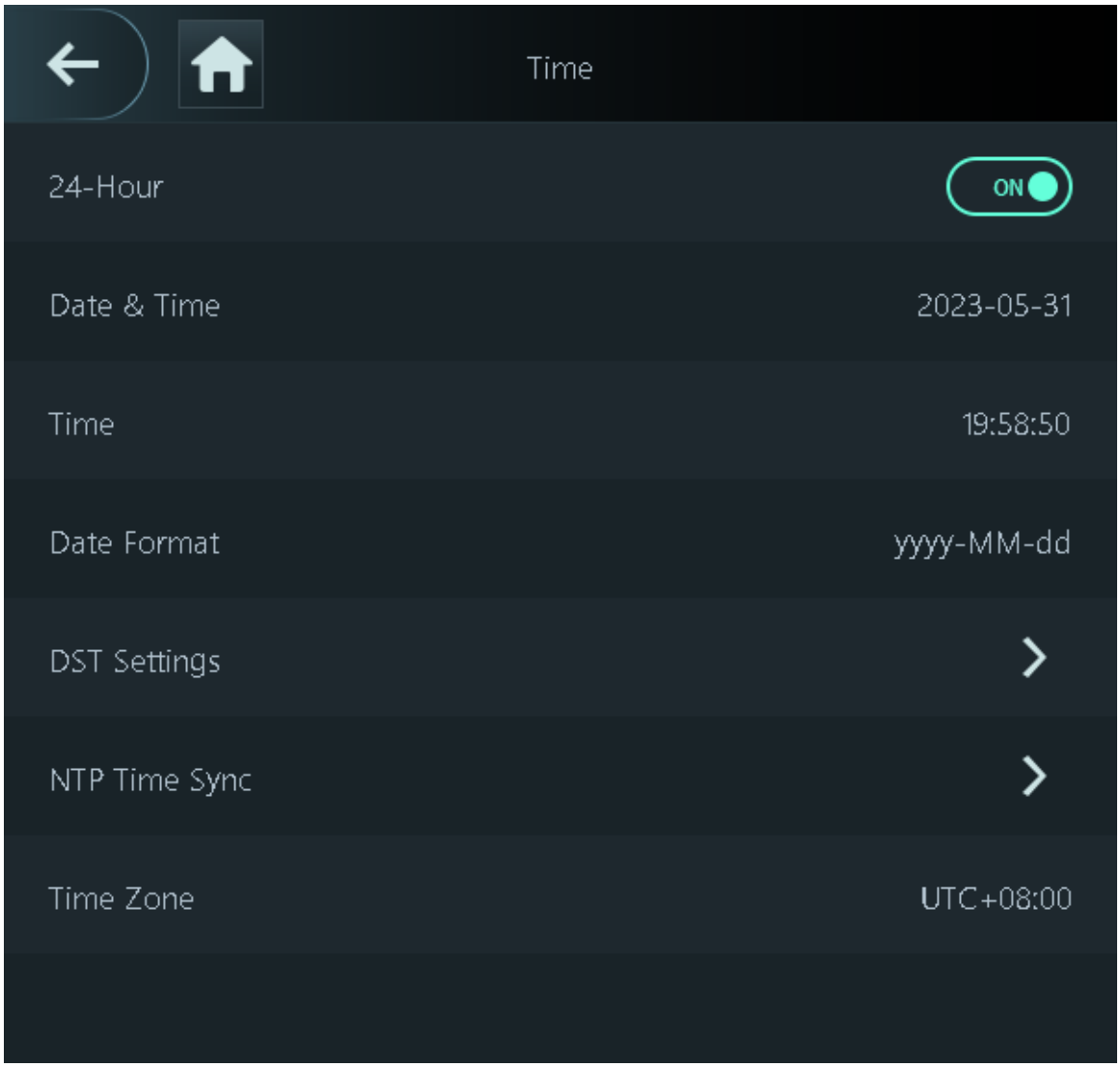


Tabla 2-14 Descripción de los parámetros de tiempo

Parámetro	Descripción
Sistema de 24 horas	La hora se muestra en formato de 24 horas.
Fecha y hora	Establecer la fecha.
Tiempo	Establezca la hora.
Formato de fecha	Seleccione un formato de fecha.
Configuración del horario de verano	1. Toque**Configuración del horario de verano**y habilitarlo. 2. Seleccionar**Fecha**o**Semana**desde**Horario de verano**Lista de tipos. 3. Introduzca la hora de inicio y la hora de finalización. 4. Toque✓

Parámetro	Descripción
Sincronización horaria NTP	Un servidor de protocolo de hora de red (NTP) es una máquina dedicada a funcionar como servidor de sincronización horaria para todos los equipos cliente. Si su equipo está configurado para sincronizarse con un servidor horario de la red, su reloj mostrará la misma hora que el servidor. Cuando el administrador cambia la hora (para el horario de verano), también se actualizan todos los equipos cliente de la red. 1. Toque**Comprobación NTP**y luego habilítelo. 2. Configure los parámetros. ● **Dirección del servidor**:Ingrese la dirección IP del servidor NTP y el controlador de acceso sincronizará automáticamente la hora con el servidor NTP. ● **Puerto**:Introduzca el puerto del servidor NTP. ● **Intervalo**:Introduzca el intervalo de sincronización horaria.
Huso horario	Seleccione la zona horaria.

2.11.2 Configuración de parámetros faciales

Procedimiento

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

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

Figura 2-23 Parámetro de rostro (01)

Tabla 2-15 Descripción de los parámetros del rostro

Nombre	Descripción
Umbral de reconocimiento facial	Ajuste el nivel de precisión del reconocimiento facial. Un umbral más alto significa mayor precisión y menor tasa de reconocimiento falso.
Desviación máxima del ángulo de reconocimiento facial	Establezca el ángulo más grande en el que se puede colocar un rostro para su detección. Cuanto mayor sea el valor, mayor será el rango del ángulo del rostro. Si el ángulo en el que se coloca un rostro no está dentro del rango definido, es posible que no se detecte correctamente.
Distancia pupilar	Para que el reconocimiento sea exitoso, se requiere una cierta cantidad de píxeles entre los ojos, llamada distancia pupilar. La cantidad predeterminada es 45 píxeles. Esta cantidad varía según el tamaño de la cara y la distancia entre la cara y la lente. Si un adulto está a 1,5 metros de la lente, la distancia pupilar suele ser de 50 a 70 píxeles.
Intervalo de cara válido (seg.)	Cuando se verifica con éxito el rostro de una persona demasiadas veces, Access Controller indica que la verificación fue exitosa dentro del intervalo de tiempo definido.
Intervalo de cara no válido (seg.)	Cuando una persona no logra verificar su rostro demasiadas veces, Access Controller indica que la verificación falló dentro del intervalo de tiempo definido.
Habilitar anti-spoofing	Esto evita que las personas puedan usar fotos, vídeos, máscaras y otros sustitutos para obtener acceso no autorizado.
Habilitar embellecedor	Embellece las imágenes de rostros capturadas.
Habilitar detección de casco	Detecta cascos de seguridad. La puerta no se desbloqueará si la persona no lleva casco.
Parámetros de la máscara	● Modo máscara: ◇ **No detectar**:La máscara no se detecta durante el reconocimiento facial. ◇ **Recordatorio de uso de mascarilla**:Se detecta la mascarilla durante el reconocimiento facial. Si la persona no lleva mascarilla, el sistema le recordará que se la ponga, pero se le permitirá el acceso. ◇ **Sin autorización sin uso de mascarilla**:Se detecta la mascarilla durante el reconocimiento facial. Si una persona no lleva mascarilla, el sistema le recordará que debe usarla y le negará el acceso. ● Umbral de reconocimiento de mascarilla: cuanto mayor sea el umbral, más preciso será el reconocimiento facial cuando una persona lleve mascarilla y habrá una menor tasa de reconocimiento falso.

Nombre	Descripción
Reconocimiento de múltiples caras	Detecta de 4 a 6 imágenes de rostros a la vez. No se puede utilizar el desbloqueo con combinación con este dispositivo y la puerta se desbloqueará cuando una de las personas se verifique correctamente.  La cantidad de imágenes de rostros admitidas puede variar según el modelo del producto.
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.

2.11.3 Ajuste del volumen

Puede ajustar el volumen del altavoz y del micrófono.

Procedimiento

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

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

2.11.4 Configuración del idioma

Cambie el idioma en el controlador de acceso.**Menú principal**, seleccionar**Configuración del sistema**> **Idioma**, seleccione el idioma para el controlador de acceso.

2.11.5 Configuración de pantalla

Configure cuándo debe apagarse la pantalla y la hora de cierre de sesión.

Procedimiento

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

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

- Tiempo de cierre de sesión: el sistema vuelve a la pantalla de espera después de un tiempo definido de inactividad.
- Configuración de apagado de pantalla: el sistema vuelve a la pantalla de espera y luego la pantalla se apaga después de un tiempo de inactividad definido. 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 apaga después de otros 15 segundos.

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

2.11.6 (Opcional) Configuración de parámetros de huellas dactilares

Configure la precisión de 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 seleccionados y algunos admiten la conexión a una huella digital. módulo de extensión.

Procedimiento

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

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

2.11.7 Restauración de los valores predeterminados de fábrica

Procedimiento

Paso 1 En el**Menú principal**, seleccionar**Configuración del sistema**>**Valores predeterminados de fábrica**.

Paso 2 Si es necesario, restablezca los valores predeterminados de fábrica. Si es necesario, restablezca la configuración predeterminada de fábrica.

- **Valores predeterminados 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 del usuario y los registros)**:Restablece todas las configuraciones excepto la información del usuario y los registros.

2.11.8 Reinicio del dispositivo

En el**Menú principal**, seleccionar**Configuración del sistema**>**Reanudar**y se reiniciará el controlador de acceso.

2.12 Configuración de funciones

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

Las funciones pueden variar según el modelo del producto.

Figura 2-24 Funciones

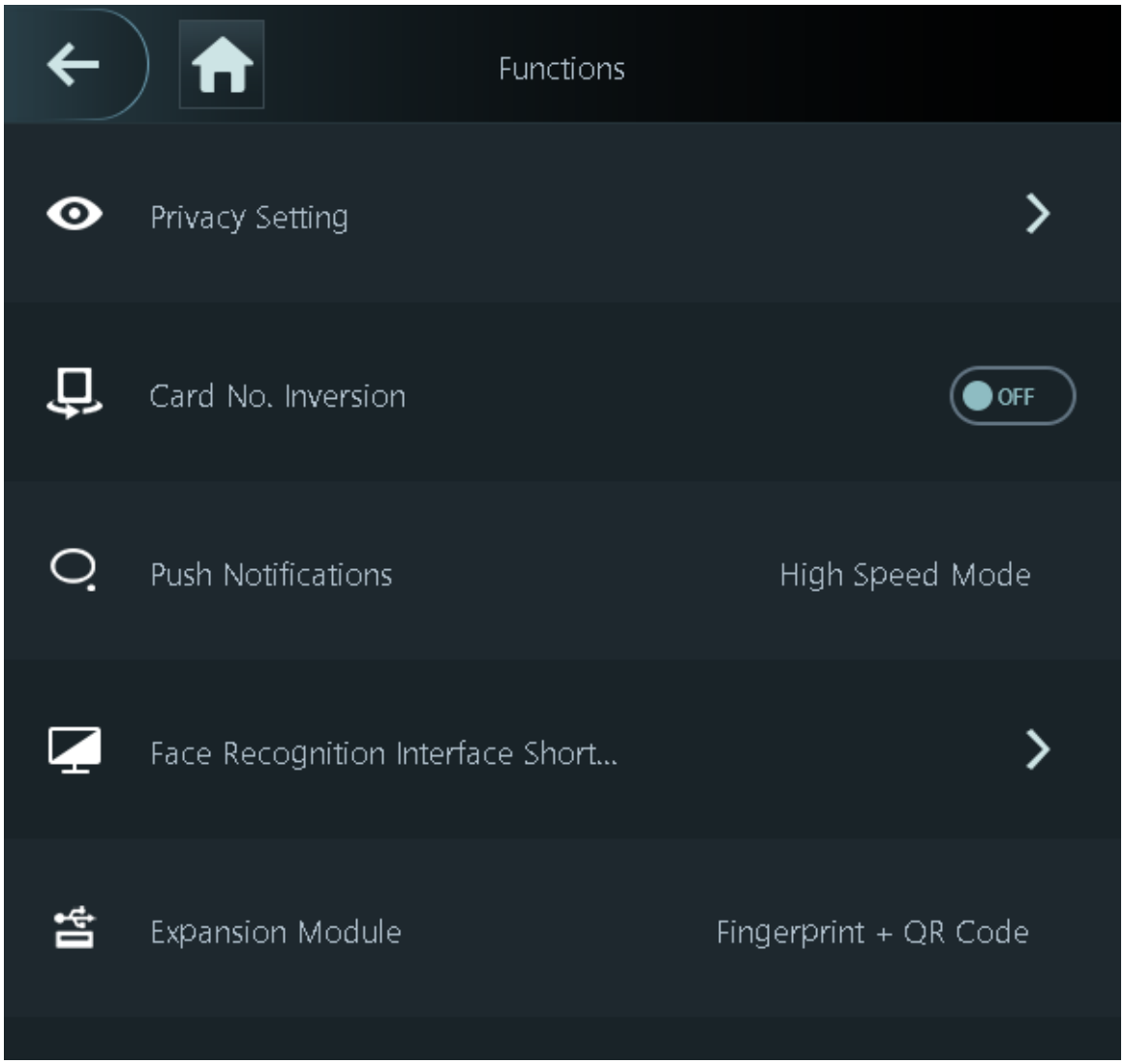


Tabla 2-16 Descripción de funciones

Parámetro	Descripción
Configuración privada	● Restablecimiento de 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, se utilizará HTTPS para acceder a los comandos CGI; de lo contrario, se utilizará HTTP.  Cuando HTTPS está habilitado, el controlador de acceso se reiniciará automáticamente. ● Habilitar CGI: Common Gateway Interface (CGI) ofrece un protocolo estándar para que los servidores web ejecuten programas de forma similar a cómo se ejecutan las aplicaciones de consola en un servidor que genera páginas web de forma dinámica. La interfaz de puerta de enlace común (CGI) está habilitada de forma predeterminada. ● Habilitar SSH: Secure Shell (SSH) es un protocolo de red criptográfico para operar servicios de red de forma segura en una red no segura. Los datos transmitidos se cifrarán después de habilitar esta función. ● Imagen de huella dactilar: La imagen de huella dactilar se muestra cuando desbloquea mediante huella dactilar.  Esta función solo está disponible en modelos seleccionados. ● Capturar: Las imágenes de los rostros se capturarán automáticamente cuando las personas abran la puerta. La función está habilitada de manera predeterminada. ● Borrar todas las instantáneas: elimina todas las fotos capturadas automáticamente.
Tarjeta N° Inversión	Cuando el controlador de acceso se conecta a un dispositivo de terceros a través del puerto de entrada Wiegand y el número de tarjeta leído por el controlador de acceso está en orden inverso al número de tarjeta real, puede activar esta función.

Parámetro	Descripción
Notificaciones push	Muestra la notificación en la pantalla cuando una persona está verificando su identidad en el controlador de acceso. ● Modo de alta velocidad: el sistema le indica**Verificado exitosamente**o**No autorizado**en la pantalla. ● Modo simple: muestra el ID del usuario, el nombre y el tiempo de verificación después de conceder el acceso, y muestra**No autorizado**y el tiempo de autorización después de que se deniega el acceso. ● Estándar: muestra la imagen del rostro registrado del usuario, la identificación del usuario, el nombre y el tiempo de verificación después de conceder 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 el tiempo de autorización después de que se otorga el acceso, y muestra**No autorizado**después de que se deniega el acceso.
Acceso directo a la interfaz de reconocimiento facial	Seleccione los 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. ● Timbre: Su icono se muestra en la pantalla de espera. ◇ Timbre: Toque el ícono de timbre en la pantalla de espera y el controlador de acceso sonará. ◇ Alarma: toque el ícono de campana y sonará el dispositivo de alarma externo. Esta función solo está disponible en modelos seleccionados. ◇ Configuración de tono de llamada: seleccione un tono de llamada ◇ Duración del tono de llamada (seg): configure el tiempo de llamada (entre 1 y 30 segundos). El valor predeterminado es 3. ● Llamada: Su icono se muestra en la pantalla de espera. ● Tipo de llamada: ◇ Sala de llamada: 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. Asegúrese de que el controlador de acceso se haya agregado a DMSS. ● Habilitar SIP: puede activar SIP para configurar el controlador de acceso como servidor SIP.

Parámetro	Descripción
Módulo de expansión	Seleccione un módulo de expansión y el controlador de acceso se reiniciará. ● Se muestra en la esquina derecha de la pantalla de espera, lo que significa que se configuró correctamente. ● Se muestra en la esquina derecha de la pantalla de espera, lo que significa que la configuración falló. ● El módulo de expansión solo está disponible en modelos seleccionados. ● El módulo de expansión no admite intercambio en caliente. ● La configuración para el módulo de expansión permanece sin cambios incluso después de que el sistema se restaure a su configuración de fábrica.

2.13 Gestión USB

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

- Asegúrese de que haya un USB insertado en el controlador de acceso antes de exportar datos o actualizar el Sistema. Para evitar fallas, no extraiga el USB ni realice ninguna operación del Access Controlador durante el proceso.
- Debes utilizar un USB para exportar la información de un controlador de acceso a otros dispositivos. Cara No se permite importar imágenes a través de USB.
- La importación/exportación de registros de asistencia solo está disponible en algunos modelos.

2.13.1 Exportación a USB

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

Procedimiento

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

Paso 2 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.

2.13.2 Importación desde USB

Puede importar datos desde USB al controlador de acceso.

Procedimiento

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

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

2.13.3 Actualización del sistema

Actualizar el sistema del Controlador de Acceso 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 controlador de acceso.

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

Paso 3 **ACUERDO**.

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

No apague el controlador de acceso durante la actualización.

2.14 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.

2.15 Información del sistema

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

2.15.1 Visualización de la capacidad de datos

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

2.15.2 Visualización de la versión del dispositivo

En 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.

3 Operaciones web

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

Las configuraciones web difieren según los modelos del controlador de acceso.

3.1 Inicialización

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

Prerrequisitos

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

Procedimiento

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

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

Paso 2 Seleccione un idioma en el controlador de acceso.

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

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

3.2 Iniciar sesión

Procedimiento

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

Paso 2 Introduzca el nombre de usuario y la contraseña.

- El nombre de administrador predeterminado es admin y la contraseña es la que usted configura. Durante la inicialización, le recomendamos que cambie la contraseña de administrador periódicamente. Para aumentar la seguridad.
- Si olvida la contraseña de inicio de sesión del administrador, puede hacer clic en**¿Olvidaste tu contraseña?**Para detalles,

Paso 3 Hacer clic**Acceso**.

3.3 Restablecimiento de la contraseña

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

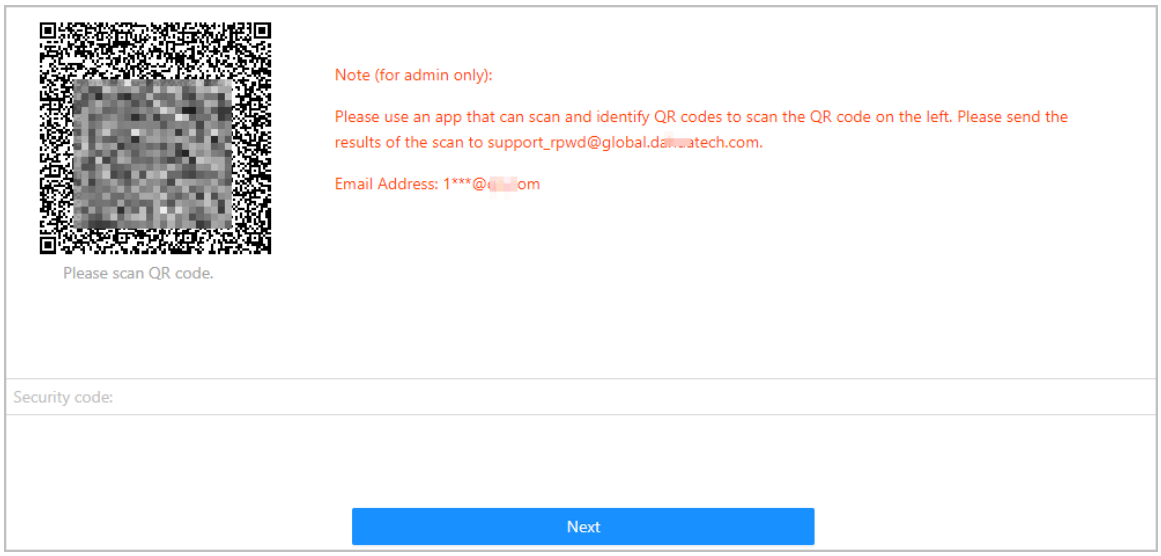
Procedimiento

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

Paso 2 Lea atentamente las instrucciones que aparecen en la pantalla y luego haga clic

Paso 3 en**DE 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 El código de seguridad deja de ser válido, actualice el código QR y escanéelo nuevamente.
- Después de escanear el código QR, recibirás un código de seguridad en tu correo electrónico vinculado. Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, se le enviará un correo electrónico. se vuelve inválido.
- Si se ingresa el código de seguridad incorrecto 5 veces seguidas, la cuenta de administrador será eliminada. congelado durante 5 minutos.

Paso 4 Introduzca el código de seguridad.

Paso 5 Haga clic en**Próximo**.

Paso 6 Restablecer y confirmar la contraseña.

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

Paso 7 Hacer clic**DE ACUERDO**.

3.4 Página de inicio

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

Figura 3-2 Página de inicio

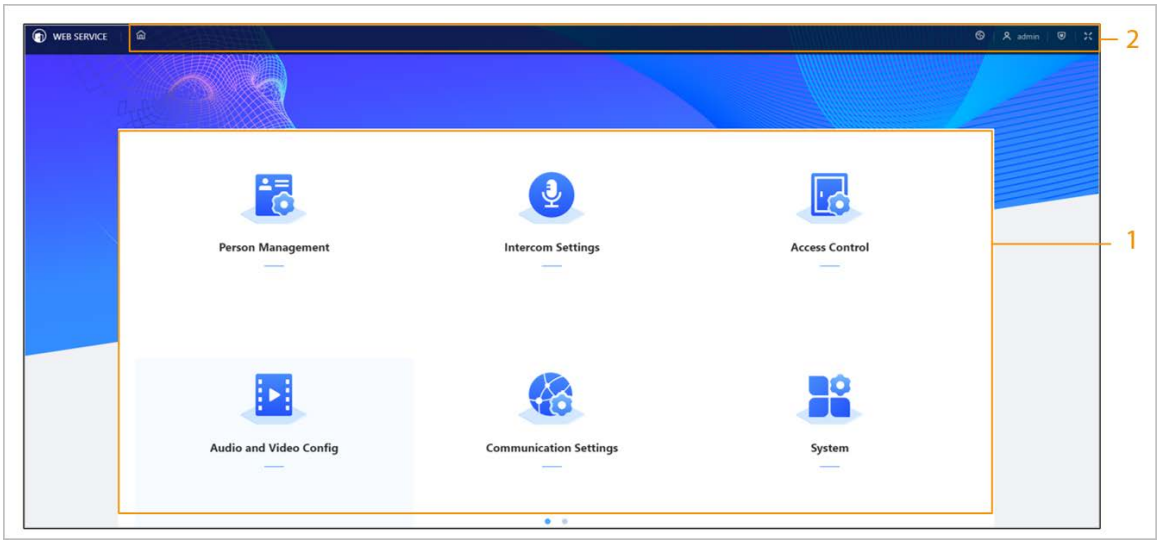


Tabla 3-1 Descripción de la página de inicio

No.	Descripción
1	Menú principal.
2	• :Ingresa a la página de inicio. • :Mostrar en pantalla completa. • :Ingresa el**Seguridad**página. • admin:Cierre la sesión o reinicie el dispositivo. • :Seleccione un idioma en el dispositivo.

3.5 Agregar usuarios

Procedimiento

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

Paso 2 Configurar la información del usuario.

Figura 3-3 Agregar usuarios

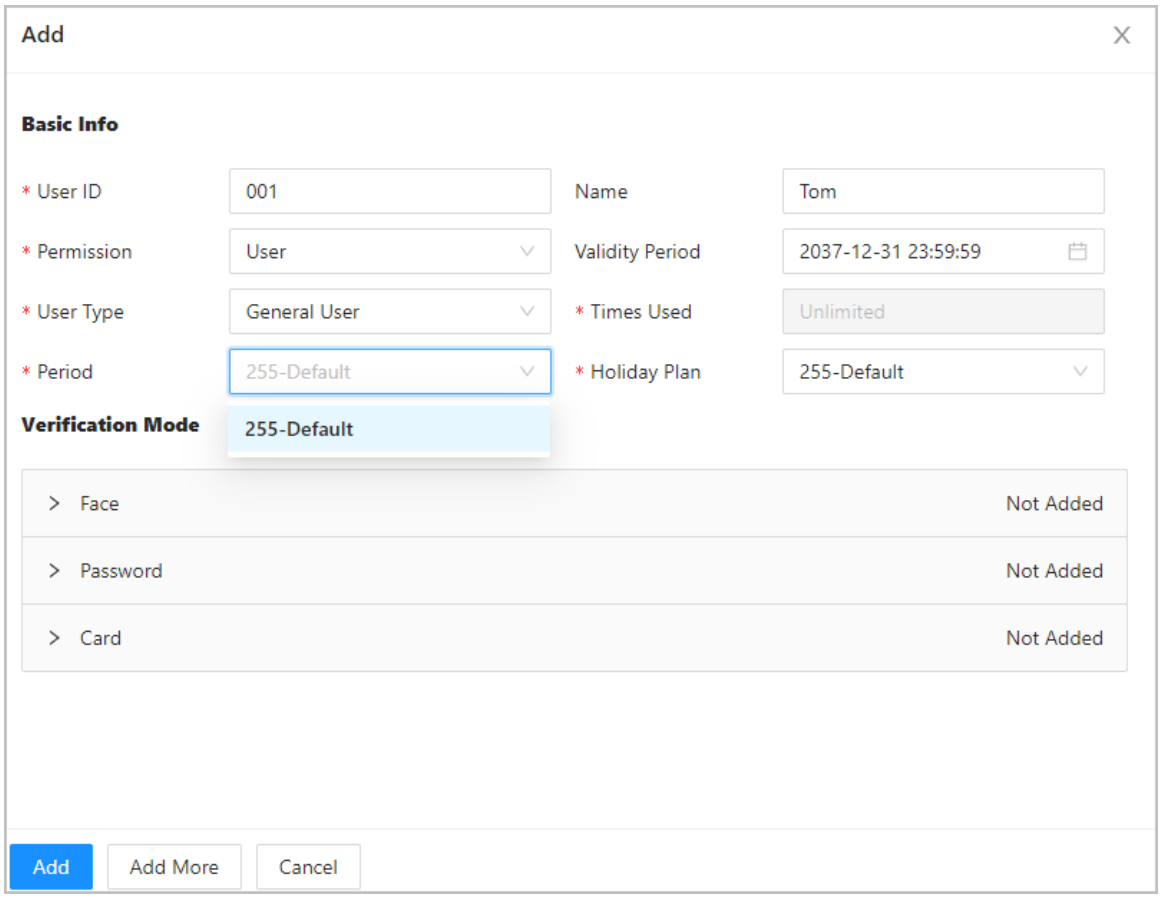


Tabla 3-2 Descripción de parámetros

Parámetro	Descripción
ID de usuario	El ID de usuario es como el ID de empleado, que puede ser números, letras y sus combinaciones, y la longitud máxima del número es de 32 caracteres.
Nombre	El nombre puede tener hasta 30 caracteres (incluidos números, símbolos y letras).
Permiso	● **Usuario**:Los usuarios solo tienen permisos de acceso a puertas o de control de asistencia. ● **Administración**:Los administradores pueden configurar el controlador de acceso además del acceso a la puerta y los permisos de asistencia.
Periodo de validez	Establecer una fecha en la que caducarán los permisos de acceso a la puerta y de asistencia de la persona.

Parámetro	Descripción
Tipo de usuario	● **Usuario general**:Los usuarios generales pueden desbloquear la puerta. ● **Usuario de la lista negra**: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 que expire el período definido o se agote el tiempo de desbloqueo, no podrán desbloquear la puerta. ● **Usuario de patrulla**:Los usuarios de patrulla pueden tomar asistencia en el controlador de acceso, pero no tienen puerta. permisos. ● **Usuario VIP**:Cuando el VIP desbloquee la puerta, el personal de servicio recibirá un aviso. ● **Otro usuario**:Cuando desbloqueen la puerta, ésta permanecerá desbloqueada durante 5 segundos más. ● Usuario personalizado 1/Usuario personalizado 2: Lo mismo que los usuarios generales.
Tiempo utilizado	Establezca un límite de desbloqueo para los usuarios invitados. Una vez que se agote el tiempo de desbloqueo, no podrán desbloquear la puerta.
Período	Las personas pueden desbloquear la puerta o tomar asistencia durante el período definido.
Plan de vacaciones	Las personas pueden desbloquear la puerta o tomar asistencia durante el período definido.
Rostro	Hacer clic**Subir**para subir una imagen de rostro. Cada persona solo puede agregar hasta 2 imágenes de rostro. Puedes ver o eliminar la imagen de rostro después de subirla.  La imagen del rostro es jpg y debe tener menos de 100 KB.

Parámetro	Descripción
Tarjeta	● Introduzca el número de tarjeta manualmente. 1. Haga clic**Agregar**. 2. Ingrese el número de tarjeta y luego haga clic en**Agregar**. ● Lee el número automáticamente a través de un lector de tarjetas. 1. Asegúrese de que el lector de tarjetas esté conectado a su computadora. 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 tarjeta automáticamente. Si la cuenta regresiva de 60 segundos expira, haga clic en**Leer tarjeta**de nuevo 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 deslícela y luego el controlador de acceso leerá la información de la tarjeta. Puedes habilitar el**Tarjeta de coacción**Función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta. ● :Establecer tarjeta de coacción. ● :Cambiar número de tarjeta. Un usuario sólo puede configurar una tarjeta de coacción.
Contraseña	Introduzca 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.
FP	Registrar huellas dactilares. Un usuario puede registrar hasta 3 huellas dactilares y puede configurar una huella dactilar como huella de coacción. Se activará una alarma cuando se use la huella dactilar de coacción para desbloquear la puerta. ● La función de huella dactilar solo está disponible en algunos modelos modelos. ● No recomendamos que configure la primera huella digital como La huella de la coacción. ● Un usuario solo puede configurar una huella digital de coacción. ● La función de huella dactilar está disponible si el acceso El controlador admite la conexión de un módulo de huellas dactilares.
Departamento	Agregar usuarios a un departamento. Si el cronograma de un departamento es

Parámetro	Descripción
Modo de programación	Asignados a la persona, estos seguirán el horario establecido del departamento. Para saber cómo crear un departamento, consulte "2.9.1 Configuración de departamentos". ● Horario de departamento: asigne un horario de departamento al usuario. Para obtener más información, consulte "2.9.4 Configuración de horarios de trabajo". ● Horario personal: asigne un horario personal al usuario. Para obtener más información, consulte "2.9.4 Configuración de horarios de trabajo".  ◇ Esta función solo está disponible en modelos seleccionados. ◇ Si configura el modo de programación en departamento agenda aquí, la agenda personal que tienes configurado para el usuario en**Asistencia**>**Configuración de programación**>**Horario personal**no es válido.

Paso 3 Hacer clic**DE ACUERDO**.

Operaciones relacionadas

- Importar información del usuario: Haga clic en**Plantilla de exportación**, 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 del usuario** para importar la carpeta.

  Se pueden importar hasta 10.000 usuarios a la vez.
- Borrar: Borrar todos los usuarios.

3.6 Configuración del intercomunicador

El controlador de acceso puede funcionar como una estación de puerta para realizar intercomunicación con vídeo.

La función de intercomunicador solo está disponible en modelos seleccionados.

3.6.1 Uso del dispositivo como servidor SIP

3.6.1.1 Configuración del servidor SIP

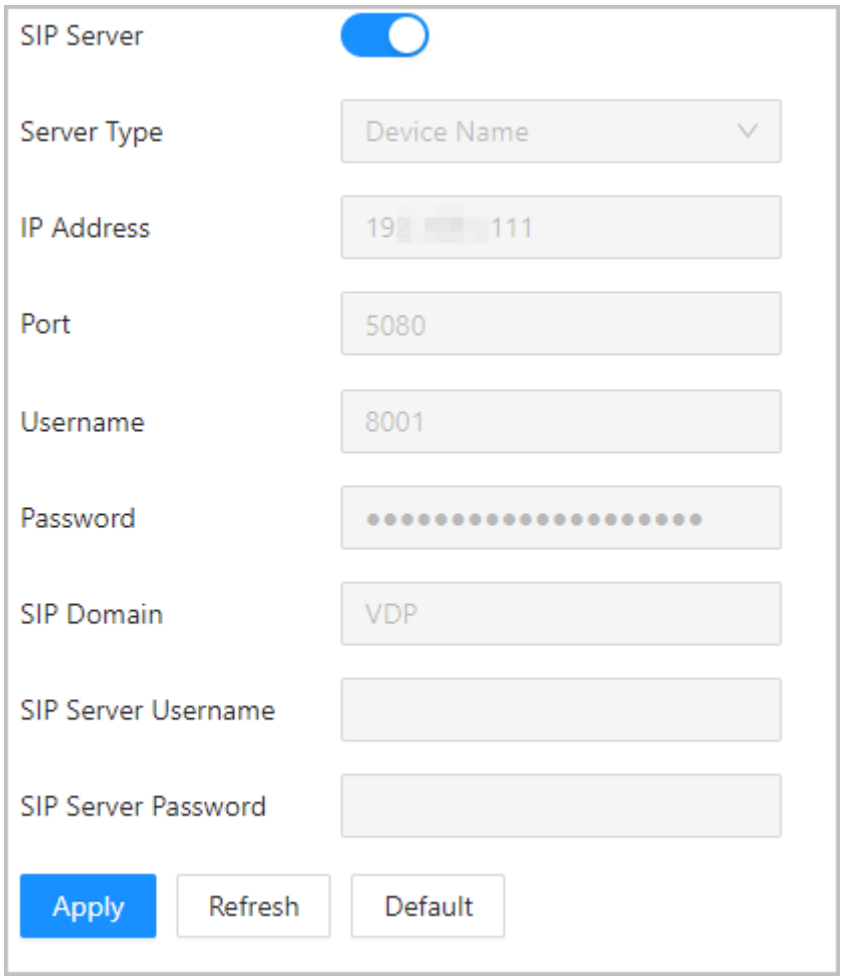
Cuando el controlador de acceso funciona como servidor SIP, puede conectar hasta 500 dispositivos de control de acceso y VTH.

