

# **Controlador de acceso con reconocimiento facial**

**Manual del usuario**








# Prefacio

## General

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

## Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

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

## Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
Versión 1.0.1	Se revisaron las precauciones y advertencias importantes.	Agosto de 2024
Versión 1.0.0	Primer lanzamiento.	Julio de 2024

## 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, audio, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: Proporcionar una identificación clara y visible para informar a las personas de la existencia del área de vigilancia y proporcionar la información de contacto requerida.

## Acerca del manual

- El manual es solo de referencia. Pueden existir ligeras diferencias entre el manual y el producto.
- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas que no cumplan con el manual.

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

## Medidas de seguridad y advertencias importantes

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

### Requerimientos de transporte



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

### Requisito de almacenamiento



Guarde el dispositivo en condiciones de humedad y temperatura permitidas.

### Requisitos de instalación



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



- 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 dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- Instale el dispositivo sobre una superficie estable para evitar que se caiga.
- Instale el dispositivo en un lugar bien ventilado y no bloquee su ventilación.

- Utilice un adaptador o 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.
- El dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectada a una toma de corriente con conexión a tierra.
- El dispositivo debe instalarse a una altura de 2 metros o menos.

## Requisitos de funcionamiento



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

# Tabla de contenido

Prólogo.....	I
Medidas de seguridad y advertencias importantes.....	III
1 Descripción general.....	1
2 Operaciones locales.....	2
2.1 Preparación.....	2
2.1.1 Procedimiento de configuración básica.....	2
2.1.2 Descripción de los botones.....	2
2.1.3 Introducción al método de entrada.....	4
2.2 Inicialización.....	4
2.3 Pantalla de inicio.....	5
2.4 Métodos de desbloqueo.....	5
2.4.1 Desbloqueo con Tarjetas.....	5
2.4.2 Desbloqueo por huella dactilar.....	6
2.4.3 Desbloqueo por reconocimiento facial.....	6
2.4.4 Desbloqueo por contraseña de usuario.....	6
2.4.5 Desbloqueo por contraseña de administrador.....	7
2.4.6 Desbloqueo mediante contraseña temporal.....	8
2.5 Inicio de sesión.....	9
2.6 Gestión de personas.....	9
2.6.1 Agregar usuarios.....	10
2.6.2 Visualización de la información del usuario.....	12
2.6.3 Configuración de la contraseña de desbloqueo del administrador.....	14
2.7 Gestión del control de acceso.....	14
2.7.1 Configuración de combinaciones de desbloqueo.....	15
2.7.2 Configuración de alarmas.....	15
2.7.3 Configuración del estado de la puerta.....	17
2.7.4 Configuración del intervalo de tiempo de verificación.....	17
2.8 Configuración de comunicación.....	18
2.8.1 Configuración de la red.....	18
2.8.2 Configuración de RS-485.....	20
2.8.3 Configuración de Wiegand.....	21
2.9 Configuración del sistema.....	23
2.9.1 Configuración de la hora.....	23
2.9.2 Configuración de parámetros faciales.....	24
2.9.3 Configuración del volumen.....	25
2.9.4 Configuración del idioma.....	26
2.9.5 Configuración de parámetros de pantalla.....	26

2.9.6 Restauración de valores predeterminados de fábrica.....	27
2.9.7 Reinicio del dispositivo.....	27
2.10 Administración USB.....	27
2.10.1 Exportación a USB.....	28
2.10.2 Importación desde USB.....	28
2.10.3 Actualización del sistema.....	28
2.11 Gestión de registros.....	29
2.12 Información del sistema.....	29
2.12.1 Visualización de la capacidad de datos.....	29
2.12.2 Visualización de la versión del dispositivo.....	29
3 Operaciones de la página web.....	30
3.1 Inicialización.....	30
3.2 Restablecimiento de la contraseña.....	30
3.3 Página de inicio.....	31
3.4 Gestión de personas.....	32
3.5 Configuración del control de acceso.....	36
3.5.1 Gestión de personas.....	36
3.5.2 Configuración de parámetros de control de acceso.....	40
3.5.3 Configuración de alarmas.....	44
3.5.4 Configuración de la vinculación de eventos de alarma.....	46
3.5.5 Configuración de parámetros faciales.....	47
3.5.6 Configuración de los ajustes de la tarjeta.....	49
3.5.7 Configuración de horarios.....	52
3.5.8 Configuración de privacidad.....	54
3.5.9 Configuración de la comparación de back-end.....	54
3.6 Configuración de asistencia.....	55
3.6.1 Configuración de departamentos.....	55
3.6.2 Configuración de turnos.....	55
3.6.3 Configuración de vacaciones.....	58
3.6.4 Configuración de horarios de trabajo.....	58
3.6.5 Configuración de modos de asistencia.....	61
3.7 Configuración de audio y vídeo.....	63
3.7.1 Configuración de vídeo.....	63
3.7.2 Configuración de audio.....	67
3.8 Configuración de comunicación.....	68
3.8.1 Configuración de red.....	68
3.8.2 Configuración de RS-485.....	79
3.8.3 Configuración de Wiegand.....	80
3.9 Configuración del sistema.....	81
3.9.1 Gestión de usuarios.....	82

3.9.2 Configuración de la hora.....	84
3.10 Centro de mantenimiento.....	86
3.10.1 Diagnóstico con un solo clic.....	86
3.10.2 Información del sistema.....	87
3.10.3 Capacidad de datos.....	87
3.10.4 Visualización de registros.....	87
3.10.5 Gestión del mantenimiento.....	89
3.10.6 Mantenimiento.....	90
3.10.7 Actualización del sistema.....	90
3.10.8 Mantenimiento avanzado.....	91
3.11 Configuración de seguridad (opcional) .....	92
3.11.1 Estado de seguridad.....	92
3.11.2 Configuración del servicio del sistema.....	93
3.11.3 Defensa de ataque.....	93
3.11.4 Instalación del certificado del dispositivo.....	96
3.11.5 Instalación del certificado CA de confianza.....	101
3.11.6 Cifrado de datos.....	100
3.11.7 Advertencia de seguridad.....	101
3.11.8 Autenticación de seguridad.....	101
4 Operaciones telefónicas.....	103
4.1 Inicio de sesión en la página web.....	103
4.2 Página de inicio.....	104
4.3 Gestión de personas.....	106
4.4 Configuración del sistema.....	109
4.4.1 Visualización de la información de la versión.....	110
4.4.2 Mantenimiento.....	110
4.4.3 Configuración de la hora.....	110
4.4.4 Capacidad de datos.....	112
4.5 Configuración de asistencia.....	112
4.5.1 Configuración de departamentos.....	112
4.5.2 Configuración de turnos.....	113
4.5.3 Configuración de vacaciones.....	117
4.5.4 Configuración de horarios de trabajo.....	117
4.5.5 Configuración de los modos de asistencia.....	119
4.6 Configuración del control de acceso.....	121
4.6.1 Configuración de métodos de desbloqueo.....	121
4.6.2 Configuración de parámetros faciales.....	122
4.6.3 Configuración de parámetros de control de acceso.....	124
4.6.4 Configuración de alarmas.....	126
4.6.5 Configuración de la vinculación de eventos de alarma.....	129



4.6.6 Configuración de los ajustes de la tarjeta.....	130
4.6.7 Configuración de privacidad.....	132
4.7 Configuración de comunicación.....	132
4.7.1 Configuración de TCP/IP.....	132
4.7.2 Configuración de Wi-Fi.....	134
4.7.3 Configuración del punto de acceso Wi-Fi.....	134
4.7.4 Configuración del servicio en la nube.....	135
4.7.5 Configuración del registro automático.....	135
4.7.6 Configuración de Wiegand.....	136
4.7.7 Configuración de RS-485.....	138
4.8 Configuración de indicaciones de audio.....	139
4.9 Visualización de registros.....	141
4.9.1 Registros del sistema.....	141
4.9.2 Desbloquear registros.....	141
4.9.3 Registros de alarmas.....	142
5 Configuración de Smart PSS Lite.....	143
5.1 Instalación e inicio de sesión.....	143
5.2 Agregar dispositivos.....	143
5.2.1 Agregar dispositivos uno por uno.....	143
5.2.2 Agregar dispositivos en lotes.....	144
5.3 Gestión de usuarios.....	146
5.3.1 Configuración del tipo de tarjeta.....	146
5.3.2 Agregar usuarios.....	146
5.3.3 Asignación de permisos de acceso.....	151
5.3.4 Asignación de permisos de asistencia.....	152
5.4 Gestión de accesos.....	154
5.4.1 Apertura y cierre remoto de la puerta.....	154
5.4.2 Configuración de Siempre abierto y Siempre cerrado.....	155
5.4.3 Monitoreo del estado de la puerta.....	155
Apéndice 1 Puntos importantes del registro facial.....	157
Apéndice 2 Puntos importantes de las instrucciones para el registro de huellas dactilares.....	160
Apéndice 3 Recomendación de seguridad.....	162

## 1 Descripción general

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

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.
- Algunos modelos admiten la conexión de módulos de extensión, como el módulo de huellas dactilares, entre otros. El tipo de módulos de extensión que admite el dispositivo puede variar.

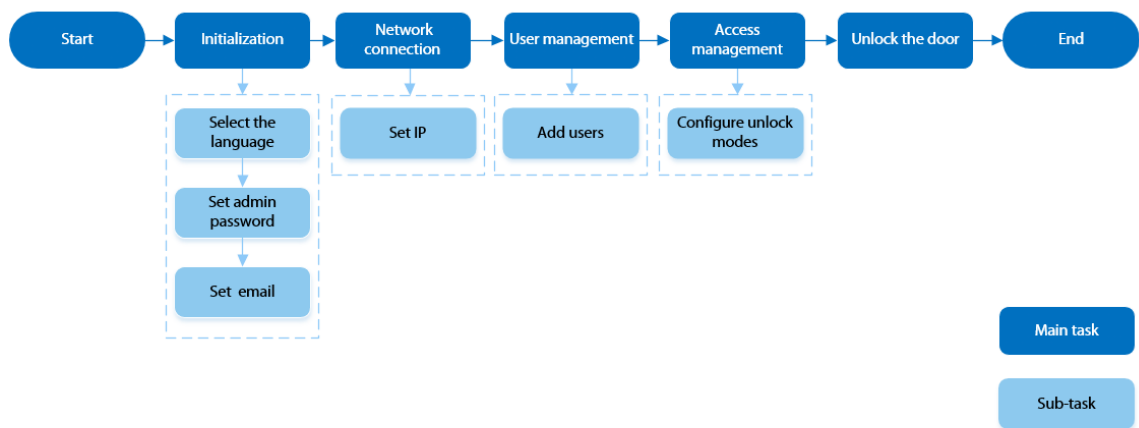
## 2 Operaciones locales

- Las configuraciones pueden variar según el producto real.
- Los módulos de expansión externos solo están disponibles en modelos seleccionados.

### 2.1 Preparación

#### 2.1.1 Procedimiento de configuración básica

Figura 2-1 Procedimiento de configuración básica



#### 2.1.2 Descripción del botón

El dispositivo no tiene pantalla táctil. Utilice el dispositivo mediante los botones. Cuando la pantalla del dispositivo esté apagada, presione cualquier botón excepto el del timbre para iluminar la pantalla.

Figura 2-2 Botones




Tabla 2-1 Descripción de los botones

Botón	Descripción
ESC	Regresar al menú anterior.
DE ACUERDO	Botón de confirmación
	La opción seleccionada se puede desplazar hacia arriba o hacia abajo en la pantalla utilizando los botones.
	La opción seleccionada se puede desplazar hacia la izquierda o hacia la derecha en la pantalla mediante los botones. También se puede pasar a la página anterior o a la siguiente mediante los botones.
	Timbre: Presione el botón y el dispositivo de timbre externo conectado suena.
0-9	<ul style="list-style-type: none"> <li>● 0: Indica el número 0 y espacio.</li> <li>● 1: Indica el número 1.</li> <li>● 2-9: Los botones se comparten por número y letra.</li> </ul>
	Eliminar el contenido del cuadro de entrada.
	<ul style="list-style-type: none"> <li>● Cambiar el método de entrada en el cuadro de entrada.</li> <li>● En la pantalla de inicio, presione el botón para ver la pantalla de inicio de sesión en segundo plano.</li> <li>● En la pantalla de configuración, presione el botón para volver a la pantalla de inicio.</li> </ul>

## 2.1.3 Introducción al método de entrada

Cambiar el método de entrada

Prensa  en el cuadro de entrada para cambiar el método de entrada.

Introduzca la letra

En esta parte se utiliza la introducción de M como ejemplo.



1. Presione el botón 6 en el cuadro de entrada.
2. Pulse el botón 4.

Introduzca el número

Cambie al método de ingreso de números y luego presione el botón numérico correspondiente.

Introduzca el caracter

Cambie al método de ingreso de caracteres y luego presione el botón numérico correspondiente.

Prensa  o  para cambiar a la página anterior o siguiente de caracteres.

## 2.2 Inicialización

Información de contexto


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.

Procedimiento

**Paso 1** Seleccione el idioma y luego presione la tecla OK.

**Paso 2** Prensa  Para seleccionar **Introducir contraseña** y luego presione OK.




**Paso 3** Configure la contraseña y luego presione OK.

- El método de entrada predeterminado es el método de letras. Método de  cambiar al numero pulsación.
- Ingresar la letra: Presione la tecla de la letra correspondiente y luego presione el número para seleccionar la letra. Por ejemplo, si desea ingresar la letra a, debe presionar la tecla 2 y luego la tecla 1.



- Si olvida la contraseña de administrador, envíe una solicitud de restablecimiento a su dirección de correo electrónico registrada.

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

- Paso 4**  Prensa **confirmar Contraseña** y luego presione OK.
- Paso 5** Repetir **Paso 3**, ingrese la misma contraseña y luego presione OK. Ingrese la
- Paso 6** dirección de correo electrónico y luego seleccione la zona horaria.
- Paso 7**  Prensa **Para seleccionar**  y luego presione OK.

## 2.3 Pantalla de inicio

Figura 2-3 Pantalla de inicio

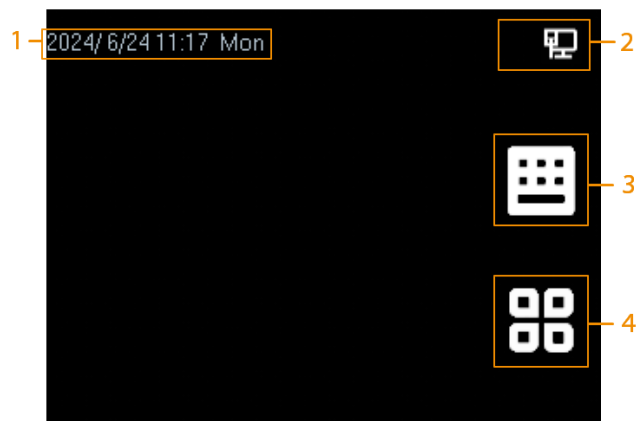



Tabla 2-2 Descripción de la pantalla de inicio

No.	Descripción
1	Muestra la fecha, hora y día actuales.
2	Muestra el estado de la conexión de red.  La función Wi-Fi y Wi-Fi AP están disponibles en modelos seleccionados.
3	Desbloquear por contraseña: Ingrese la contraseña de usuario, contraseña temporal o contraseña de administrador para abrir la puerta.
4	Menú principal: Seleccione el ícono mediante el botón y luego seleccione el método de verificación para ver el menú principal.

## 2.4 Métodos de desbloqueo

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

### 2.4.1 Desbloqueo por tarjetas

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



Esta función solo está disponible en modelos seleccionados.

## 2.4.2 Desbloqueo por huella dactilar

Coloque el dedo en el escáner de huellas dactilares para desbloquear la puerta.



Esta función solo está disponible en modelos seleccionados.

## 2.4.3 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.



No use la mascarilla durante la verificación.

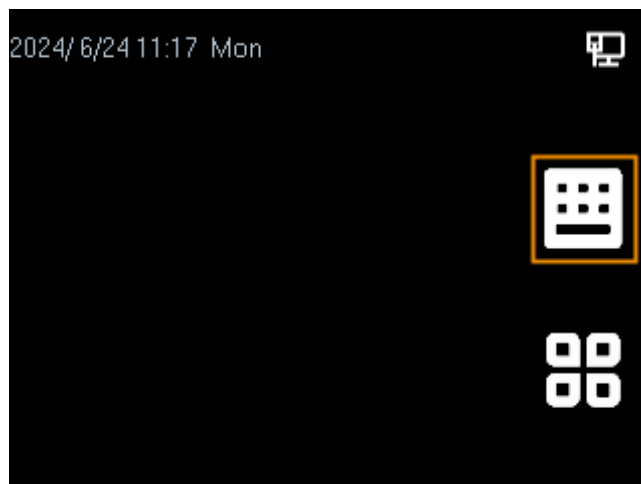
## 2.4.4 Desbloqueo por contraseña de usuario

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

Procedimiento

Paso 1    Prensa  O  Para seleccionar  y luego presione OK.