Procedimiento

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

Paso 2 **SIP**. Encender**Servidor SIP**.

Figura 3-4 Utilice el controlador de acceso como servidor SIP



Paso 3 Hacer clic**Aplicar**.

3.6.1.2 Configuración de parámetros locales

Cuando el dispositivo funciona como servidor SIP, configure los parámetros del dispositivo.

Procedimiento

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

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

Figura 3-5 Parámetros básicos

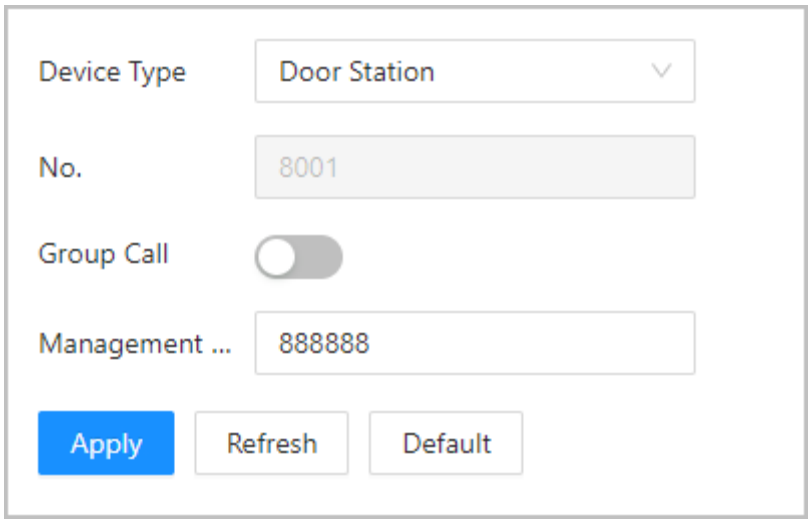


Tabla 3-3 Descripción de los parámetros básicos

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

Paso 3 Hacer clic**Aplicar**.

3.6.1.3 Adición del VTO

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

Procedimiento

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

Paso 2 **dispositivo**Haga clic en**Agregar**y luego configure el VTO.

Figura 3-6 Agregar VTO

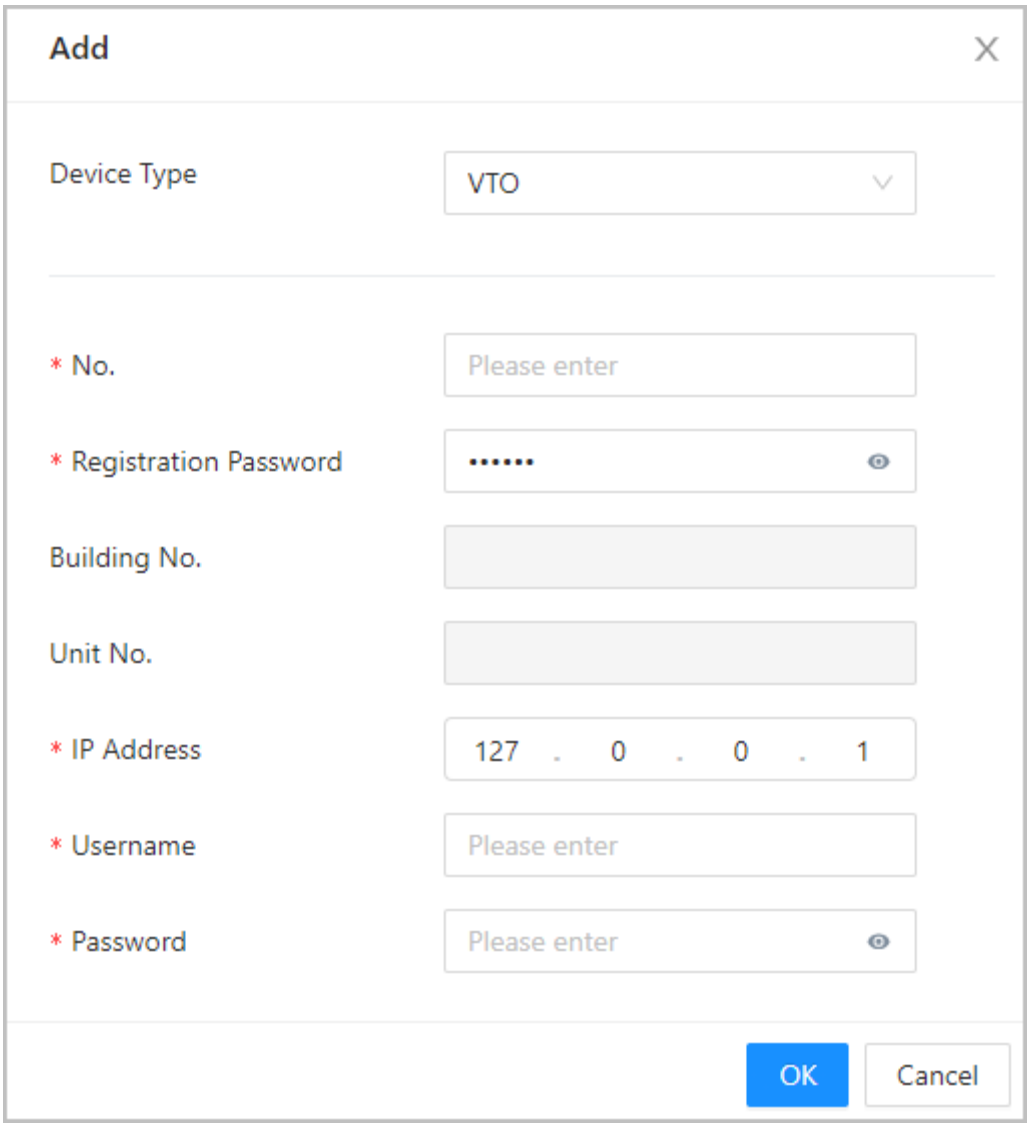


Tabla 3-4 Agregar configuración de VTO

Parámetro	Descripción
Tipo de dispositivo	Seleccionar**VTO**.
No.	Ingrese el número de VTO. Para obtener el número de VTO, vaya a**Dispositivo**Pantalla de VTO.
Registro Contraseña	Mantenlo por defecto
Edificio No.	No se puede configurar.
Unidad No.	
Dirección IP	La dirección IP del VTO agregado.
Nombre de usuario	El nombre de usuario y la contraseña que se utilizan para iniciar sesión en la página web del VTO agregado.
Contraseña	

Paso 3 Hacer clic**DE ACUERDO**.

3.6.1.4 Adición del VTH

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

para asegurarse de que puedan llamarse entre sí.

Información de contexto

- Cuando hay un VTH principal y una extensión, primero debe activar la función de llamada grupal y Luego agregue VTH principal y extensión en el**Gestión de VTH**Página. Para saber cómo activar el grupo función de llamada, consulte "3.6.1.2 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 del intercomunicador**>**Configuración del**

Paso 2 **dispositivo**Añade el VTH.

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

Figura 3-7 Agregar uno por uno

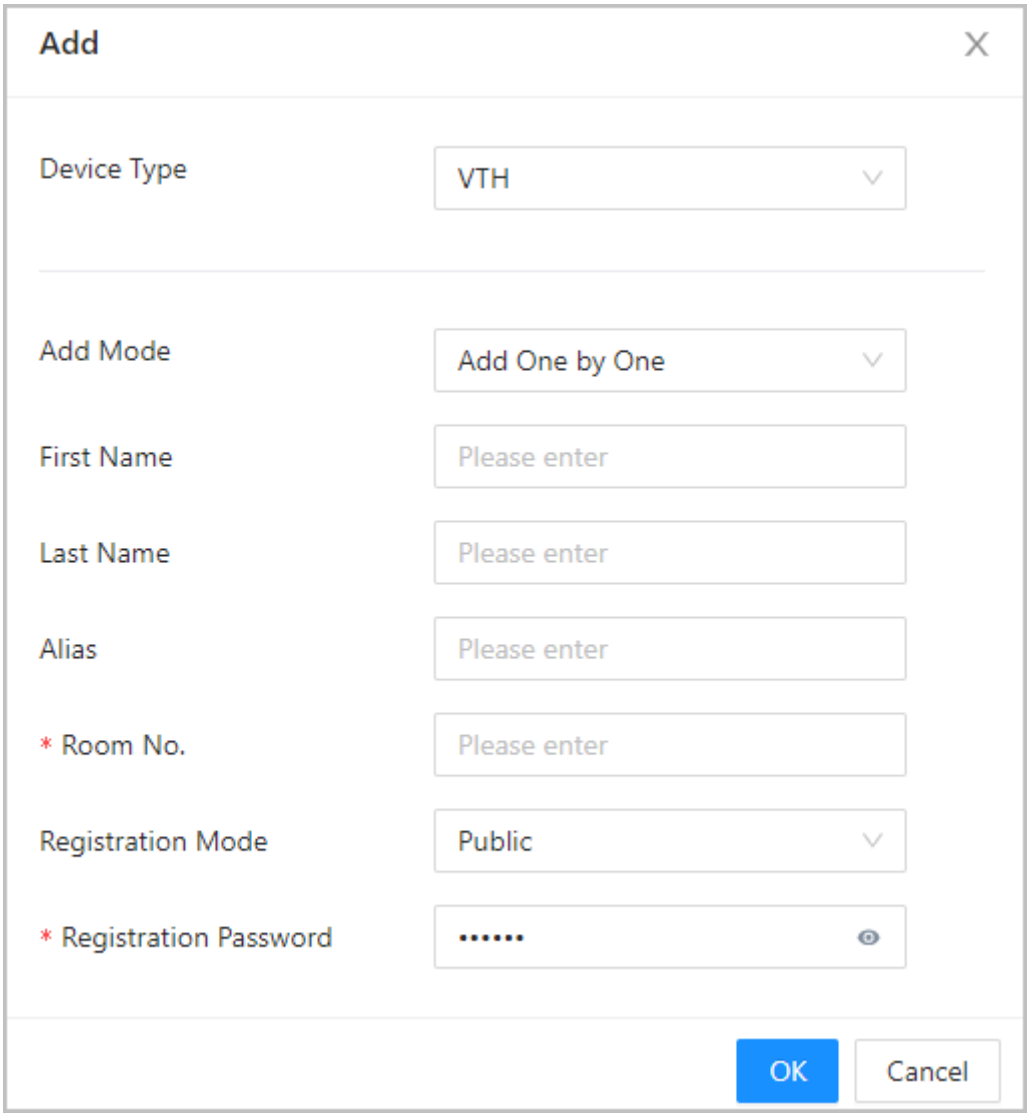


Tabla 3-5 Información de la habitación

Parámetro	Descripción
Nombre de pila	Introduzca el nombre del VTH para ayudarle a diferenciarlos.
Apellido	
Alias	
Habitación N°	Introduzca el número de habitación del VTH. ● El número de habitación consta de 1 a 5 dígitos y debe coincidir con el número de habitación configurado en el VTH. ● Cuando hay un VTH principal y extensiones, el número de habitación del VTH principal termina en -0 y el número de habitación de la extensión termina en -1, -2 o -3. Por ejemplo, el VTH principal es 101-0 y el número de habitación de la extensión es 101-1, 101-2... ● Si la función de llamada grupal no está activada, no se puede configurar el número de habitación en el formato 9901-xx.
Habitación N°	Introduzca el número de habitación del VTH. ● El número de habitación consta de 1 a 5 dígitos y debe coincidir con el número de habitación configurado en el VTH. ● Cuando hay un VTH principal y extensiones, el número de habitación del VTH principal termina en -0 y el número de habitación de la extensión termina en -1, -2 o -3. Por ejemplo, el VTH principal es 101-0 y el número de habitación de la extensión es 101-1, 101-2... ● Si la función de llamada grupal no está activada, no se puede configurar el número de habitación en el formato 9901-xx.
Modo de registro	Mantenlos como predeterminados.
Contraseña de registro	

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

Figura 3-8 Adición por lotes

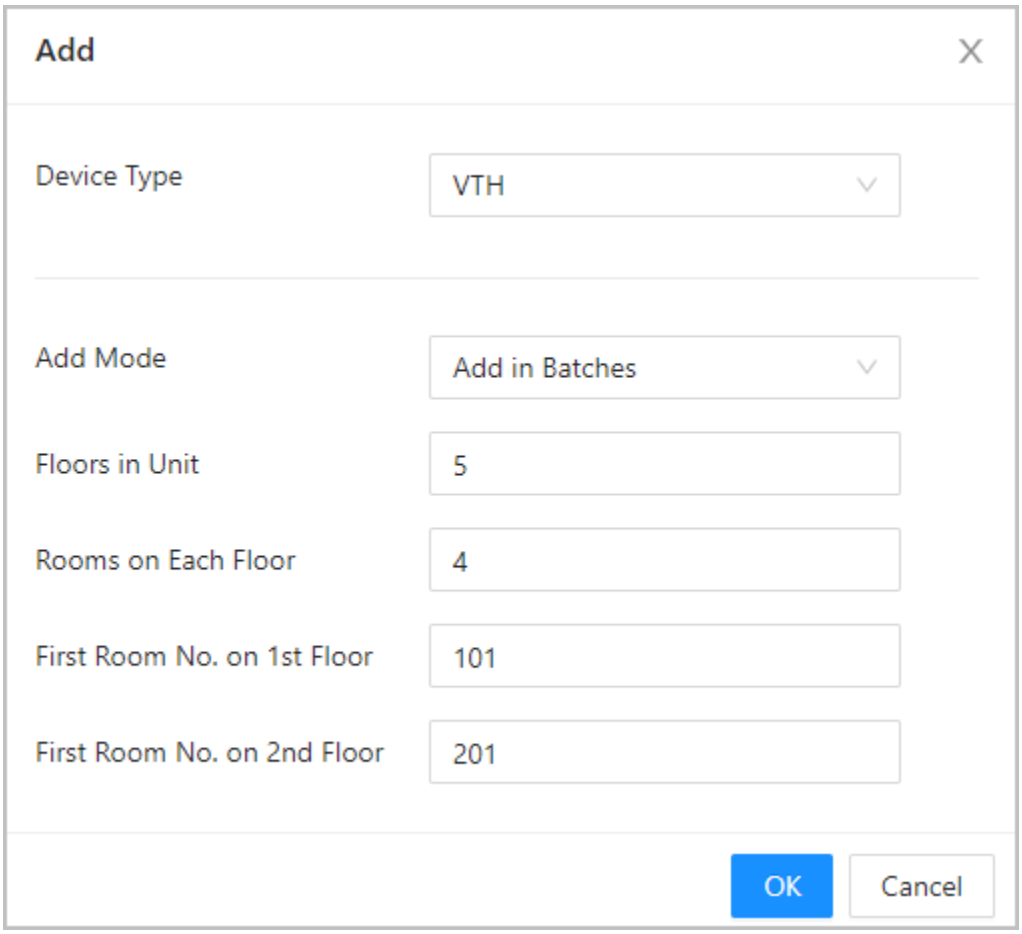


Tabla 3-6 Añadir en lotes

Parámetro	Descripción
Pisos en Unidad	El número de pisos del edificio, que varía de 1 a 99.
Habitaciones en cada piso	El número de habitaciones en cada piso, que varía de 1 a 99.
Primera habitación n.° del 1.er piso	La primera habitación del primer piso.
Primera habitación n.° del 2.° piso	El número de la primera habitación del segundo piso = el primer dígito del número de la primera habitación del primer piso más 1. Por ejemplo, si el número de la primera habitación del primer piso es 101, el número de la primera habitación del segundo piso debe ser 201.

3.6.1.5 Adición del VTS

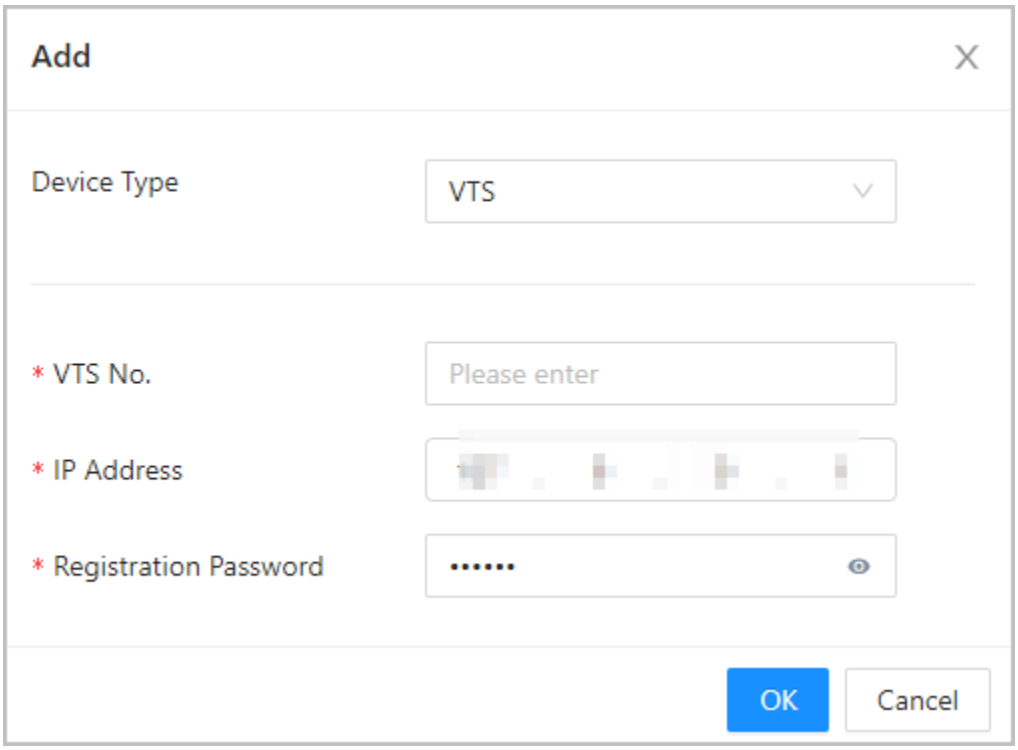
Cuando el dispositivo funciona como servidor SIP, puede agregar VTS al servidor SIP para asegurarse de que puedan llamarse entre sí.

Procedimiento

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

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

Figura 3-9 Gestión de VTS



Paso 3 Hacer clic**DE ACUERDO**.

3.6.2 Uso de VTO como servidor SIP

3.6.2.1 Configuración del servidor SIP

Utilice otro VTO como servidor SIP.

Procedimiento

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

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

No habilitar**Servidor SIP**.

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

Figura 3-10 Utilice VTO como servidor SIP

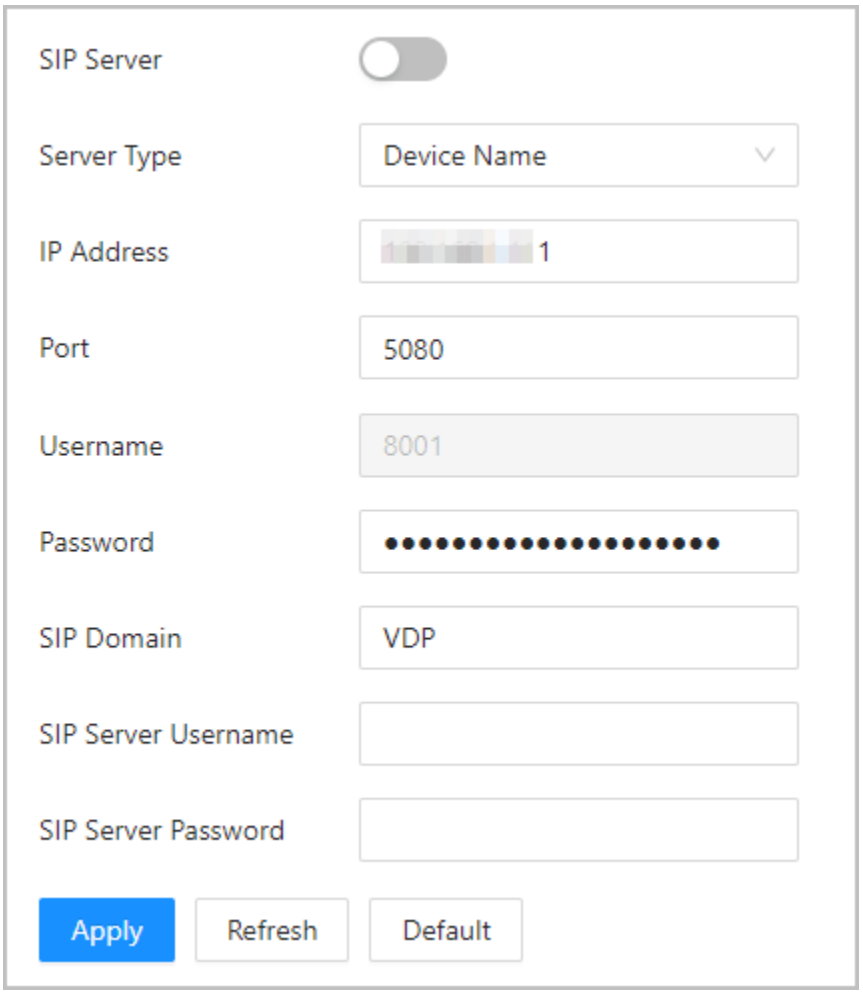


Tabla 3-8 Configuración del servidor SIP

Parámetro	Descripción
Dirección IP	Dirección IP del VTO.
Puerto	5060 por defecto cuando VTO funciona como servidor SIP.
Nombre de usuario	Déjalos como predeterminados.
Contraseña	
Dominio SIP	VDP.
Nombre de usuario del servidor SIP	El nombre de usuario y la contraseña de inicio de sesión del servidor SIP.
Contraseña del servidor SIP	

Paso 4 Hacer clic**Aplicar**.

3.6.2.2 Configuración de parámetros locales

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

Procedimiento

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

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

Figura 3-11 Configurar los parámetros

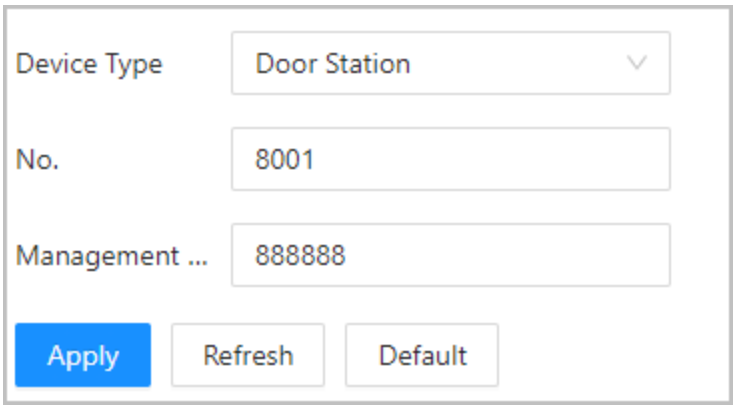


Tabla 3-9 Descripción de parámetros

Parámetro	Descripción
Tipo de dispositivo	Seleccionar**Estación de puerta**.
No.	El número del VTO. ● El número debe tener 4 dígitos. Los 2 primeros dígitos deben ser 80 y Los dos últimos dígitos empiezan 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 llamada para el centro de gestión es 888888. Manténgalo como predeterminado.

Paso 3 Hacer clic**Aplicar**.

3.6.3 Utilización de la Plataforma como servidor SIP

3.6.3.1 Configuración del servidor SIP

La plataforma de gestión se utiliza como servidor SIP.

Procedimiento

Paso 1 Seleccionar**Configuración del intercomunicador**>**Servidor SIP**

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

No habilitar**Servidor SIP**.

Figura 3-12 Utilice la plataforma de administración como servidor SIP

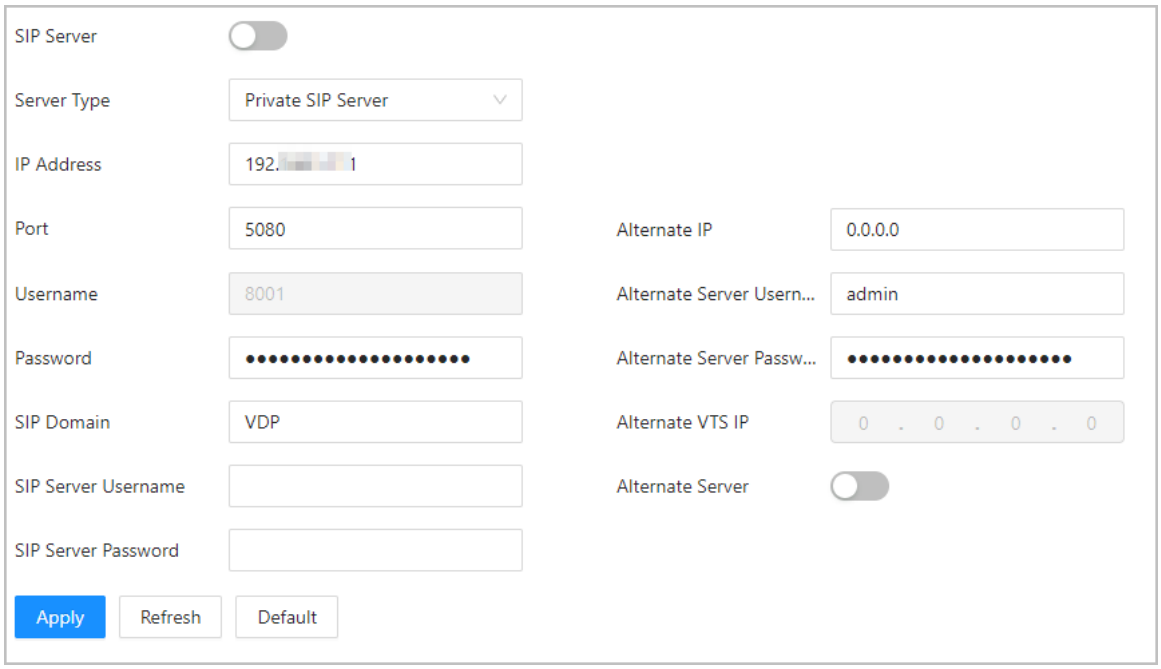


Tabla 3-10 Configuración del servidor SIP

Parámetro	Descripción
Dirección IP	Dirección IP de la plataforma.
Puerto	5080 por defecto cuando la plataforma funciona como servidor SIP.
Nombre de usuario	Déjalos como predeterminados.
Contraseña	
Dominio SIP	Déjalo como predeterminado.
Nombre de usuario del servidor SIP	El nombre de usuario y la contraseña de inicio de sesión de la plataforma.
Contraseña del servidor SIP	
IP alternativa	El servidor alternativo se utilizará como servidor SIP cuando la plataforma no responda. ● Si enciendes el**Servidor alternativo**función, configurará el controlador de acceso como servidor alternativo. ● Si desea que otro VTO funcione como servidor alternativo, Es necesario introducir la dirección IP, el nombre de usuario y la contraseña del VTO. No habilitar**Servidor alternativo**en este caso. ● Le recomendamos que configure el VTO principal como servidor alternativo.
Servidor alternativo Nombre de usuario	Se utiliza para iniciar sesión en el servidor alternativo.
Servidor alternativo Contraseña	

Parámetro	Descripción
IP VTS alternativa	Ingrese la dirección IP del VTS alternativo. Cuando la plataforma de administración no responde, se activará el VTS alternativo para asegurarse de que VTO, VTH y VTS puedan comunicarse entre sí.

Paso 3 Hacer clic**Aplicar**.

3.6.3.2 Configuración de parámetros locales

Configure los parámetros del controlador de acceso cuando la plataforma se utiliza como servidor SIP.

Procedimiento

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

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

Figura 3-13 Parámetro básico

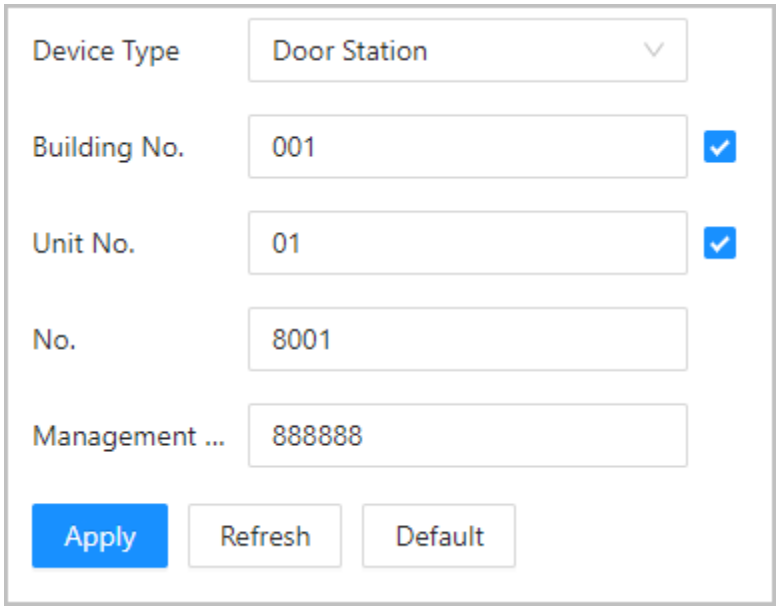


Tabla 3-11 Descripción de parámetros

Parámetro	Descripción
Tipo de dispositivo	Seleccione la estación de cerca o la estación de puerta según su sitio de instalación.
Edificio No.	Seleccione la casilla de verificación y luego ingrese el número del edificio donde está instalada la estación de puerta de la unidad.
Unidad No.	Seleccione la casilla de verificación y luego ingrese el número de la unidad donde está instalada la estación de puerta de la unidad.
No.	● El número debe tener 4 dígitos. Los 2 primeros dígitos deben ser 80 y los 2 últimos dígitos deben empezar 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. Manténgalo 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 administración.

plataforma.

3.7 Configuración del control de acceso

3.7.1 Configuración de parámetros básicos

Procedimiento

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

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

Figura 3-14 Parámetros básicos

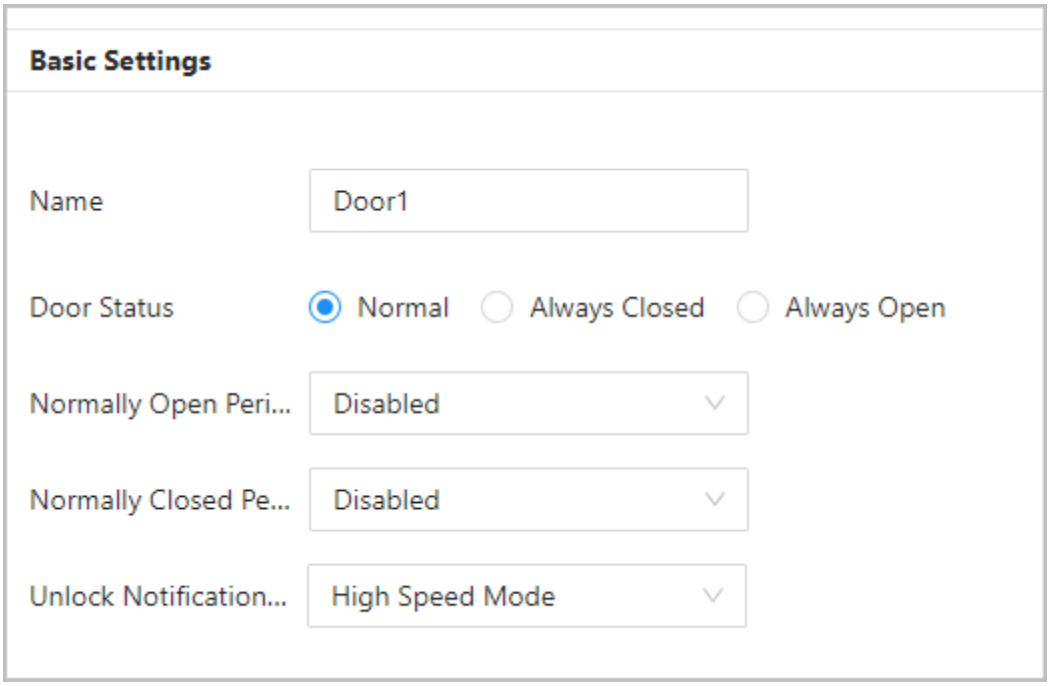


Tabla 3-12 Descripción de los parámetros básicos

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 abierto: la puerta permanece desbloqueada todo el tiempo. ● Siempre cerrado: la puerta permanece bloqueada todo el tiempo.
Periodo normalmente abierto	Cuando seleccionas**Normal**, puede seleccionar una plantilla de tiempo de la lista desplegable. La puerta permanece abierta o cerrada durante el tiempo definido.
Periodo normalmente cerrado	

Parámetro	Descripción
Desbloquear notificación	Muestra la notificación en la pantalla cuando una persona verifica su identidad en el controlador de acceso. ● Modo de alta velocidad: el sistema le indica**Verificado exitosamente**o **No autorizado**en la pantalla. ● Modo simple: muestra el ID del usuario, el nombre y el tiempo de verificación después de conceder el acceso; muestra**No autorizado**y tiempo de autorización después de denegar el acceso. ● Estándar: muestra la imagen del rostro registrado del usuario, la identificación del usuario, el nombre y el tiempo de verificación después de otorgar el acceso; muestra**No autorizado**y tiempo de verificación después de denegar 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 el tiempo de autorización después de otorgar el acceso; muestra**No autorizado**y tiempo de autorización después de denegar el acceso.

Paso 3 Hacer clic**Aplicar**.

3.7.2 Configuración de métodos de desbloqueo

Puede utilizar varios métodos de desbloqueo para desbloquear la puerta, como la tarjeta Bluetooth, la huella dactilar, la tarjeta y el desbloqueo con contraseña. También puede combinarlos para crear su propio método de desbloqueo personal.

Procedimiento

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

Paso 2 **configuraciones**, seleccione un modo de desbloqueo.