Figura 2-4 Pantalla de inicio

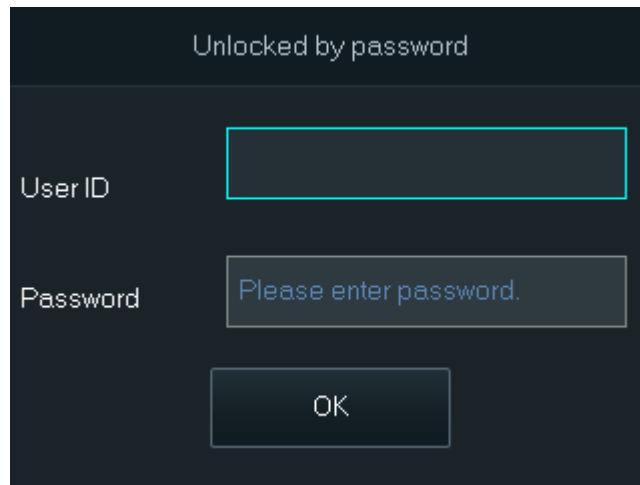


Paso 2    Seleccionar **Desbloqueado por contraseña** y luego presione OK.

Paso 3    Ingrese el ID de usuario y contraseña registrados o entregados.

Después de la verificación exitosa, puedes desbloquear la puerta.

Figura 2-5 Desbloqueo por contraseña



**Paso 4** Seleccionar **DE ACUERDO** y luego presione OK.

## 2.4.5 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 siempre cerrada. Cada dispositivo solo permite una contraseña de administrador.

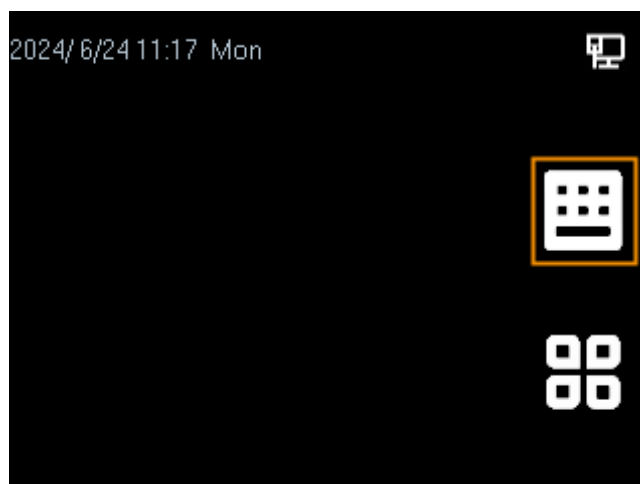
### Prerrequisitos

Se configuró la contraseña de administrador. Para obtener más información, consulte "2.6.3 Configuración de la contraseña de desbloqueo del administrador".

### Procedimiento

**Paso 1** Presiona  o  Para seleccionar  y luego presione OK.

Figura 2-6 Pantalla de inicio



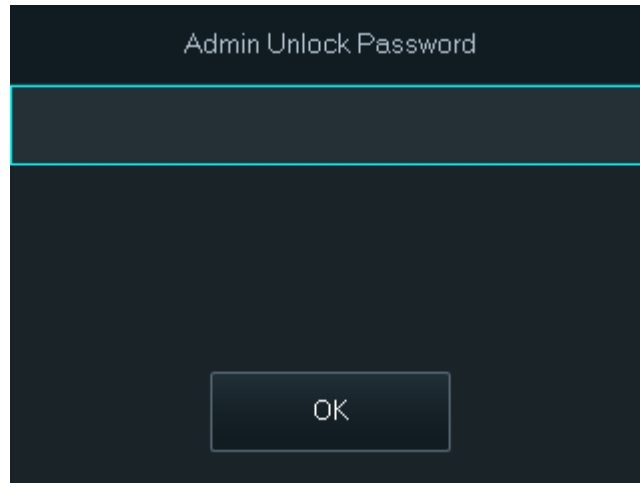
**Paso 2** Seleccionar **Desbloqueo de contraseña de administrador** y luego presione OK. Ingrese

**Paso 3** la contraseña de administrador, seleccione **DE ACUERDO** y luego presione OK.

Después de la verificación exitosa, puedes desbloquear la puerta.



Figura 2-7 Desbloqueo por contraseña de administrador



## 2.4.6 Desbloqueo mediante contraseña temporal

Desbloquee la puerta con la contraseña temporal.

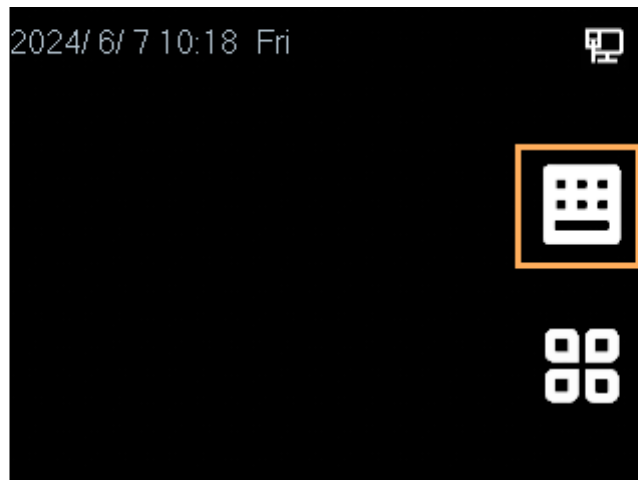
### Procedimiento

Paso 1 Agregue el dispositivo a DMSS.

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

Paso 2 Prensione  o  Para seleccionar  y luego presione OK.

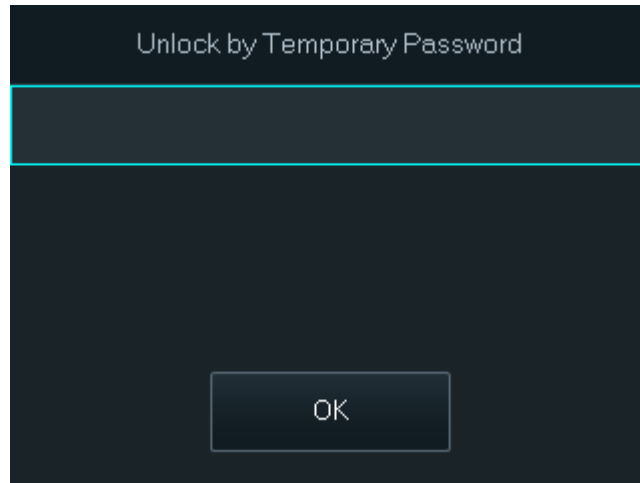
Figura 2-8 Pantalla de inicio



Paso 3 Seleccione **Contraseña temporal** y luego presione OK.

Paso 4 Ingrese la contraseña temporal, seleccione **DE ACUERDO** y luego presione OK.

Figura 2-9 Desbloqueo con contraseña temporal



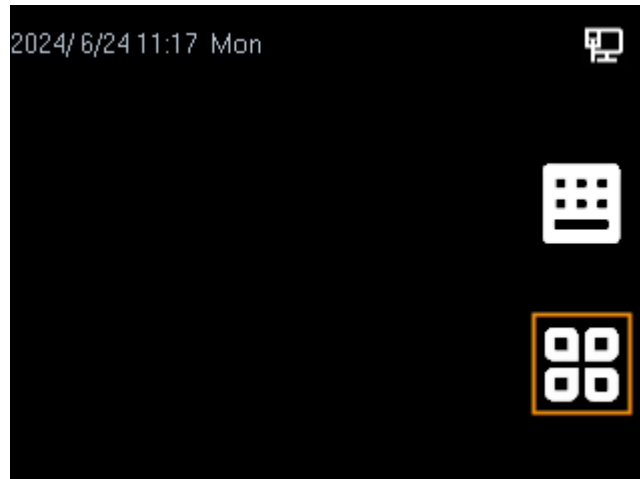
## 2.5 Iniciar sesión

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

Procedimiento

Paso 1 Prensa  o  Para seleccionar  y luego presione OK.

Figura 2-10 Pantalla de inicio



Paso 2 Prensa , ,  o  Para seleccionar **administración** y luego presione OK.

Paso 3 Presione OK y luego ingrese la contraseña que se configuró durante la inicialización.

Paso 4 Prensa  o  Para seleccionar **DE ACUERDO** y luego presione OK.

## 2.6 Gestión de personas

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.

## 2.6.1 Agregar usuarios

Agregue el nuevo usuario, configure el nombre, rostro, huella dactilar, permisos, periodo de validez y otra información.

### Procedimiento


**Paso 1** En el **Menú principal**, seleccionar **Usuarios > Crear**



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



Figura 2-11 Agregar el usuario

Create User(1/3)		Create User(2/3)		Create User(3/3)	
No.	4	Password		User Type	General User >
Name		User Permission	User >	Department	1-Default
Fingerprint	0	Period	255-Default	Schedule Mode	Dept Schedule
Face	0	Holiday Plan	255-Default		
Card	0	Validity Period	2037-12-31		

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).
Huella dactilar	<p>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.</p>  <ul style="list-style-type: none"> <li>● La función de huella dactilar solo está disponible en modelos seleccionados.</li> <li>● No recomendamos que configure la primera huella digital como huella digital de coacción.</li> <li>● Un usuario sólo puede configurar una huella digital de coacción.</li> <li>● La función de huella dactilar está disponible si el controlador de acceso admite la conexión de un módulo de extensión de huella dactilar.</li> </ul>
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.

Parámetro	Descripción
Tarjeta	<p>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.</p> <p>Puedes habilitar el <b>Tarjeta de coacción</b> Función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta.</p>  <p>Un usuario sólo puede configurar una tarjeta de coacción.</p>
Contraseña	<p>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.</p>
Permiso de usuario	<ul style="list-style-type: none"> <li>● <b>Usuario:</b> Los usuarios sólo tienen permisos de acceso a puertas o de control de asistencia.</li> <li>● <b>Administración:</b> Los administradores pueden configurar el controlador de acceso además del acceso a la puerta y los permisos de asistencia.</li> </ul>
Período	<p>Las personas pueden desbloquear la puerta o tomar asistencia durante el período definido.</p>
Plan de vacaciones	<p>Las personas pueden desbloquear la puerta o tomar asistencia durante el día festivo definido.</p>
Periodo de validez	<p>Establecer una fecha en la que caducarán los permisos de acceso a la puerta y de asistencia de la persona.</p>
Tipo de usuario	<ul style="list-style-type: none"> <li>● <b>Usuario general:</b> Los usuarios generales pueden desbloquear la puerta.</li> <li>● <b>Usuario de la lista negra:</b> Cuando los usuarios de la lista de bloqueo desbloqueen la puerta, se activará una alarma de la lista de bloqueo.</li> <li>● <b>Usuario invitado:</b> Los huéspedes pueden desbloquear la puerta dentro de un período definido o durante un número determinado de veces. Una vez que expire el período definido o se agoten los tiempos de desbloqueo, no podrán desbloquear la puerta.</li> <li>● <b>Usuario de patrulla:</b> Los usuarios de patrulla pueden tomar asistencia en el controlador de acceso, pero no tienen puerta.</li> </ul> <p><b>permisos.</b></p> <ul style="list-style-type: none"> <li>● <b>Usuario VIP:</b> Cuando los usuarios VIP desbloqueen la puerta, el personal de servicio recibirá una notificación.</li> <li>● <b>Otro usuario:</b> Cuando desbloqueen la puerta, ésta permanecerá desbloqueada durante 5 segundos más.</li> </ul>  <p>El tiempo de retraso no está disponible para los métodos de verificación remota.</p> <ul style="list-style-type: none"> <li>● <b>Usuario personalizado 1/Usuario personalizado 2:</b> Lo mismo ocurre con los usuarios generales.</li> </ul>

Parámetro	Descripción
Departamento	<p>Seleccionar departamentos, lo cual resulta útil al configurar los horarios de los departamentos.</p>  <p>Esta función solo está disponible en modelos seleccionados.</p>
Modo de programación	<ul style="list-style-type: none"> <li>● Horario de departamento: aplica los horarios de departamento al usuario.</li> <li>● Horario personal: aplica horarios personales al usuario.</li> </ul>  <ul style="list-style-type: none"> <li>◇ Esta función solo está disponible en modelos seleccionados.</li> <li>◇ Si aquí configura el modo de programación en programación de departamento, se aplicará la programación personal que haya configurado para el usuario en <b>Asistencia&gt;Configuración de programación&gt;Horario personal</b> deja de ser válido.</li> </ul>

**Paso 3** Presione la tecla Esc y luego presione OK para guardar las configuraciones.

## 2.6.2 Visualización de la información del usuario

Ver la información del usuario o administrador. Puede editar o eliminar la información del usuario y administrador.

### Procedimiento

**Paso 1** En el **Menú principal**, seleccionar **Usuarios**. Seleccionar **Lista de**

**Paso 2** **usuarios**, o seleccione **Lista de administradores**.

- La lista de usuarios muestra toda la información del usuario en el dispositivo.
- La lista de administradores muestra toda la información del administrador en el dispositivo.

**Paso 3** Ver todos los usuarios o cuentas de administrador agregados.





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

Figura 2-12 Lista de usuarios

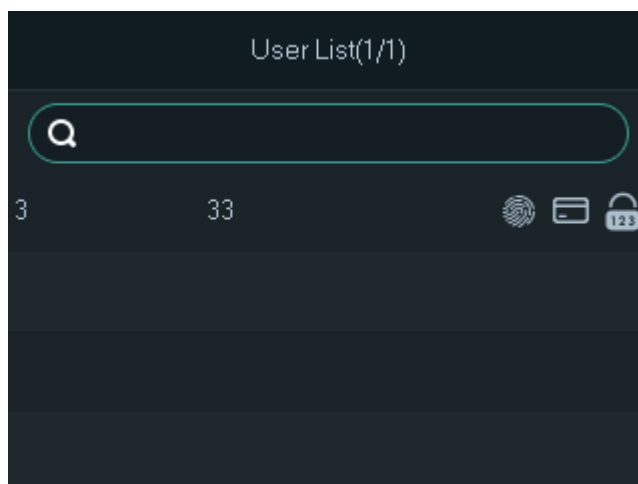
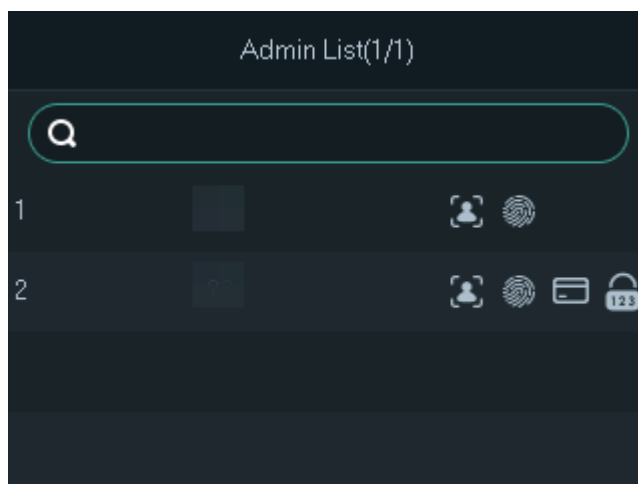










Figura 2-13 Lista de administradores



### Operaciones relacionadas

- **Buscar usuarios o administradores:** Pulsar  o  para seleccionar el cuadro de búsqueda, ingrese el usuario número, nombre de usuario, número de administrador o nombre de administrador y luego presione OK.
- **Editar usuarios o administradores:** Presione y  o  para seleccionar el usuario o el administrador, y luego presione OK.
- **Eliminar usuarios o administradores**
  - ◇ **Eliminar uno por uno:**
    1. En la pantalla de lista de usuarios o de lista de administradores,  o  para seleccionar el usuario o el presione administrador y luego presione OK.
    2. Prensar  para seleccionar  y luego presione OK.
    3. Pulse OK para eliminar el usuario.
  - ◇ **Eliminar todos los usuarios:** En el **Gestión de personas** pantalla, seleccionar **Eliminar todos los usuarios**, presione OK y luego presione OK nuevamente para eliminar todos los usuarios, incluidos los administradores.

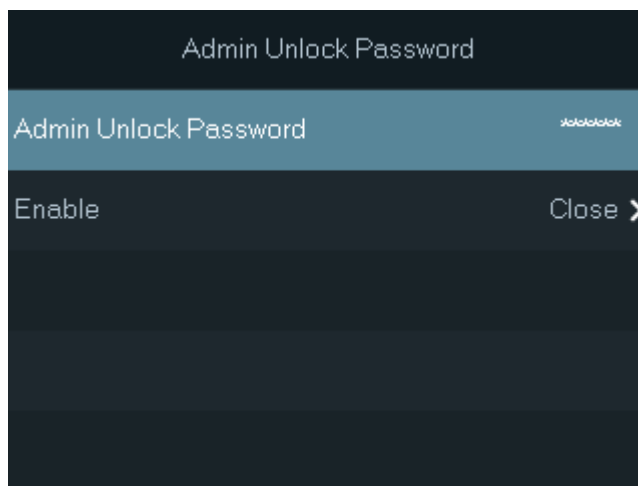
## 2.6.3 Configuración de la contraseña de desbloqueo del administrador

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

### Procedimiento

- Paso 1** En el **Menú principal** pantalla, seleccionar **Usuarios > Desbloqueo de contraseña de administrador**
- Paso 2** Introduzca la contraseña y luego presione OK.