- Desbloqueo de combinación
  1. Seleccione**Desbloqueo de combinación**desde**Modo de desbloqueo**lista.
  2. Seleccionar**O**o**Y**.
     - ◇ O bien: 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 3-15 Configuración de desbloqueo

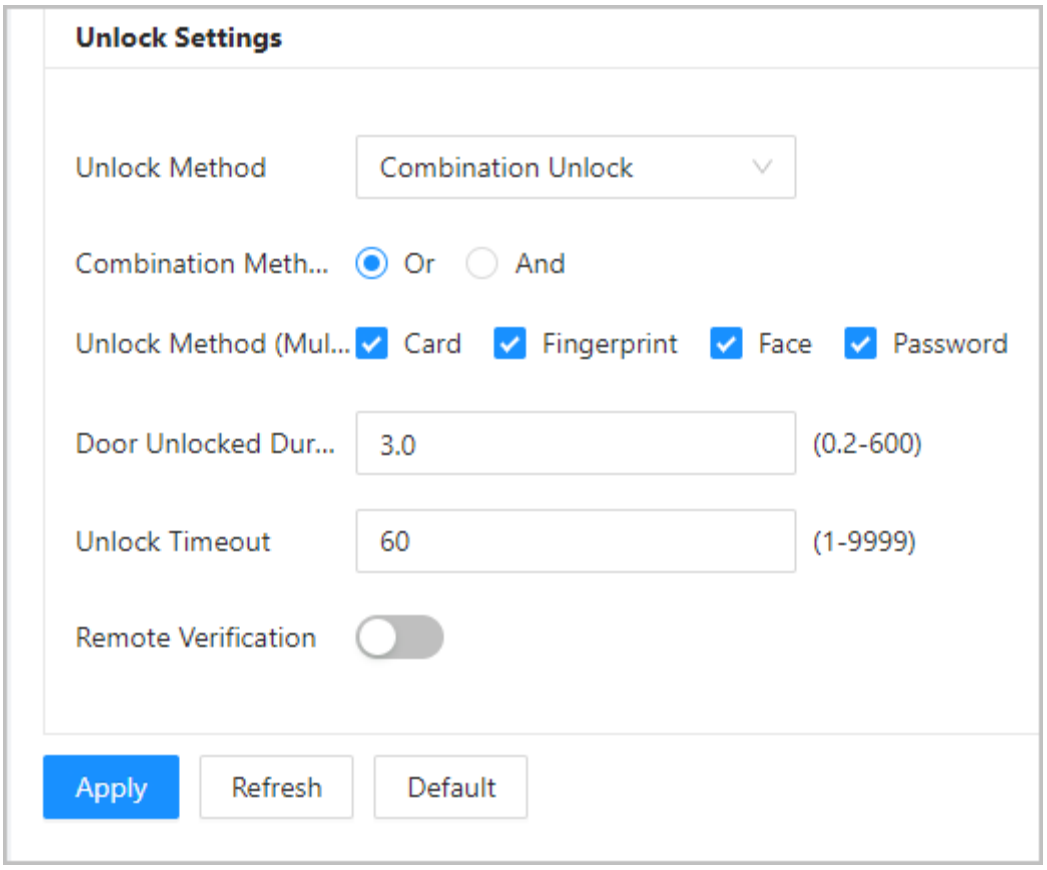


Tabla 3-13 Descripción de la configuración de desbloqueo

Parámetro	Descripción
Método de desbloqueo (selección múltiple)	Los métodos de desbloqueo pueden variar según los modelos de producto.
Duración del desbloqueo de la puerta	Una vez que se le concede el acceso a una persona, la puerta permanecerá desbloqueada durante un tiempo definido para que pueda pasar. Varía entre 0,2 s y 600 segundos.
Desbloquear tiempo de espera	Cuando el detector de puerta y la alarma de tiempo de desbloqueo están habilitados, se activará una alarma de tiempo de espera si la puerta permanece desbloqueada más tiempo que el tiempo de desbloqueo definido.
Verificación remota	Abrir la puerta de forma remota.

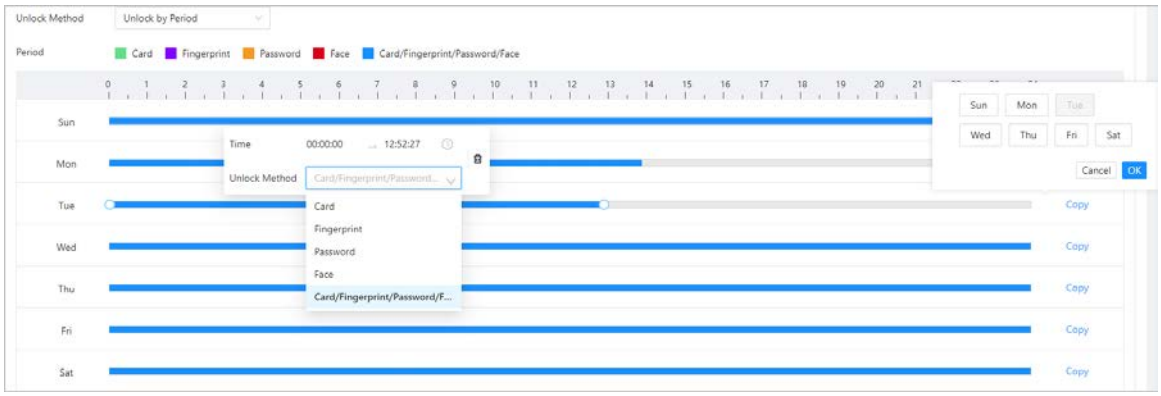
- Desbloqueo por periodo

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

También puedes hacer clic**Copiar**para aplicar el período de tiempo configurado a otros días.

3. Seleccione un método de desbloqueo para el período de tiempo y luego configure otros parámetros.

Figura 3-16 Desbloqueo por período



- Desbloqueo por múltiples usuarios.

  1. En el**Modo de desbloqueo**lista, seleccionar**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 la cantidad de personas en el grupo que otorgan acceso sea igual al número válido definido.
     - ◇ Si se agrega más de un grupo, la puerta se desbloquea solo después de que el número de personas en cada grupo que otorgan acceso sea igual al número válido definido.

     - ◇ Puedes agregar hasta 4 grupos.
     - ◇ El número válido indica el número de personas de cada grupo que necesitan verificar su identidad. identidades en el controlador de acceso antes de que se desbloquee la puerta. Por ejemplo, si la El número se establece en 3 para un grupo, por lo que 3 personas del grupo deben verificar su identidad para Desbloquea la puerta.

Paso 3 Hacer clic**Aplicar**.

3.7.3 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 parámetros de alarma.

Figura 3-17 Alarma

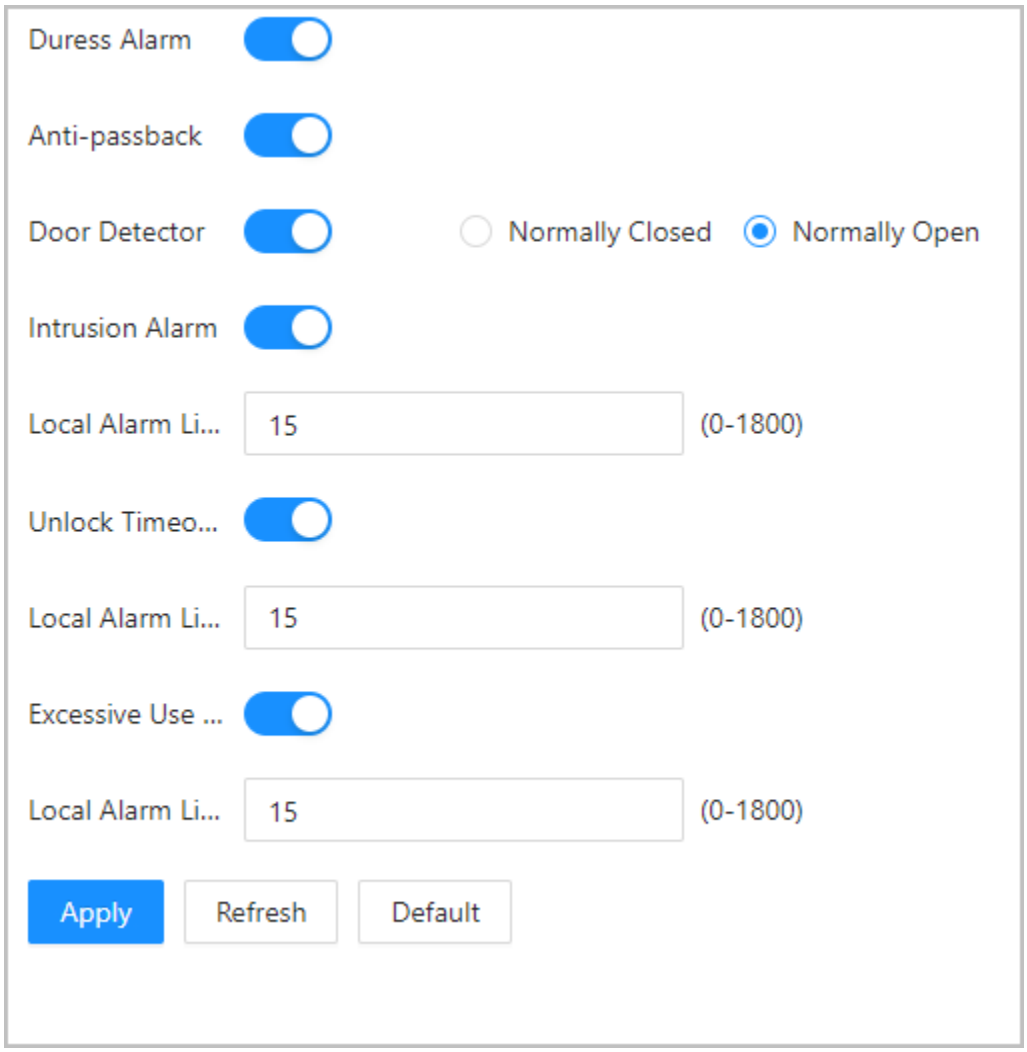


Tabla 3-14 Descripción de los parámetros de alarma

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 su identidad tanto para entrar como para salir; de lo contrario, se activará una alarma. Esto ayuda a evitar que el titular de una tarjeta le pase la tarjeta de acceso a otra persona para poder entrar. Cuando se activa la función antirretorno, el titular de la tarjeta debe abandonar el área protegida a través de un lector de salida antes de que el sistema le permita entrar nuevamente. ● Si una persona ingresa después de la autorización y sale sin autorización, se activará una alarma cuando intente ingresar nuevamente y se le negará el acceso al mismo tiempo. ● Si una persona entra sin autorización y sale después de la autorización, se activará una alarma cuando intente entrar nuevamente y se le negará el acceso al mismo tiempo.  Si el controlador de acceso solo puede conectar una cerradura, la verificación en el controlador de acceso significa la dirección de entrada y Verificar en el lector de tarjetas externo significa dirección de salida De forma predeterminada, puede modificar la configuración en la plataforma de administración.
Detector de puerta	Con el detector de puerta conectado a su dispositivo, se puede activar la alarma 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	Cuando el detector de puerta y la alarma de intrusión están habilitados, se activará una alarma de intrusión si la puerta se abre de forma anormal.
Alarma de tiempo de espera para desbloqueo	Cuando el detector de puerta y la alarma de tiempo de desbloqueo están habilitados, se activará una alarma de tiempo de espera si la puerta permanece desbloqueada más tiempo que el tiempo de desbloqueo definido.
Alarma de uso excesivo	Si se utiliza una contraseña o tarjeta incorrecta 5 veces seguidas en 60 segundos, se activará la alarma por uso excesivo de tarjeta ilegal y durará 15 segundos de forma predeterminada.
Enlace de alarma local	Duración de la alarma. 15 s por defecto.

Paso 3 Hacer clic**Aplicar**.

3.7.4 Configuración de vínculos de alarma global (opcional)

Puede configurar vínculos de alarmas globales.

Procedimiento

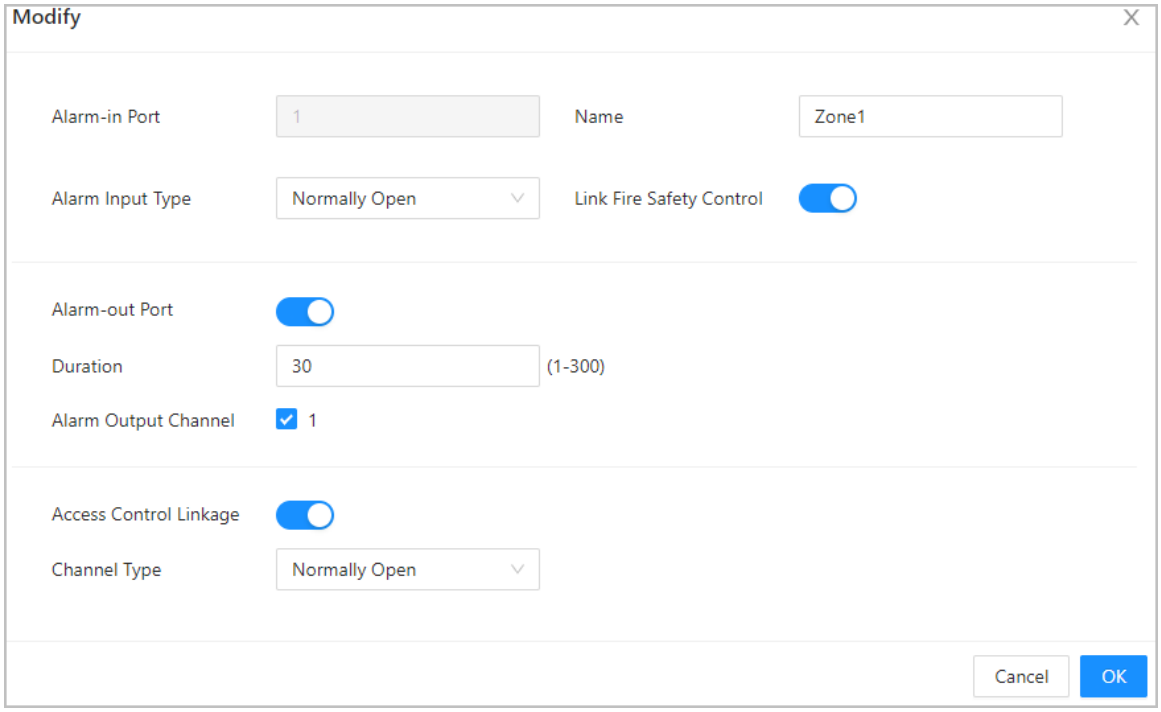
Paso 1 Seleccionar**Control de acceso**>**Alarma**>**Configuración de vinculación de alarma**.

- Si se agrega una plataforma de administración al controlador de acceso, la configuración de la alarma será sincronizado 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 Configure la entrada de alarma. 1.

Haga clic en .

Figura 3-18 Vinculación de alarma global



2. Configure el nombre de la alarma.

3. Seleccione un tipo para el dispositivo de entrada de alarma.

- Normalmente cerrado: la entrada de alarma se encuentra en un estado de circuito normalmente cerrado (NC) cuando la alarma no se ha disparado. Al abrir un circuito normalmente cerrado, se activa la alarma.
- Normalmente abierto: el dispositivo de entrada de alarma se encuentra en un estado de circuito normalmente abierto (NO) cuando la alarma no se ha disparado. Al cerrar el circuito, se activa la alarma.

4. Haga clic**Permitir**para activar la función de vinculación de la puerta.

Si activa el control de seguridad contra incendios del enlace, la salida de alarma y todos los enlaces de la puerta se activan. cambio habilitado automáticamente a**Siempre abierto**estado, y todas las puertas se abrirán cuando Se activa la alarma de incendio.

1. Seleccione una entrada de alarma de la lista de canales de entrada de alarma y luego haga clic en**Salida de alarma de enlace**.

2. Haga clic**Agregar**, seleccione un canal de salida de alarma y luego haga clic en**DE ACUERDO**.

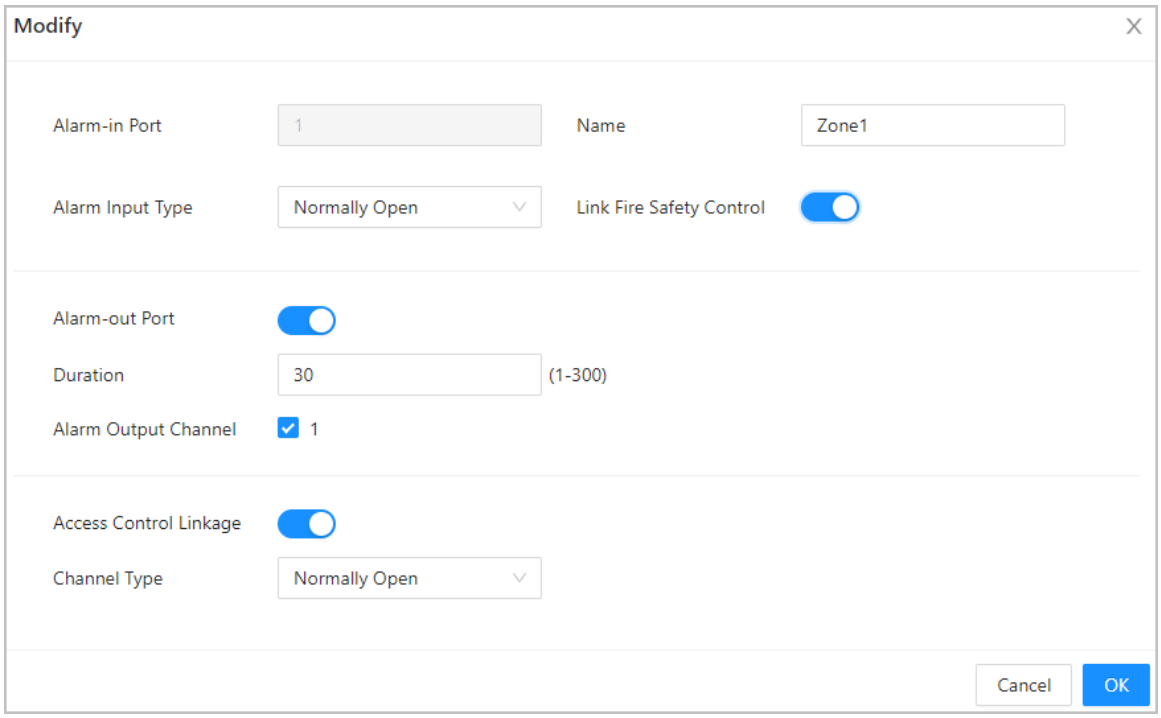
3. Haga clic**Aplicar**.

Paso 3 Active la función de salida de alarma y luego ingrese la duración de la alarma. Active el

Paso 4 enlace de control de acceso electrónico y luego seleccione un estado de puerta.

- Normalmente cerrado: la puerta se bloquea automáticamente cuando se activa una alarma.
- Normalmente abierto: la puerta se desbloquea automáticamente cuando se activa una alarma.

Figura 3-19 Salida de alarma



3.7.5 Configuración de la detección de rostros

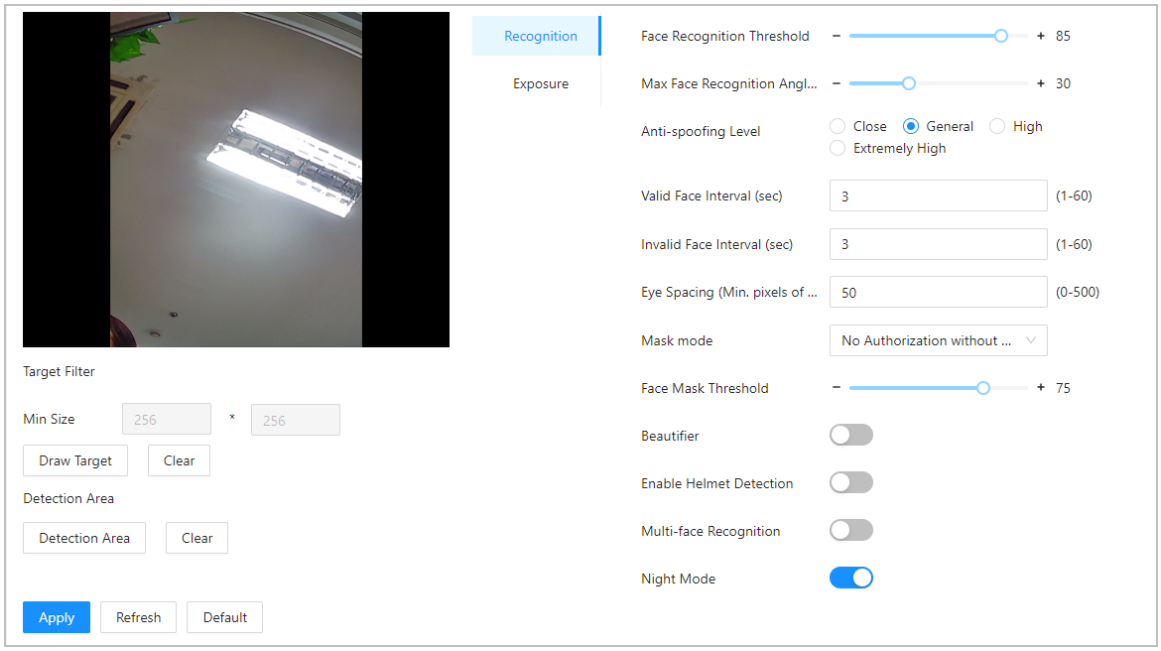
Configurar los parámetros de detección de rostros.

Procedimiento

Paso 1 Inicie sesión en la página web.

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

Figura 3-20 Parámetros de detección de rostros



Paso 3 Configurar los parámetros.

Tabla 3-15 Descripción de los parámetros del rostro

Nombre	Descripción
Umbral de reconocimiento facial	Ajuste el nivel de precisión del reconocimiento facial. Un umbral más alto significa mayor precisión y menor tasa de reconocimiento falso.
Desviación máxima del ángulo de reconocimiento facial	Establezca el ángulo más grande en el que se puede colocar un rostro para su detección. Cuanto mayor sea el valor, mayor será el rango del ángulo del rostro. Si el ángulo en el que se coloca un rostro no está dentro del rango definido, es posible que no se detecte correctamente.
Nivel anti-spoofing	Esto evita que las personas puedan usar fotos, vídeos, máscaras y otros sustitutos para obtener acceso no autorizado.
Intervalo de cara válido (seg.)	Cuando se verifica con éxito el rostro de una persona demasiadas veces, Access Controller indica que la verificación fue exitosa dentro del intervalo de tiempo definido.
Intervalo de rostro no válido (seg.)	Cuando una persona no logra verificar su rostro demasiadas veces, Access Controller indica que la verificación falló dentro del intervalo de tiempo definido.
Espaciado entre ojos (píxeles mínimos de espaciado entre ojos)	Para que el reconocimiento sea exitoso, se requiere una cierta cantidad de píxeles entre los ojos, llamada distancia pupilar. La cantidad predeterminada es 45 píxeles. Esta cantidad varía según el tamaño de la cara y la distancia entre la cara y la lente. Si un adulto está a 1,5 metros de la lente, la distancia pupilar suele ser de 50 a 70 píxeles.
Modo máscara	● Modo máscara: ◇ **No detectar**:La máscara no se detecta durante el reconocimiento facial. ◇ **Recordatorio de uso de mascarilla**:Se detecta la mascarilla durante el reconocimiento facial. Si la persona no lleva mascarilla, el sistema le recordará que se la ponga, pero se le permitirá el acceso. ◇ **Sin autorización sin uso de mascarilla**:Se detecta la mascarilla durante el reconocimiento facial. Si una persona no lleva mascarilla, el sistema le recordará que debe usarla y le negará el acceso. ● Umbral de reconocimiento de mascarilla: cuanto mayor sea el umbral, más preciso será el reconocimiento facial cuando una persona lleve mascarilla y habrá una menor tasa de reconocimiento falso.
Embellecedor	Embellece las imágenes de rostros capturadas.
Habilitar detección de casco	Detecta cascos de seguridad. La puerta no se desbloqueará si la persona no lleva casco.

Nombre	Descripción
Reconocimiento de múltiples caras	Detecta de 4 a 6 imágenes de rostros a la vez. No se puede utilizar el desbloqueo con combinación con este dispositivo y la puerta se desbloqueará cuando una de las personas se verifique correctamente. La cantidad de imágenes de rostros admitidas puede variar según el modelo del producto.
Modo nocturno	En entornos oscuros, la pantalla de espera muestra una imagen de fondo blanca para mejorar el brillo al verificar el rostro o el código QR.
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.

Paso 4 Configurar los parámetros de exposición.

Figura 3-21 Parámetros de exposición

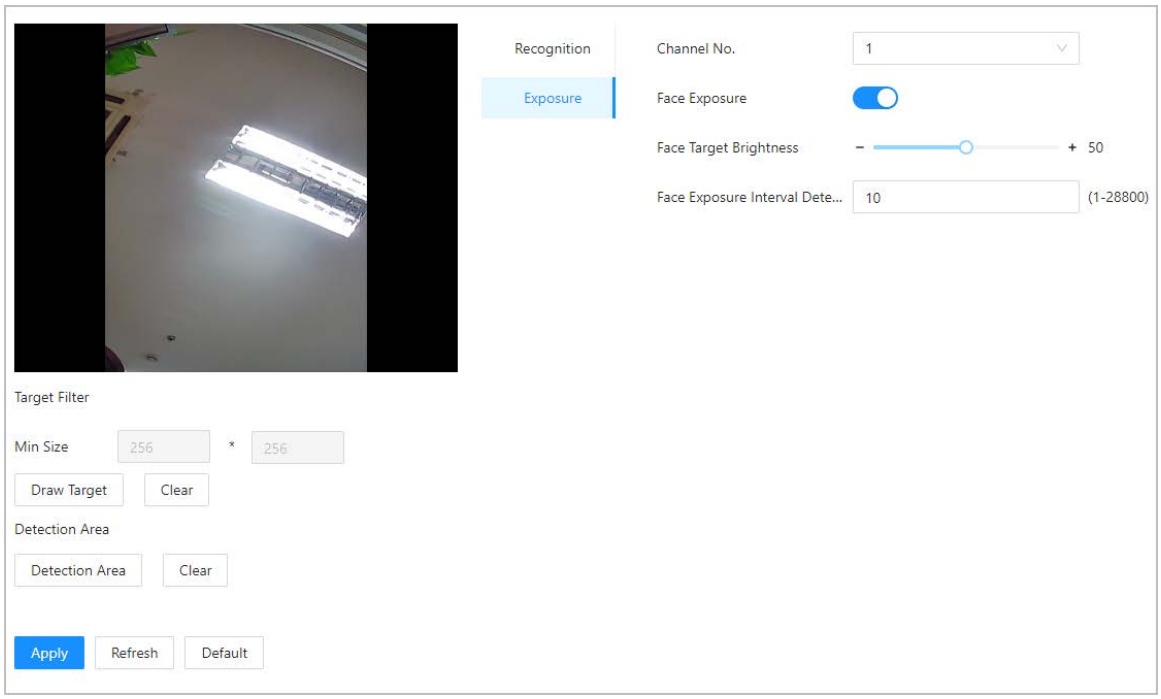


Tabla 3-16 Descripción de los parámetros de exposición

Parámetro	Descripción
Canal No.	● El canal 1 es el modo de luz blanca. ● El canal 2 es el modo de luz infrarroja.
Exposición de la cara	Una vez habilitada la función de exposición del rostro, este se expondrá con el brillo definido para detectar la imagen del rostro con claridad.
Detección del intervalo de exposición del rostro	El rostro se expondrá solo una vez en un intervalo definido.

Paso 5 Dibuje el área de detección de rostros.

1) Haga clic**Detectar región**.

2) Haga clic derecho para dibujar el área de detección y luego suelte el botón izquierdo del mouse para

dibujo completo

Paso 6 Se detectará el rostro en el área definida. Dibuje el tamaño 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 sea mayor que el tamaño definido, el controlador de acceso podrá detectar la cara.

Paso 7 Dibuje el área de detección. Haga clic

Paso 8 **DE ACUERDO**.

3.7.6 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 la**

Paso 3 **tarjeta**. Configure los parámetros de la tarjeta.

Figura 3-22 Parámetros de la tarjeta

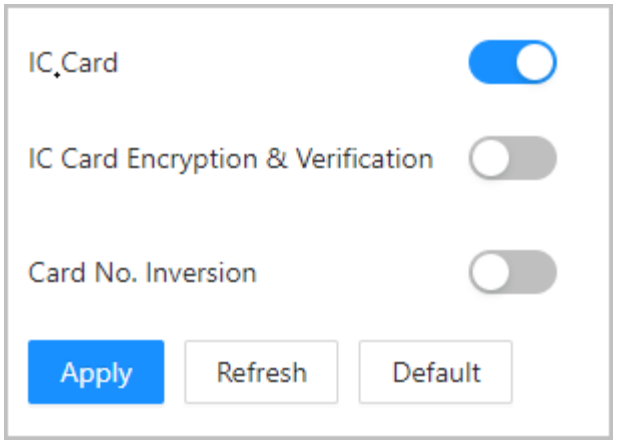


Tabla 3-17 Descripción de los parámetros de la tarjeta

Parámetro	Descripción
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.
Tarjeta N° Inversión	Cuando el controlador de acceso se conecta a un dispositivo de terceros a través de la entrada Wiegand y el número de tarjeta leído por el controlador de acceso está en orden inverso al número de tarjeta real, puede activar esta función.

3.7.7 Configuración del código QR

Procedimiento

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

Figura 3-23 Código QR

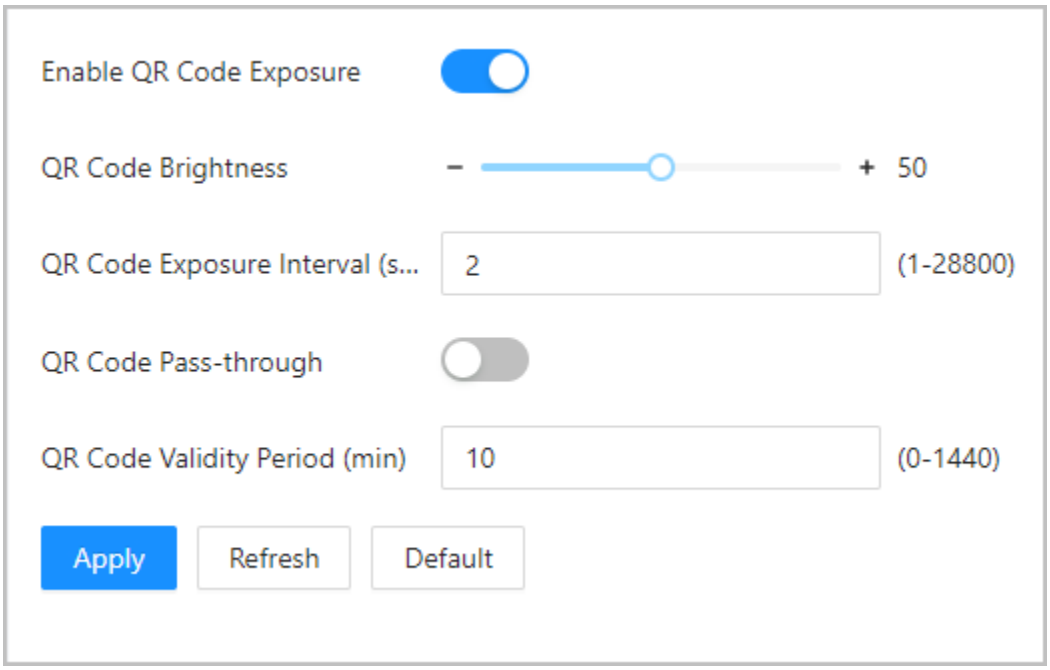


Tabla 3-18 Parámetros del código QRR

Parámetros	Descripción
Habilitar la exposición del código QR	El código QR se expondrá con el brillo definido y se podrá detectar y leer con claridad.
Brillo del código QR	
Intervalo de exposición del código QR (seg.)	El código QR se expondrá solo una vez durante el intervalo definido.
Paso a través de código QR	El código QR leído por una plataforma de terceros.
Periodo de validez del código QR (min)	Una vez generado el código QR, la validez de sus códigos QR durará un tiempo definido antes de que expire.

3.7.8 Configuración de horarios

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

3.7.8.1 Configuración de períodos de tiempo

Puede configurar hasta 128 grupos (del n.° 0 al n.° 127) de períodos de tiempo. En cada período, debe configurar los horarios de acceso a las puertas para una semana completa. Las personas solo pueden desbloquear la puerta durante el tiempo programado.

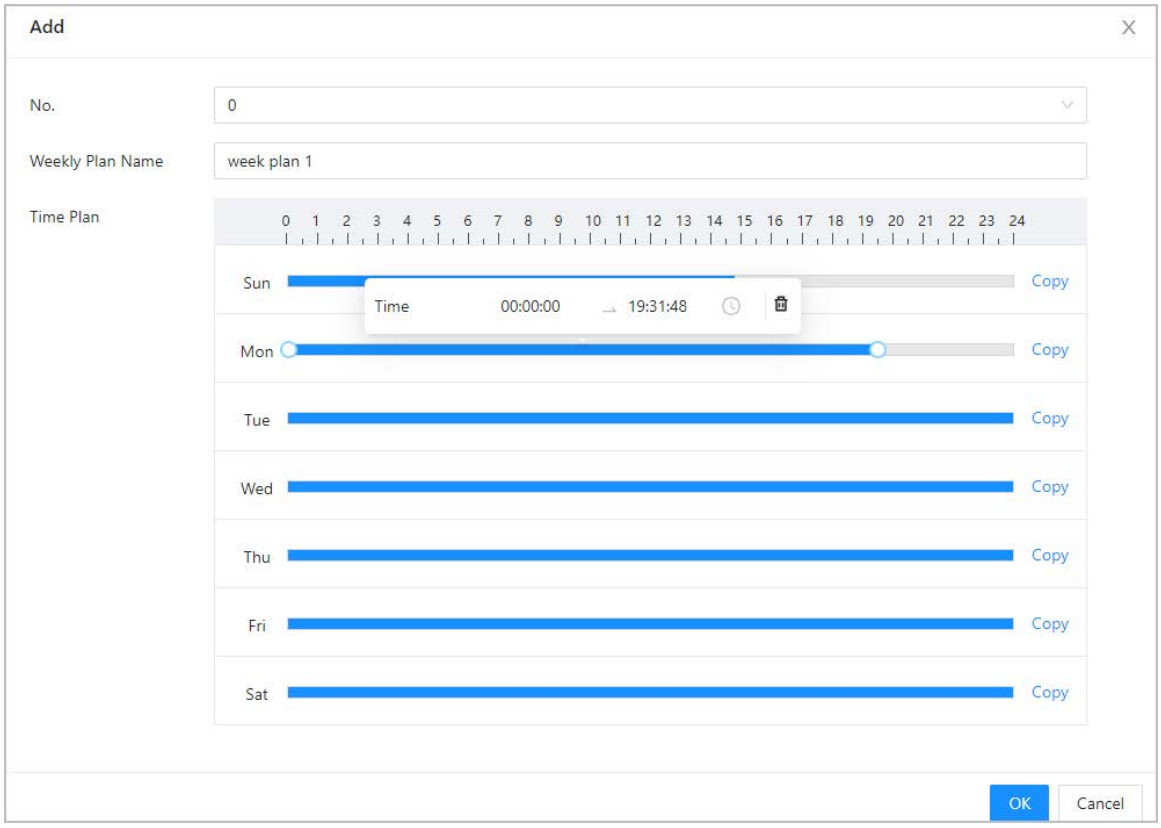
Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Control de acceso**>**Configuración del período**>**Plan semanal**Haga clic

Paso 3 en**Agregar**.