Figura 2-14 Contraseña de desbloqueo de administrador

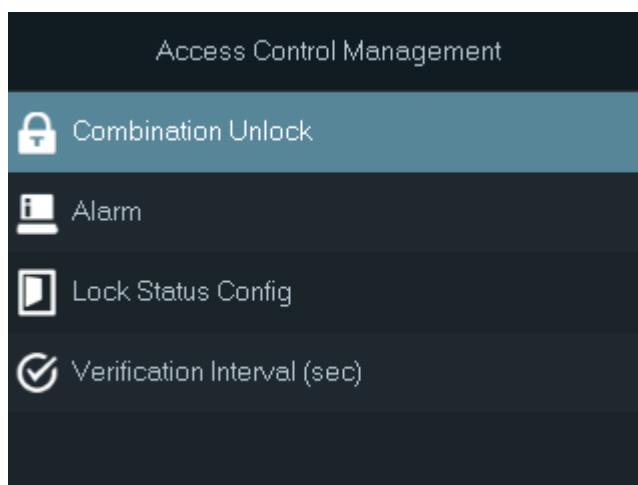


- Paso 3** Seleccionar **Permitir** luego presione OK para habilitar esta función.

## 2.7 Gestión del control 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.

Figura 2-15 Gestión del control de acceso



## 2.7.1 Configuración de combinaciones de desbloqueo

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

Procedimiento

**Paso 1** En el **Menú principal**, seleccionar **Gestión de control de acceso > Desbloqueo de combinación**.

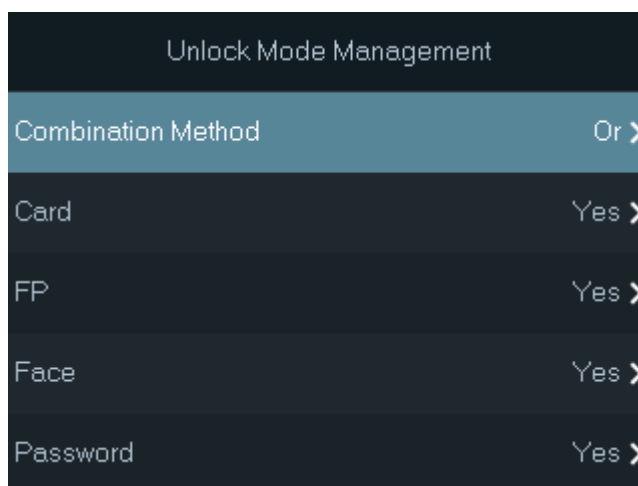
**Paso 2** Pulse OK para configurar el método de combinación y el método de verificación.

- Por ejemplo, configure el **Método de combinación** como **Y**, configurar **Sí** Para tarjeta y contraseña. Puede desbloquear la puerta reconociendo el rostro e ingresando la contraseña.
- Por ejemplo, configure el **Método de combinación** como **O**, configurar **Sí** Para tarjeta y contraseña. Puede desbloquear la puerta reconociendo el rostro o ingresando la contraseña.



El método de verificación de la huella dactilar está disponible en el modelo con función de huella dactilar.

Figura 2-16 Desbloqueo de combinación



**Paso 3** Presione Esc y luego presione OK para guardar las configuraciones.

## 2.7.2 Configuración de alarmas

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

Procedimiento

**Paso 1** En el **Menú principal**, seleccionar **Gestión de control de acceso > Alarma**.

**Paso 2** Configure los parámetros de alarma.



Figura 2-17 Configuración de alarma

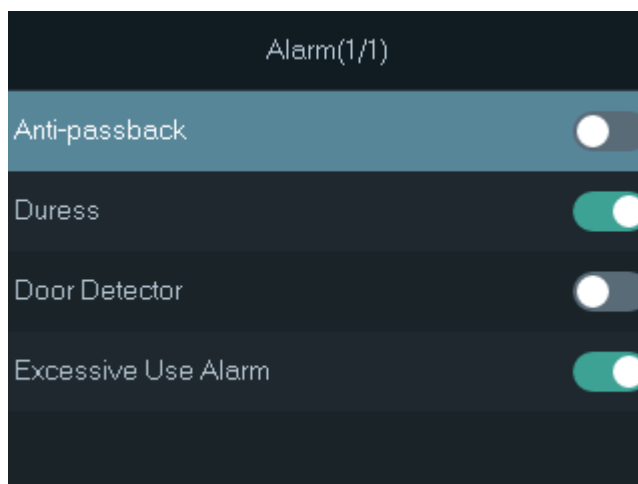



Tabla 2-4 Descripción de los parámetros de alarma

Parámetro	Descripción
Anti-passback	<p>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 antipassback, el titular de la tarjeta debe abandonar el área segura a través de un lector de salida antes de que el sistema le conceda el acceso nuevamente.</p> <p>Las personas deben pasar su tarjeta por el lector de "entrada" para ingresar a un área segura y pasarla por el lector de "salida" para salir de ella.</p> <ul style="list-style-type: none"> <li>● 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.</li> <li>● Si una persona ingresa sin ser verificada, se activará una alarma si intenta salir y se le negará el acceso.</li> </ul> <p></p> <p>Si el Dispositivo solo puede conectarse a una cerradura, la verificación a través del Dispositivo significa que la persona entró en la dirección de "entrada" y la verificación a través del lector de tarjetas externo significa que salió en la dirección de "salida". Puede modificar la configuración en la plataforma.</p>
Coacción	Se activará una alarma cuando se utilice una tarjeta de coacción, una contraseña de coacción o una huella digital de coacción para desbloquear la puerta.
Detector de puerta	Con el detector de puerta conectado a su dispositivo, se pueden activar alarmas cuando las puertas se abren o cierran de manera anormal. Hay 2 tipos de detectores de puerta: detector NC y detector NO.
Tipo de detector de puerta	<ul style="list-style-type: none"> <li>● <b>Normalmente cerrado:</b>El sensor está en una posición de cortocircuito cuando la puerta o ventana está cerrada.</li> <li>● <b>Normalmente abierto:</b>Se crea un circuito abierto cuando la ventana o puerta está realmente cerrada.</li> </ul>

Parámetro	Descripción
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 un tiempo definido.

**Paso 3** Presione Esc y luego presione OK para guardar las configuraciones.

## 2.7.3 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**.

**Paso 2** Configure los parámetros.

Figura 2-18 Estado de bloqueo

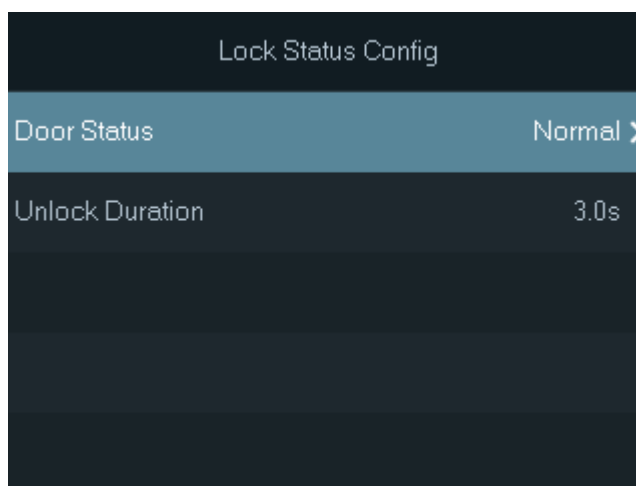


Tabla 2-5 Descripción de parámetros

Parámetro	Descripción
Estado de la puerta	<ul style="list-style-type: none"> <li>● <b>Normalmente abierto:</b> La puerta permanece desbloqueada todo el tiempo.</li> <li>● <b>Normalmente cerrado:</b> La puerta permanece cerrada todo el tiempo.</li> <li>● <b>Normal:</b> Si <b>Normal</b> se selecciona, la puerta se bloqueará y desbloqueará según su configuración.</li> </ul>
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.

## 2.7.4 Configuración del intervalo de tiempo de verificación

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

Procedimiento

**Paso 1** En el **Menú principal** pantalla, seleccionar **Gestión de control de acceso > Intervalo de verificación (seg.)**.

**Paso 2** Introduzca el intervalo de tiempo, seleccione **DE ACUERDO** y luego presione OK.

## 2.8 Configuración de comunicación

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



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

### 2.8.1 Configuración de la red

#### 2.8.1.1 Configuración de la dirección IP

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

Procedimiento

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

**Paso 2** Establecer la dirección IP.



Los parámetros mostrados pueden variar según los diferentes modelos de dispositivo.

Figura 2-19 Configuración de IP

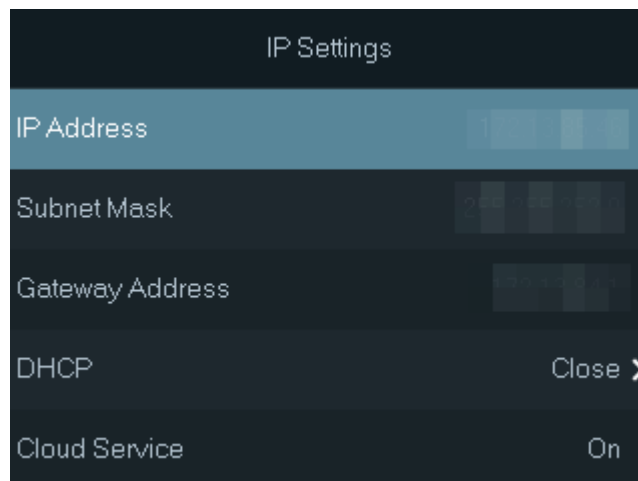


Tabla 2-6 Parámetros de configuración de IP

Parámetro	Descripción
Dirección IP/Máscara de subred/Dirección de puerta de enlace	Ingrese la dirección IP, la máscara de subred y la dirección IP de la puerta de enlace. Deben estar en el mismo segmento de red.
DHCP	Significa Protocolo de configuración dinámica de host. Cuando se activa DHCP, al dispositivo se le asignará automáticamente la dirección IP, la máscara de subred y la puerta de enlace.

Parámetro	Descripción
Servicio en la nube	Si esta función está activada, puede administrar dispositivos sin solicitar DDNS, configurar el mapeo de puertos o implementar servidores de tránsito.

### 2.8.1.2 Configuración de Wi-Fi

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

#### Información de contexto



- Esta función solo está disponible en modelos seleccionados.
- El punto de acceso Wi-Fi y la función Wi-Fi no se pueden habilitar al mismo tiempo.

#### Procedimiento

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

**Paso 2** Seleccionar **Buscar** y luego presione OK. Presione OK para activar el Wi-Fi.

**Paso 3**



Una vez habilitado el Wi-Fi, espere aproximadamente 1 minuto para conectarlo.

**Paso 4** Seleccione una red inalámbrica y luego presione OK.

**Paso 5** Introduzca la contraseña del Wi-Fi, seleccione **Conectar** y luego presione OK.

**Paso 6** (Opcional) Si el sistema no encuentra una red Wi-Fi, seleccione **SSID** para introducir el nombre de la red WiFi.

#### Resultados

Si el teléfono y el dispositivo se conectan a la misma red Wi-Fi, ingrese la dirección IP que se muestra en la pantalla de Wi-Fi en la barra de direcciones del navegador para acceder al dispositivo.

#### Operaciones relacionadas

DHCP: active esta función y se le asignará automáticamente una dirección Wi-Fi al dispositivo. Desactive esta función y podrá configurar la dirección IP.

### 2.8.1.3 Configuración del punto de acceso Wi-Fi

Habilite la función AP Wi-Fi para acceder al dispositivo a través del AP.



- Esta función solo está disponible en modelos seleccionados.
- El punto de acceso Wi-Fi y la función Wi-Fi no se pueden habilitar al mismo tiempo.

#### Procedimiento

**Paso 1** En el **Menú principal**, seleccionar **Configuración de comunicación > Punto de acceso wifi** Encienda el

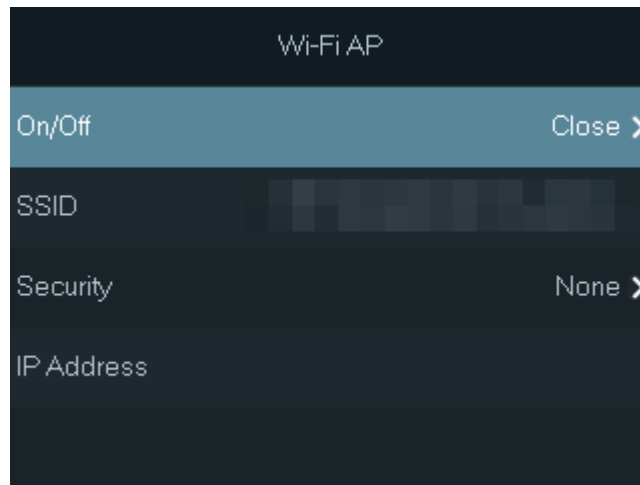
**Paso 2** punto de acceso Wi-Fi.

Puede modificar el SSID y configurar la contraseña a través de **Seguridad**.



- Después de habilitar el AP Wi-Fi, espere aproximadamente 1 minuto para conectarlo.
- La seguridad es **Ninguno** por defecto.

Figura 2-20 Conectarse a un punto de acceso Wi-Fi



#### Resultados

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

## 2.8.2 Configuración de RS-485

#### Procedimiento

Paso 1 En el **Menú principal**, seleccionar **Configuración de comunicación** > **Configuración RS-485**.

Paso 2 Seleccione el dispositivo externo.

Figura 2-21 Tipo de dispositivo externo

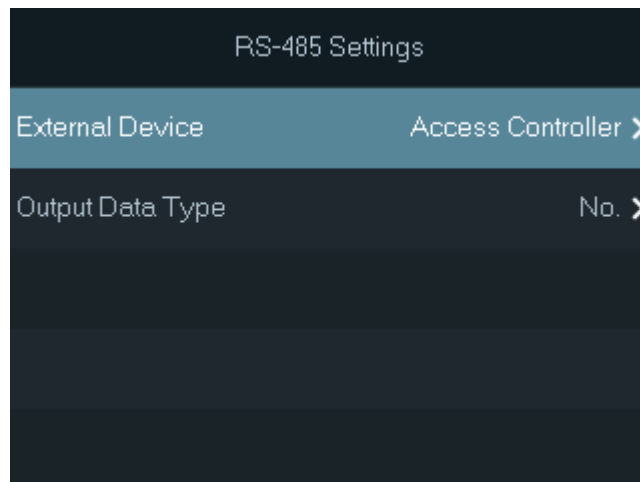


Tabla 2-7 Descripción de parámetros

Dispositivo externo	Descripción
Controlador de acceso	<p>El dispositivo funciona como un lector de tarjetas y envía datos a otros controladores de acceso externos para controlar el acceso.</p> <p>Tipo de datos de salida:</p> <ul style="list-style-type: none"> <li>● Seleccionar <b>Número de tarjeta</b> 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.</li> <li>● Seleccionar <b>No</b>. Genera datos basados en el ID del usuario.</li> </ul>
Lector de tarjetas	El dispositivo se conecta a un lector de tarjetas externo. La información de la tarjeta se envía al controlador de acceso o a la plataforma de gestión.
Lector (OSDP)	El dispositivo se conecta a un lector de tarjetas basado en el protocolo OSDP. La información de la tarjeta se envía al controlador de acceso o a la plataforma de gestión.
Módulo de seguridad para control de puertas	Una vez que se activa el módulo de seguridad, el botón de salida de la puerta, el control de la cerradura y la conexión contra incendios del dispositivo dejan de ser válidos, pero el botón de salida de la puerta y el control de la cerradura que se conectan al módulo de seguridad entran en vigencia. Puede desbloquear la puerta (solo se admite el deslizamiento de la tarjeta) a través del lector de tarjetas externo que está conectado al módulo de seguridad de control de la puerta.

### 2.8.3 Configuración de Wiegand

El dispositivo permite el modo de entrada y salida Wiegand.

Seleccione el tipo de Wiegand según el dispositivo conectado.

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



Esta función solo está disponible en modelos seleccionados.