Figura 3-24 Configurar períodos de tiempo



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

Paso 5 (Opcional) Haga clic en**Copiar**Para copiar la configuración al resto de días, haga clic en**DE**

Paso 6 **ACUERDO**.

3.7.8.2 Configuración de planes de vacaciones

Puede configurar hasta 128 grupos de vacaciones (del n.º 0 al n.º 127) y, para cada grupo de vacaciones, puede agregar hasta 16 días festivos. Después, puede asignar los grupos de vacaciones configurados al plan de vacaciones. Los usuarios solo pueden desbloquear la puerta en el horario definido en el plan de vacaciones.

Procedimiento

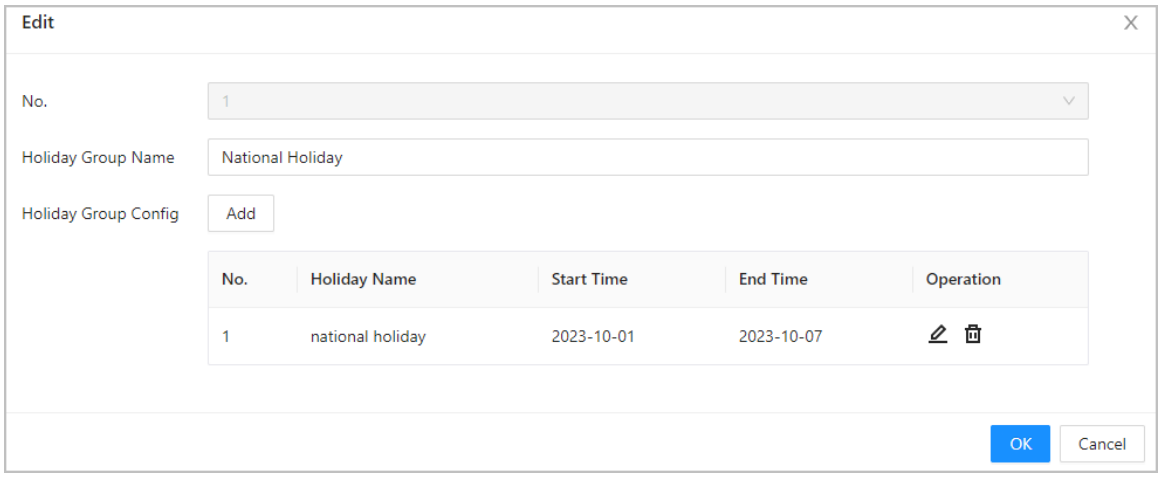
Paso 1 Inicie sesión en la página web.

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

Paso 3 Haga clic en**Gestión de vacaciones**y luego haga clic en**Agregar**.

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

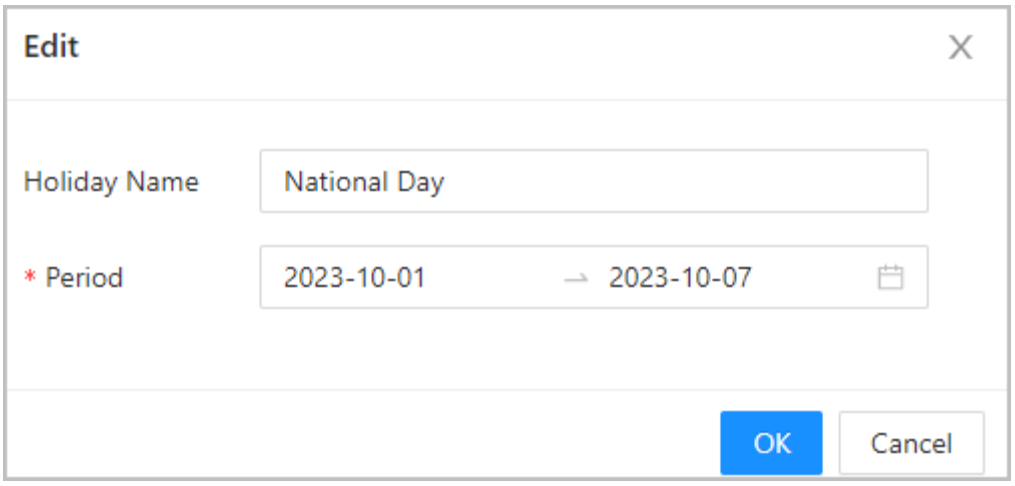
Figura 3-25 Agregar un grupo de vacaciones



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

Paso 6 **ACUERDO**.

Figura 3-26 Agregar un día festivo a un grupo de días festivos

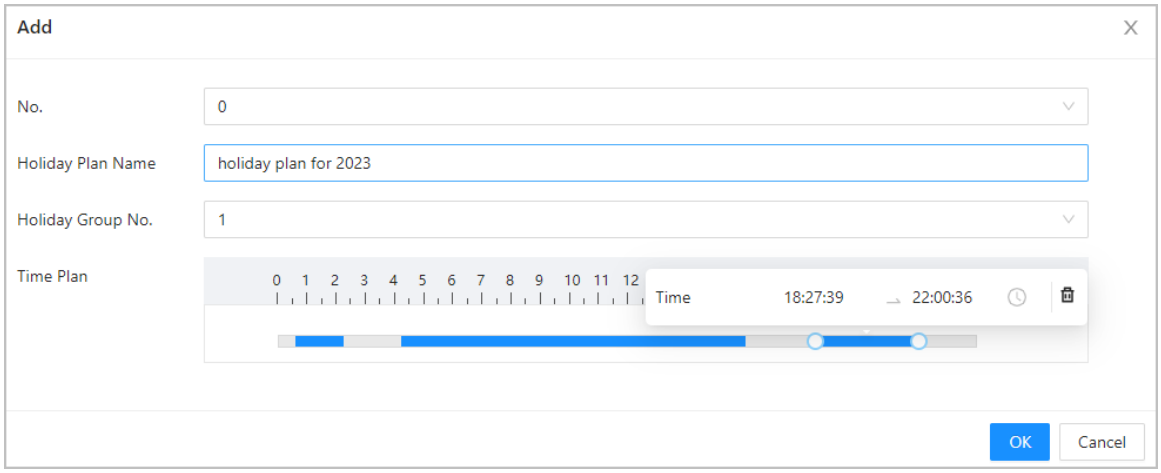


Paso 7 Hacer clic**Gestión de planes**y luego haga clic en**Agregar**.

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

Paso 9 Seleccione un grupo de días festivos y, a continuación, arrastre el control deslizante para configurar la hora de cada día. Admite la adición de hasta 4 secciones horarias por día.

Figura 3-27 Agregar plan de vacaciones



Paso 10 Hacer clic**DE ACUERDO**.

3.7.9 Configuración de módulos de expansión

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

Información de contexto

- El tipo de módulo de expansión puede variar según los modelos del controlador de acceso.
- Las configuraciones del módulo de expansión permanecen después de restaurar el controlador de acceso 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 controlador de acceso. Haga clic

Paso 3 en**Aplicar**.

Las configuraciones se hacen efectivas después de reiniciar Access Controller.

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

3.7.10 Configuración de funciones del puerto

Algunos puertos pueden funcionar como puertos diferentes, puedes configurarlos como puertos diferentes según las necesidades reales.

Información de contexto

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

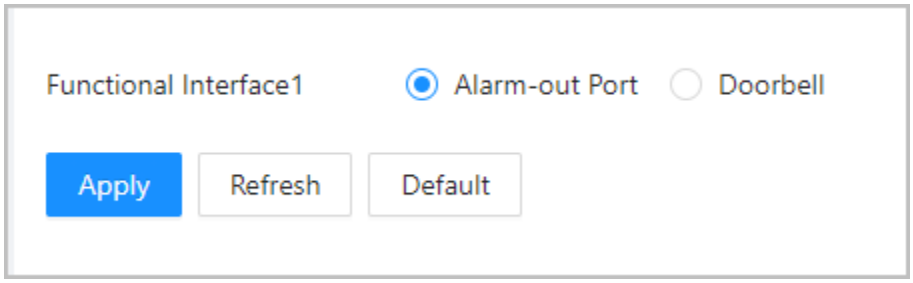
Procedimiento

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

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

Paso 3 Hacer clic**Aplicar**.

Figura 3-28 Configurar puertos



3.8 Configuración de audio y vídeo

3.8.1 Configuración de vídeo

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

Información de contexto

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

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

3.8.1.1 Configuración del canal 1

Procedimiento

Paso 1 Seleccionar**Configuración de audio y video**>**Video**

Paso 2 . Seleccionar**1**desde**Canal No.**Lista. Configure la

Paso 3 tasa de bits.

Figura 3-29 Tasa de fecha

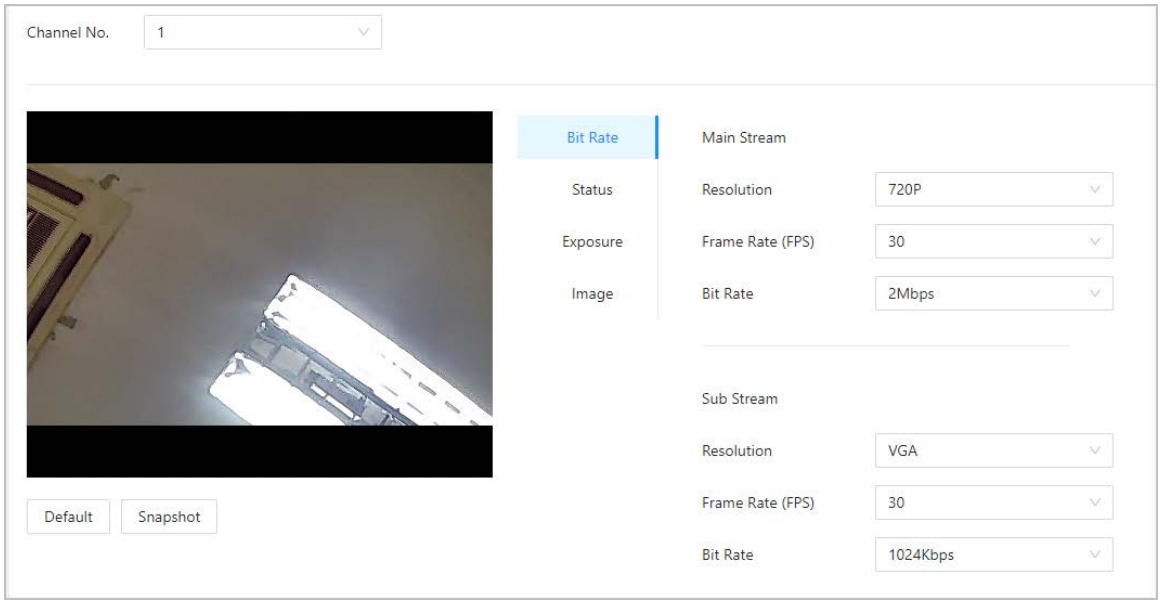


Tabla 3-19 Descripción de la velocidad de bits

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

Paso 4 Configurar el estado.

Figura 3-30 Estado

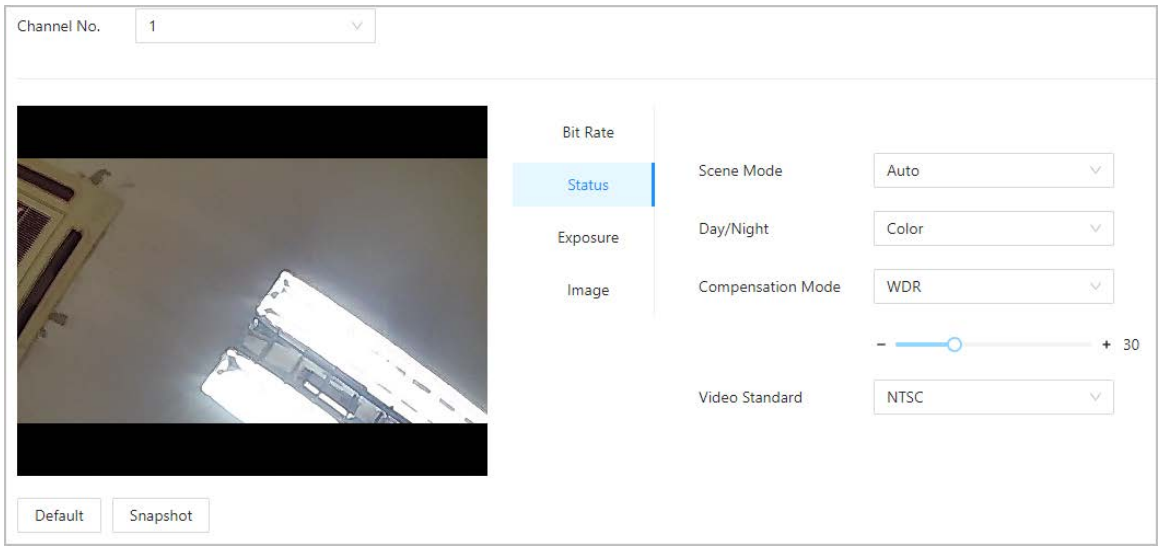


Tabla 3-20 Descripción de la imagen

Parámetro	Descripción
Modo de escena	El tono de la imagen es diferente en distintos modos de escena. ● **Cerca**:La función de modo de escena está desactivada. ● **Auto**:El sistema ajusta automáticamente el modo de escena según la sensibilidad fotográfica. ● **Soleado**:En este modo, se reducirá el tono de la imagen. ● **Noche**:En este modo, se aumentará el tono de la imagen.

Parámetro	Descripción
Día/Noche	El modo Día/Noche afecta la compensación de luz en diferentes situaciones. ● **Auto**:El sistema ajusta automáticamente el modo día/noche en función de la sensibilidad fotográfica. ● **Vistoso**:En este modo, las imágenes son coloridas. ● **En blanco y negro**:En este modo, las imágenes son en blanco y negro.
Modo de compensación	● **Desactivar**:La compensación está desactivada. ● **BLC**:La compensación de luz de fondo aporta automáticamente más luz a las áreas más oscuras de una imagen cuando la luz brillante que brilla detrás la oscurece. ● **Amplio rango dinámico (WDR)**:El sistema atenúa las áreas brillantes y compensa las áreas oscuras para crear un equilibrio que mejore la calidad general de la imagen. ● **HLCC (Centro de Información de Conducta Humana)**:La compensación de luces altas (HLC) es una tecnología que se utiliza en las cámaras de seguridad CCTV/IP para tratar imágenes expuestas a luces como faros o focos. El sensor de imagen de la cámara detecta luces fuertes en el video y reduce la exposición en esos puntos para mejorar la calidad general de la imagen.

Paso 5 Configurar los parámetros de exposición.

Figura 3-31 Exposición

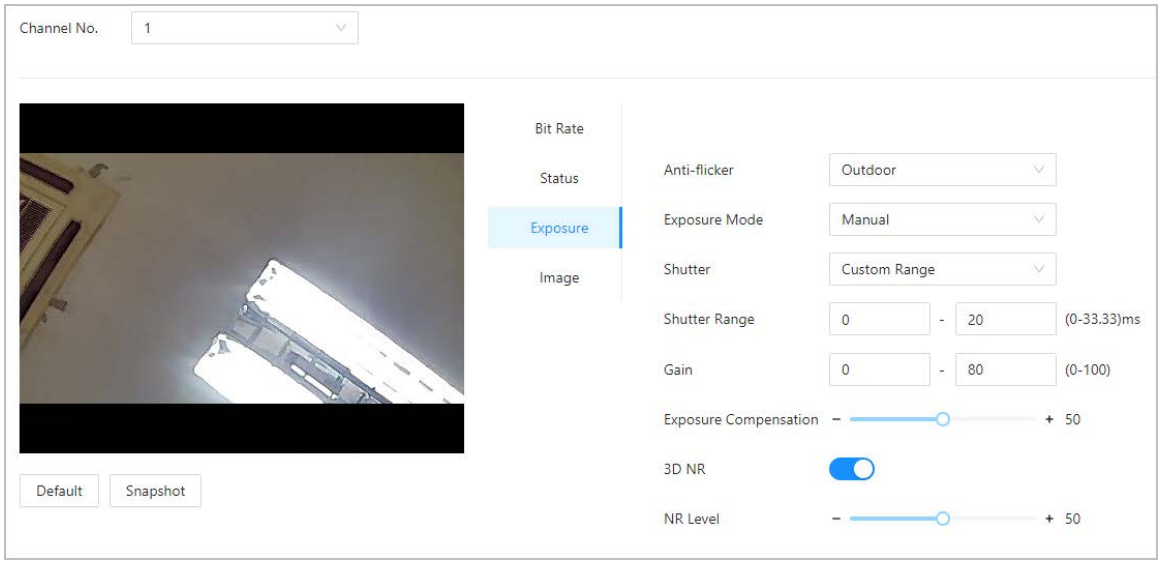


Tabla 3-21 Descripción de los parámetros de exposición

Parámetro	Descripción
Anti-parpadeo	Configure el antiparpadeo para reducir el parpadeo y disminuir o reducir los colores desiguales o la exposición. ● **50 Hz**: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. ● **60 Hz**: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**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 controlador de acceso ajusta automáticamente el brillo de las imágenes según el entorno. ● **Prioridad de obturador**:El controlador de acceso ajusta el brillo de la imagen según 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 controlador de acceso 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**Anti-parpadeo**lista, puedes seleccionar **Prioridad de obturador**como el modo de exposición. ◇ El modo de exposición puede variar según los modelos de controlador de acceso.
Obturador	El obturador es un componente que permite el paso de la luz durante un tiempo determinado. Cuanto mayor sea la velocidad de obturación, menor será el tiempo de exposición y más oscura será la imagen.
Ganar	Cuando se establece el rango de valores de ganancia, se mejorará la calidad del video.
Exposición Compensación	El vídeo será más brillante al ajustar el valor de compensación de exposición.
Reducción de ruido 3D	Cuando la Reducción de ruido 3D (RD) está activada, se puede reducir el ruido del video para garantizar una mayor definición de los videos. Puede configurar su grado cuando esta función está activada. Un grado más alto significa una imagen más clara.
Calificación	

Paso 6 Configurar la imagen.

Figura 3-32 Imagen

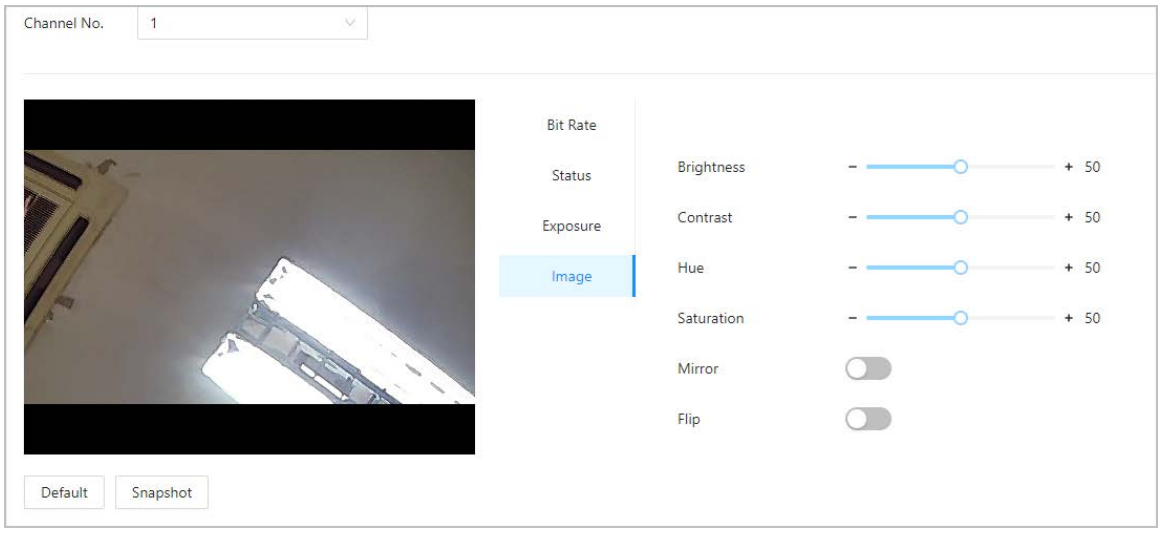


Tabla 3-22 Descripción de la imagen

Parámetro	Descripción
Brillo	El brillo de la imagen. Cuanto mayor sea el valor, más brillantes serán las imágenes.
Contraste	El contraste es la diferencia de luminancia o color que permite distinguir un objeto. Cuanto mayor sea el valor de contraste, mayor será el contraste de color.
Matiz	Se refiere a la fuerza o saturación de un color. Describe la intensidad del color o su pureza.
Saturación	La saturación del color indica la intensidad del color en una imagen. A medida que aumenta la saturación, el color se vuelve más intenso, por ejemplo, más rojo o más azul. El valor de saturación no cambia el brillo de la imagen.
Espejo	Cuando la función está activada, las imágenes se mostrarán con el lado izquierdo y el derecho invertidos.
Voltear	Cuando esta función está activada, las imágenes se pueden voltear.

3.8.1.2 Configuración del canal 2

Procedimiento

Paso 1 Seleccionar**Configuración de audio y video**>

Paso 2 **Video**. Seleccionar**2**desde**Canal No.**lista.

Paso 3 Seleccione 2 de la**Canal No.**. Configure el

Paso 4 estado del vídeo.

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

Figura 3-33 Estado de configuración

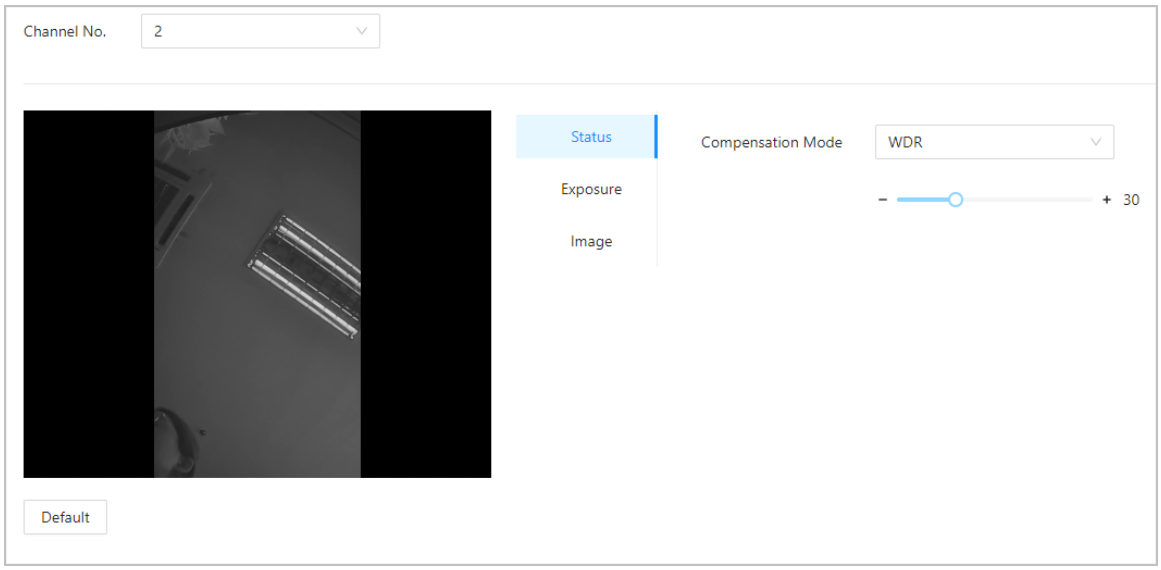


Tabla 3-23 Descripción del estado

Parámetro	Descripción
Modo de compensación	● **Desactivar**:La compensación está desactivada. ● **BLC**:La compensación de luz de fondo aporta automáticamente más luz a las áreas más oscuras de una imagen cuando la luz brillante que brilla detrás la oscurece. ● **Amplio rango dinámico (WDR)**:El sistema atenúa las áreas brillantes y compensa las áreas oscuras para crear un equilibrio que mejore la calidad general de la imagen. ● **HLCC (Centro de Información de Conducta Humana)**:La compensación de luces altas (HLC) es una tecnología que se utiliza en las cámaras de seguridad CCTV/IP para tratar imágenes expuestas a luces como faros o focos. El sensor de imagen de la cámara detecta luces fuertes en el video y reduce la exposición en esos puntos para mejorar la calidad general de la imagen.

Paso 5 Configurar los parámetros de exposición.

Figura 3-34 Parámetro de exposición

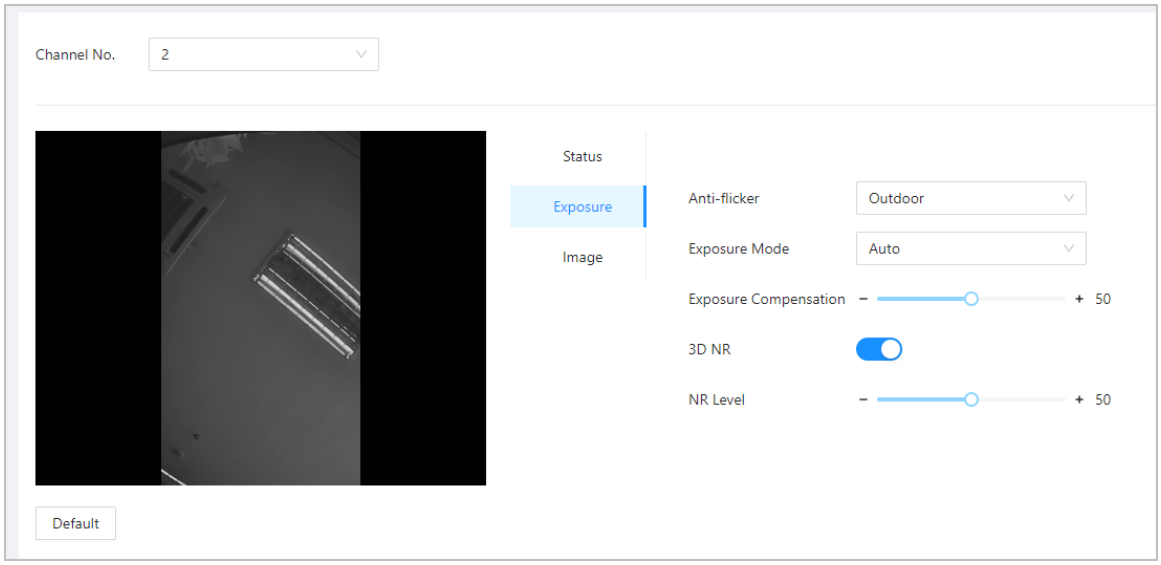


Tabla 3-24 Descripción de los parámetros de exposición

Parámetro	Descripción
Anti-parpadeo	Configure el antiparpadeo para reducir el parpadeo y disminuir o reducir los colores desiguales o la exposición. ● **50 Hz**: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. ● **60 Hz**: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**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 controlador de acceso ajusta automáticamente el brillo de las imágenes según el entorno. ● **Prioridad de obturador**:El controlador de acceso ajusta el brillo de la imagen según 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 controlador de acceso 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**Anti-parpadeo**lista, puedes seleccionar**Prioridad de obturador**como el modo de exposición. ◇ El modo de exposición puede variar según los modelos de controlador de acceso.
Exposición Compensación	El vídeo será más brillante al ajustar el valor de compensación de exposición.
Reducción de ruido 3D	Cuando la Reducción de ruido 3D (RD) está activada, se puede reducir el ruido del video para garantizar una mayor definición de los videos.
Nivel NR	Puede configurar su grado cuando esta función está activada. Un grado más alto significa una imagen más clara.

Paso 6 Configurar los parámetros de la imagen.

Figura 3-35 Parámetros de la imagen

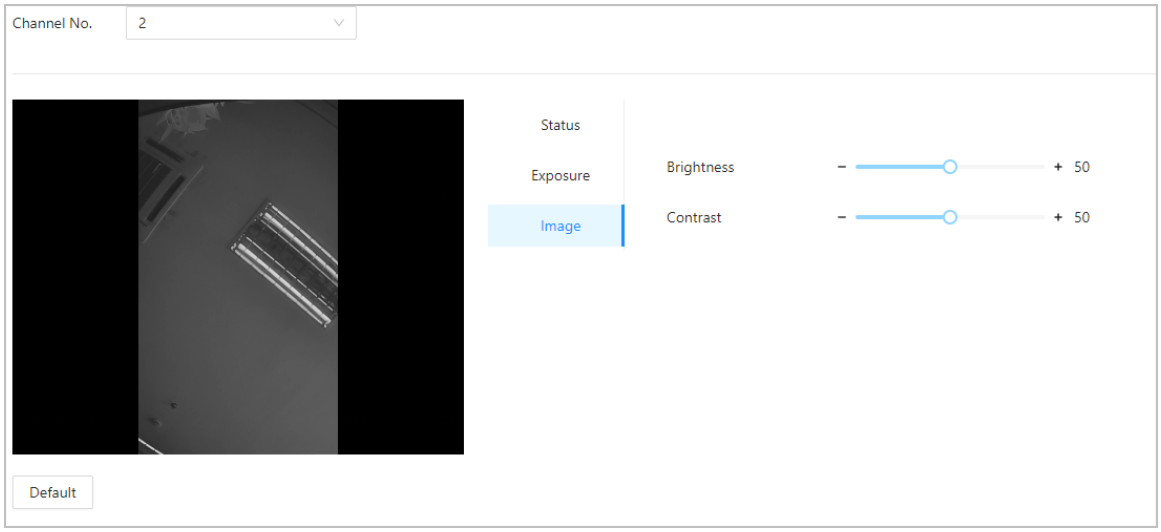


Tabla 3-25 Descripción de la imagen

Parámetro	Descripción
Brillo	El brillo de la imagen. Cuanto mayor sea el valor, más brillantes serán las imágenes.
Contraste	El contraste es la diferencia de luminancia o color que permite distinguir un objeto. Cuanto mayor sea el valor de contraste, mayor será el contraste de color.

3.8.2 Configuración de indicaciones de audio

Establecer indicaciones de audio durante la verificación de identidad.

Procedimiento

Paso 1 Seleccionar**Configuración de audio y video**>**Audio**

Paso 2 . Configure los parámetros de audio.

Figura 3-36 Configurar parámetros de audio

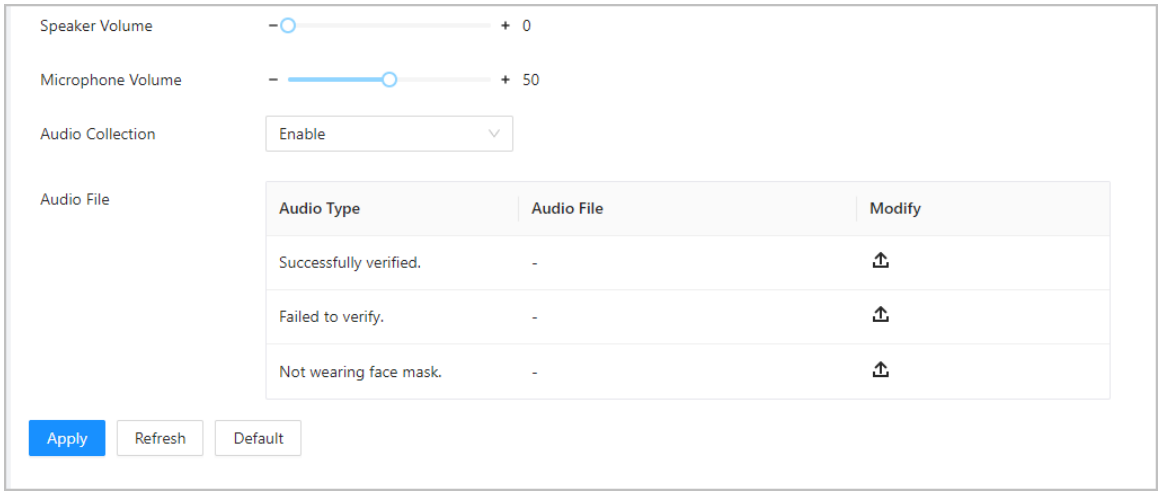


Tabla 3-26 Descripción de parámetros

Parámetros	Descripción
Vocero	Arrastre el control deslizante para ajustar el volumen del altavoz.
Volumen del micrófono	Arrastre el control deslizante para ajustar el volumen del micrófono.
Colección de audio	El audio no se grabará durante la conversación por vídeo cuando esta función no esté habilitada.
Archivo de audio	Haga clic en Subir archivos de audio a la plataforma.

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

El formato es MP3 y el tamaño es inferior a 20 KB.

Paso 4 Hacer clic**Aplicar**.