#### Procedimiento

- Paso 1** En el **Menú principal**, seleccionar **Configuración de comunicación > Configuración de Wiegand** Seleccione un tipo de Wiegand y luego configure los parámetros.
- Paso 2**

Figura 2-22 Configuración de Wiegand

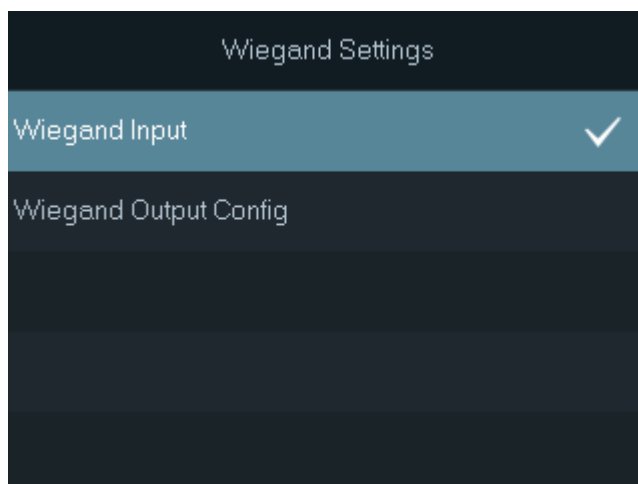
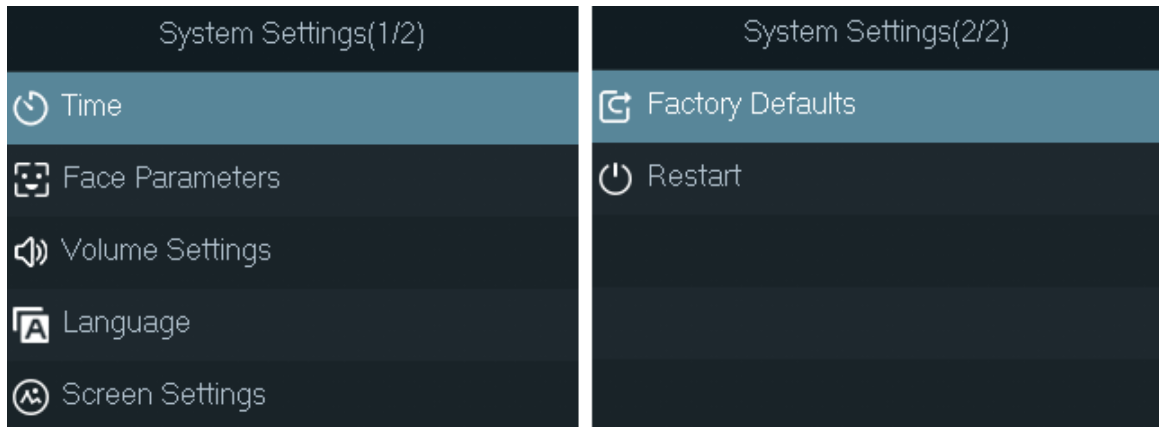


Tabla 2-8 Descripción de la configuración de Wiegand

Parámetro		Descripción
Entrada Wiegand	Tarjeta N° Inversión	Cuando el dispositivo se conecta a un dispositivo de terceros a través del puerto de entrada Wiegand y el número de tarjeta leído por el dispositivo está en orden inverso al número de tarjeta real, en este caso puede activar <b>Tarjeta N° Inversión</b> función.
Salida Wiegand <small>Configuración</small>	Tipo de salida Wiegand	<p>Seleccione un formato Wiegand para leer números de tarjetas o números de identificación.</p> <ul style="list-style-type: none"> <li>● <b>Wiegand26</b>: Lee 3 bytes o 6 dígitos.</li> <li>● <b>Wiegand34</b>: Lee 4 bytes u 8 dígitos.</li> <li>● <b>Wiegand66</b>: Lee 8 bytes o 16 dígitos.</li> </ul>
	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	<p>Seleccione el tipo de datos de salida.</p> <ul style="list-style-type: none"> <li>● <b>No.</b>: El sistema genera datos en función del ID del usuario. El formato de los datos es hexadecimal o decimal.</li> <li>● <b>Número de tarjeta</b>: El sistema genera datos basados en el primer número de tarjeta del usuario.</li> </ul>
Formato de salida	Cuando el <b>Tipo de datos de salida</b> está configurado como <b>No.</b> , puedes seleccionar <b>Hexadecimal</b> o <b>Decimal</b> como formato de salida.	

## 2.9 Configuración del sistema

Figura 2-23 Configuración del sistema



### 2.9.1 Configuración de la hora

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

#### Procedimiento

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

**Paso 2** Configure los parámetros de tiempo.

Figura 2-24 Ajustes de hora

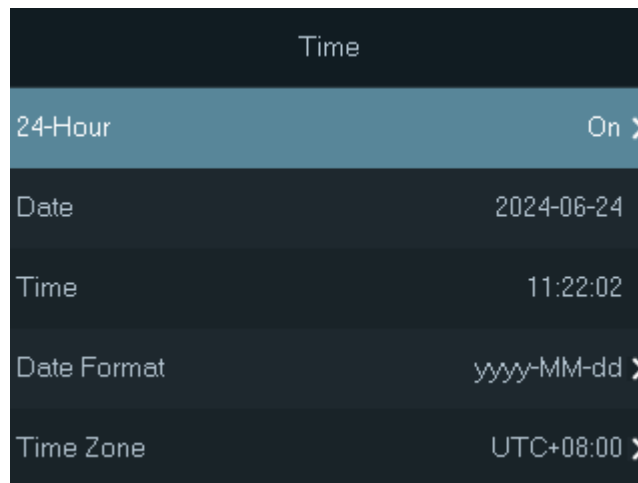
















Tabla 2-9 Descripción de los parámetros de tiempo

Parámetro	Descripción
24 horas	<p>   o OK para activar o desactivar el formato de 24 horas.                 </p> <p>                     Enciéndalo y la hora se mostrará en formato de 24 horas. Apáguelo y la hora se mostrará en formato de 12 horas.                 </p>



Parámetro	Descripción
Fecha y hora	1. Prensa  O  Para seleccionar <b>Fecha y hora</b> y luego presione OK. 2. Presione el botón numérico para ingresar la fecha y luego presione Esc.
Tiempo	1. Prensa  O  Para seleccionar <b>Tiempo</b> y luego presione OK. 2. Presione el botón numérico para ingresar la hora y luego presione Esc.
Formato de fecha	1. Prensa  O  Para seleccionar <b>Formato de fecha</b> . 2. Prensa  ,  o OK para seleccionar el formato de fecha.
Huso horario	1. Prensa  O  Para seleccionar <b>Huso horario</b> . 2. Prensa  ,  o OK para seleccionar la zona horaria.

## 2.9.2 Configuración de parámetros faciales

Configure los parámetros faciales para cambiar la precisión de la reorganización y mejorar la capacidad de protección del control de acceso.

### Información de contexto



Recomendamos que esta función la utilice una persona profesional para depurar.

### Procedimiento


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

**Paso 2** Configure los parámetros de la cara.

Figura 2-25 Parámetros faciales

Face Parameters	
Face Recognition Threshold	85
Valid Face Interval (sec)	3
Invalid Face Interval (sec)	10
Recognition Distance	2.0m >
Enable Anti-spoofing	General >

Tabla 2-10 Descripción de los parámetros del rostro

Nombre	Descripción
Umbral de reconocimiento facial	<p>Ajuste el nivel de precisión del reconocimiento facial. Un umbral más alto significa mayor precisión y menor tasa de reconocimiento falso.</p>  <p>Cuando el umbral es demasiado bajo, como 0, la tasa de reconocimiento falso será extremadamente alta. Tenga en cuenta lo siguiente.</p>
Intervalo de cara válido (seg.)	Cuando el mismo rostro permanece frente a la lente después del primer reconocimiento exitoso, el dispositivo realizará nuevamente el reconocimiento del rostro después de un intervalo definido.
Intervalo de rostro no válido (seg.)	Cuando el mismo rostro permanece frente a la lente después del primer reconocimiento fallido, el dispositivo realizará nuevamente el reconocimiento del rostro después de un intervalo definido.
Distancia de reconocimiento	La distancia entre la cara y la lente.
Habilitar anti-spoofing	Esto evita que las personas puedan usar fotos, vídeos, máscaras y otros sustitutos para obtener acceso no autorizado.

## 2.9.3 Configuración del volumen

### Procedimiento

- Paso 1** En el **Menú principal**, seleccionar **Sistema > Ajustes de volumen**.
- Paso 2** Configure los parámetros.

Figura 2-26 Configuración del volumen

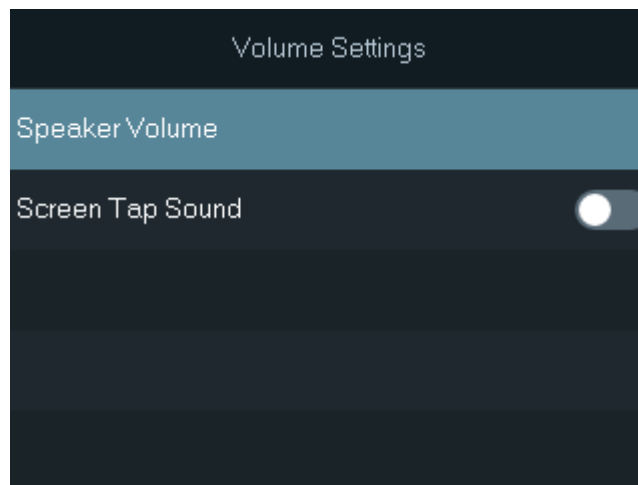




Tabla 2-11 Descripción de parámetros

Parámetros	Descripción
Volumen del altavoz	Seleccionar <b>Volumen del altavoz</b> , presione OK y luego presione el  o  Ajustar volumen.

Parámetros	Descripción
Sonido al tocar la pantalla	Cuando esta función está habilitada, hay sonido si presiona los botones.

## 2.9.4 Configuración del idioma

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

## 2.9.5 Configuración de parámetros 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**

**Paso 2** **pantalla**. Configure los parámetros.

Figura 2-27 Configuración de pantalla

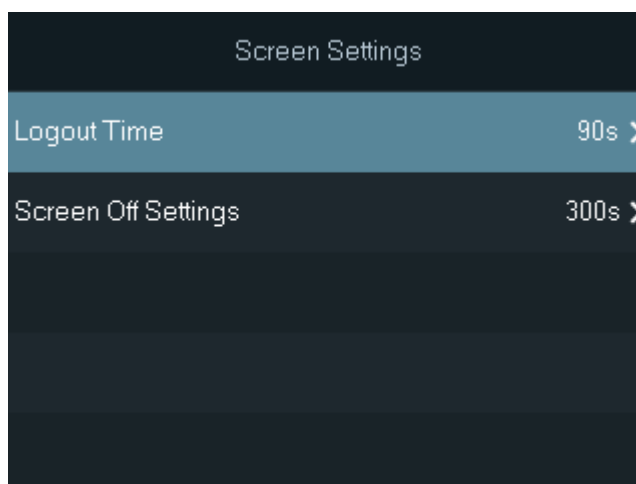


Tabla 2-12 Descripción de parámetros

Parámetros	Descripción
Hora de cerrar sesión	El sistema vuelve a la pantalla de espera después de un tiempo definido de inactividad.
Configuración de pantalla apagada	El sistema vuelve a la pantalla de espera y luego la pantalla se apaga después de un tiempo definido de inactividad.

## Ejemplo

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



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

## 2.9.6 Restauración de los valores predeterminados de fábrica

### Información de contexto



La restauración de los valores predeterminados de fábrica provocará la pérdida de datos. Tenga en cuenta lo siguiente.

### Procedimiento

#### Paso 1

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

## 2.9.7 Reinicio del dispositivo

En el **Menú principal**, seleccionar **Sistema** > **Reanudar**, presione OK y luego presione OK para que aparezca el mensaje. El dispositivo se reiniciará.

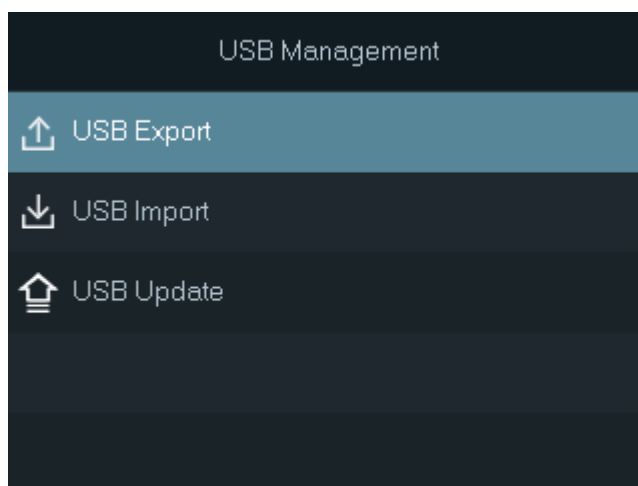
## 2.10 Gestión USB

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



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

Figura 2-28 Gestión USB



## 2.10.1 Exportación a USB

Puede exportar datos del dispositivo a un USB. Los datos exportados están encriptados y no se pueden editar.

Procedimiento

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

**Paso 2** Seleccione el tipo de datos que desea exportar.



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

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

**Paso 3** Pulse OK para confirmar.

Los datos exportados se guardan en el USB.

## 2.10.2 Importación desde USB

Puede importar datos desde USB al dispositivo.

Procedimiento

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

**Paso 2** tipo de datos que desea importar y luego presione **DE ACUERDO**.



Le recomendamos que importe los datos a un dispositivo con el mismo modelo y versión. La transmisión de datos entre dispositivos con diferentes modelos y versiones provocará la pérdida de datos.

## 2.10.3 Actualización del sistema

Actualizar el sistema del Dispositivo a través de USB.



Si inicia el dispositivo por primera vez o restaura el dispositivo a la configuración predeterminada de fábrica, el dispositivo realiza automáticamente una copia de seguridad de los archivos del sistema dentro de los primeros 10 minutos. No actualice durante este período.

Procedimiento

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

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

**Paso 3** **ACUERDO**.

El dispositivo se reiniciará cuando se complete la actualización.



No apague el dispositivo durante la actualización.

## 2.11 Gestión de registros

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

Figura 2-29 Desbloquear registros



No.	Time	Results
3	06-24 11:24	Succeed
3	06-24 11:24	Succeed
3	06-24 11:24	Succeed
3	06-24 11:24	Succeed

## 2.12 Información del sistema

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

### 2.12.1 Visualización de la capacidad de datos

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

### 2.12.2 Visualización de la versión del dispositivo

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

#### Operaciones relacionadas

Seleccionar **Código QR del material del producto**, presione OK y luego escanee el código QR con su teléfono para ver los documentos del producto.



Esta función solo está disponible en modelos seleccionados.

## 3 Operaciones de la página web

En la página web también puedes configurar y actualizar el dispositivo.



Las configuraciones web difieren según los modelos del dispositivo.

### 3.1 Inicialización

Inicialice el dispositivo cuando inicie sesión en la página web por primera vez o después de que el dispositivo se 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 dispositivo.

#### Procedimiento

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



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

**Paso 2** Seleccione un idioma en el dispositivo.

**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 (excepto ' ' ; : &). Establezca una contraseña de alta seguridad siguiendo las indicaciones de seguridad de la contraseña.
- Mantenga la contraseña segura después de la inicialización y cámbiela periódicamente para mejorar la seguridad.

### 3.2 Restablecimiento de la contraseña

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

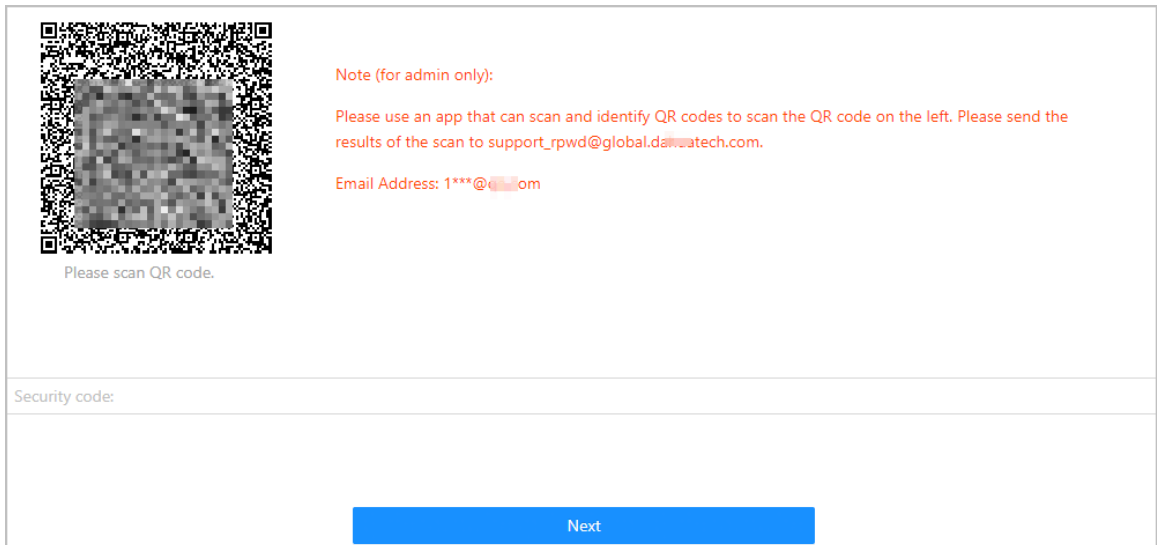
#### Procedimiento

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

Figura 3-1 Restablecer contraseña



Please scan QR code.

Note (for admin only):  
Please use an app that can scan and identify QR codes to scan the QR code on the left. Please send the results of the scan to support\_rpwd@global.dawatech.com.  
Email Address: 1\*\*\*@q...om

Security code:

Next



- Se generarán hasta dos códigos de seguridad al escanear el mismo código QR. Si el código de seguridad deja de ser válido, actualice el código QR y escanéelo nuevamente.
- Después de escanear el código QR, recibirá un código de seguridad en la dirección de correo electrónico vinculada. Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, perderá su validez.
- Si se ingresa un código de seguridad incorrecto 5 veces seguidas, la cuenta de administrador se congelará durante 5 minutos.