3.8.3 Configuración de la detección de movimiento

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

Procedimiento

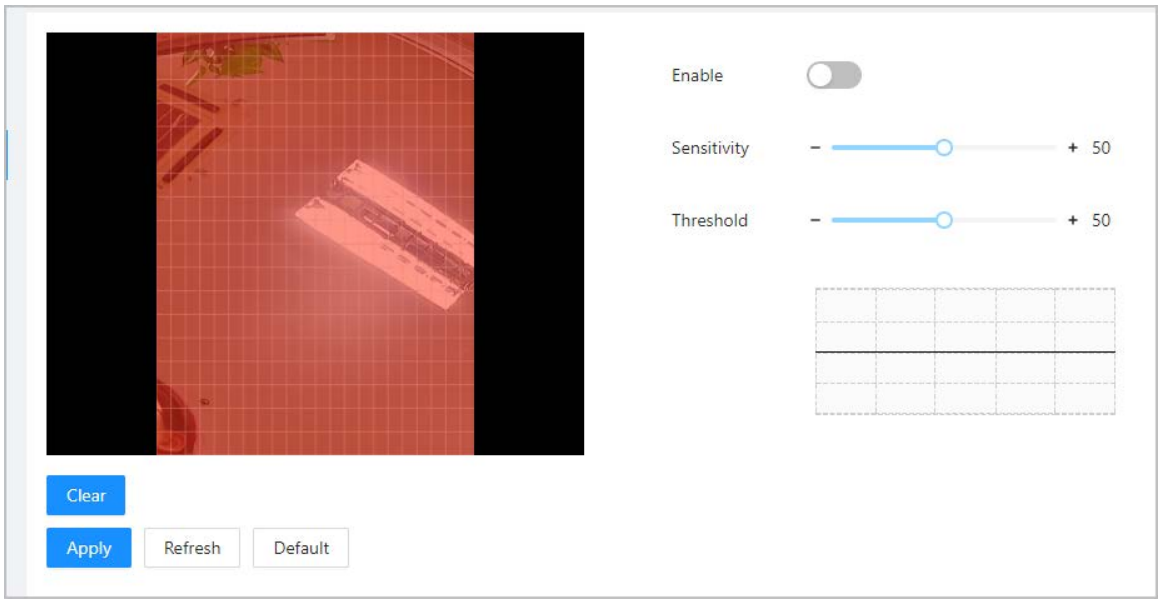
Paso 1 Seleccionar**Configuración de audio y video**>**Configuración de detección de**

Paso 2 **movimiento**. 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 3-37 Área de detección de movimiento



Paso 4 Configurar los parámetros.

- Sensibilidad: Sensibilidad al entorno. Cuanto mayor sea la sensibilidad, más fácil será activar las alarmas.
- Umbral: porcentaje del área del objeto en movimiento en el área de detección de movimiento. Cuanto más alto sea el umbral, más fácil será activar las alarmas.

Paso 5 Hacer clic**Aplicar**.

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

3.8.4 Configuración de la codificación local

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

Información de contexto

- Esta función solo está disponible en modelos seleccionados.
- Esta función está habilitada de manera predeterminada cuando funciona con un VTH. La vista previa puede no ser accesible cuando esta función está deshabilitada.

Procedimiento

Paso 1 Inicie sesión en la página web.

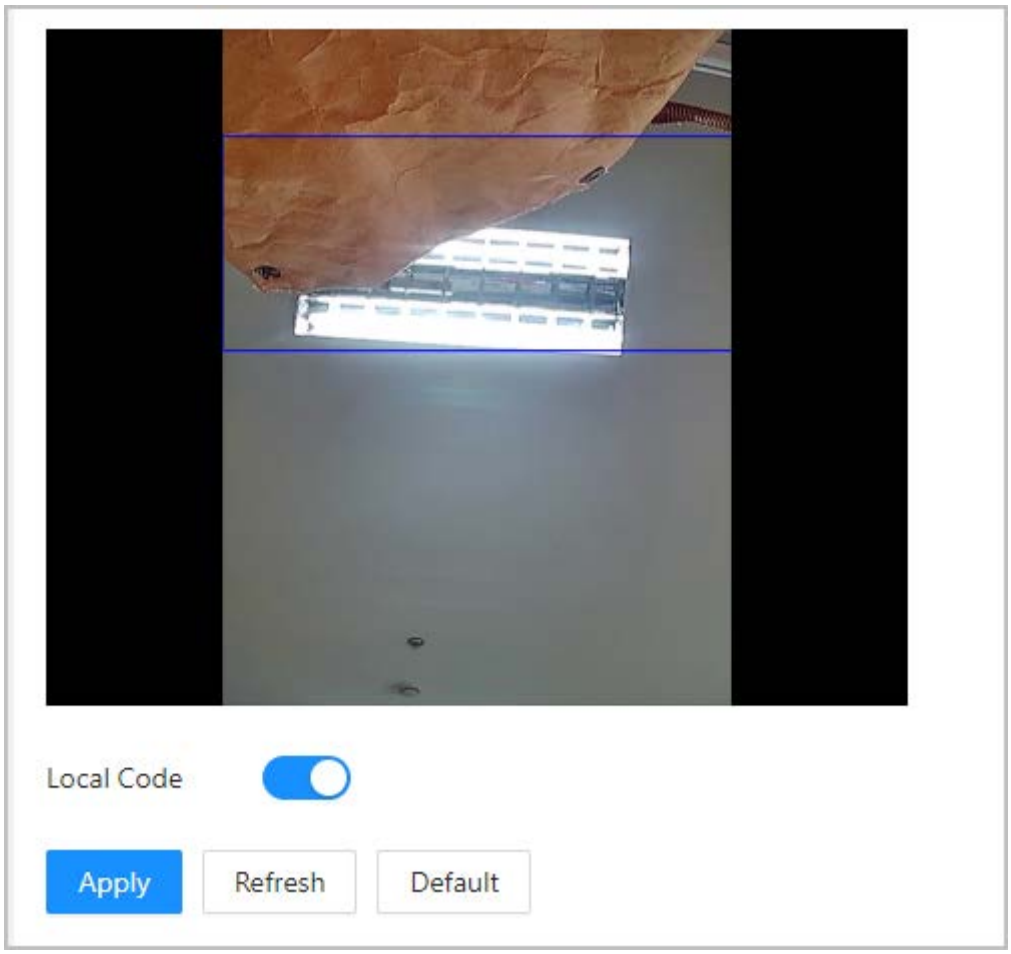
Paso 2 Seleccionar**Configuración de audio y video**>**Configuración de detección de**

Paso 3 **movimiento**. Seleccionar**Permitir**Para activar la función, arrastre el cuadro a la

Paso 4 posición designada.

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

Figura 3-38 Codificación local



Paso 5 Hacer clic**Aplicar**.

3.9 Configuración de la red

3.9.1 Configuración de TCP/IP

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

Procedimiento

Paso 1 Seleccionar**Configuración de comunicación**>**Protocolo TCP/**

Paso 2 **IP**. Configure los parámetros.

Figura 3-39 TCP/IP

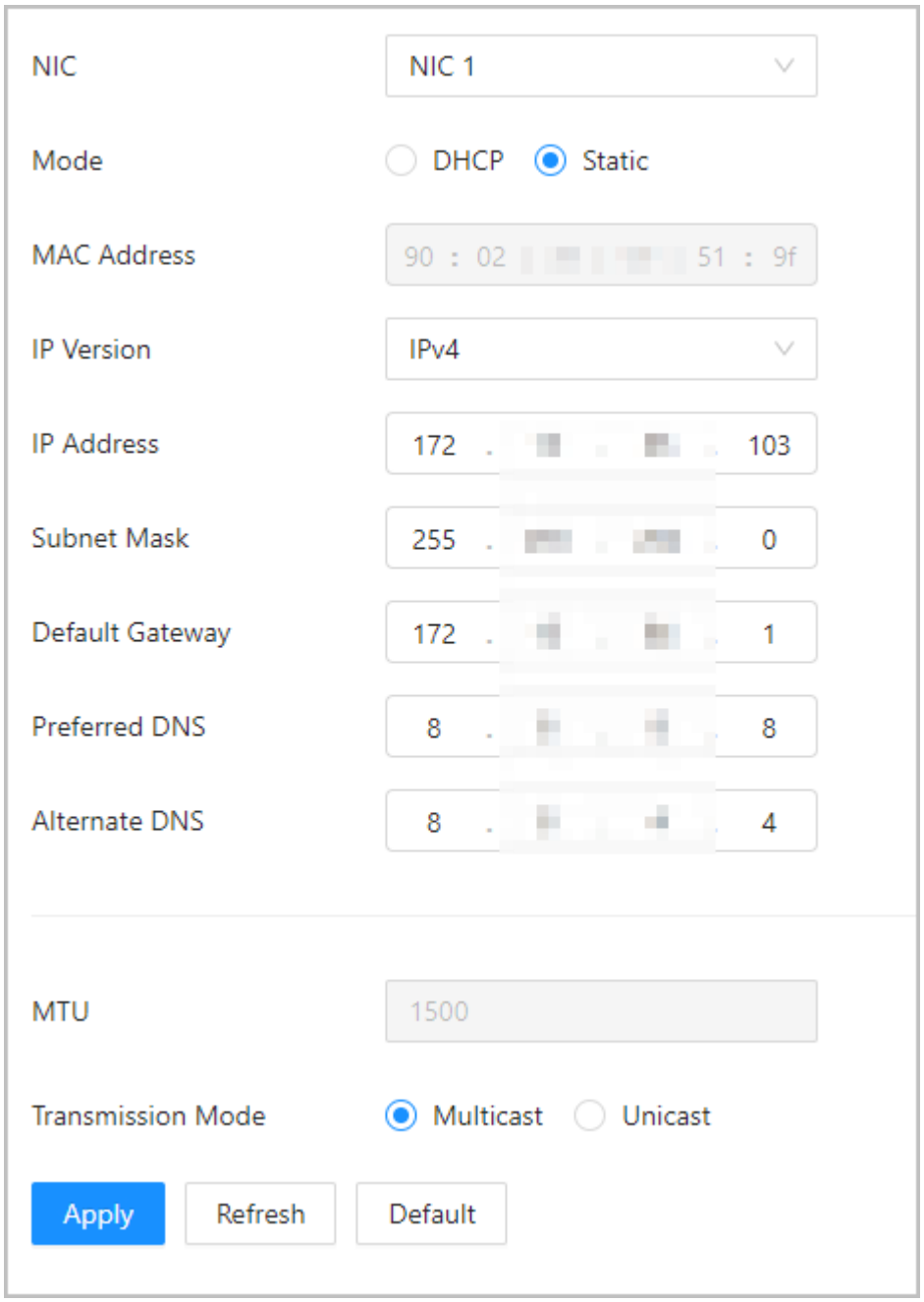


Tabla 3-27 Descripción de TCP/IP

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 se activa DHCP, se le asignará automáticamente una dirección IP, una máscara de subred y una puerta de enlace al controlador de acceso.
Dirección MAC	Dirección MAC del controlador de acceso.
Versión IP	IPv4 o IPv6.
Dirección IP	Si configura el modo en**Estático**, configure la dirección IP, la máscara de subred y la puerta de enlace.
Máscara de subred	

Parámetro	Descripción
Puerta de enlace predeterminada	 ● La dirección IPv6 se representa en hexadecimal. ● La versión IPv6 no requiere que se configuren máscaras de subred. ● La dirección IP y la puerta de enlace predeterminada deben estar en el mismo segmento de red.
DNS preferido	Establezca la dirección IP del servidor DNS preferido.
DNS alternativo	Establecer la dirección IP del servidor DNS alternativo.
Unidad de medida máxima	MTU (Unidad máxima de transmisión) se refiere al tamaño máximo de datos que se pueden transmitir en un único 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 red no puede manejar paquetes de un tamaño específico, puede producirse una fragmentación de paquetes o errores de transmisión. En las redes Ethernet, el valor de MTU común es de 1500 bytes. Sin embargo, en ciertos casos, como el uso de PPPoE o VPN, pueden requerirse valores de MTU más pequeños para satisfacer los requisitos de protocolos o servicios de red específicos. A continuación, se indican los 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 conversaciones por vídeo. ● Unicast: ideal para llamadas grupales.

Paso 3 Hacer clic**DE ACUERDO**.

3.9.2 Configuración de Wi-Fi

Procedimiento

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

Paso 2 Encienda el Wi-Fi.

Se muestran todas las conexiones WiFi disponibles.

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

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

3.9.3 Configuración del puerto

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

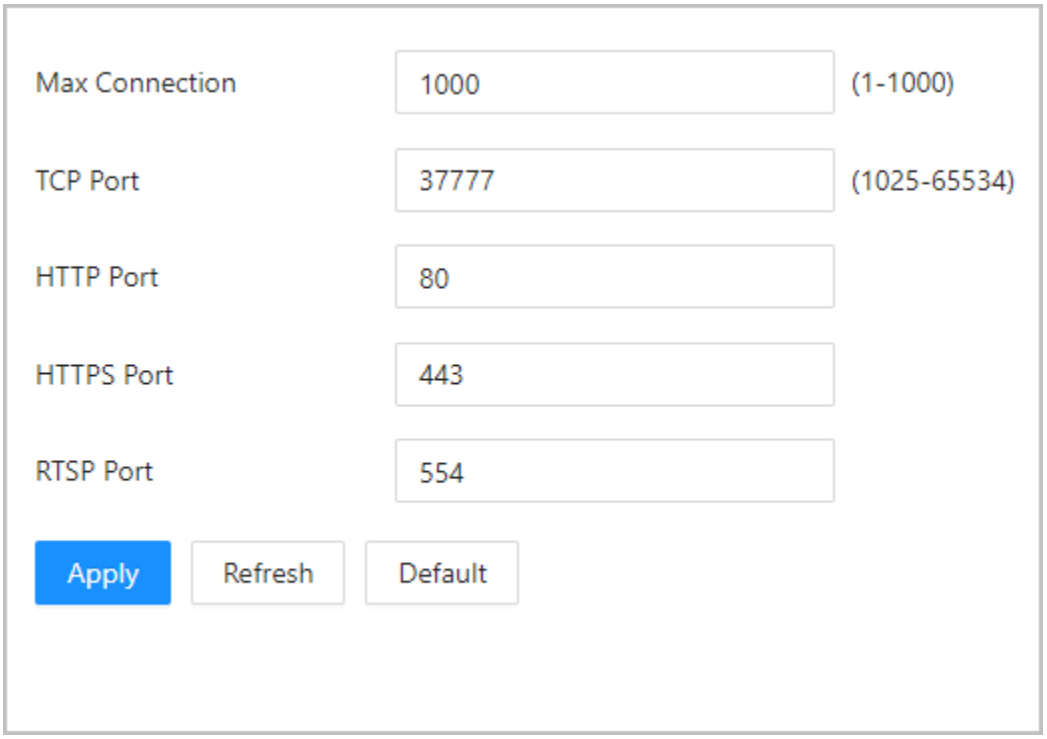
Cliente móvil.

Procedimiento

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

Paso 2 Configurar los puertos.

Figura 3-40 Configurar puertos



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

Tabla 3-28 Descripción de los 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 controlador de acceso al mismo tiempo.
Puerto TCP	El valor predeterminado es 37777.
Puerto HTTP	El valor predeterminado es 80. Si ha cambiado el número de puerto, agregue el número de puerto 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**.

3.9.4 Configuración del servicio básico

Cuando desee conectar el controlador de acceso a una plataforma de terceros, active el CGI y

Funciones ONVIF.

Procedimiento

Paso 1 Seleccionar**Configuración de red**>**Servicios básicos**.

Paso 2 Configurar el servicio básico.

Figura 3-41 Servicio básico

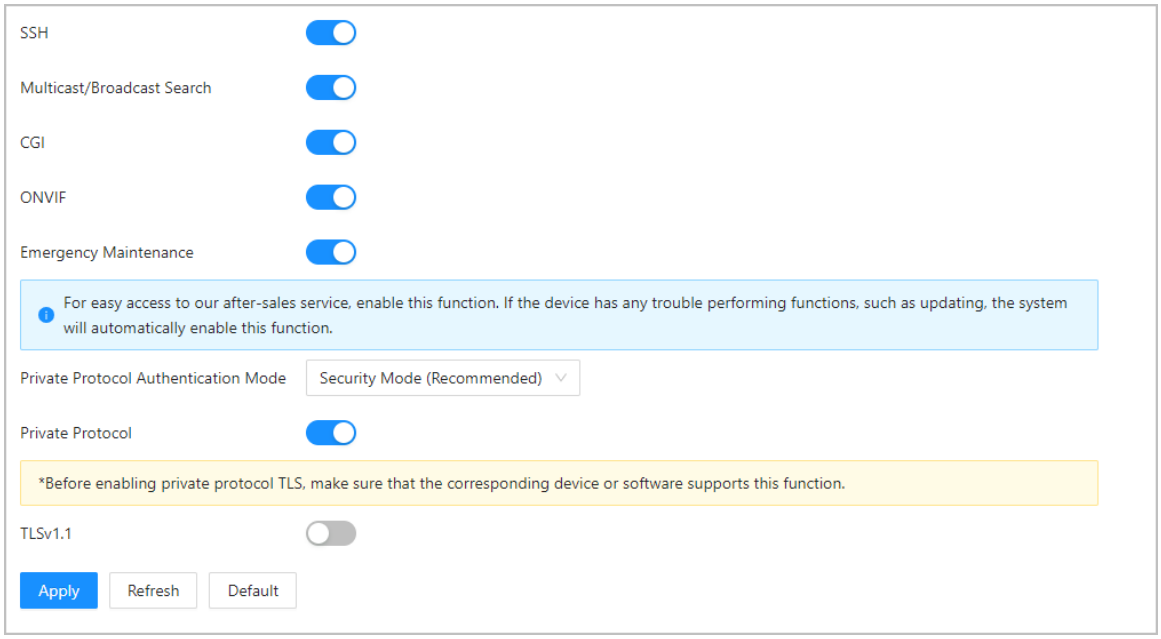


Tabla 3-29 Descripción de los parámetros básicos del servicio

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 multicast/transmisión	Busque dispositivos a través del protocolo multicast o broadcast.
CGI	La Interfaz de Puerta de Enlace Común (CGI) es una intersección entre servidores web a través de la cual es posible el intercambio de datos estandarizado entre aplicaciones externas y servidores.
ONVIF	ONVIF son las siglas de Open Network Video Interface Forum. Su objetivo es proporcionar un estándar para la interfaz entre diferentes dispositivos de seguridad basados en IP. Estos estándares ONVIF Las especificaciones son como un lenguaje común que todos los dispositivos pueden usar para comunicarse.
Mantenimiento de emergencia	Está activado de forma predeterminada.
Protocolo privado Modo de autenticación	Establezca 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 los métodos de autenticación Digest, DES y texto sin formato, lo que mejora la seguridad del dispositivo. ● Modo compatible: admite el acceso al dispositivo a través de métodos de autenticación Digest, DES y texto simple, con seguridad reducida.

Parámetro	Descripción
Protocolo privado	La plataforma agrega dispositivos a través del protocolo TLSv1.1.  Pueden presentarse riesgos de seguridad cuando se habilita TLSv1.1. Tenga en cuenta lo siguiente.

Paso 3 Hacer clic**Aplicar**.

3.9.5 Configuración del servicio en la nube

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

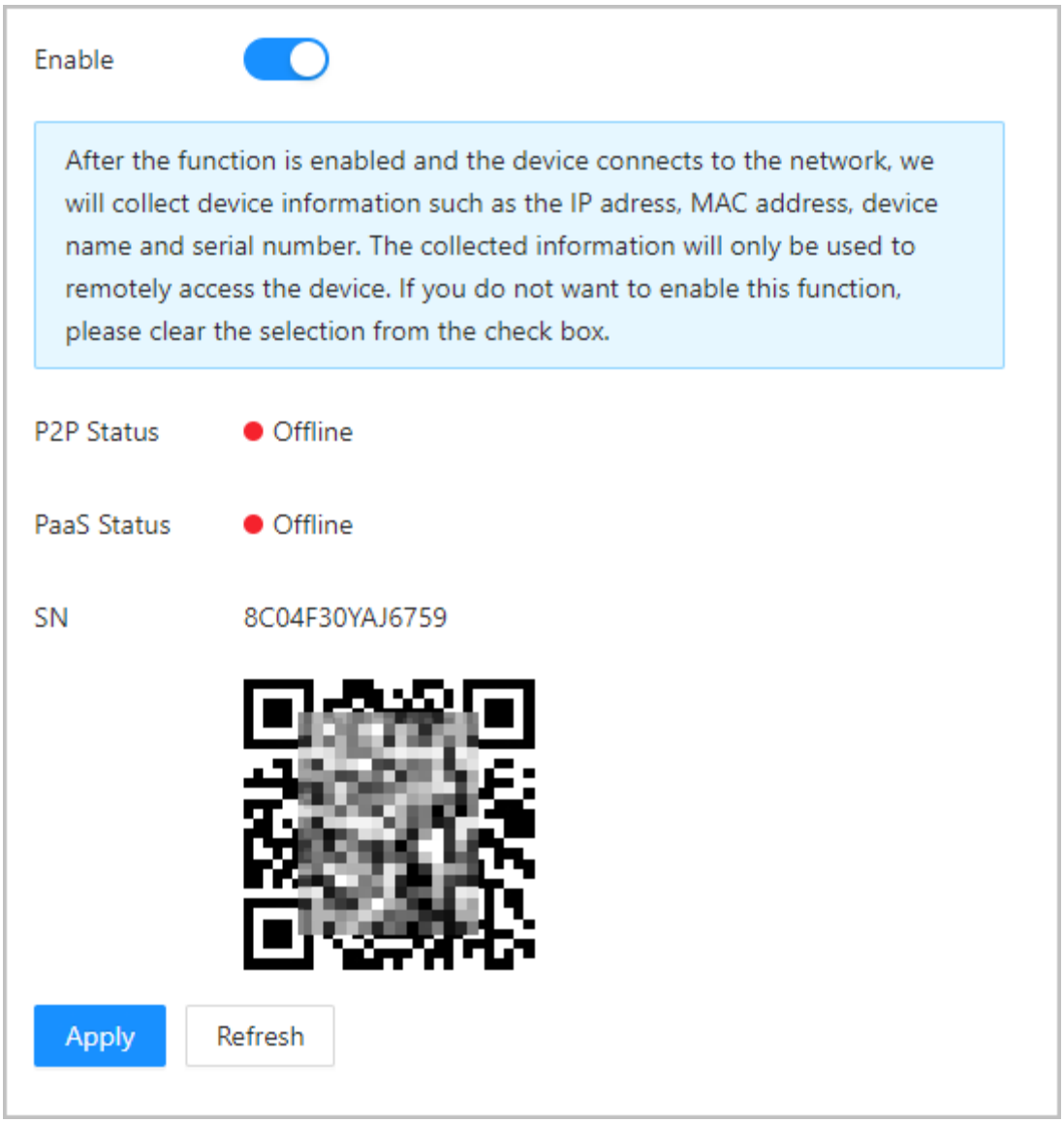
Procedimiento

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

Paso 2 . Activa la función de servicio en la nube.

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

Figura 3-42 Servicio en la nube



Paso 3 Hacer clic**Aplicar**.

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

3.9.6 Configuración del registro activo

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

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 3-43 Registro automático

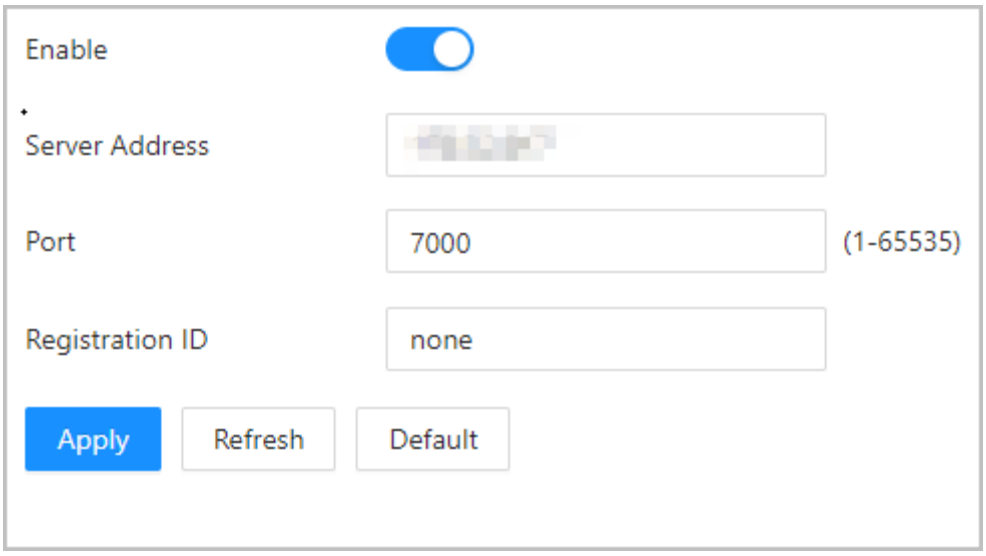


Tabla 3-30 Descripción del registro automático

Parámetro	Descripción
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.
ID 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 Configuración de RS-485

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

Procedimiento

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

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

Figura 3-44 Configurar parámetros

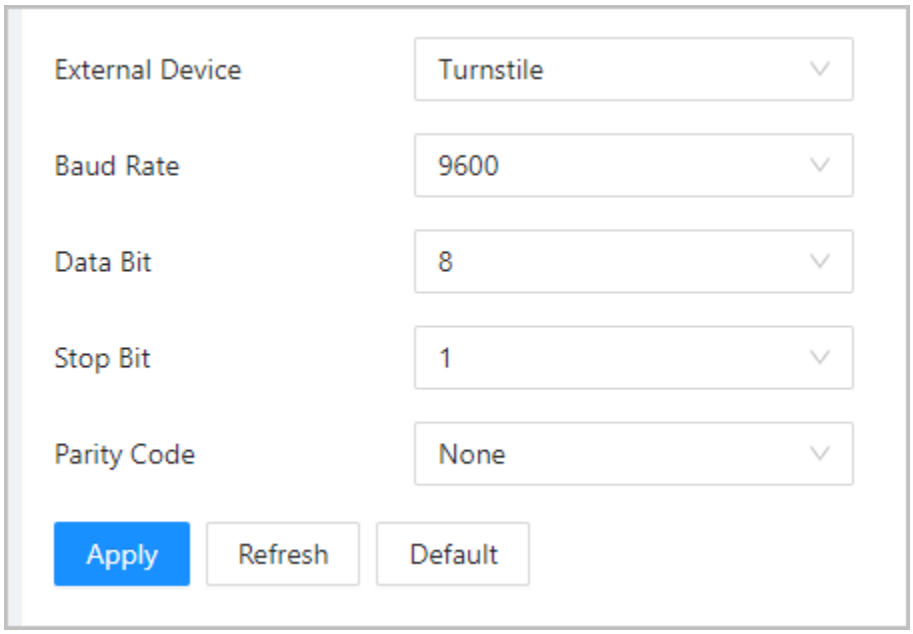


Tabla 3-31 Configurar el formato Wiegand

Parámetro	Descripción
Dispositivo externo	● Controlador de acceso: Seleccionar**Controlador de acceso**cuando el controlador de acceso funciona como un lector de tarjetas, y el controlador de acceso enviará datos al controlador de acceso para controlar el acceso. Tipo de datos de salida: ◇ Número de tarjeta: emite datos basados en el número de tarjeta cuando los usuarios pasan la tarjeta para desbloquear la puerta; emite datos basados en el primer número de tarjeta del usuario cuando utilizan otros métodos de desbloqueo. ◇ No.: Genera datos en función del ID del usuario. ● Lector de tarjetas: el controlador de acceso se conecta a un lector de tarjetas. ● Lector (OSDP): El controlador de acceso 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 después de que se habilita el módulo de seguridad. ● Torniquete: cuando el controlador de acceso se conecta a un torniquete, y la placa del controlador de acceso del torniquete se conecta a un módulo de código QR externo o un módulo de deslizamiento de tarjeta, la placa transmitirá los datos de verificación al torniquete.
Bit de datos	Número de bits que se utilizan para transmitir los datos reales en una comunicación serial. Representa los dígitos binarios que contienen 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 al receptor prepararse para el siguiente byte de datos y proporciona sincronización en el protocolo de comunicación.
Código de paridad	Un bit adicional que se envía después de los bits de datos para detectar errores de transmisión. Ayuda a verificar la integridad de los datos transmitidos al garantizar una cantidad específica de bits lógicos altos o bajos.

Paso 3 Hacer clic**Aplicar**.

3.11 Configuración de Wiegand

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

Procedimiento

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

Paso 2 Configure los parámetros.

Figura 3-45 Configurar parámetros

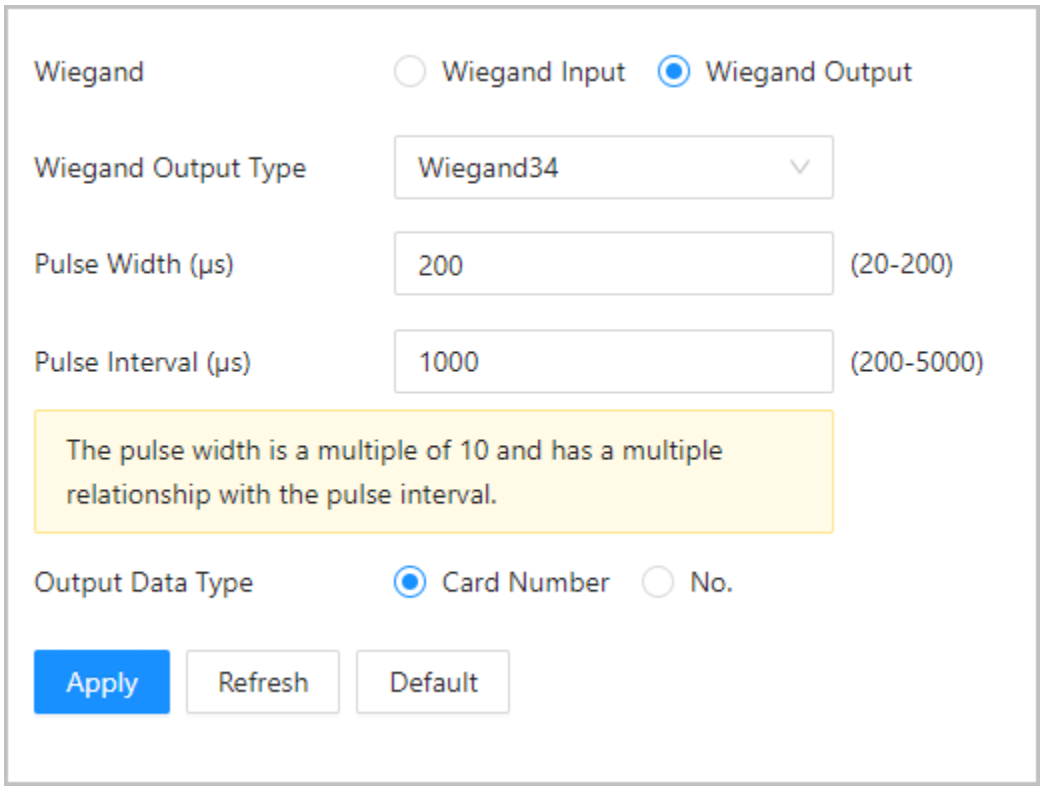


Tabla 3-32 Descripción de la salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	Seleccione un formato Wiegand para leer números de tarjeta o números de identificación. ● **Wiegand26**:Lee 3 bytes o 6 dígitos. ● **Wiegand34**:Lee 4 bytes u 8 dígitos. ● **Wiegand66**:Lee 8 bytes o 16 dígitos.

Parámetro	Descripción
Ancho de pulso	Introduzca el ancho de pulso y el intervalo de pulso de la salida Wiegand.
Intervalo de pulso	
Tipo de datos de salida	Seleccione el tipo de datos de salida. ● **No.**: Genera datos en función del ID del usuario. El formato de los datos es hexadecimal o decimal. ● **Número de tarjeta**:Emite datos basados en el primer número de tarjeta del usuario.

Paso 3 Hacer clic**Aplicar**.

3.12 Configuración del sistema

3.12.1 Gestión de usuarios

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

3.12.1.1 Agregar administradores

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

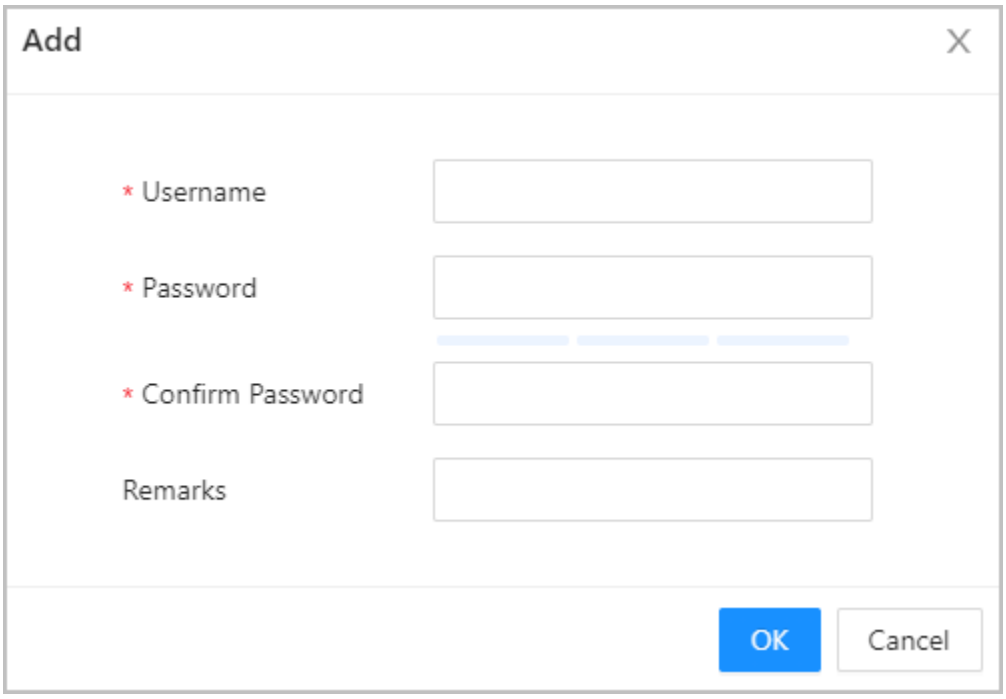
Procedimiento

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

Paso 2 en**Agregar**, e ingrese la información del usuario.

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

Figura 3-46 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.

3.12.1.2 Agregar usuarios ONVIF

Información de contexto

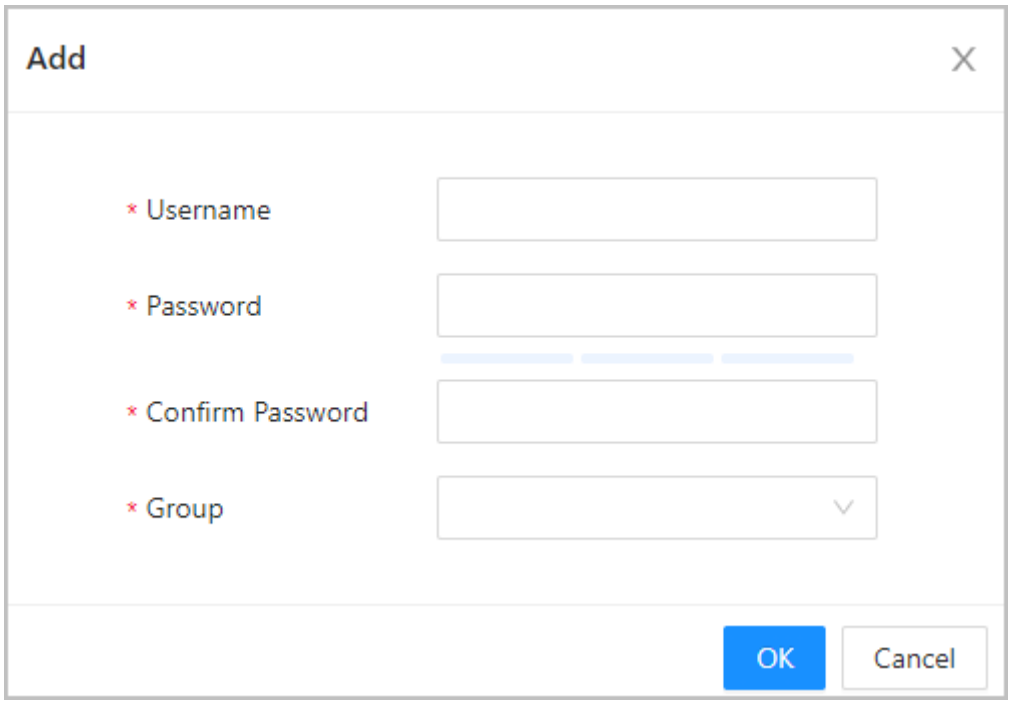
Open Network Video Interface Forum (ONVIF), un foro industrial abierto y global creado para desarrollar un estándar abierto global para la interfaz de productos de seguridad basados en IP físicos, que permite la compatibilidad de diferentes fabricantes. Los usuarios de ONVIF tienen sus identidades verificadas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

Procedimiento

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

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

Figura 3-47 Agregar usuario ONVIF



Paso 3 Hacer clicDE ACUERDO.

3.12.1.3 Restablecimiento de la contraseña

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

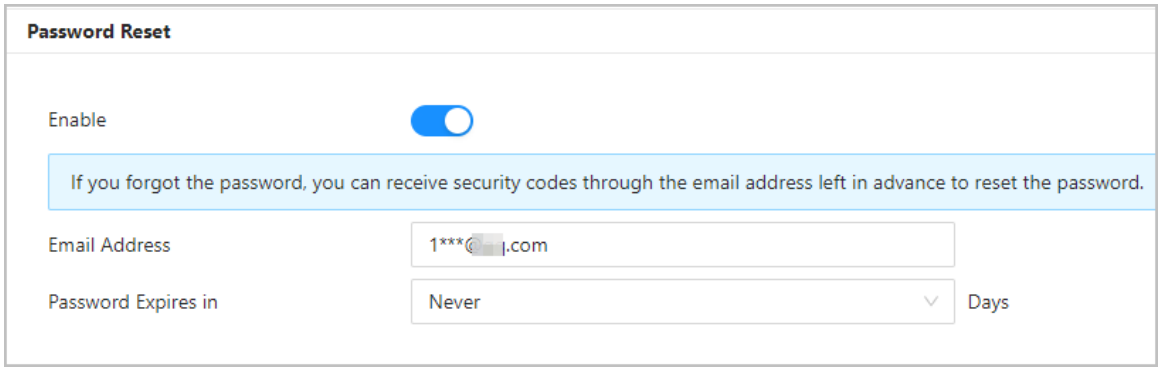
Procedimiento

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

Paso 2 Ingrese la dirección de correo electrónico y configure el tiempo de expiración de la contraseña.

Paso 3 Active la función de restablecimiento de contraseña.

Figura 3-48 Restablecer contraseña



Si olvidó la contraseña, puede recibir códigos de seguridad a través del correo electrónico vinculado Dirección para restablecer la contraseña.

Paso 4 Hacer clic**Aplicar**.

3.12.1.4 Visualización de usuarios en línea

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

Usuario en línea.

3.12.2 Configuración de la hora

Procedimiento

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

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

Figura 3-49 Configuración de fecha

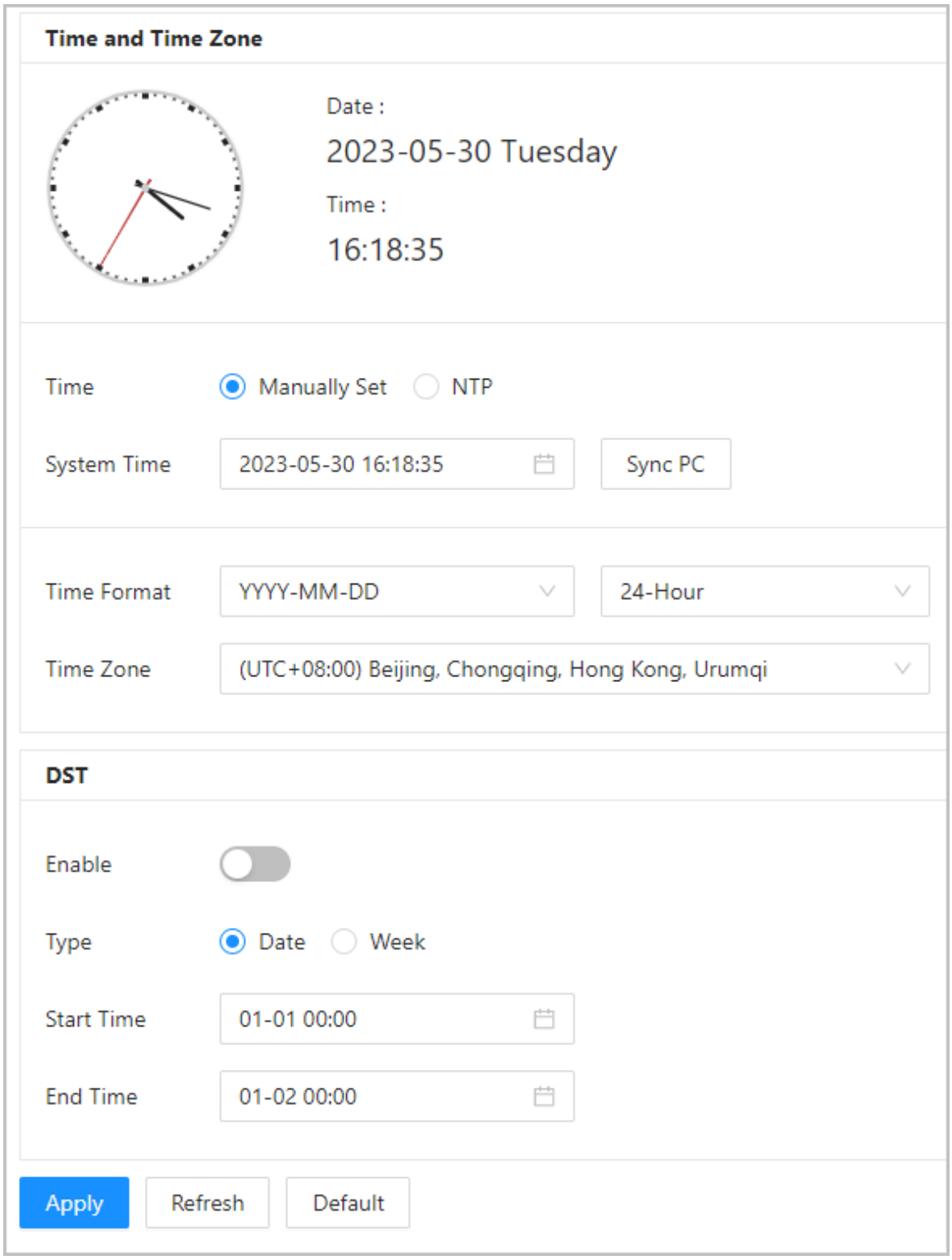


Tabla 3-34 Descripción de la configuración de tiempo

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

Paso 3 Hacer clic**Aplicar**.

3.12.3 Mantenimiento

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

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccione

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

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

El controlador de acceso se reiniciará a la hora programada, o puede hacer clic**Reanudar**para reiniciarlo inmediatamente.

3.12.4 Gestión de la configuración

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

3.12.4.1 Exportación e importación de archivos de configuración

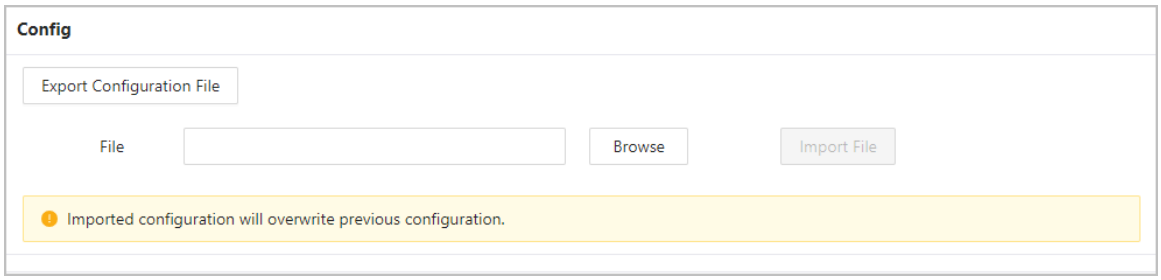
Puede importar y exportar el archivo de configuración del controlador de acceso. Cuando desee aplicar las mismas configuraciones a varios dispositivos, puede importarles el archivo de configuración.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccione**Sistema**>**Configuración**.

Figura 3-50 Gestión de configuración



Paso 3 Exportar o importar archivos de configuración.

- Exportar el archivo de configuración.

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

  La IP no se exportará.

- Importar 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.

3.12.4.2 Restauración de la configuración predeterminada de fábrica

Procedimiento

Paso 1 Seleccionar**Sistema**>**Configuración**.

Restaurando el**Controlador de acceso**a sus configuraciones predeterminadas resultará en pérdida de datos. Por favor estar aconsejado.

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

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

Sólo el controlador principal es compatible**Restaurar a valores predeterminados (excepto información de usuario y registros)**.

3.12.5 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 Access Controlador durante la actualización.

3.12.5.1 Actualización de archivos

Procedimiento

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

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

El archivo de actualización debe ser un archivo .bin.

Paso 3 Hacer clic**Actualizar**.

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

3.12.5.2 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**Búsqueda automática de actualizaciones**y el controlador de acceso buscará automáticamente la última actualización de la versión.
- Seleccionar**Comprobación manual**y podrás comprobar inmediatamente si la última versión está disponible.

Paso 3 (Opcional) Haga clic en**Actualizar ahora**para actualizar el controlador de acceso inmediatamente.

3.12.6 Visualización de la información de la versión

En la página web, seleccione**Sistema**>**Versión**, y puede ver la información de la versión del controlador de acceso.

3.12.7 Visualización de la capacidad de datos

En la página web, seleccione**Sistema**>**Capacidad de datos**, ver la capacidad de datos del controlador de acceso.

3.12.8 Visualización de información legal

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

3.13 Personalización

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

3.13.1 Agregar recursos

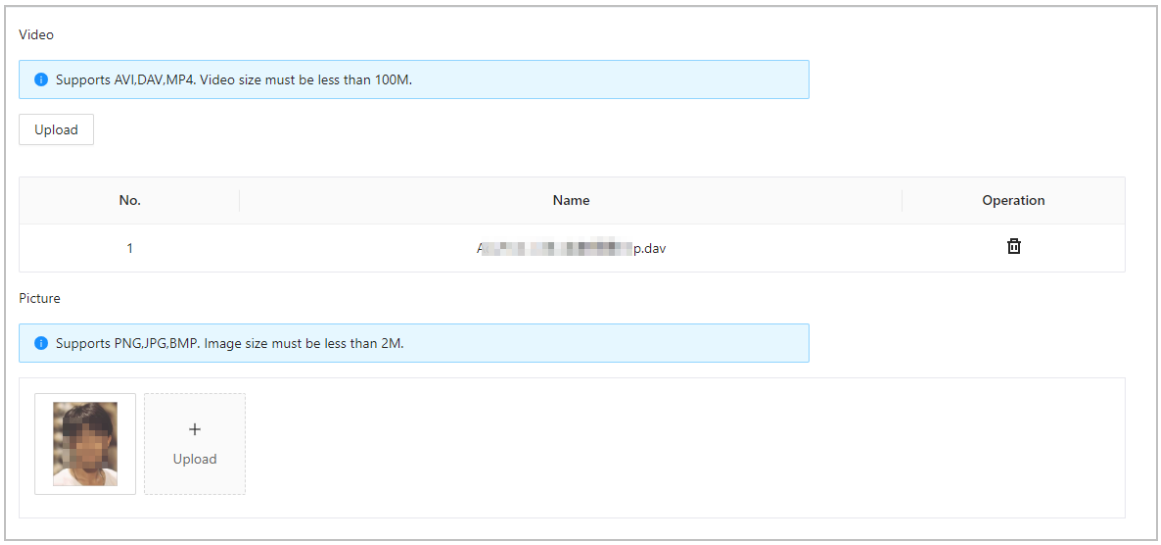
Agregue imágenes o videos para que se muestren en la pantalla de espera del controlador de acceso.

Procedimiento

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

Paso 2 videos o imágenes.

Figura 3-51 Agregar videos o imágenes



- Añadir videos.

  1. Haga clic**Subir**.

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

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

     - Puedes cargar hasta 5 archivos de vídeo.
     - Admite DAV, AVI y MP4. El tamaño del vídeo debe ser inferior a 100 M.
     - Solo es compatible con las últimas versiones de FireFox y Chrome para cargar archivos de vídeo.

- Añadir imágenes.

  1. Haga clic en .

2. Seleccione una imagen del local y cárguela.

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

Operaciones relacionadas

Hacer clic para eliminar imágenes o vídeos cargados.

Los vídeos y las imágenes en uso no se pueden eliminar.

3.13.2 Configuración de temas

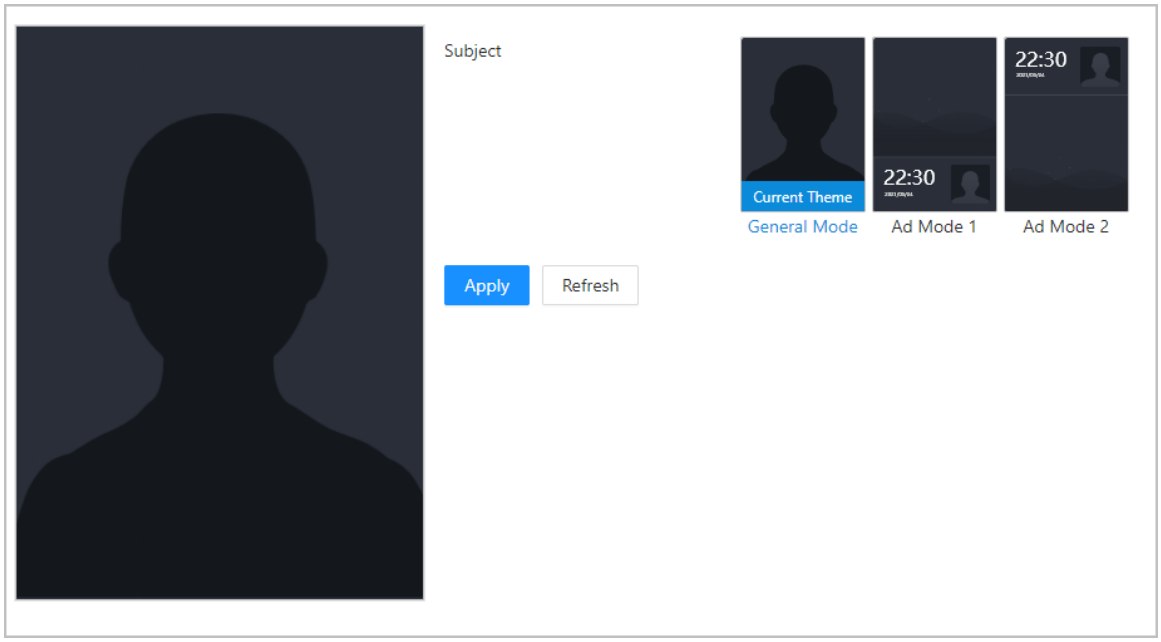
Procedimiento

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 rostro.
- Modo de anuncio 2: el área superior muestra la hora y el cuadro de detección de rostro, y el área inferior muestra los anuncios.

Figura 3-52 Tema

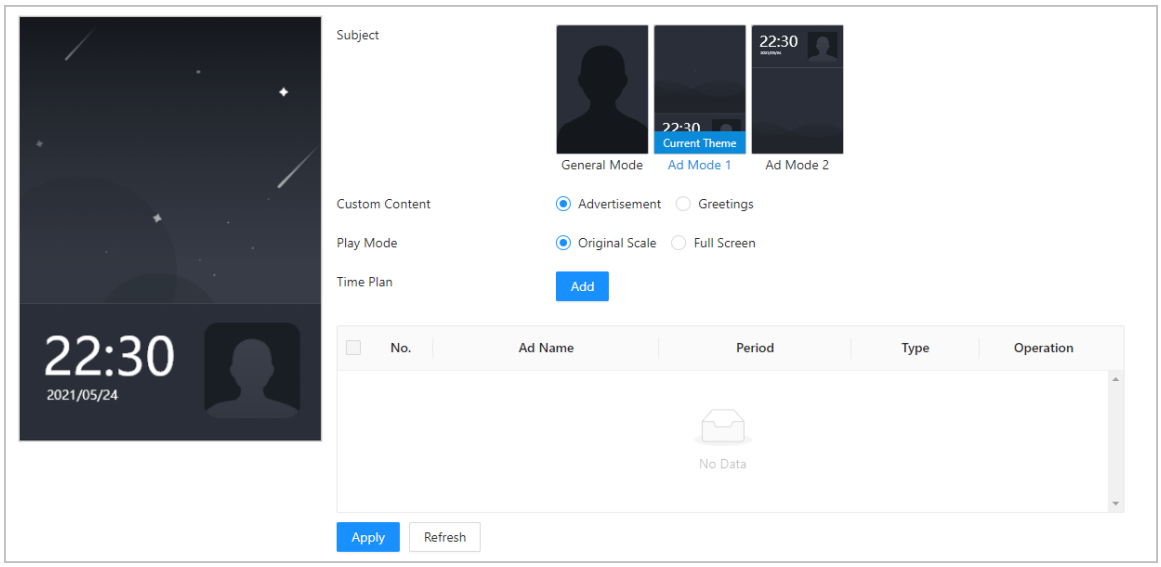


Paso 3 Seleccione el mensaje de voz para verificar la identidad correctamente.

Paso 4 Configure la visualización de anuncios.

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

Figura 3-53 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.

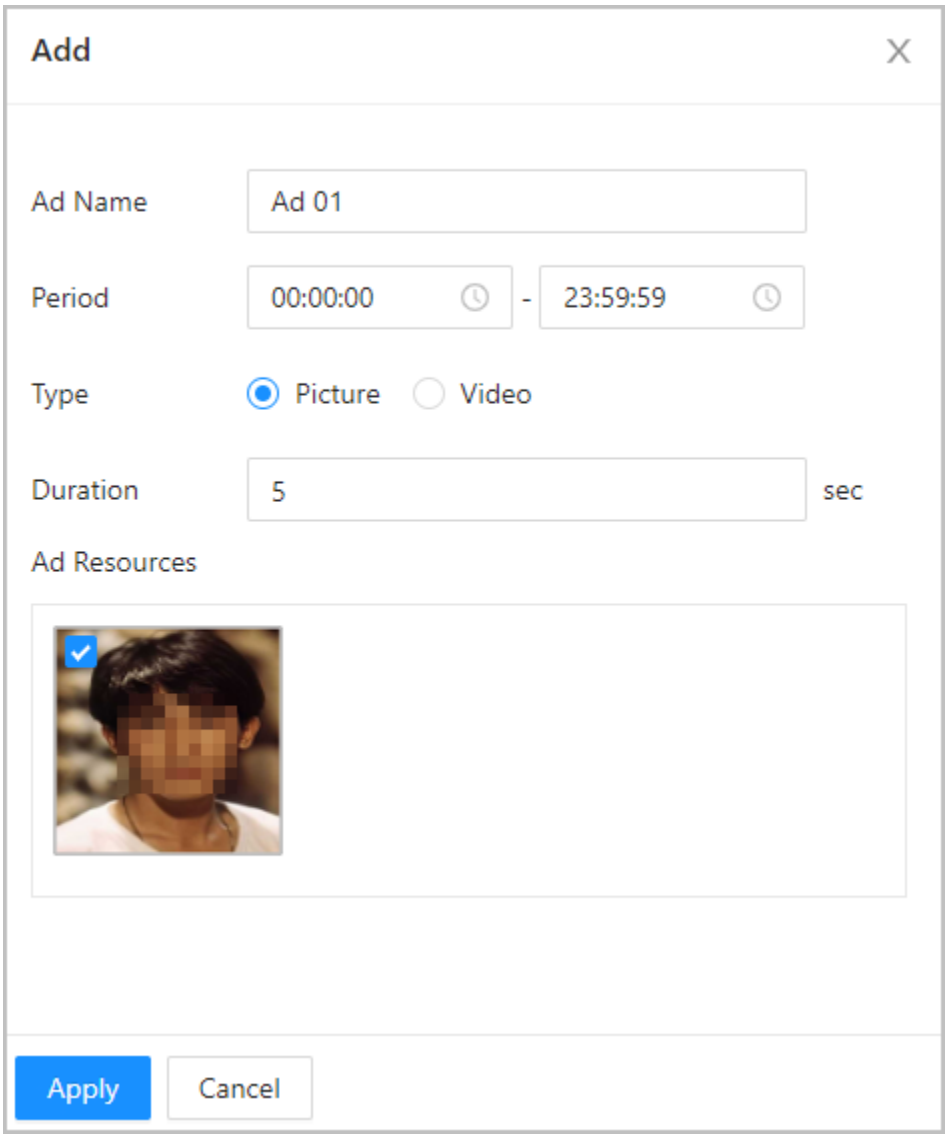
4. Ingrese el nombre del anuncio.

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

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

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

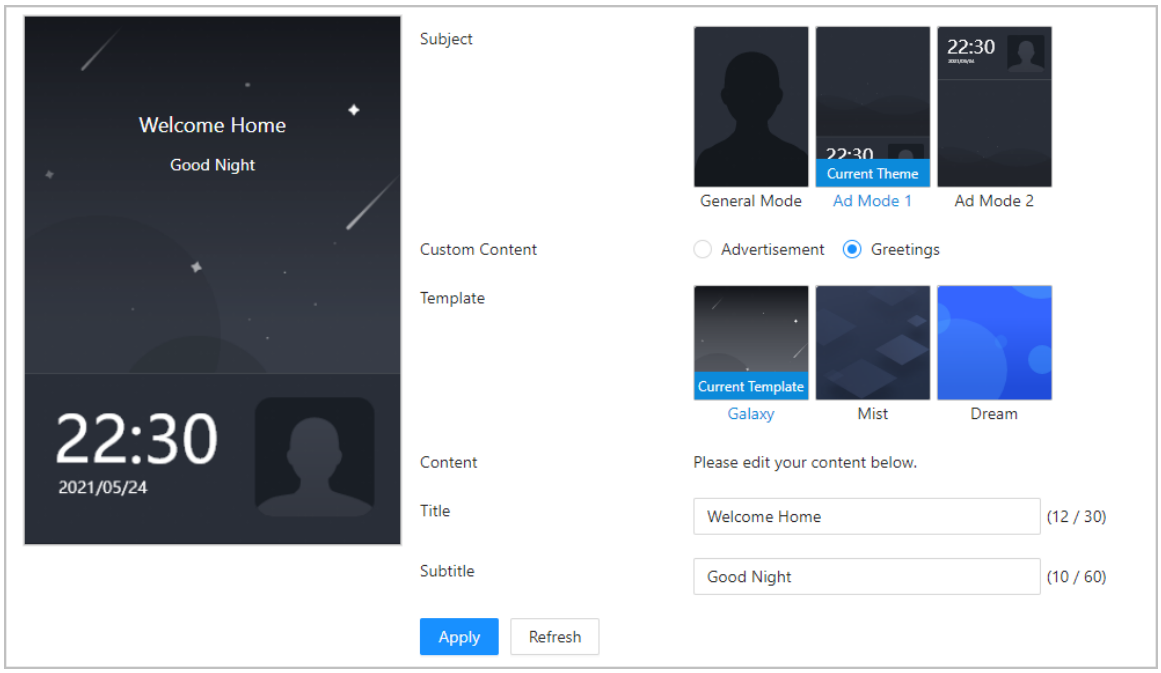
Figura 3-54 Agregar horarios



Paso 5 Configurar saludos.

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

Figura 3-55 Saludos



4. Haga clic**Aplicar**.

3.13.3 Configuración de los accesos directos

Procedimiento

Paso 1 En la página web del Controlador de Acceso, seleccione**Personalización**>**Configuración de acceso directo**.

Paso 2 Configure los parámetros del acceso directo.

Figura 3-56 Configuración de acceso directo

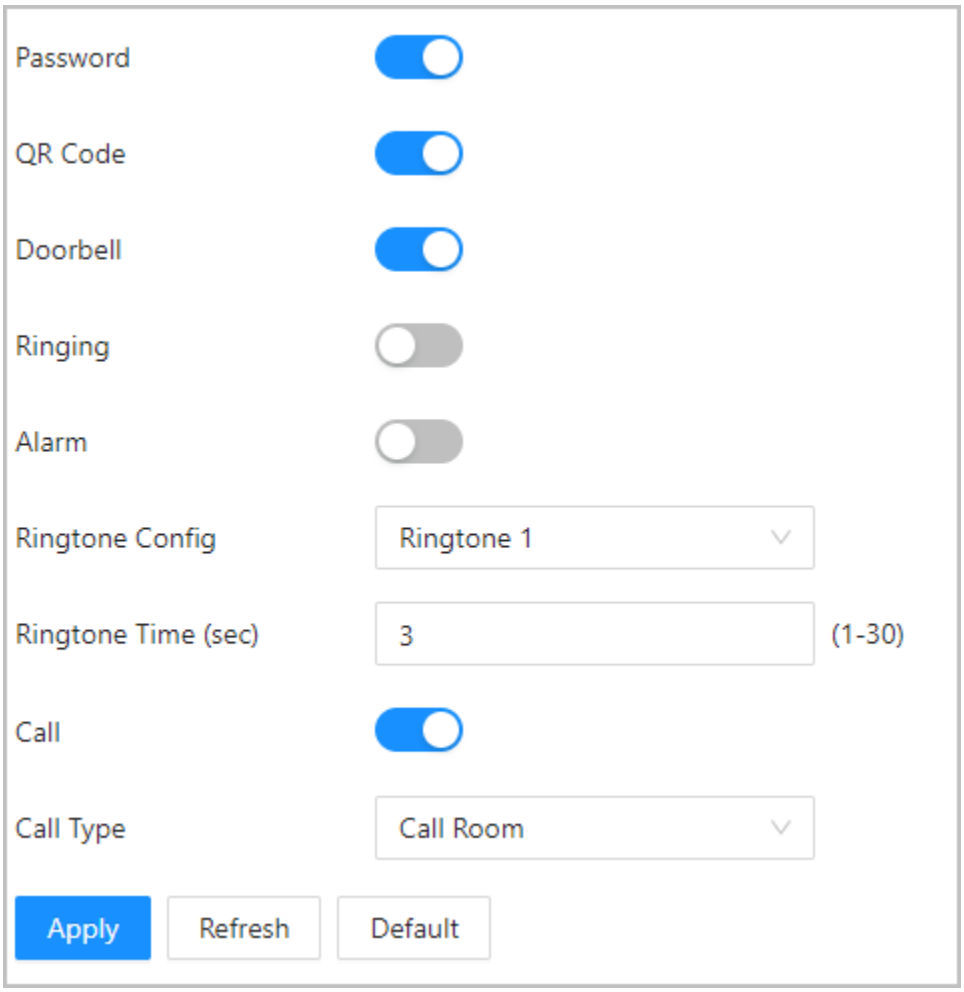


Tabla 3-35 1

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 el controlador de acceso con un módulo de código QR independiente.
Timbre de la puerta	Después de activar la función de timbre, el icono del timbre se muestra en la pantalla de espera. ● Timbre: Toque el ícono de timbre en la pantalla de espera y el controlador de acceso sonará. ● Alarma: active la función de vinculación de alarma y luego suena el timbre. Esta función solo está disponible en modelos seleccionados. ● Configuración de tono de llamada: seleccione el timbre de llamada. ● Duración del tono de llamada (seg): configure el tiempo de llamada (1-30 s). El valor predeterminado es 3.
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 habitación y luego puede tocar el ícono de llamada en la pantalla de espera para llamar al número de habitación predefinido.  Asegúrese de que el controlador de acceso se haya agregado a DMSS.

3.14 Visualización de registros

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

3.14.1 Registros del sistema

Ver y buscar registros del sistema.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccione**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**Copia de seguridad de registros cifrada**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.

3.14.2 Registros de administración

Busque registros de administración utilizando el ID de administrador.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccione

Paso 2 **Registro**>**Registro de administración**.

Paso 3 Ingrese el ID de administrador y luego haga clic en**Buscar**Haga clic en **Exportar**para exportar registros de administración.

3.14.3 Desbloqueo de registros

Busque registros de desbloqueo y expórtelos.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccione

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

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

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

3.14.4 Registros de alarmas

Ver registros de alarmas.

Procedimiento

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

Paso 2 **de alarmas**Seleccione el tipo y el rango de tiempo. Ingrese

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

Paso 4

3.14.5 Registros de llamadas

Ver registros de llamadas.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccione

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

3.14.6 Gestión USB

Exportar información del usuario desde/hacia USB.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccione**Registro**>**Gestión USB**.

- Asegúrese de que haya un USB insertado en el controlador de acceso antes de exportar datos o Actualizar el sistema. Para evitar fallas, no desconecte el USB ni realice ninguna operación. del Controlador de Acceso durante el proceso.
- Debe utilizar un USB para exportar la información de un controlador de acceso a otro dispositivos. No se permite importar imágenes faciales 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.

3.15 Capacidad de datos

Puede ver cuántos usuarios, tarjetas e imágenes faciales puede almacenar el controlador de acceso. Inicie sesión en la página web y seleccione**Capacidad de datos**.

3.16 Configuración de seguridad (opcional)

3.16.1 Estado de seguridad

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

Información de contexto

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

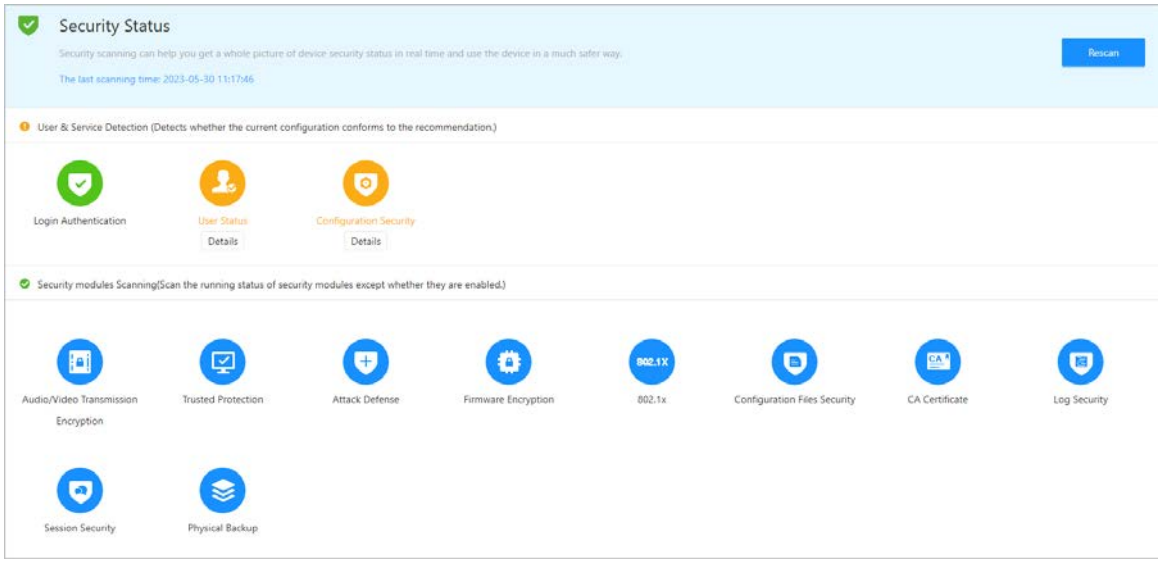
Procedimiento

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

Paso 2 Hacer clic**Volver a escanear**para realizar un escaneo de seguridad del controlador de acceso.

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

Figura 3-57 Estado de seguridad



Operaciones relacionadas

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

- Hacer clic**Detalles**para ver los detalles de los resultados del escaneo.
- Hacer clic**Ignorar**para ignorar la anomalía, y no se escaneará. La anomalía que se detectó

Los ignorados se resaltarán en gris.

- Hacer clic**Optimizar**para solucionar la anomalía.

3.16.2 Configuración de 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**Seguridad**>**Servicio del sistema**>

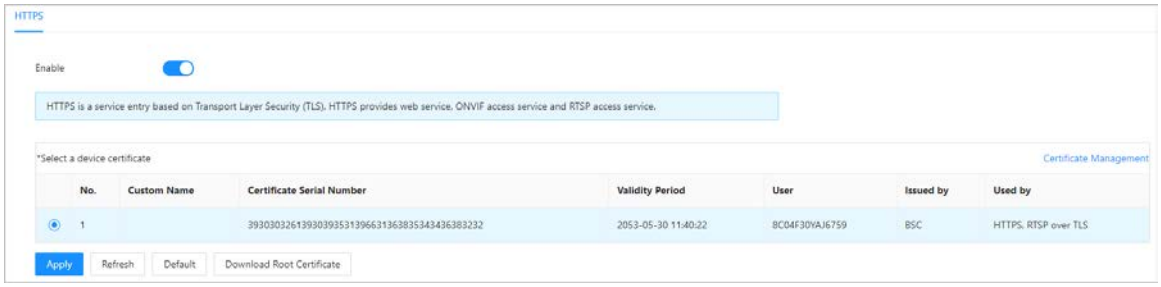
Paso 2 **HTTPS**. Activa el servicio HTTPS.

Si activa la compatibilidad con TLS v1.1 y versiones anteriores, podrían producirse 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 3-58 HTTPS



Paso 4 Hacer clic**Aplicar**.

Introduzca "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.