**Paso 4** Introduzca el código de seguridad.

**Paso 5** Haga clic en **Próximo**.

**Paso 6** Restablecer y confirmar la 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**.

### 3.3 Página de inicio

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



Figura 3-2 Página de inicio

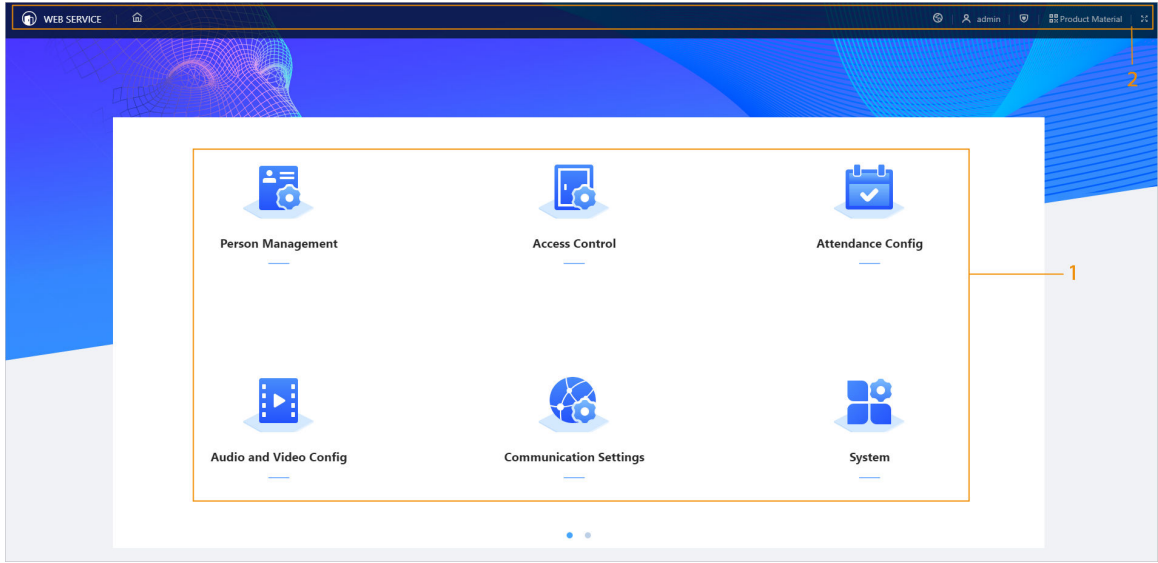


Tabla 3-1 Descripción de la página de inicio

No.	Descripción
1	Menú principal.
2	<ul style="list-style-type: none"> <li>● : Ingresa a la página de inicio.</li> <li>● : Mostrar en pantalla completa.</li> <li>● : Ingresa el <b>Seguridad</b> página.</li> <li>● : Escanee el código QR con su teléfono para ver los documentos del producto.</li> </ul> <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p>Esta función solo está disponible en modelos seleccionados</p> </div> <ul style="list-style-type: none"> <li>● : Cierre la sesión o reinicie el dispositivo.</li> <li>● : Seleccione un idioma en el dispositivo.</li> </ul>

## 3.4 Gestión de personas

### Procedimiento

- Paso 1 En la página de inicio, seleccione **Gestión de personas**, y luego haga clic **Agregar**. Configurar
- Paso 2 la información del usuario.

Figura 3-3 Agregar usuarios

**Add**
✕

---

**Basic Info**

<b>* User ID</b> <input type="text"/>	<b>Name</b> <input type="text"/>
<b>* Department</b> <input type="text" value="1-"/> <span style="float: right;">▼</span>	<b>* Schedule Mode</b> <input type="text" value="Department Schedule"/> <span style="float: right;">▼</span>
<b>Validity Period</b> <input type="text" value="2037-12-31 23:59:59"/> <span style="float: right;">📅</span>	<b>* Permission</b> <input type="text" value="User"/> <span style="float: right;">▼</span>
<b>* User Type</b> <input type="text" value="General User"/> <span style="float: right;">▼</span>	<b>* Times Used</b> <input type="text" value="Unlimited"/>
<b>* Period</b> <input type="text" value="255-Default"/> <span style="float: right;">▼</span>	<b>* Holiday Plan</b> <input type="text" value="255-Default"/> <span style="float: right;">▼</span>

**Verification Mode**

▼ Face
Not Added

+  
Upload

i The image size must not exceed 100KB. Supported formats: jpg.




> Password
Not Added






> Card
Not Added


Add
Add More
Cancel

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 30 caracteres.
Nombre	El nombre puede tener hasta 32 caracteres (incluidos números, símbolos y letras).

Parámetro	Descripción
Departamento	Agregar usuarios a un departamento. Si se le asigna un horario de departamento a la persona, esta seguirá el horario de departamento establecido.
Modo de programación	<ul style="list-style-type: none"> <li>● <b>Horario del departamento:</b> Asigna el horario del departamento al usuario.</li> <li>● <b>Horario personal:</b> Asigna un horario personal al usuario.</li> </ul>  <ul style="list-style-type: none"> <li>◇ Esta función solo está disponible en modelos seleccionados.</li> <li>◇ Si aquí configura el modo de programación en programación de departamento, se aplicará la programación personal que haya configurado para el usuario en <b>Asistencia&gt;Configuración de programación&gt;Horario personal</b> no es válido.</li> </ul>
Periodo de validez	Establecer una fecha en la que caducarán los permisos de acceso a la puerta y de asistencia de la persona.
Permiso	<ul style="list-style-type: none"> <li>● <b>Usuario:</b> Los usuarios sólo tienen permisos de acceso a puertas o de control de asistencia.</li> <li>● <b>Administración:</b> Los administradores pueden configurar el dispositivo además del acceso a la puerta y los permisos de asistencia.</li> </ul>
Tipo de usuario	<ul style="list-style-type: none"> <li>● <b>Usuario general:</b> Los usuarios generales pueden desbloquear la puerta.</li> <li>● <b>Usuario de la lista negra:</b> Cuando los usuarios de la lista de bloqueo desbloqueen la puerta, el personal de servicio recibirá una notificación.</li> <li>● <b>Usuario invitado:</b> Los huéspedes pueden desbloquear la puerta dentro de un período definido o durante un tiempo determinado. Una vez que el período definido o el tiempo de desbloqueo se agoten, no podrán desbloquear la puerta.</li> <li>● <b>Usuario de patrulla:</b> Los usuarios de patrulla pueden tomar asistencia en el dispositivo, pero no tienen permisos de puerta.</li> <li>● <b>Usuario VIP:</b> Cuando el VIP desbloquee la puerta, el personal de servicio recibirá un aviso.</li> <li>● <b>Otro usuario:</b> Cuando desbloqueen la puerta, ésta permanecerá desbloqueada durante 5 segundos más.</li> <li>● Usuario personalizado 1/Usuario personalizado 2: Lo mismo que los usuarios generales.</li> </ul>
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.  Puede seleccionar más de un período.
Plan de vacaciones	Las personas pueden desbloquear la puerta o tomar asistencia durante el día festivo definido.  Puede seleccionar más de un día festivo.

Parámetro	Descripción
Rostro	<p>Hacer clic <b>Subir</b> 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.</p>  <p>La imagen del rostro está en formato jpg, jpeg, png y debe ser menor a 100 KB.</p>
Tarjeta	 <p>Esta función solo está disponible en modelos seleccionados.</p> <ul style="list-style-type: none"> <li>● Introduzca el número de tarjeta manualmente. <ol style="list-style-type: none"> <li>1. Haga clic <b>Agregar</b>.</li> <li>2. Ingrese el número de tarjeta y luego haga clic en <b>Agregar</b>.</li> </ol> </li> <li>● Lea el número automáticamente a través del lector de inscripción o del Dispositivo. <ol style="list-style-type: none"> <li>1. Haga clic <b>Agregar</b>, y luego haga clic <b>Modificar</b> para seleccionar un lector de inscripción o el Dispositivo.</li> <li>2. Haga clic <b>Leer tarjeta</b> y luego pase las tarjetas por el lector de tarjetas. <p style="margin-left: 20px;">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 <b>Leer tarjeta</b> de nuevo para iniciar una nueva cuenta regresiva.</p> </li> <li>3. Haga clic <b>Agregar</b>.</li> </ol> </li> </ul> <p>Un usuario puede registrar hasta 5 tarjetas como máximo. Ingrese el número de su tarjeta o deslícela y el dispositivo leerá la información de la tarjeta.</p> <p>Puedes habilitar el <b>Tarjeta de coacción</b> Función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta.</p> <ul style="list-style-type: none"> <li>●  Establecer tarjeta de coacción. :</li> <li>●  Cambiar número de tarjeta.</li> </ul>  <p>Un usuario sólo puede configurar una tarjeta de coacción.</p>
Contraseña	<p>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.</p>

Parámetro	Descripción
Huella dactilar	<p>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.</p> <p>Inscriba huellas dactilares a través de un lector de inscripción o del Dispositivo.</p> <ol style="list-style-type: none"> <li>Haga clic <b>Agregar</b>, y luego haga clic <b>Modificar</b> para seleccionar un lector de inscripción o el Dispositivo.</li> <li>Presione el dedo sobre el escáner de acuerdo con las instrucciones en pantalla.</li> <li>Haga clic <b>Agregar</b>.</li> </ol> <p></p> <ul style="list-style-type: none"> <li>● La función de huella dactilar solo está disponible en modelos seleccionados.</li> <li>● No recomendamos que configure la primera huella digital como huella digital de coacción.</li> <li>● Un usuario solo puede configurar una huella digital de coacción.</li> <li>● La función de huella dactilar está disponible si el dispositivo admite la conexión de un módulo de huella dactilar.</li> </ul>

### Paso 3

Hacer clic **DE ACUERDO**.

#### Operaciones relacionadas

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



Se pueden importar hasta 10.000 usuarios a la vez.

- Borrar: Borrar todos los usuarios.
- Actualizar: Actualiza la lista de usuarios.
- Buscar: Busque por nombre de usuario o ID de usuario.

## 3.5 Configuración del control de acceso

### 3.5.1 Gestión de personas

#### Procedimiento

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

**Paso 2** la información del usuario.

Figura 3-4 Agregar usuarios

**Add**
✕

---

**Basic Info**

<b>* User ID</b> <input type="text"/>	<b>Name</b> <input type="text"/>
<b>* Department</b> <input type="text" value="1-"/>	<b>* Schedule Mode</b> <input type="text" value="Department Schedule"/>
<b>Validity Period</b> <input type="text" value="2037-12-31 23:59:59"/>	<b>* Permission</b> <input type="text" value="User"/>
<b>* User Type</b> <input type="text" value="General User"/>	<b>* Times Used</b> <input type="text" value="Unlimited"/>
<b>* Period</b> <input type="text" value="255-Default"/>	<b>* Holiday Plan</b> <input type="text" value="255-Default"/>

**Verification Mode**

▼ Face Not Added

+  
Upload

ⓘ The image size must not exceed 100KB. Supported formats: jpg.




> Password Not Added






> Card Not Added

Add
Add More
Cancel


Tabla 3-3 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 30 caracteres.
Nombre	El nombre puede tener hasta 32 caracteres (incluidos números, símbolos y letras).

Parámetro	Descripción
Departamento	Agregar usuarios a un departamento. Si se le asigna un horario de departamento a la persona, esta seguirá el horario de departamento establecido.
Modo de programación	<ul style="list-style-type: none"> <li>● <b>Horario del departamento:</b> Asigna el horario del departamento al usuario.</li> <li>● <b>Horario personal:</b> Asigna un horario personal al usuario.</li> </ul>  <div style="background-color: #f0f0f0; padding: 5px;"> <ul style="list-style-type: none"> <li>◇ Esta función solo está disponible en modelos seleccionados.</li> <li>◇ Si aquí configura el modo de programación en programación de departamento, se aplicará la programación personal que haya configurado para el usuario en <b>Asistencia&gt;Configuración de programación&gt;Horario personal</b> no es válido.</li> </ul> </div>
Periodo de validez	Establecer una fecha en la que caducarán los permisos de acceso a la puerta y de asistencia de la persona.
Permiso	<ul style="list-style-type: none"> <li>● <b>Usuario:</b> Los usuarios sólo tienen permisos de acceso a puertas o de control de asistencia.</li> <li>● <b>Administración:</b> Los administradores pueden configurar el dispositivo además del acceso a la puerta y los permisos de asistencia.</li> </ul>
Tipo de usuario	<ul style="list-style-type: none"> <li>● <b>Usuario general:</b> Los usuarios generales pueden desbloquear la puerta.</li> <li>● <b>Usuario de la lista negra:</b> Cuando los usuarios de la lista de bloqueo desbloqueen la puerta, el personal de servicio recibirá una notificación.</li> <li>● <b>Usuario invitado:</b> Los huéspedes pueden desbloquear la puerta dentro de un período definido o durante un tiempo determinado. Una vez que el período definido o el tiempo de desbloqueo se agoten, no podrán desbloquear la puerta.</li> <li>● <b>Usuario de patrulla:</b> Los usuarios de patrulla pueden tomar asistencia en el dispositivo, pero no tienen permisos de puerta.</li> <li>● <b>Usuario VIP:</b> Cuando el VIP desbloquee la puerta, el personal de servicio recibirá un aviso.</li> <li>● <b>Otro usuario:</b> Cuando desbloqueen la puerta, ésta permanecerá desbloqueada durante 5 segundos más.</li> <li>● Usuario personalizado 1/Usuario personalizado 2: Lo mismo que los usuarios generales.</li> </ul>
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.  Puede seleccionar más de un período.
Plan de vacaciones	Las personas pueden desbloquear la puerta o tomar asistencia durante el día festivo definido.  Puede seleccionar más de un día festivo.

Parámetro	Descripción
Rostro	<p>Hacer clic <b>Subir</b> 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.</p>  <p>La imagen del rostro está en formato jpg, jpeg, png y debe ser menor a 100 KB.</p>
Tarjeta	 <p>Esta función solo está disponible en modelos seleccionados.</p> <ul style="list-style-type: none"> <li>● Introduzca el número de tarjeta manualmente. <ol style="list-style-type: none"> <li>1. Haga clic <b>Agregar</b>.</li> <li>2. Ingrese el número de tarjeta y luego haga clic en <b>Agregar</b>.</li> </ol> </li> <li>● Lea el número automáticamente a través del lector de inscripción o del Dispositivo. <ol style="list-style-type: none"> <li>1. Haga clic <b>Agregar</b>, y luego haga clic <b>Modificar</b> para seleccionar un lector de inscripción o el Dispositivo.</li> <li>2. Haga clic <b>Leer tarjeta</b> y luego pase las tarjetas por el lector de tarjetas. <p style="margin-left: 20px;">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 <b>Leer tarjeta</b> de nuevo para iniciar una nueva cuenta regresiva.</p> </li> <li>3. Haga clic <b>Agregar</b>.</li> </ol> </li> </ul> <p>Un usuario puede registrar hasta 5 tarjetas como máximo. Ingrese el número de su tarjeta o deslícela y el dispositivo leerá la información de la tarjeta.</p> <p>Puedes habilitar el <b>Tarjeta de coacción</b> Función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta.</p> <ul style="list-style-type: none"> <li>●  Establecer tarjeta de coacción. :</li> <li>●  Cambiar número de tarjeta.</li> </ul>  <p>Un usuario sólo puede configurar una tarjeta de coacción.</p>
Contraseña	<p>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.</p>



Parámetro	Descripción
Huella dactilar	<p>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.</p> <p>Inscriba huellas dactilares a través de un lector de inscripción o del Dispositivo.</p> <ol style="list-style-type: none"> <li>Haga clic <b>Agregar</b>, y luego haga clic <b>Modificar</b> para seleccionar un lector de inscripción o el Dispositivo.</li> <li>Presione el dedo sobre el escáner de acuerdo con las instrucciones en pantalla.</li> <li>Haga clic <b>Agregar</b>.</li> </ol> <p></p> <ul style="list-style-type: none"> <li>● La función de huella dactilar solo está disponible en modelos seleccionados.</li> <li>● No recomendamos que configure la primera huella digital como huella digital de coacción.</li> <li>● Un usuario solo puede configurar una huella digital de coacción.</li> <li>● La función de huella dactilar está disponible si el dispositivo admite la conexión de un módulo de huella dactilar.</li> </ul>

### Paso 3

Hacer clic **DE ACUERDO**.

#### Operaciones relacionadas

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



Se pueden importar hasta 10.000 usuarios a la vez.

- Borrar: Borrar todos los usuarios.
- Actualizar: Actualiza la lista de usuarios.
- Buscar: Busque por nombre de usuario o ID de usuario.