3.16.3 Defensa de ataque

3.16.3.1 Configuración del firewall

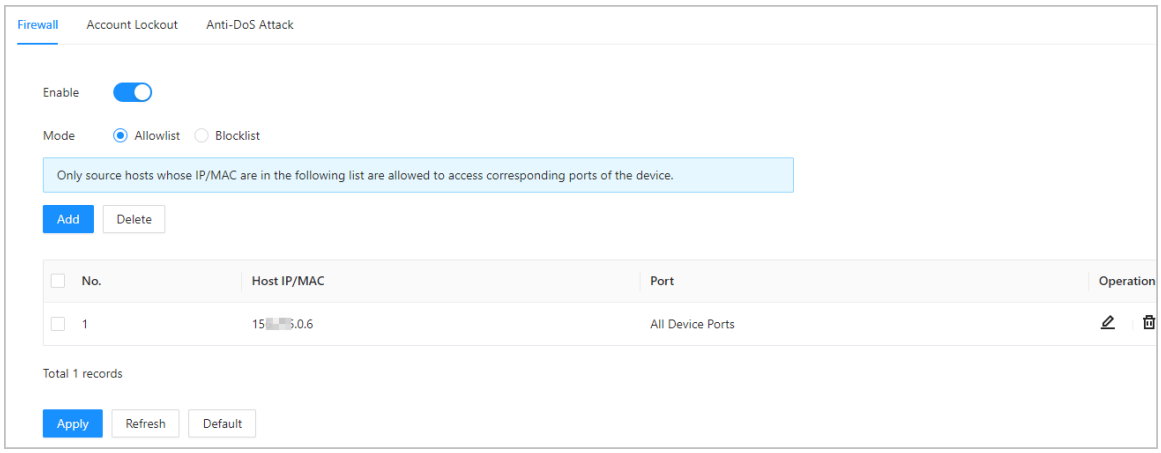
Configure el firewall para limitar el acceso al controlador de acceso.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Ataque Defensa**>**Cortafuegos**.

Paso 2 Haga clic para habilitar la función de firewall.

Figura 3-59 Cortafuegos

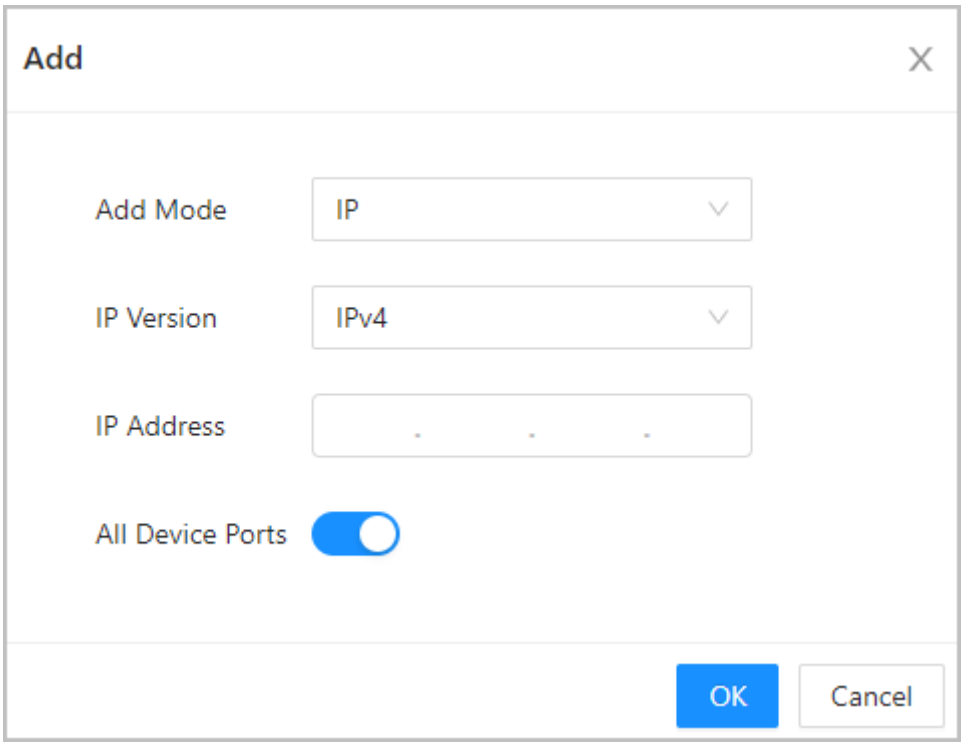


Paso 3 Seleccione el modo:**Lista de permitidos**y**Lista de bloqueo**.

- **Lista de permitidos**:Solo las direcciones IP/MAC en la lista blanca pueden acceder al controlador de acceso.
- **Lista de bloqueo**:Las direcciones IP/MAC en la lista de bloqueo no pueden acceder al controlador de acceso. Haga clic en

Paso 4 **Agregar**para ingresar la información de IP.

Figura 3-60 Agregar información de IP



Paso 5 Hacer clic**DE ACUERDO**.

Operaciones relacionadas

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

3.16.3.2 Configuración del bloqueo de cuenta

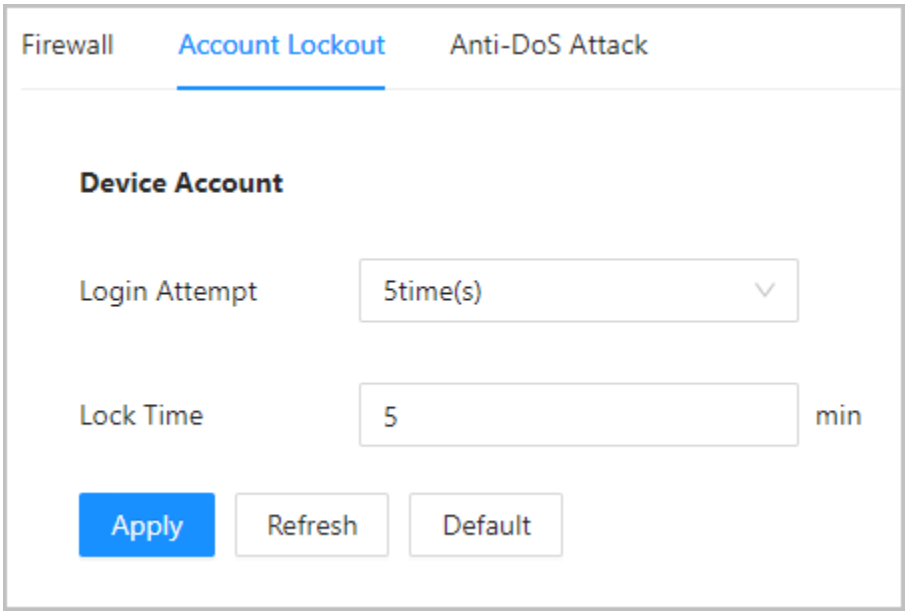
Si se ingresa la contraseña incorrecta un número definido de veces, la cuenta se bloqueará.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Ataque Defensa**>**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 3-61 Bloqueo de cuenta



- Intento de inicio de sesión: límite de intentos de inicio de sesión. Si se ingresa una contraseña incorrecta una cantidad determinada de veces, se bloqueará la cuenta.
- Tiempo de bloqueo: el tiempo durante el cual no puede iniciar sesión después de que se bloquea la cuenta. Haga clic en**Aplicar**.

Paso 3

3.16.3.3 Configuración de ataques anti-DoS

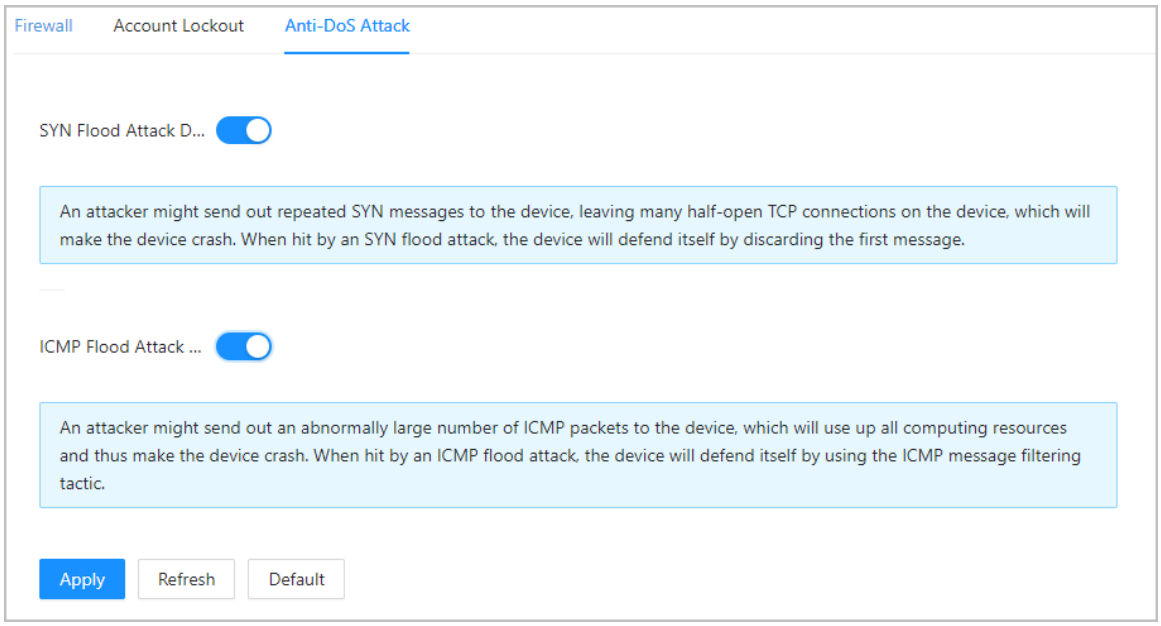
Puedes habilitar**Defensa contra ataques de inundación SYN**y**Defensa contra ataques de inundación ICMP**para defender el controlador de acceso contra ataques DoS.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Ataque Defensa**>**Ataque anti-DoS**.

Paso 2 Encender**Defensa contra ataques de inundación SYN**o**Defensa contra ataques de inundación ICMP**para proteger el controlador de acceso contra ataques DoS.

Figura 3-62 Ataque anti-DoS



Paso 3 Hacer clic**Aplicar**.

3.16.4 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.

3.16.4.1 Creación de certificado

Cree un certificado para el controlador de acceso.

Procedimiento

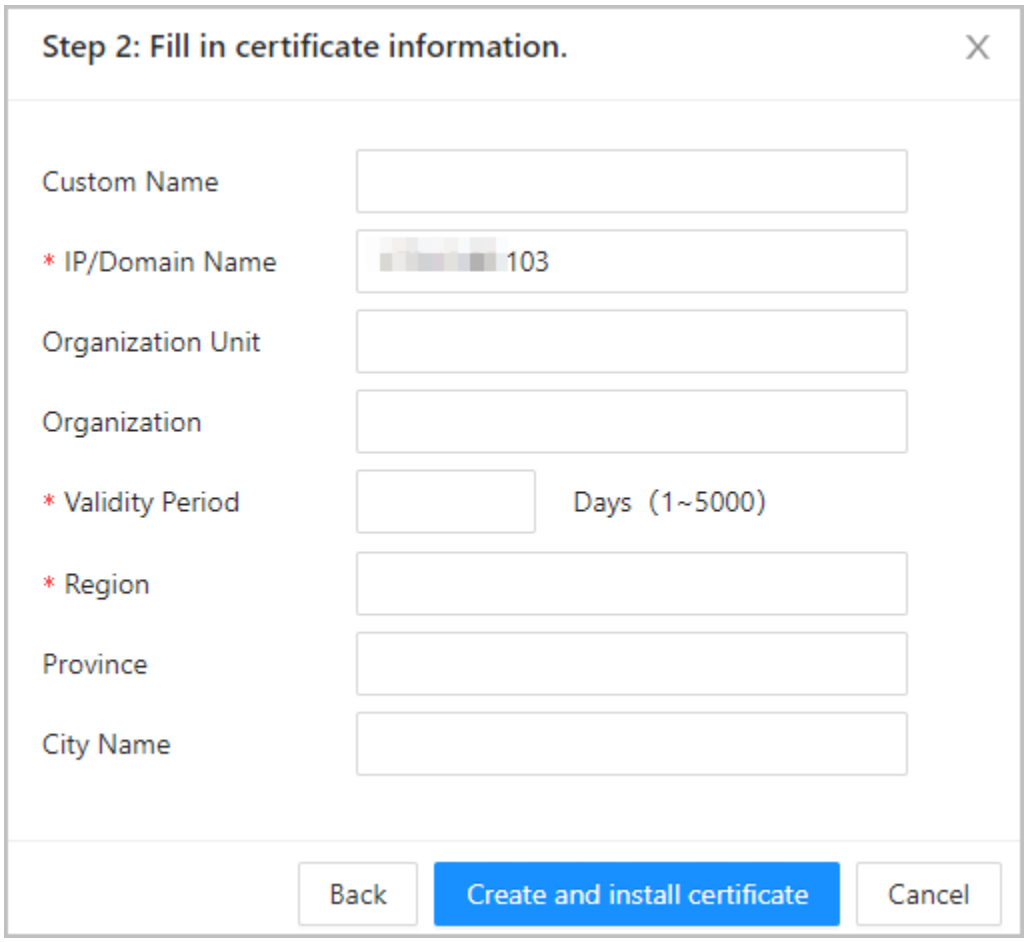
Paso 1 Seleccionar**Seguridad**>**Certificado CA**>**Certificado del dispositivo**.

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

Paso 3 **certificado**y haga clic**Próximo**. Ingrese la información del certificado.

Paso 4

Figura 3-63 Información del certificado



El nombre de la región no puede superar los 2 caracteres. Recomendamos introducir la abreviatura del nombre de la región.

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

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

Operaciones relacionadas

- Hacer clic**Entrar al modo de edición**en el**Certificado del dispositivo**Página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

3.16.4.2 Solicitud e importación de un certificado de CA

Importe el certificado de CA de terceros al controlador de acceso.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Certificado CA**>**Certificado del dispositivo**Haga clic

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

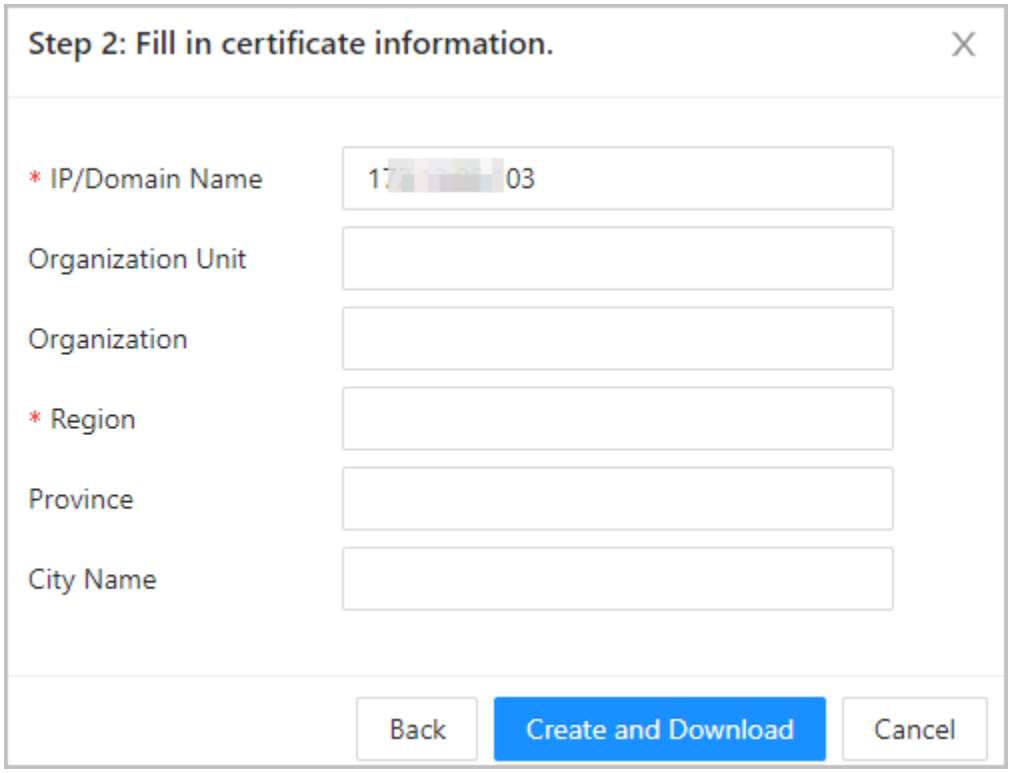
Paso 3 Seleccionar**Solicitar certificado CA e importación (recomendado)**y haga clic**Próximo**.

Paso 4 Ingrese la información del certificado.

- IP/Nombre de dominio: la dirección IP o el nombre de dominio del controlador de acceso.
- Región: El nombre de la región no debe superar los 3 caracteres. Le recomendamos que ingrese

La abreviatura del nombre de la región.

Figura 3-64 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 certificación externa mediante el archivo de solicitud. Importe el certificado de

Paso 7 la autoridad de certificación firmado.

1) Guarde el certificado CA en su computadora.

2) Haga clic**Instalación del certificado del dispositivo**.

3) Haga clic**Navegar**para seleccionar el certificado CA.

4) Haga clic**Importar e instalar**.

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

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

Operaciones relacionadas

- Hacer clic**Entrar al modo de edición**en el**Certificado del dispositivo**Página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

3.16.4.3 Instalación de un certificado existente

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

Procedimiento

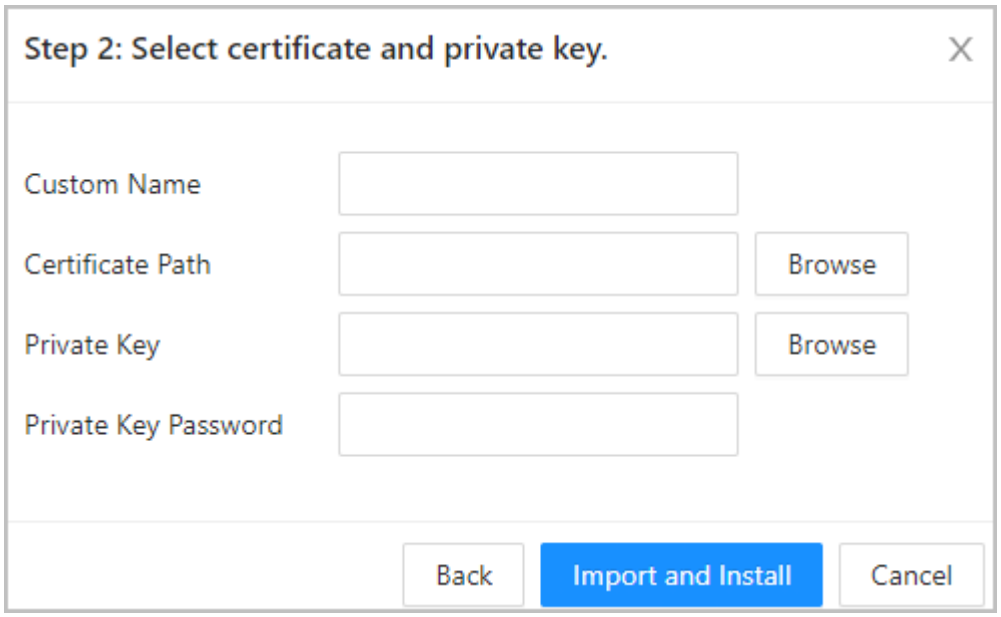
Paso 1 Seleccionar**Seguridad**>**Certificado CA**>**Certificado del dispositivo**Haga clic

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

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

Paso 4 Hacer clic**Navegar**para seleccionar el certificado y el archivo de clave privada e ingresar la contraseña de la clave privada.

Figura 3-65 Certificado y clave privada



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

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

Operaciones relacionadas

- Hacer clic**Entrar al modo de edición**en el**Certificado del dispositivo**Página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

3.16.5 Instalación del certificado CA de confianza

Un certificado CA de confianza 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 CA para 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.

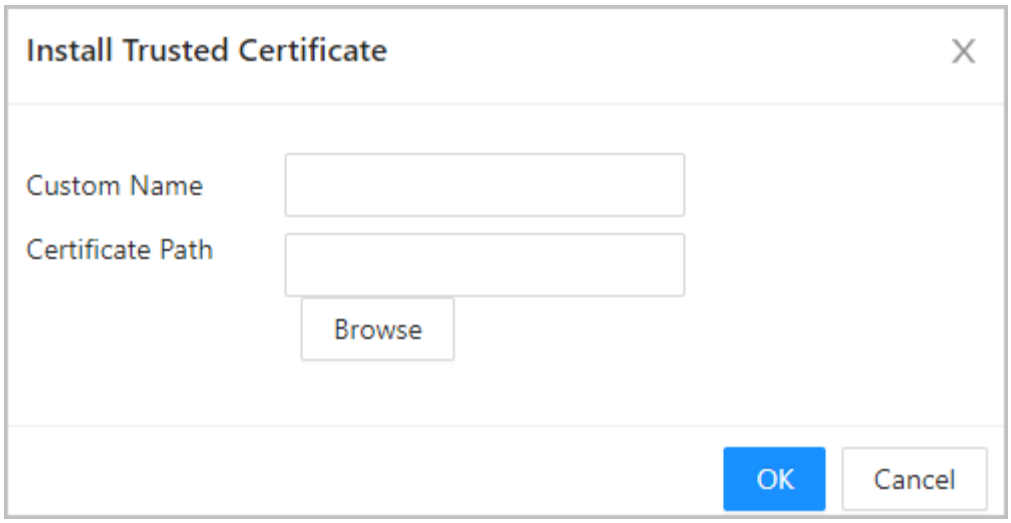
Procedimiento

Paso 1 Seleccionar**Seguridad**>**Certificado CA**>**Certificados CA de confianza**.

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

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

Figura 3-66 Instalar el certificado de confianza



Paso 4 Hacer clic**DE ACUERDO**.

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

Operaciones relacionadas

- Hacer clic**Entrar al modo de edición**en el**Certificado del dispositivo**Página para editar el nombre del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

3.16.6 Cifrado de datos

Procedimiento

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

Paso 2 Configure los parámetros.

Figura 3-67 Cifrado de datos

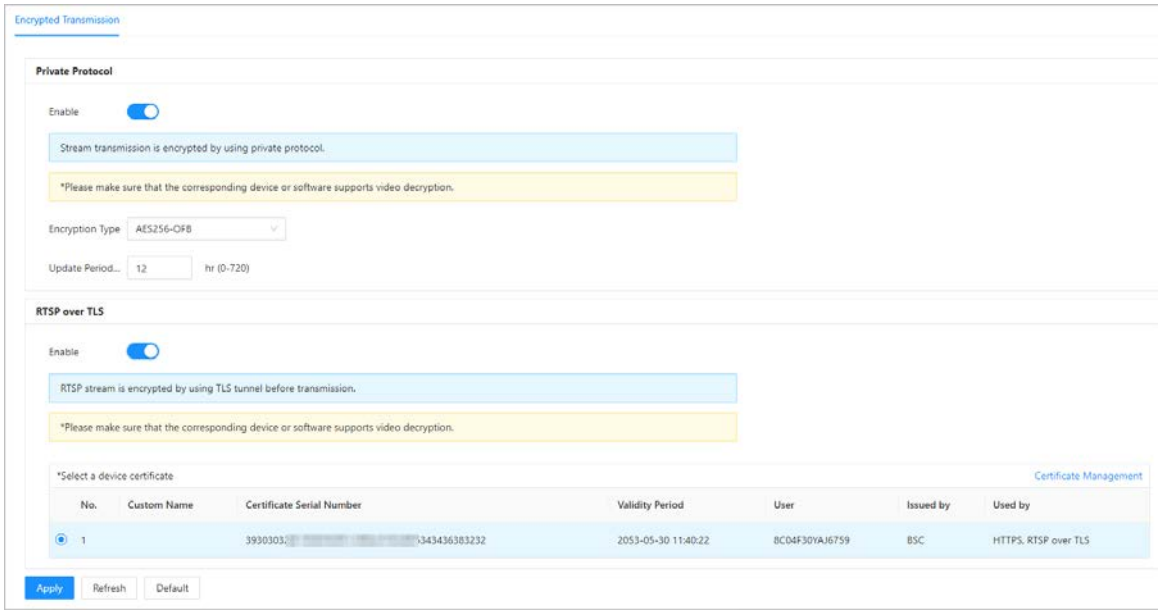


Tabla 3-36 Descripción del cifrado de datos

	Parámetro	Descripción
Protocolo privado	Permitir	Las transmisiones se cifran durante la transmisión a través de un protocolo privado.
	Tipo de cifrado	Mantenlo como predeterminado
	Periodo de actualización de Clave secreta	El rango va desde 0 h hasta 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.
	Certificado Gestión	Cree o importe un certificado. Para obtener más información, consulte "3.16.4 Instalación del certificado del dispositivo". Los certificados instalados se muestran en la lista.

3.16.7 Advertencia de seguridad

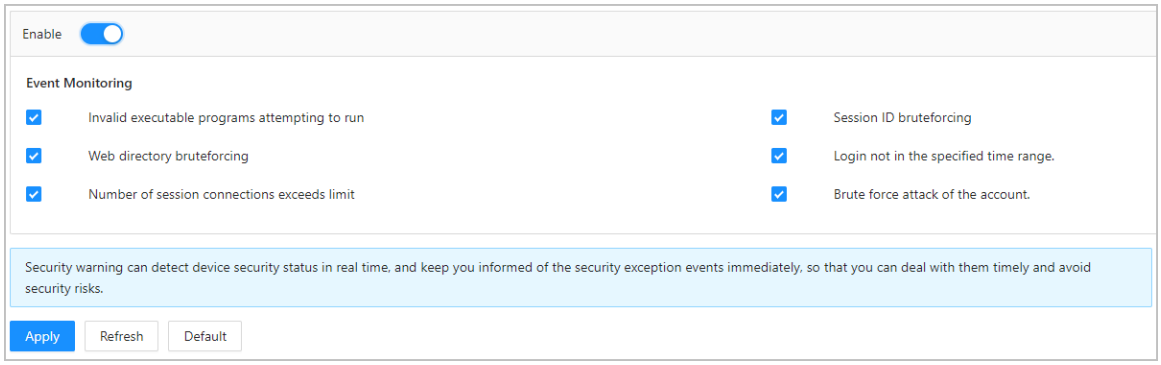
Procedimiento

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

Paso 2 Habilite la función de advertencia de seguridad.

Paso 3 Seleccione los elementos de monitoreo.

Figura 3-68 Advertencia de seguridad



Paso 4 Hacer clic**Aplicar**.

4. Configuración inteligente de PSS Lite

En esta sección se presenta cómo administrar y configurar el controlador de acceso 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 del usuario de Smart PSS Lite.

Procedimiento

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

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

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

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

4.2 Agregar dispositivos

Debe agregar el controlador de acceso a Smart PSS Lite. Puede agregarlos en lotes o de forma individual.

4.2.1 Agregar uno por uno

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

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

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

Figura 4-1 Información del dispositivo

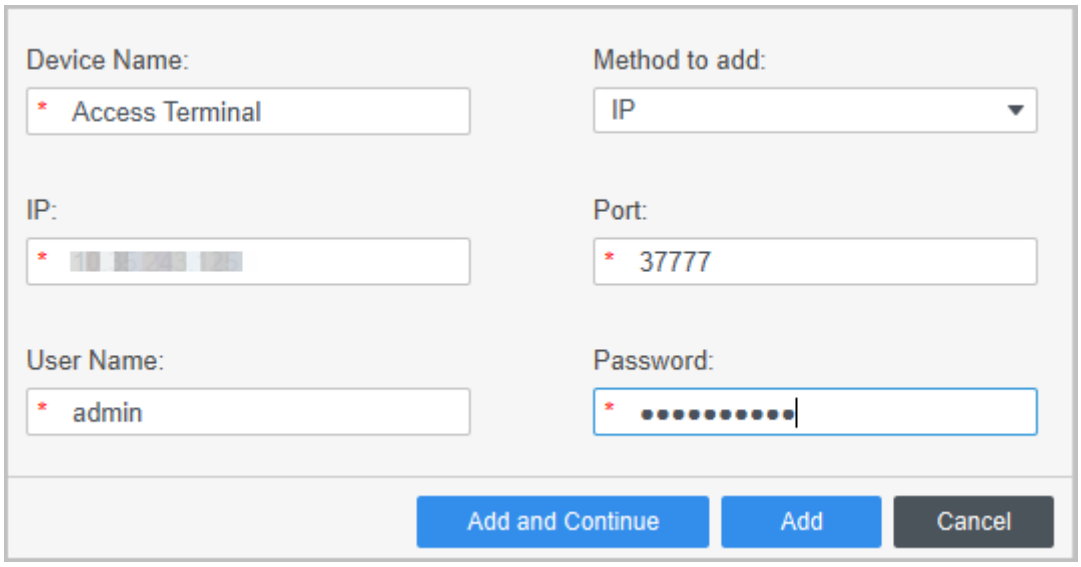


Tabla 4-1 Descripción de los parámetros del dispositivo

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

Paso 4 Hacer clic**Agregar**.

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

4.2.2 Adición en lotes

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

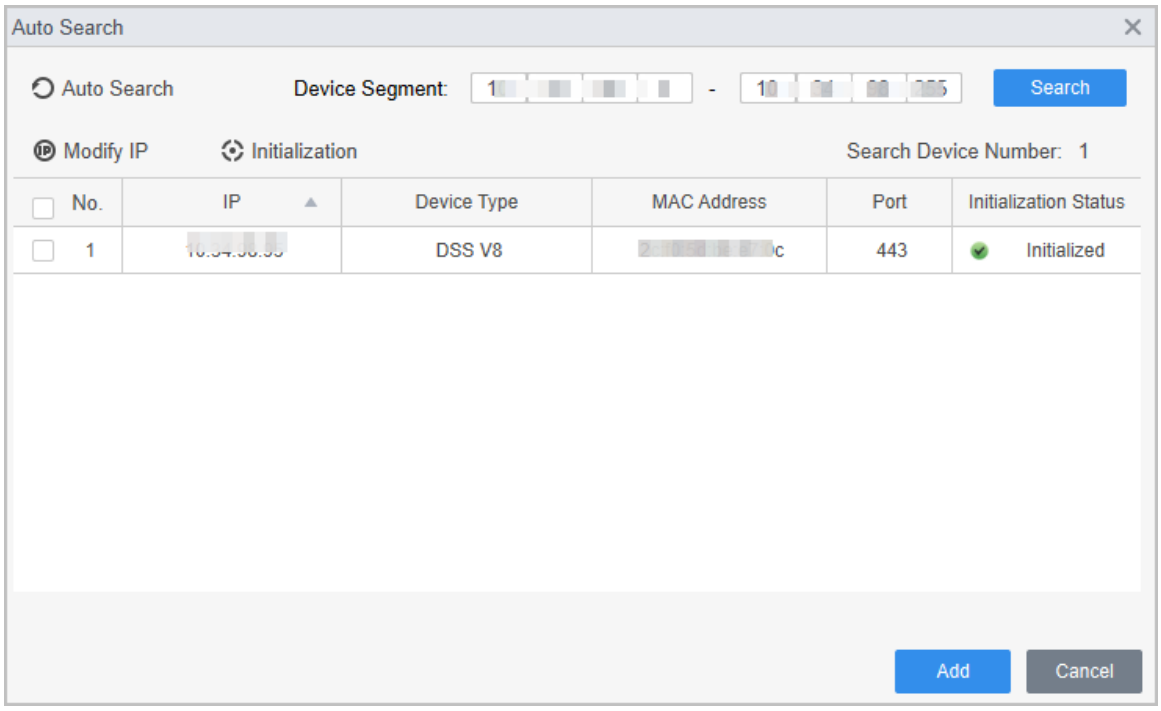
Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

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

Figura 4-2 Búsqueda automática



Se mostrará una lista de dispositivos.

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

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

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

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

El controlador de acceso inicia sesión automáticamente en Smart PSS Lite después de agregarse.**En línea**es se muestra después de iniciar sesión correctamente.

4.3 Gestión de usuarios

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

4.3.1 Configuración del tipo de tarjeta

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

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

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

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

Paso 4 Hacer clic**DE ACUERDO**.

4.3.2 Agregar usuarios

4.3.2.1 Agregar uno por uno

Puede agregar usuarios uno por uno.

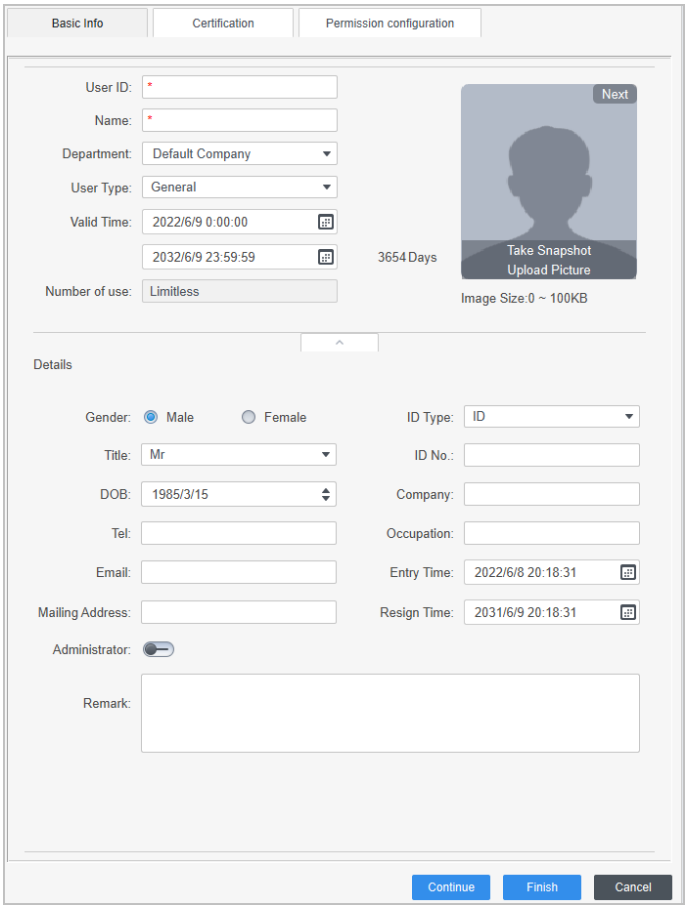
Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

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

Figura 4-3 Agregar información básica



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

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

  1. En el**Tarjeta**área, haga clic y seleccione**Emisor de la tarjeta**y luego haga clic en**DE ACUERDO**.

2. Haga clic**Agregar**Pase una tarjeta por el lector de tarjetas. Se mostrará el número de la tarjeta.

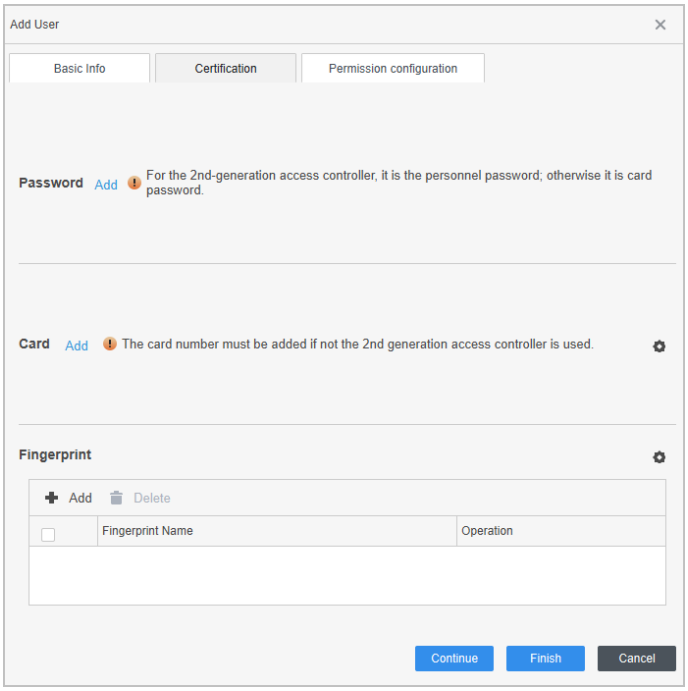
3. Haga clic**DE ACUERDO**.

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

- Configurar huella digital.

1. En el**Huella dactilar**área, haga clic y seleccione**Escáner de huellas dactilares**y luego haga clic en **DE ACUERDO**.
2. Haga clic**Agregar huella digital**, presione su dedo sobre el escáner tres veces seguidas.

Figura 4-4 Agregar contraseña, tarjeta y huella digital



Paso 5 Configure los permisos para el usuario. Para obtener más información, consulte "4.3.3 Asignación de permisos de acceso". Haga clic

Paso 6 en**Finalizar**.

4.3.2.2 Adición en lotes

Puede agregar usuarios en lotes.

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

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

Figura 4-5 Agregar usuarios en lotes

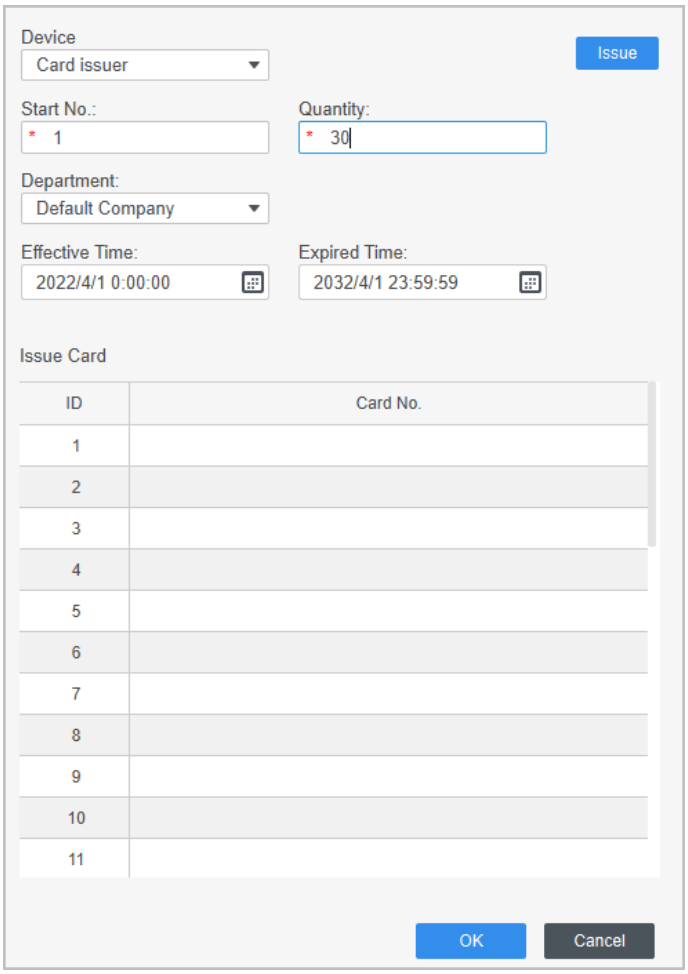


Tabla 4-2 Parámetros para agregar usuarios en lotes

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

Paso 4 Hacer clic**Asunto**.

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

Paso 5 **ACUERDO**.

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

4.3.3 Asignación de permisos de acceso

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

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

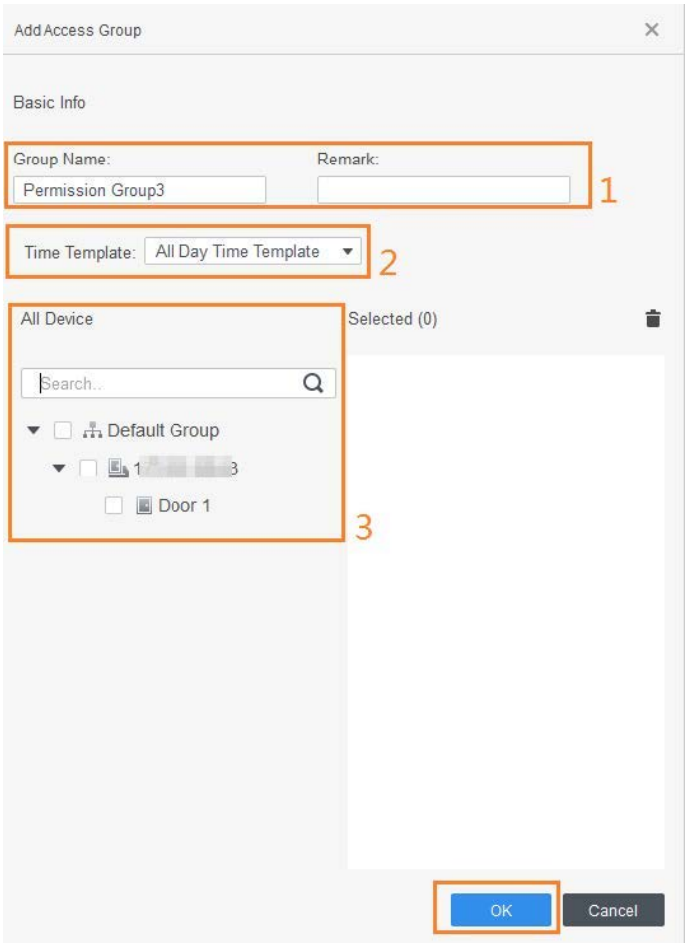
Paso 3 en .

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

Paso 5 Seleccione el dispositivo de control de acceso.

Paso 6 Hacer clic**DE ACUERDO**.

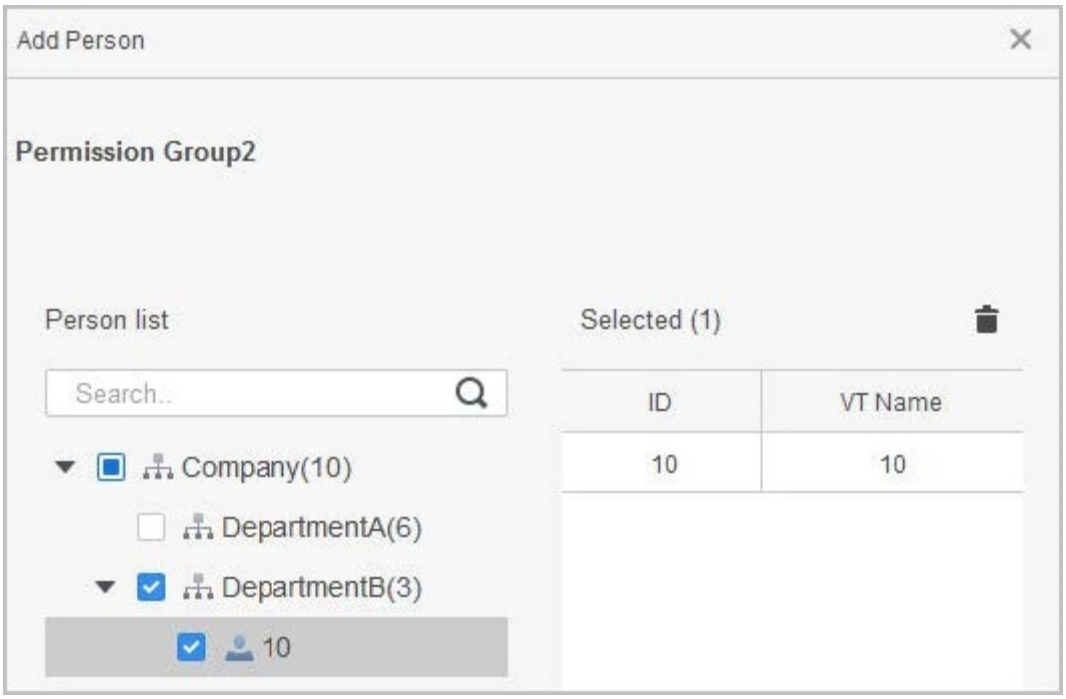
Figura 4-6 Crear un grupo de permisos



Paso 7 Hacer clic del grupo de permisos que agregó.

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

Figura 4-7 Agregar usuarios a un grupo de permisos



Paso 9 Hacer clic**DE ACUERDO**.

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

4.3.4 Asignación de permisos de asistencia

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

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

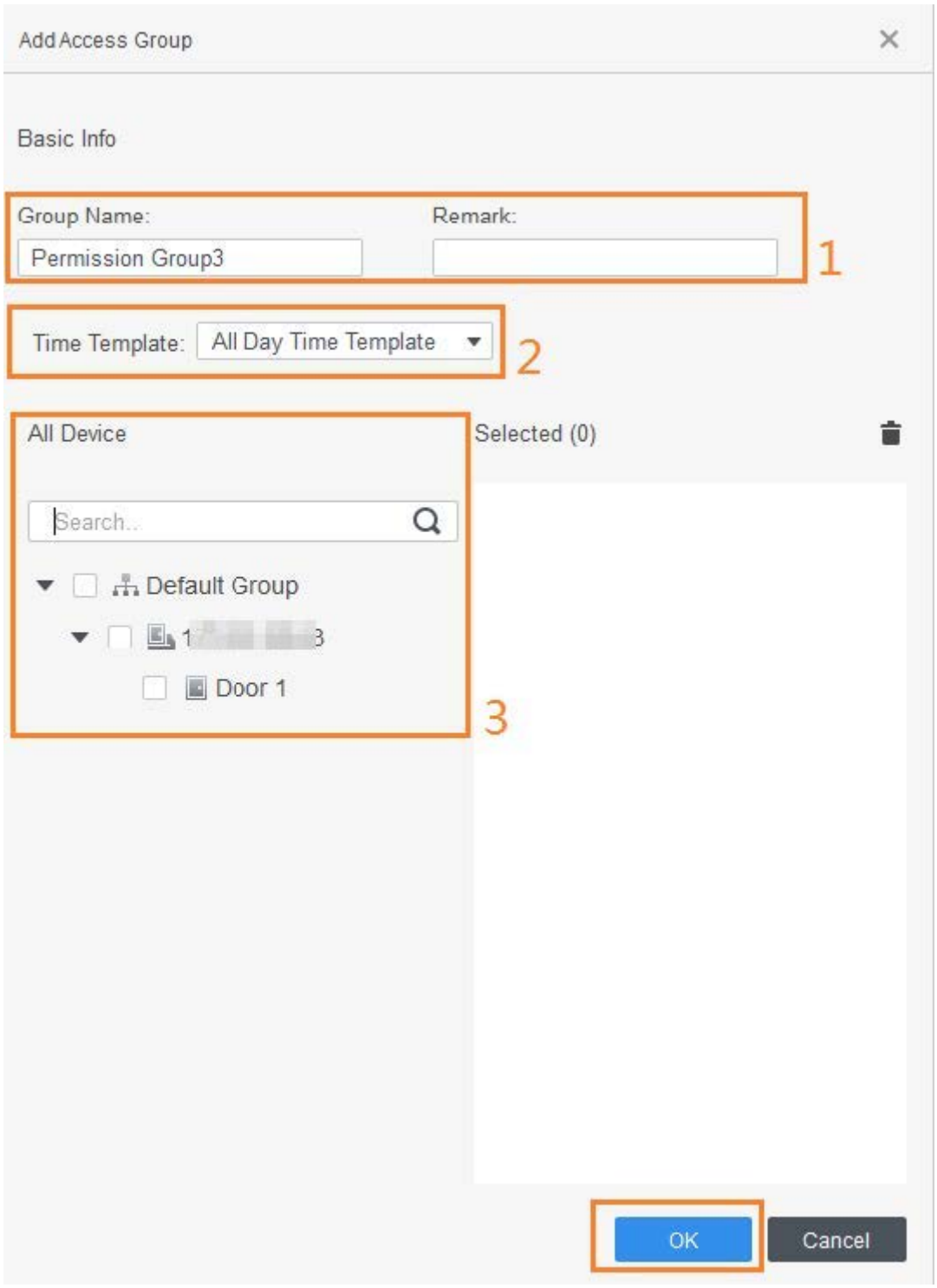
Paso 3 en .

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

Paso 5 Seleccione el dispositivo de control de acceso.

Paso 6 Hacer clic**DE ACUERDO**.

Figura 4-8 Crear un grupo de permisos



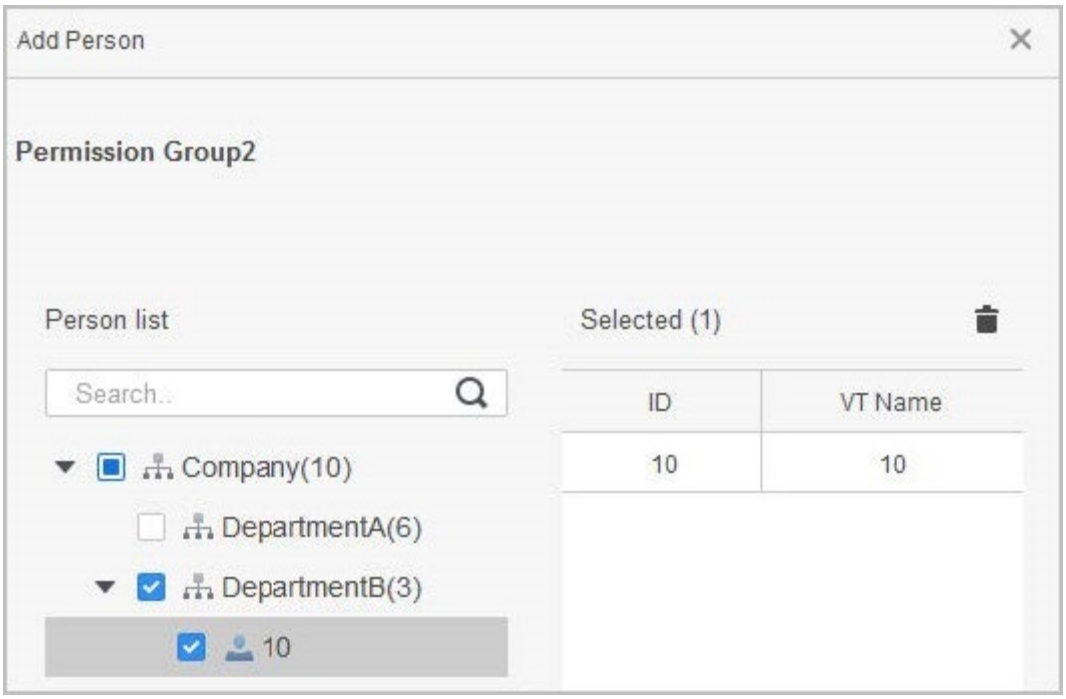
El control de tiempo y asistencia solo admite el registro de entrada y salida mediante contraseña y reconocimiento facial.

asistencia.

Paso 7 Hacer clic del grupo de permisos que agregó.

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

Figura 4-9 Agregar usuarios a un grupo de permisos



Paso 9 Hacer clic**DE ACUERDO**.

4.4 Gestión de acceso

4.4.1 Apertura y cierre remoto de la puerta

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

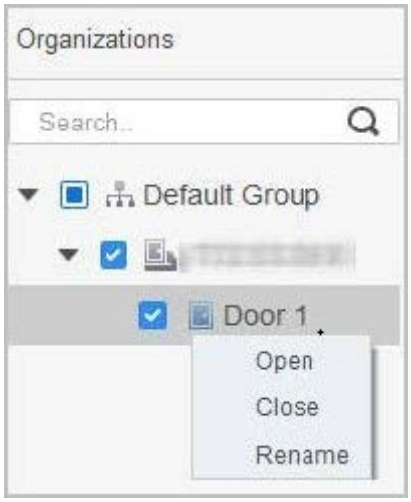
Procedimiento

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

Paso 2 la puerta de forma remota.

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

Figura 4-10 Puerta abierta



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

Operaciones relacionadas

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

4.4.2 Configuración de Siempre abierto y Siempre cerrado

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

Procedimiento

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

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

Figura 4-11 Siempre abierto o cerrado

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

4.4.3 Monitoreo del estado de la puerta

Procedimiento

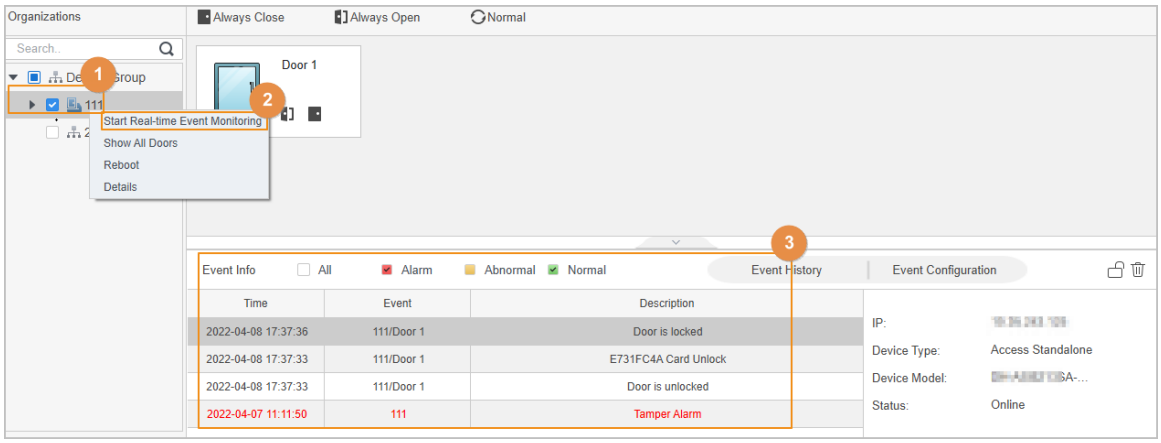
Paso 1 Hacer clic**Solución de acceso**>**Administrador de acceso**en la página de inicio.

Paso 2 Seleccione el Controlador de acceso en el árbol de dispositivos, haga clic derecho en el Controlador de acceso 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 el monitor**, los eventos de control de acceso en tiempo real no se mostrarán.

Figura 4-12 Estado de la puerta del monitor



Operaciones relacionadas

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

Apéndice 1 Puntos importantes del rostro

Registro

Antes de la inscripción

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

Durante el registro

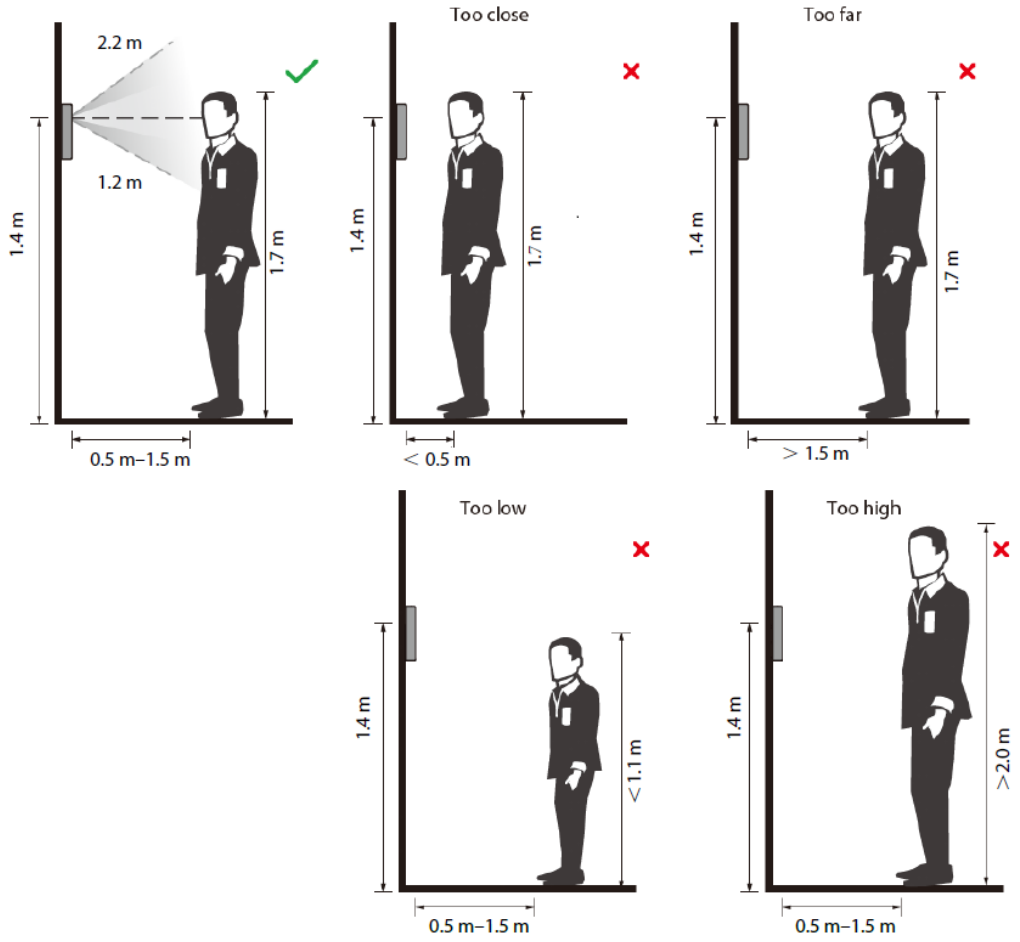
- Puede registrar rostros a través del Controlador de Acceso o a través de la plataforma. Para el registro a través de la plataforma, consulte el manual de usuario de la plataforma.
- Centra tu cabeza en el marco de captura de fotos. La imagen de tu rostro se capturará automáticamente.

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

Posición de la cara

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

Apéndice Figura 1-1 Posición adecuada de la cara



Requisitos de las caras

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

Apéndice Figura 1-2 Posición de la cabeza

Apéndice Figura 1-3 Distancia entre caras

- Al importar imágenes de rostros a través de la plataforma de administración, asegúrese de que la imagen La resolución está dentro del rango de 150 × 300 píxeles a 600 × 1200 píxeles; los píxeles de la imagen son más de 500 × 500 píxeles; el tamaño de la imagen es inferior a 100 KB y el nombre de la imagen y la identificación de la persona son los mismos.
- Asegúrese de que el rostro ocupe más de 1/3 pero no más de 2/3 del área total de la imagen. y la relación de aspecto no exceda de 1:2.

Apéndice 2 Puntos importantes del intercomunicador

Operación

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

Prerrequisitos

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

Procedimiento

Paso 1 En la pantalla de espera, toque Ingresar.

Paso 2 número de habitación y luego toque .

Apéndice 3 Puntos importantes de la toma de huellas dactilares

Instrucciones de registro

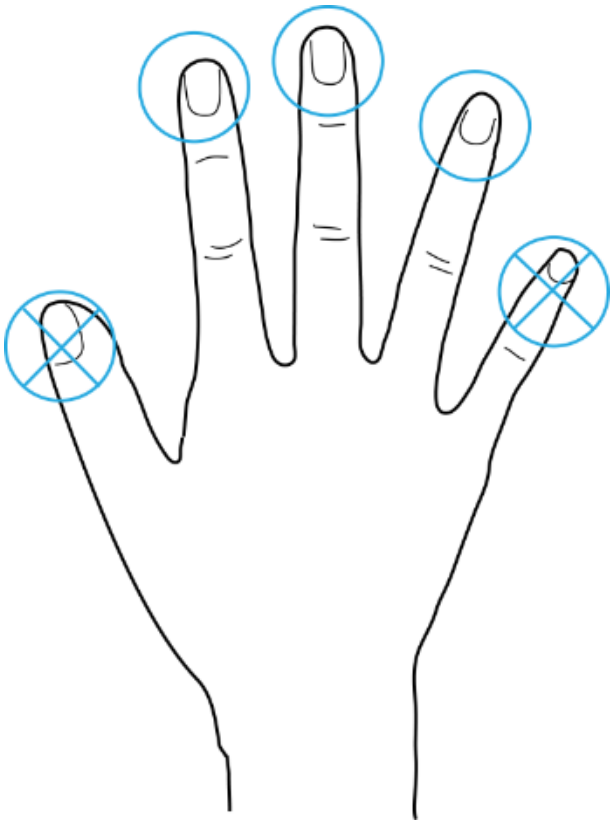
Al registrar la huella dactilar, preste atención a los siguientes puntos:

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

Se recomiendan los dedos

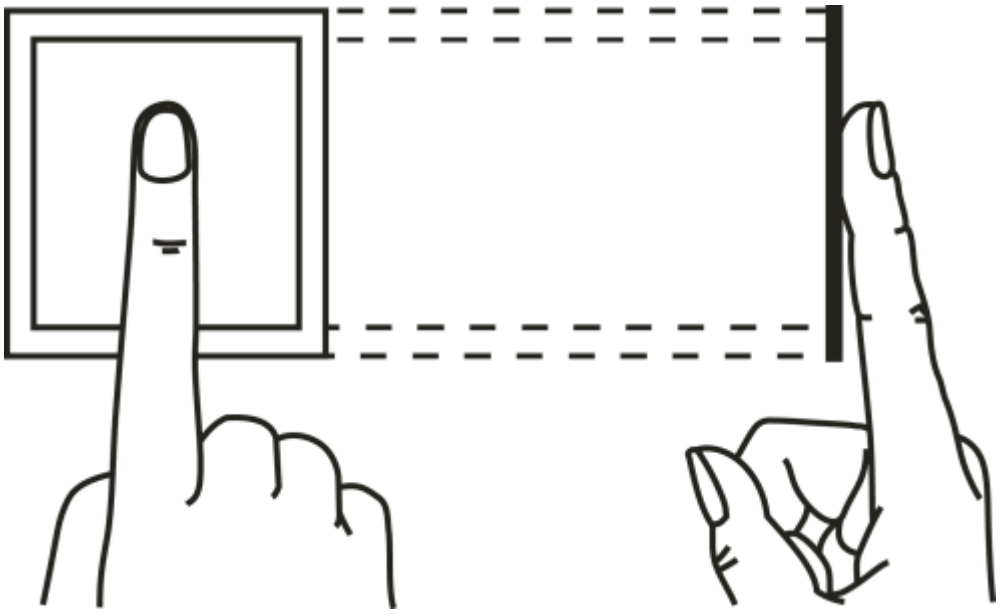
Se recomiendan los dedos índice, medio y anular. Los pulgares y meñiques no se pueden colocar fácilmente en el centro de la grabación.

Apéndice Figura 3-1 Dedos recomendados

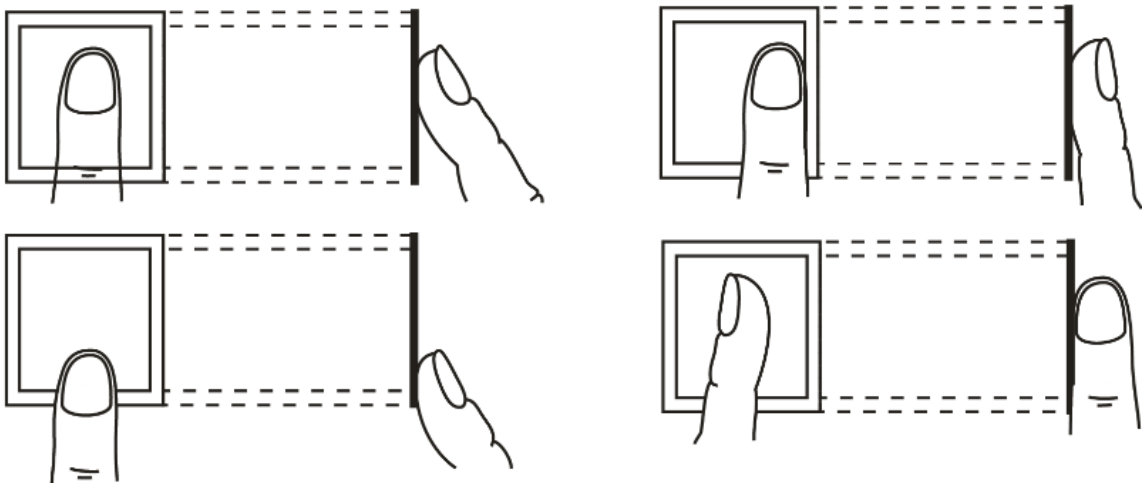


Cómo presionar su huella digital en el escáner

Apéndice Figura 3-2 Colocación correcta



Apéndice Figura 3-3 Colocación incorrecta



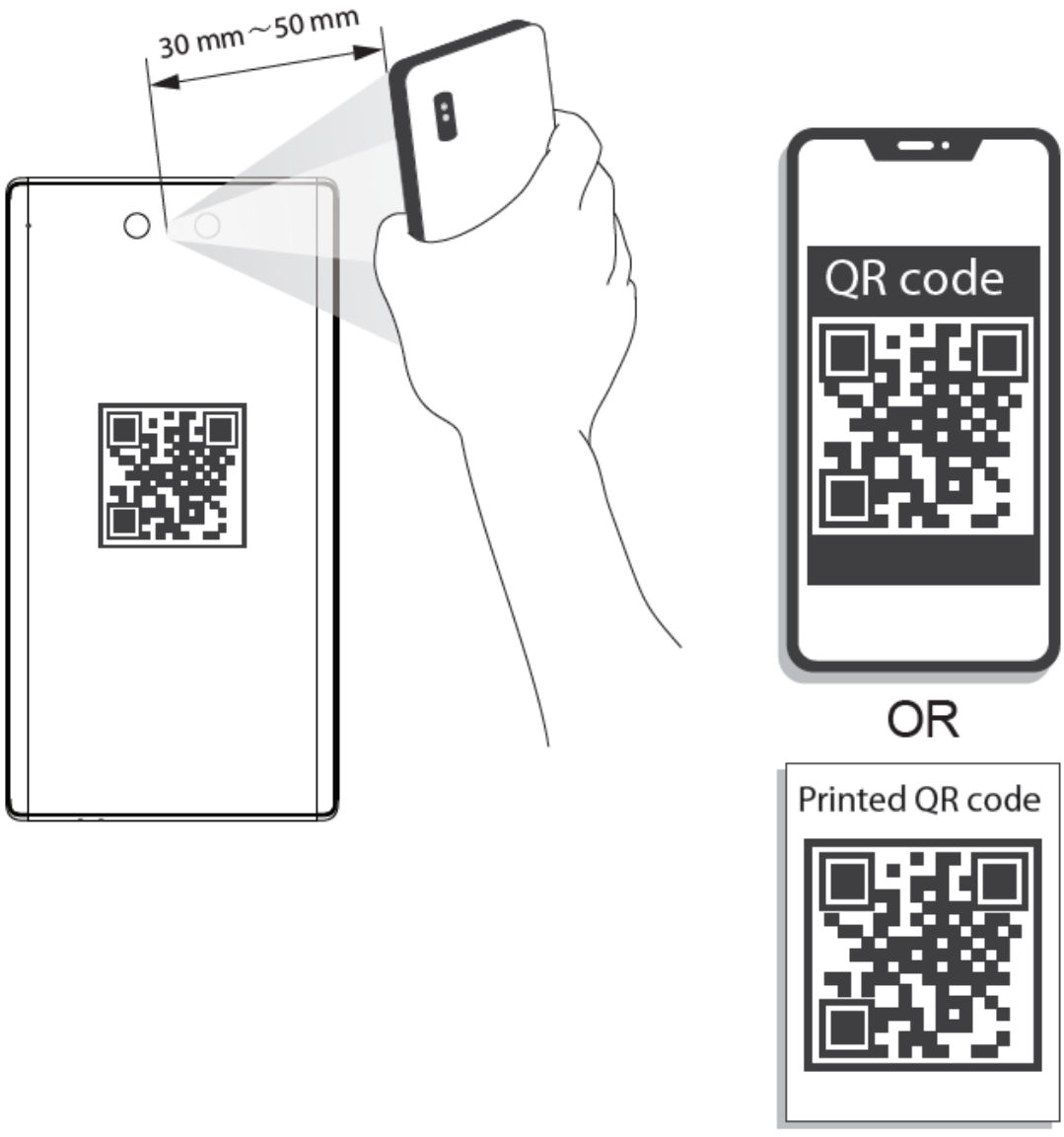
Apéndice 4 Puntos importantes del código QR

Exploración

Controlador de acceso: coloque el código QR en su teléfono a una distancia de 30 mm a 50 mm de la lente de lectura del código QR. Admite códigos QR que deben tener un tamaño mayor a 30 mm × 30 mm y un tamaño menor a 128 bytes.

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

Apéndice Figura 4-1 Escaneo de código QR



Apéndice 5 Recomendaciones de ciberseguridad

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

1.**Utilice contraseñas seguras**

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

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

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

1.**Protección física**

Le sugerimos que proteja físicamente el dispositivo, especialmente los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras y un gabinete especiales e implemente un control de acceso y una gestión de claves bien hechos para evitar que personal no autorizado realice contactos físicos, como dañar el hardware, conectar sin autorización dispositivos extraíbles (como un disco flash USB, un puerto serial), etc.

2.**Cambie las contraseñas periódicamente**

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

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

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

4.**Habilitar bloqueo de cuenta**

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

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

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

6.**Habilitar HTTPS**

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

7.**Vinculación de dirección MAC**

Le recomendamos vincular la dirección IP y MAC del gateway al dispositivo, reduciendo así

el riesgo de suplantación de ARP.

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

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

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

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

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

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

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

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

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

11.**Auditoría segura**

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

12.**Registro de red**

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

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

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

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde la red externa.
- La red debe estar dividida y aislada de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se recomienda utilizar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establecer el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts a los que se les permite acceder al dispositivo.