## 3.5.2 Configuración de parámetros de control de acceso

### 3.5.2.1 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 3-5 Parámetros básicos

**Basic Settings**

Name

Door Status  Normal  Always Closed  Always Open


Normally Open Period Period  Holiday Plan

Normally Closed Period Period  Holiday Plan

Unlock Notifications Mode

Verification Interval  s (0-180)

Tabla 3-4 Descripción de los parámetros básicos

Parámetro	Descripción
Nombre	El nombre de la puerta.
Estado de la puerta	<p>Establecer el estado de la puerta.</p> <ul style="list-style-type: none"> <li>● <b>Normal:</b> La puerta se desbloqueará y bloqueará según su configuración.</li> <li>● Siempre abierto: la puerta permanece desbloqueada todo el tiempo.</li> <li>● Siempre cerrado: la puerta permanece bloqueada todo el tiempo.</li> </ul>
Periodo normalmente abierto	<p>Cuando seleccionas <b>Normal</b>, puede seleccionar una plantilla de horario de la lista desplegable. La puerta permanece abierta o cerrada durante el tiempo definido. Para obtener más información sobre cómo configurar períodos y planes de vacaciones, consulte "3.5.7 Configuración de horarios".</p>
Periodo normalmente cerrado	<p></p> <ul style="list-style-type: none"> <li>● Cuando el período normalmente abierto entra en conflicto con el período normalmente cerrado, el período normalmente abierto tiene prioridad sobre el período normalmente cerrado.</li> <li>● Cuando el período entra en conflicto con el plan de vacaciones, los planes de vacaciones tienen prioridad sobre los períodos.</li> </ul>
Desbloquear notificación	<p>Muestra la notificación en la pantalla cuando una persona verifica su identidad en el dispositivo.</p> <ul style="list-style-type: none"> <li>● <b>Modo de alta velocidad:</b> el sistema le indica <b>Verificado exitosamente</b> <b>No autorizado</b> en la pantalla.</li> <li>● <b>Modo simple:</b> muestra el ID del usuario, el nombre y el tiempo de verificación después de conceder el acceso; muestra <b>No autorizado</b> tiempo de autorización después de denegar el acceso.</li> <li>● <b>Estándar:</b> 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 <b>No autorizado</b> y tiempo de verificación después de denegar el acceso.</li> <li>● <b>Modo de contraste:</b> 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 <b>No autorizado</b> tiempo de autorización después de denegar el acceso.</li> </ul>

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

**Paso 3** Hacer clic **Aplicar**.

### 3.5.2.2 Configuración de métodos de desbloqueo

Puede utilizar varios métodos de desbloqueo para desbloquear la puerta, como huella dactilar, tarjeta y 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 **OoY**.
    - ◇ 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 3-6 Configuración de desbloqueo

**Unlock Settings**

Unlock Method: Combination Unlock

Combination Method:  Or  And

Unlock Method (Multi-select):  Card  Fingerprint  Face  Password

Door Unlocked Duration: 3.0 s (0.2-600)

Remote Verification:

Apply Refresh Default

Tabla 3-5 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 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

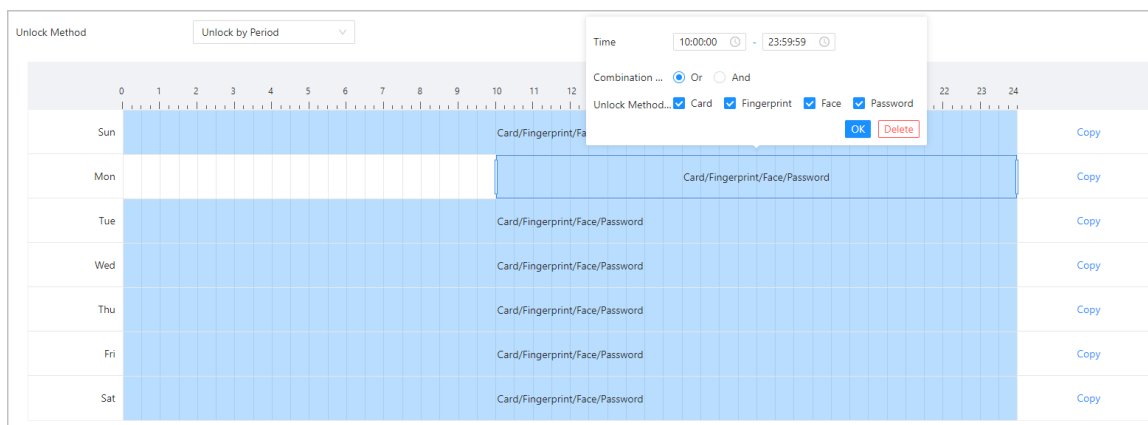
1. En el **Modo de desbloqueo** lista, seleccionar **Desbloqueo por periodo**.
2. Arrastre el control deslizante para ajustar el período de tiempo para cada día.



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 3-7 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 el número de personas del 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 la cantidad de personas de cada grupo que deben verificar su identidad en el dispositivo antes de desbloquear la puerta. Por ejemplo, si el número válido se establece en 3 para un grupo, 3 personas del grupo deben verificar su identidad para desbloquear la puerta.

**Paso 3** Hacer clic **Aplicar**.

### 3.5.3 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 3-8 Alarma

Duress Alarm

Anti-passback

Door Detector   Normally Closed  Normally Open

Intrusion Alarm




Unlock Timeout Alarm

Unlock Timeout  s (1-9999)

Excessive Use Alarm

Tabla 3-6 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	<p>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.</p> <ul style="list-style-type: none"> <li>● 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.</li> <li>● 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.</li> </ul> <p></p> <p>Si el dispositivo solo puede conectar una cerradura, la verificación en el dispositivo significa la dirección de entrada y la verificación en el lector de tarjetas externo significa la dirección de salida de manera predeterminada. Puede modificar la configuración en la plataforma de administración.</p>
Detector de puerta	<p>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.</p> <ul style="list-style-type: none"> <li>● Normalmente cerrado: el sensor está en una posición de cortocircuito cuando la puerta o ventana está cerrada.</li> <li>● Normalmente abierto: se crea un circuito abierto cuando la ventana o puerta está realmente cerrada.</li> </ul>
Alarma de intrusión	<p>Si la puerta se abre de forma anormal, se activará una alarma de intrusión que durará un tiempo definido.</p> <p></p> <p>El detector de puerta y la intrusión deben habilitarse al mismo tiempo.</p>
Alarma de tiempo de espera para desbloqueo	<p>Cuando la puerta permanece desbloqueada durante más tiempo que el tiempo de espera definido, se activará la alarma de tiempo de espera de la puerta y durará el tiempo definido.</p>
Desbloquear tiempo de espera	<p></p> <p>El detector de puerta y la función de tiempo de espera de puerta deben habilitarse al mismo tiempo.</p>
Alarma de uso excesivo	<p>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 un tiempo definido.</p>

**Paso 3** Hacer clic **Aplicar**.

### 3.5.4 Configuración de la vinculación de eventos de alarma

#### Procedimiento

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

**Paso 2** Configurar vínculos de eventos de alarma.

Figura 3-9 Vinculación de eventos de alarma

Tabla 3-7 Vinculación de eventos de alarma

Parámetro	Descripción
Vinculación de alarmas de intrusión	Si la puerta se abre de forma anormal, se activará una alarma de intrusión. Timbre: el timbre suena cuando se activa una alarma de intrusión. Puede configurar la duración de la alarma.
Alarma de tiempo de espera para desbloqueo Enlace	Cuando la puerta permanece desbloqueada durante más tiempo que el tiempo de espera definido, se activará la alarma de tiempo de espera de la puerta y durará el tiempo definido. Timbre: el timbre suena cuando se activa la alarma de tiempo de desbloqueo. Puede configurar la duración de la alarma.
Alarma de uso excesivo Enlace	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 un tiempo definido. Timbre: el timbre suena cuando se activa la alarma de uso excesivo. Puede configurar la duración de la alarma.

Parámetro	Descripción
Conexión de alarma antimanipulación	<p>La alarma de manipulación se activa cuando alguien intenta dañar físicamente el dispositivo.</p> <p>Zumbador: el zumbador suena cuando se activa la alarma antimanipulación. Puede configurar la duración de la alarma.</p>

### 3.5.5 Configuración de parámetros faciales

Configurar los parámetros de detección de rostros. Los parámetros de detección de rostros pueden variar según el modelo del producto.

#### Procedimiento


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

**Paso 2** Seleccionar **Control de acceso > Parámetros faciales**.

Figura 3-10 Parámetros de detección de rostros

**Paso 3** Configurar los parámetros.

Tabla 3-8 Descripción de los parámetros faciales

Nombre	Descripción
Umbral de reconocimiento facial	<p>Ajuste el nivel de precisión del reconocimiento facial. Un umbral más alto significa mayor precisión y menor tasa de reconocimiento falso.</p> <p></p> <p>Cuando el umbral es demasiado bajo, como 0, la tasa de reconocimiento falso será extremadamente alta. Tenga en cuenta lo siguiente.</p>



Nombre	Descripción
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 el mismo rostro permanece frente a la lente después del primer reconocimiento exitoso, el dispositivo realizará nuevamente el reconocimiento del rostro después de un intervalo definido.
Intervalo de rostro no válido (seg.)	Cuando el mismo rostro permanece frente a la lente después del primer reconocimiento fallido, el dispositivo realizará nuevamente el reconocimiento del rostro después de un intervalo definido.
Distancia de reconocimiento	La distancia entre la cara y la lente.
Iluminación de pantalla inteligente	Cuando está habilitado, en el estado de pantalla apagada, la pantalla se iluminará cuando se detecte una cara.

**Paso 4** Configurar los parámetros de exposición.

Figura 3-11 Parámetros de exposición

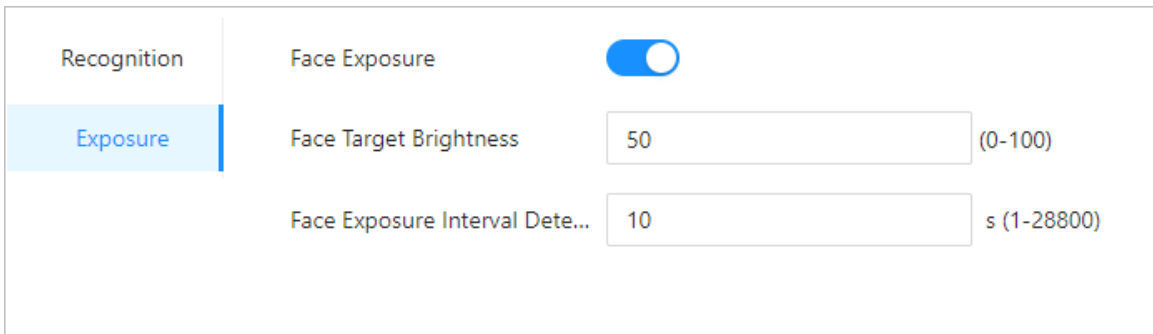


Tabla 3-9 Descripción de los parámetros de exposición

Parámetro	Descripción
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.
Brillo del objetivo de la cara	
Detección del intervalo de exposición del rostro	El rostro se expondrá solo una vez en un intervalo definido.

**Paso 5** Hacer clic **Aplicar**.

#### Operaciones relacionadas

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

Se detectará la cara en el área definida.

- 3. Haga clic **Aplicar**.
- Dibuja 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 dispositivo podrá detectar la cara.

3. Haga clic **Aplicar**.

### 3.5.6 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 Seleccione **Control de acceso** > **Configuración de la**
- Paso 3 **tarjeta**. Configure los parámetros de la tarjeta.

Figura 3-12 Parámetros de la tarjeta

### Card Settings

IC Card

IC Card Encryption & Verification

Block NFC Cards

Enable DESFire Card

DESFire Card Decryption

Apply Refresh Default

### Card No. System

After the number system is changed, the card numbers will become invalid.

Card No. System  Hexadecimal  Decimal

Apply Refresh Default


### DESFire Card Write






Please place the card on the swiping area and enable DESFire card and DESFire Card Decryption.

Card Number

Write

Tabla 3-10 Descripción de los parámetros de la tarjeta

Artículo	Parámetro	Descripción
Configuración de la tarjeta	Tarjeta IC	<p>La tarjeta IC se puede leer cuando esta función está habilitada.</p> <p></p> <p>Esta función solo está disponible en modelos seleccionados.</p>

Artículo	Parámetro	Descripción
	Cifrado y verificación de tarjetas IC	<p>La tarjeta cifrada se puede leer cuando esta función está habilitada.</p>  <p>Cerciorarse <b>Tarjeta IC</b> está habilitado.</p>
	Bloquear tarjetas NFC	<p>Evitar el desbloqueo mediante tarjeta NFC duplicada después de habilitar esta función.</p>  <ul style="list-style-type: none"> <li>● Esta función sólo está disponible en modelos que admiten tarjetas IC.</li> <li>● Cerciorarse <b>Tarjeta IC</b> está habilitado.</li> <li>● La función NFC solo está disponible en algunos modelos de teléfonos.</li> </ul>
	Habilitar tarjeta Desfire	<p>El dispositivo puede leer el número de tarjeta de la tarjeta Desfire cuando esta función está habilitada.</p>  <ul style="list-style-type: none"> <li>● Esta función sólo está disponible en modelos que admiten tarjetas IC.</li> <li>● Sólo admite formato hexadecimal.</li> </ul>
	Descifrado de la tarjeta Desfire	<p>La información de la tarjeta Desfire se puede leer cuando <b>Habilitar tarjeta Desfire</b> y <b>Descifrado de la tarjeta Desfire</b> se habilitan al mismo tiempo.</p>  <ul style="list-style-type: none"> <li>● Esta función sólo está disponible en modelos que admiten tarjetas IC.</li> <li>● Asegúrese de que la tarjeta Desfire esté habilitada.</li> </ul>
Sistema de Nro. de Tarjeta	Sistema de Nro. de Tarjeta	<p>Seleccione el formato decimal o hexadecimal para el número de tarjeta cuando esté conectado el lector de tarjetas Wiegand. El sistema de número de tarjeta es el mismo tanto para la entrada como para la salida del número de tarjeta.</p>
Escritura de tarjeta DESFire	Número de tarjeta	<p>Coloque la tarjeta en el lector, ingrese el número de tarjeta y luego haga clic <b>Escribir</b> para escribir el número de tarjeta en la tarjeta.</p>  <ul style="list-style-type: none"> <li>● La función de tarjeta Desfire debe estar habilitada.</li> <li>● Sólo admite formato hexadecimal.</li> <li>● Admite hasta 8 caracteres.</li> </ul>

**Paso 4** Hacer clic **Aplicar**.

## 3.5.7 Configuración de horarios

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

### 3.5.7.1 Configuración de períodos de tiempo

Puede configurar hasta 128 períodos (del n.º 0 al n.º 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** Seleccione **Control de acceso > Configuración del período > Período** Haga clic
- Paso 3** en **Agregar**.

Figura 3-13 Configurar períodos de tiempo

The screenshot shows a web interface for adding a time period. At the top, there's a title bar 'Add' with a close button 'X'. Below it, there are two input fields: 'No.' with the value '2' and 'Period Name' with the value 'period XX'. The main area is a 'Time Plan' table. The table has columns for days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat) and hours (0, 1, 2, 3, 4, 5, 6, 7, 8, 9). A time selection pop-up is open over the table, showing 'Time' from '00:00:00' to '23:59:59' with 'OK' and 'Delete' buttons. The table cells are filled with blue bars, and each row has a 'Copy' button. At the bottom right, there are 'OK' and 'Cancel' buttons.

- 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**.

### 3.5.7.2 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 durante el tiempo definido en el plan de vacaciones.

#### Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccione **Control de acceso>Configuración del período>Plan de vacaciones**
- Paso 3** Haga clic en **Gestión de vacaciones**, y luego haga clic **Agregar**.
- Paso 4** Seleccione un número para el grupo de vacaciones y luego ingrese un nombre para el grupo.

Figura 3-14 Agregar un grupo de vacaciones

No.	Holiday Name	Start Time	End Time	Operation
1	National Day	2023-10-01	2023-10-07	

**Paso 5** Hacer clic **Agregary** luego agregue un día festivo a un grupo de días festivos. Haga clic en

**Paso 6** **DE ACUERDO.**

Figura 3-15 Agregar un día festivo a un grupo de días festivos

Holiday Name	National Day
* Period	2023-10-01 → 2023-10-07

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

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

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

Admite agregar hasta 4 secciones de tiempo en un día.

Figura 3-16 Agregar plan de vacaciones

**Edit**

No. 0

Holiday Plan Name Holiday plan for 2023

Holiday Group No. 1

Time Plan

Time 08:30:00 - 23:59:59

OK Delete

0 1 2 3 4 5 6 7 8 24

Holid Copy

OK Cancel

Paso 10 Hacer clic **DE ACUERDO**.

### 3.5.8 Configuración de privacidad

#### Procedimiento

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

Paso 2 la función de instantánea.

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

Figura 3-17 Habilitar instantánea

Snapshot

Apply Refresh Default

Paso 3 Hacer clic **Aplicar**.

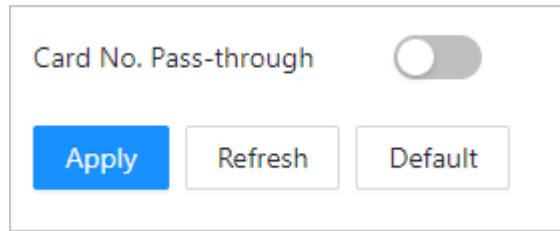
### 3.5.9 Configuración de la comparación de back-end

Pasar directamente datos como el número de tarjeta a la plataforma de terceros para la validación de datos en lugar de validar los datos en el dispositivo.

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

Una vez habilitada la función, el número de tarjeta pasa a la plataforma de terceros para la validación de datos.

Figura 3-18 Comparación del back-end




## 3.6 Configuración de asistencia

Esta función solo está disponible en modelos seleccionados.

### 3.6.1 Configuración de departamentos

Procedimiento

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

**Paso 2** Haga clic  para cambiar el nombre del departamento.

Hay 20 departamentos predeterminados. Te recomendamos cambiarles el nombre.

Figura 3-19 Crear departamentos

The screenshot shows a table with a 'Default' tab selected. The table has three columns: 'ID', 'Department Name', and 'Operation'. There are 10 rows of data, each representing a department. The 'ID' column contains numbers from 1 to 10. The 'Department Name' column contains blurred text. The 'Operation' column contains a pencil icon for each row, indicating that the department name can be edited.

ID	Department Name	Operation
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Operaciones relacionadas

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

### 3.6.2 Configuración de turnos

Configurar turnos para definir reglas de asistencia. Los empleados deben 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 **Configuración de asistencia > Configuración de**


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



Figura 3-20 Crear turnos

**Edit Shift**
✕

---

\* Shift No.

\* Shift Name

\* Period 1  →  🕒

\* Period 2  →  🕒

\* Overtime Period  →  🕒

\* Limit for Arriving Late  min (0-99)

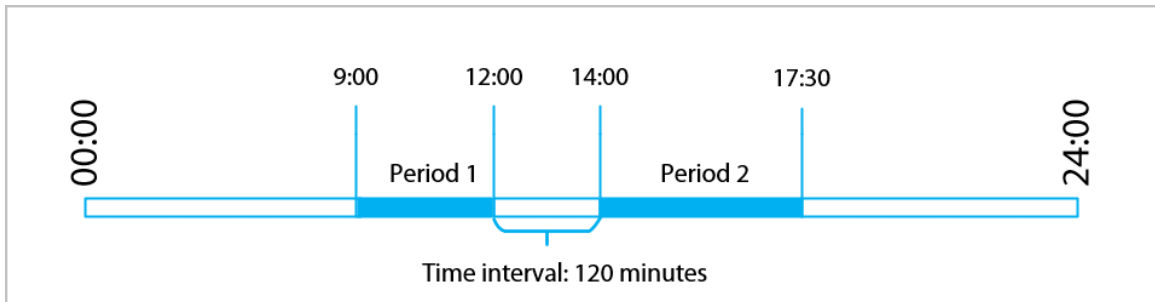
\* Limit for Leaving Early  min (0-99)

Tabla 3-11 Descripción de los parámetros de cambio

Parámetro	Descripción
Nombre del turno	Introduzca el nombre del turno.
Periodo 1	<p>Especifique un rango de tiempo en el que las personas pueden registrar su entrada y salida durante la jornada laboral.</p> <p>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.</p> <p>Si establece 2 períodos de asistencia, estos no pueden superponerse. Los empleados deben registrar su entrada y salida en ambos períodos.</p>
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 de trabajo normales.
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 3-21 Intervalo de tiempo (número par)



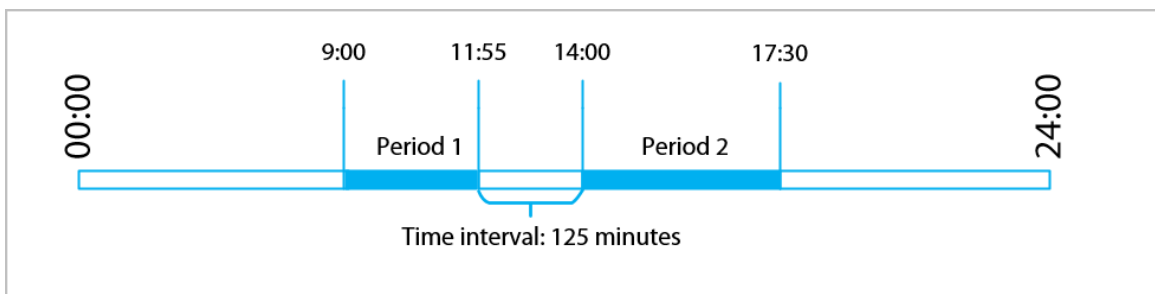
Por ejemplo: si el intervalo es de 120 minutos, entonces la hora de salida para el período 1 es de 12:00 a 12:59, y la hora de entrada para el período 2 es de 13:00 a 14:00.



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

- 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 3-22 Intervalo de tiempo (número impar)



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, será válida la hora más reciente, y si registra su entrada varias veces durante el período 2, será válida la hora más temprana.



Todos los horarios de asistencia son precisos hasta el segundo. Por ejemplo, si la hora de entrada normal está establecida a las 8:05 a. m., el empleado que ingrese a las 8:05:59 a. m. no se considerará que llegó tarde. Sin embargo, el empleado que llegue a las 8:06 a. m. se marcará como que llegó tarde por 1 minuto.

### Paso 3

Hacer clic **DE ACUERDO**.

### Operaciones relacionadas

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

### 3.6.3 Configuración 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 **Configuración de asistencia**>**Configuración de cambio**>**Día festivo**
- Paso 2** Haga clic en **Agregar** Para agregar planes de vacaciones, configure los parámetros.
- Paso 3**

Figura 3-23 Crear planes de vacaciones

The screenshot shows a dialog box titled "Add Attendance Holiday" with a close button (X) in the top right corner. It contains three main input fields, each with a red asterisk indicating it is required:

- \* Attendance Holiday ...**: A dropdown menu with the value "1" selected.
- \* Attendance Holiday**: A text input field containing "Attendance Holiday for October".
- \* Time**: A date range input field showing "2023-10-01" to "2023-10-07" with a calendar icon on the right.

At the bottom right, there are two buttons: a blue "OK" button and a white "Cancel" button with a grey border.

Tabla 3-12 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** Hacer clic **DE ACUERDO**.

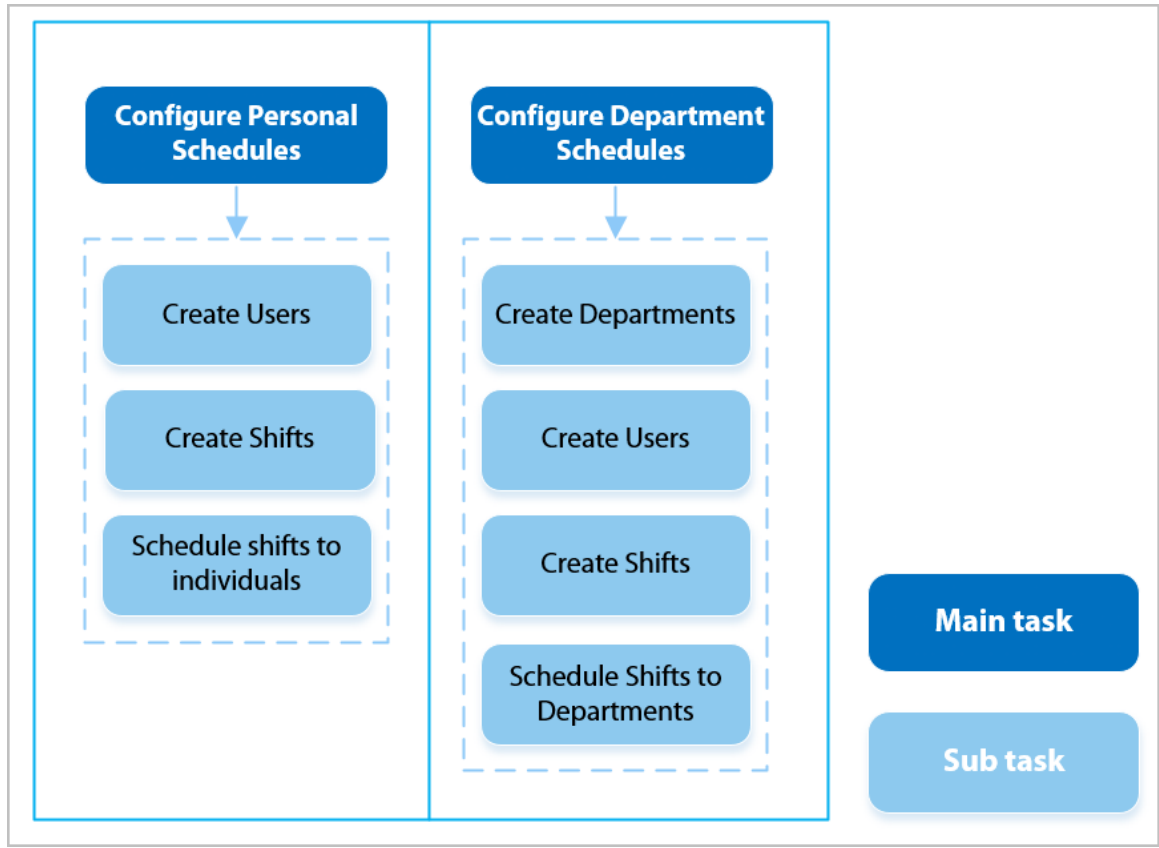
### 3.6.4 Configuración de horarios de trabajo

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 3-24 Configuración de horarios de trabajo



#### Procedimiento

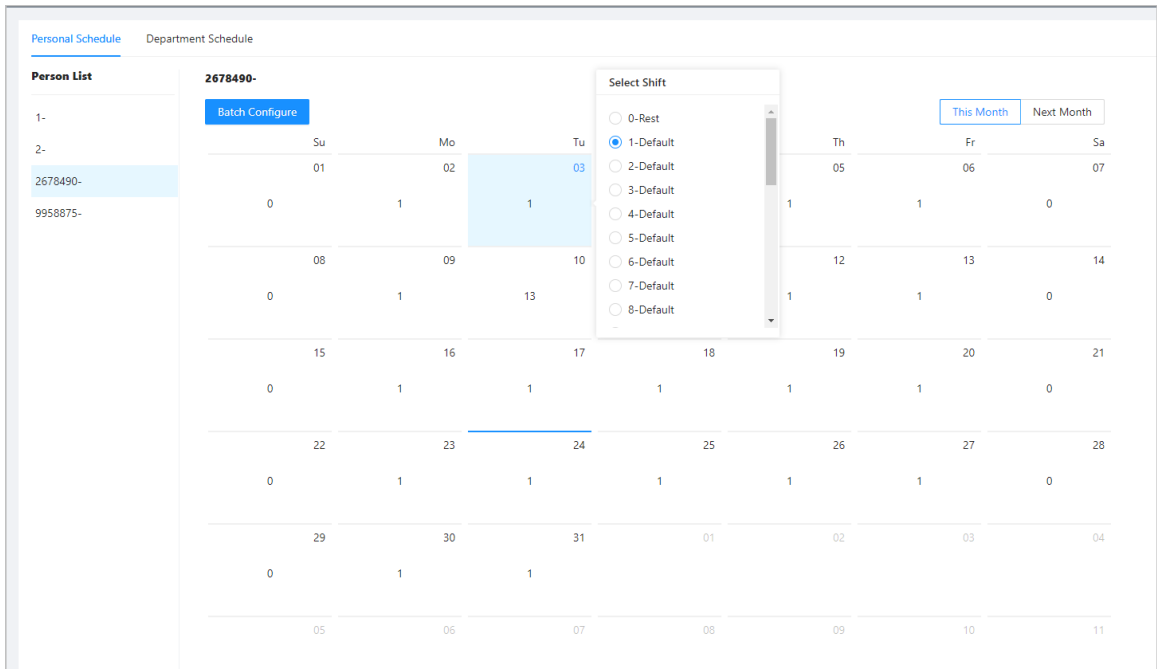
**Paso 1** Seleccionar **Configuración de asistencia > Configuración de programación**.

**Paso 2** Establecer horarios de trabajo para personas individuales.

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

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

Figura 3-25 Agenda personal



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

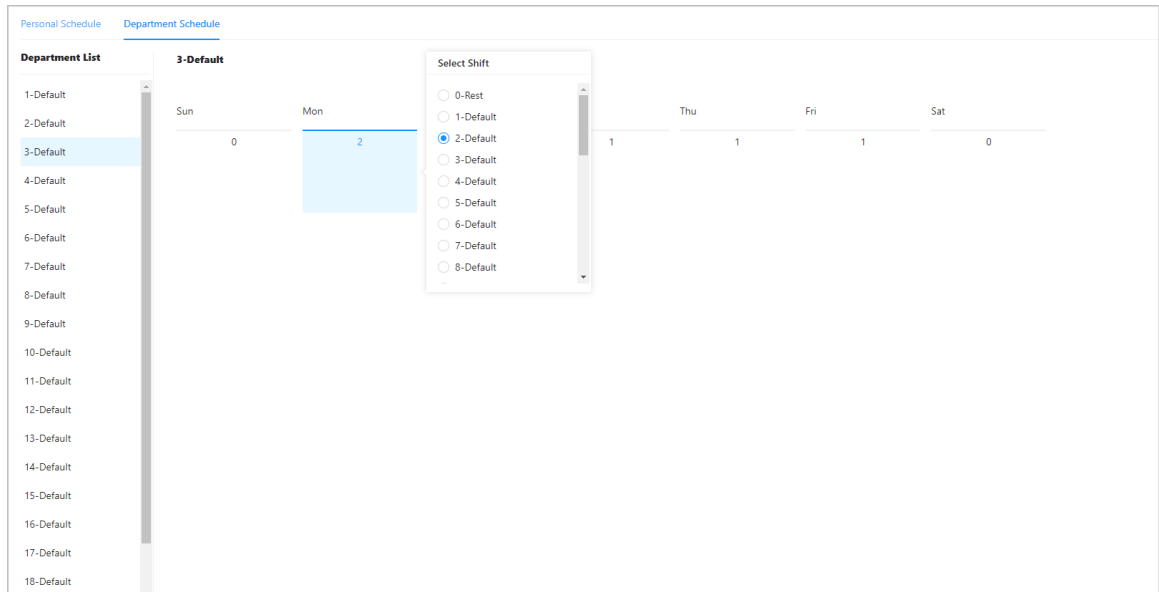
- 0 indica ruptura.
- 1 a 24 indica el número de turnos predefinidos.
- 25 indica viaje de negocios.
- 26 indica licencia de ausencia.

### Paso 3

Establecer horarios de trabajo para los departamentos.

1. Haga clic **Horario del Departamento**.
2. Seleccione un departamento en la lista de departamentos.
3. En el calendario, seleccione un día y luego seleccione un turno.
  - 0 indica descanso.
  - 1 a 24 indica el número de turnos predefinidos.
  - 25 indica viaje de negocios.
  - 26 indica licencia de ausencia.

Figura 3-26 Programar turnos para un departamento



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

### 3.6.5 Configuración de modos de asistencia

#### Procedimiento

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

**Paso 2** Introduzca el intervalo de verificación.

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

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

**Paso 4** Configure los modos de asistencia.

Figura 3-27 Modos de asistencia

Local or Remote

Mode Settings  Auto/Manual Mode  Auto Mode  Manual Mode  Fixed Mode

Check In 06:00 → 09:59 ⌚

Break Out 10:00 → 12:59 ⌚

Break In 13:00 → 15:59 ⌚

Check Out 16:00 → 20:59 ⌚

Overtime Check In 00:00 → 00:00 ⌚

Overtime Check Out 00:00 → 00:00 ⌚

**Apply** Refresh Default

Tabla 3-13 Modo de asistencia

Parámetro	Descripción
Modo automático/manual	<p>La pantalla muestra el estado de asistencia automáticamente después de registrar su entrada o salida, pero también puede cambiar manualmente su estado de asistencia.</p> <ul style="list-style-type: none"> <li>● Registra tu entrada: registra tu entrada cuando comienza tu jornada laboral normal.</li> <li>● Break Out: Marca tu salida cuando comienza tu descanso.</li> <li>● Break In: Registre su entrada cuando finalice su descanso.</li> <li>● Salida: Marque su salida cuando comience su jornada laboral normal.</li> <li>● Registro de horas extras: Registre su entrada cuando comience su período de horas extras.</li> <li>● Registro de salida de horas extra: Registre su salida cuando finalice su período de horas extra.</li> </ul>
Modo automático	<p>La pantalla muestra su estado de asistencia automáticamente después de registrar su entrada o salida.</p> <ul style="list-style-type: none"> <li>● Registra tu entrada: registra tu entrada cuando comienza tu jornada laboral normal.</li> <li>● Break Out: Marca tu salida cuando comienza tu descanso.</li> <li>● Break In: Registre su entrada cuando finalice su descanso.</li> <li>● Salida: Marque su salida cuando comience su jornada laboral normal.</li> <li>● Registro de horas extras: Registre su entrada cuando comience su período de horas extras.</li> <li>● Registro de salida de horas extra: Registre su salida cuando finalice su período de horas extra.</li> </ul>
Modo manual	<p>Seleccione manualmente su estado de asistencia al registrar su entrada o salida.</p>
Modo fijo	<p>Al registrar su entrada o salida, la pantalla mostrará el estado de asistencia definido previamente en todo momento.</p>

**Paso 5** Hacer clic **Aplicar**.

Operaciones relacionadas

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

## 3.7 Configuración de audio y vídeo

### 3.7.1 Configuración de vídeo

Inicie sesión en la página web, seleccione **Configuración de audio y vídeo > Vídeo**

- Predeterminado: restaurar la configuración predeterminada.
- Capturar: toma una instantánea de la imagen actual.

Tasa de bits

Figura 3-28 Tasa de bits

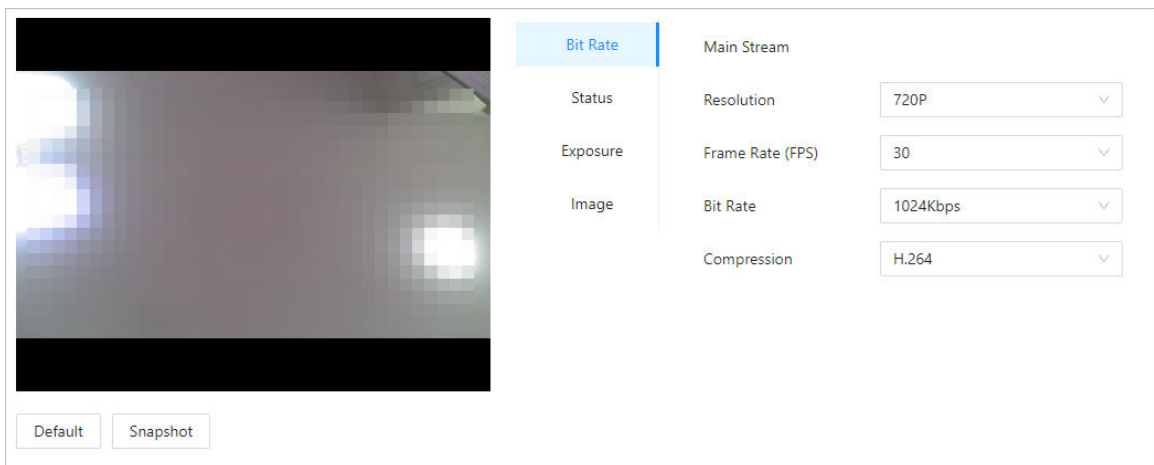



Tabla 3-14 Descripción de los parámetros de velocidad de bits

Parámetro	Descripción
Resolución	 <p>Cuando el dispositivo funciona como un VTO y se conecta al VTH, el límite de transmisión adquirida de VTH es 720p. Cuando la resolución se cambia a 1080p, la función de llamada y monitoreo podría verse afectada.</p>
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.
Compresión	Estándar de compresión de vídeo para ofrecer una buena calidad de vídeo a velocidades de bits más bajas.



## Estado

Figura 3-29 Estado

The screenshot shows a configuration interface for a camera. On the left, there is a vertical menu with four items: 'Bit Rate', 'Status' (highlighted in blue), 'Exposure', and 'Image'. The main content area displays several settings:

- Scene Mode:** A dropdown menu set to 'Auto'.
- Day/Night:** A dropdown menu set to 'Color'.
- Compensation Mode:** A dropdown menu set to 'WDR'.
- Slider:** A horizontal slider with a blue circle in the middle, labeled with a minus sign on the left and a plus sign followed by '30' on the right.
- Video Standard:** A dropdown menu set to 'NTSC'.

Tabla 3-15 Descripción de parámetros de estado

Parámetro	Descripción
Modo de escena	<p>El tono de la imagen es diferente en distintos modos de escena.</p> <ul style="list-style-type: none"> <li>● <b>Cerca:</b>La función de modo de escena está desactivada.</li> <li>● <b>Auto:</b>El sistema ajusta automáticamente el modo de escena en función de la sensibilidad fotográfica.</li> <li>● <b>Soleado:</b>En este modo, se reducirá el tono de la imagen.</li> <li>● <b>Noche:</b>En este modo, se incrementará el tono de la imagen.</li> </ul>
Día/Noche	<p>El modo Día/Noche afecta la compensación de luz en diferentes situaciones.</p> <ul style="list-style-type: none"> <li>● <b>Auto:</b>El sistema ajusta automáticamente el modo día/noche en función de la sensibilidad fotográfica.</li> <li>● <b>Vistoso:</b>En este modo, las imágenes son coloridas.</li> <li>● <b>En blanco y negro:</b>En este modo, las imágenes son en blanco y negro.</li> </ul>
Modo de compensación	<ul style="list-style-type: none"> <li>● <b>Desactivar:</b>La compensación está desactivada.</li> <li>● <b>BLC:</b>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.</li> <li>● <b>Amplio rango dinámico (WDR):</b>El sistema atenúa las áreas brillantes y compensa las áreas oscuras para crear un equilibrio que mejore la calidad general de la imagen.</li> <li>● <b>HLCC (Centro de Información de Conducta Humana):</b>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.</li> </ul>
Estándar de vídeo	Selección de CAMARADAY Sistema de clasificación de números arábigos (NTSC).

## Exposición


Figura 3-30 Exposición

The screenshot shows the 'Exposure' settings interface. On the left, a sidebar contains 'Bit Rate', 'Status', 'Exposure' (highlighted), and 'Image'. The main area lists the following settings:

- Anti-flicker:** Outdoor (dropdown)
- Exposure Mode:** Manual (dropdown)
- Shutter:** Custom Range (dropdown)
- Shutter Range:** 0 - 20 (0-40)ms
- Gain:** 0 - 80 (0-100)
- Exposure Compensation:** Slider from - to + 50, currently at 0.
- 3D NR:** Toggled ON.
- NR Level:** Slider from - to + 50, currently at 0.

Tabla 3-16 Descripción de los parámetros de exposición

Parámetro	Descripción
Anti-parpadeo	<p>Configure el antiparpadeo para reducir el parpadeo y disminuir o reducir los colores desiguales o la exposición.</p> <ul style="list-style-type: none"> <li>● <b>50 Hz:</b>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.</li> <li>● <b>60 Hz:</b>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.</li> <li>● <b>Exterior:</b>Cuando <b>Exterior</b> Se selecciona, se puede cambiar el modo de exposición.</li> </ul>

Parámetro	Descripción
Modo de exposición	<p>Puede configurar la exposición para ajustar el brillo de la imagen.</p> <ul style="list-style-type: none"> <li>● <b>Auto:</b>El dispositivo ajusta automáticamente el brillo de las imágenes según el entorno.</li> <li>● <b>Prioridad de obturador:</b>El dispositivo 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 dispositivo ajustará automáticamente el valor de ganancia para obtener el nivel de brillo ideal.</li> <li>● <b>Manual:</b>Puede ajustar manualmente la ganancia y el valor del obturador para ajustar el brillo de la imagen.</li> </ul> <p></p> <ul style="list-style-type: none"> <li>◇ Cuando seleccionas <b>Exterior</b> desde <b>Anti-parpadeo</b> lista, puedes seleccionar <b>Prioridad de obturador</b> como el modo de exposición.</li> <li>◇ El modo de exposición puede variar según los modelos del dispositivo.</li> </ul>
Obturador	<p>El obturador es un componente que permite el paso de la luz durante un período determinado. Cuanto mayor sea la velocidad de obturación, menor será el tiempo de exposición y más oscura será la imagen. Puedes seleccionar un rango de obturación o añadir un rango personalizado.</p>
Ganar	<p>Cuando se establece el rango de valores de ganancia, se mejorará la calidad del video.</p>
Exposición Compensación	<p>El vídeo será más brillante al ajustar el valor de compensación de exposición.</p>
Reducción de ruido 3D	<p>Cuando la Reducción de ruido 3D (RD) está activada, se puede reducir el ruido del video para garantizar una mayor definición de los videos.</p>
Nivel NR	<p>Puede configurar su grado cuando esta función está activada. Un grado más alto significa una imagen más clara.</p>

## Imagen

Figura 3-31 Imagen

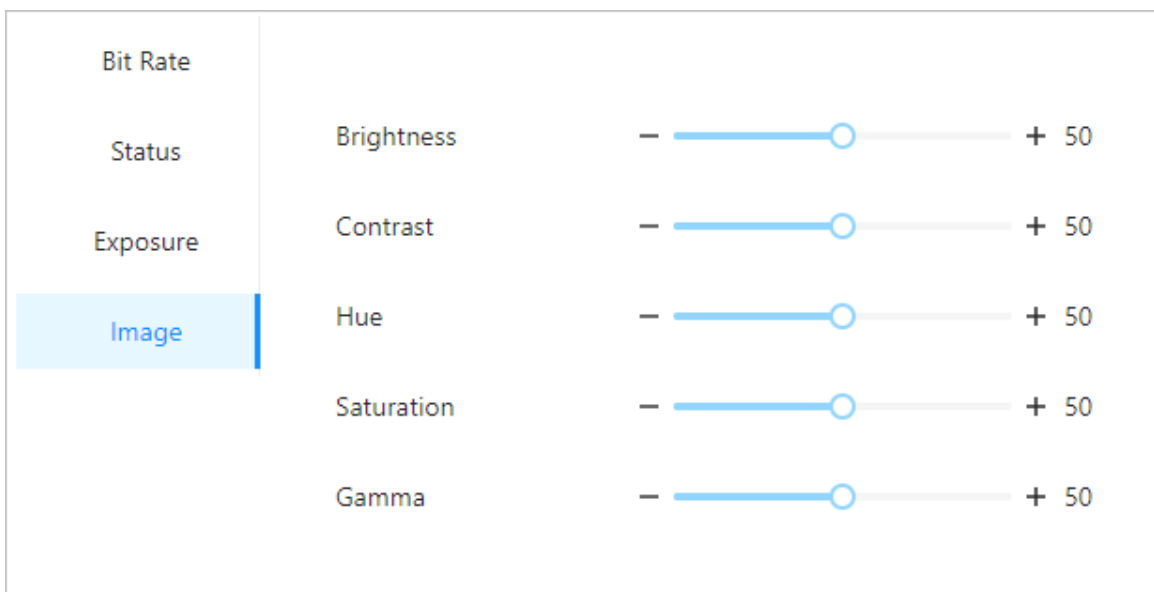



Tabla 3-17 Descripción de la imagen

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	<p>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.</p>  <p>El valor de saturación no cambia el brillo de la imagen.</p>
Gama	Cambia el brillo y el contraste de la imagen de forma no lineal. Cuanto mayor sea el valor, más brillante será la imagen.

### 3.7.2 Configuración de audio

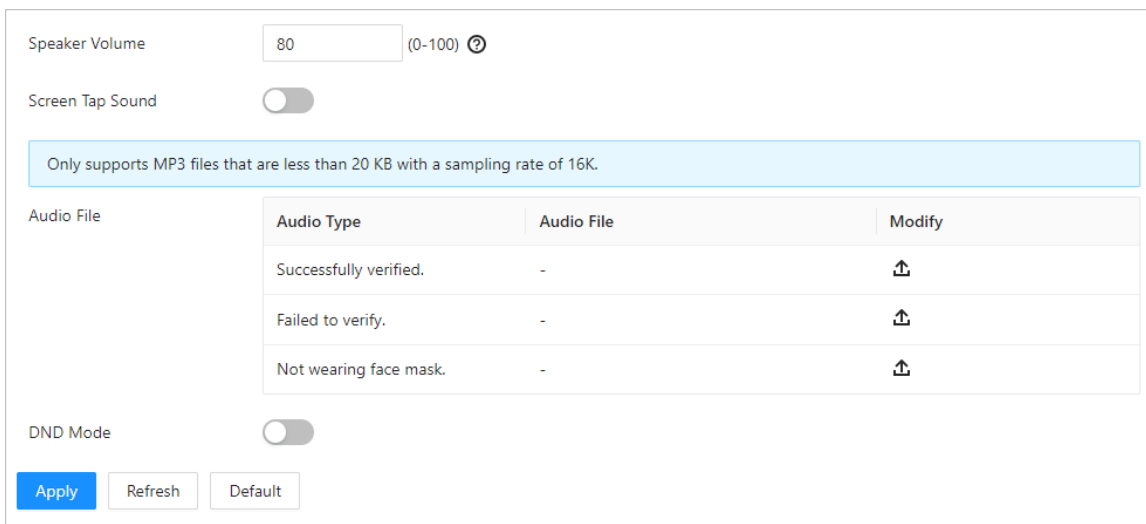
Configure el volumen del altavoz y las indicaciones de audio durante la verificación de identidad.

#### Procedimiento

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

**Paso 2** Configure los parámetros de audio.

Figura 3-32 Configurar parámetros de audio



Speaker Volume: 80 (0-100) ⓘ

Screen Tap Sound:

Only supports MP3 files that are less than 20 KB with a sampling rate of 16K.

Audio File	Audio Type	Audio File	Modify
Successfully verified.	-	-	⬆️
Failed to verify.	-	-	⬆️
Not wearing face mask.	-	-	⬆️



DND Mode:

Apply Refresh Default

Tabla 3-18 Descripción de parámetros

Parámetros	Descripción
Volumen del altavoz	Configurar el volumen del altavoz.
Sonido al tocar la pantalla	Cuando esta función está habilitada, el dispositivo producirá sonido al presionar el botón.

Parámetros	Descripción
Archivo de audio	Haga clic en Subir archivos de audio a la plataforma.
Modo DND	No se escucharán mensajes de voz durante el tiempo establecido cuando verifique su identidad en el dispositivo. Puede configurar hasta 4 períodos.

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



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

**Paso 4** Hacer clic **Aplicar**.

## 3.8 Configuración de comunicación

### 3.8.1 Configuración de red

#### 3.8.1.1 Configuración de TCP/IP

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

Procedimiento

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


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

Figura 3-33 TCP/IP

The image shows a network configuration window for TCP/IP. The 'NIC' is set to 'NIC 1'. The 'Mode' is set to 'Static' (selected with a radio button). The 'MAC Address' field is empty. The 'IP Version' is set to 'IPv4'. The 'IP Address', 'Subnet Mask', 'Default Gateway', 'Preferred DNS', and 'Alternate DNS' fields are all empty. The 'MTU' is set to '1500'. At the bottom, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Tabla 3-19 Descripción de TCP/IP

Parámetro	Descripción
Modo	<ul style="list-style-type: none"> <li>● Estático: ingrese manualmente la dirección IP, la máscara de subred y la puerta de enlace.</li> <li>● DHCP: Significa Protocolo de configuración dinámica de host. Cuando se activa el DHCP, se le asignará automáticamente al dispositivo una dirección IP, una máscara de subred y una puerta de enlace.</li> </ul>
Dirección MAC	Dirección MAC del dispositivo.
Versión IP	IPv4 o IPv6.

Parámetro	Descripción
Dirección IP	Si configura el modo en <b>Estático</b> , configure la dirección IP, la máscara de subred y la puerta de enlace.
Máscara de subred	
Puerta de enlace predeterminada	 <ul style="list-style-type: none"> <li>● La dirección IPv6 se representa en hexadecimal.</li> <li>● La versión IPv6 no requiere configurar máscaras de subred.</li> <li>● La dirección IP y la puerta de enlace predeterminada deben estar en el mismo segmento de red.</li> </ul>
DNS preferido	Establezca la dirección IP del servidor DNS preferido.
DNS alternativo	Establecer la dirección IP del servidor DNS alternativo.
Unidad de medida máxima	<p>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:</p> <ul style="list-style-type: none"> <li>● 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.</li> <li>● 1492: Valor óptimo para PPPoE</li> <li>● 1468: Valor óptimo para DHCP.</li> <li>● 1450: Valor óptimo para VPN.</li> </ul>

**Paso 3** Hacer clic DE ACUERDO.

### 3.8.1.2 Configuración de Wi-Fi



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

#### Procedimiento

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

**Paso 2** Encienda el Wi-Fi.

Se muestran todas las conexiones WiFi disponibles.

Figura 3-34 Wi-Fi

Name	Signal Strength	Status	Connect
No Data			



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

**Paso 3** Hacer clic **+** y luego ingrese la contraseña del Wi-Fi.

El wifi está conectado.

#### Operaciones relacionadas

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

#### 3.8.1.3 Configuración del punto de acceso Wi-Fi



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

#### Procedimiento

**Paso 1** Seleccionar **Configuración de comunicación > Configuración de red > Punto de acceso**

**Paso 2** **wifi** Habilite la función y luego haga clic en **Aplicar**.



Figura 3-35 Punto de acceso Wi-Fi


Enable

SSID

Security  ▼

Password

IP Address



#### Resultados

Una vez habilitado, podrá conectarse al Wi-Fi del dispositivo a través de su teléfono e iniciar sesión en la página web del dispositivo en su teléfono.

#### 3.8.1.4 Configuración del puerto

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

#### Procedimiento

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

Paso 2 Configurar los puertos.

Figura 3-36 Configurar puertos

Max Connection	<input type="text" value="1000"/>	(1-1000)
TCP Port	<input type="text" value="37777"/>	(1025-65534)
HTTP Port	<input type="text" value="80"/>	
HTTPS Port	<input type="text" value="443"/>	
RTSP Port	<input type="text" value="554"/>	
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>		



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

Tabla 3-20 Descripción de los puertos

Parámetro	Descripción
Conexión máxima	Puede establecer el número máximo de clientes (como página web, cliente de escritorio y cliente móvil) que pueden acceder al dispositivo al mismo tiempo.
Puerto TCP	El valor predeterminado es 37777.
Puerto HTTP	El valor predeterminado es 80. Si ha cambiado el número de puerto, 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**.

### 3.8.1.5 Configuración del servicio básico

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

Procedimiento


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

**Paso 2** Configurar el servicio básico.

Figura 3-37 Servicio básico

Tabla 3-21 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 multicast/transmisión	Busque dispositivos a través del protocolo de multidifusión o difusión.
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 (Foro de interfaz de vídeo en red abierta). Su objetivo es proporcionar un estándar para la interfaz entre diferentes dispositivos de seguridad basados en IP. Estas especificaciones estandarizadas de ONVIF son como un lenguaje común que todos los dispositivos pueden usar para comunicarse.
Mantenimiento de emergencia	Está activado de forma predeterminada.
Modo de autenticación de protocolo privado	<p>Establezca el modo de autenticación, incluido el modo seguro y el modo de compatibilidad. Se recomienda elegir <b>Modo de seguridad</b>.</p> <ul style="list-style-type: none"> <li>● 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.</li> <li>● Modo compatible: admite el acceso al dispositivo a través de métodos de autenticación Digest, DES y texto simple, con seguridad reducida.</li> </ul>
Protocolo privado	La plataforma agrega dispositivos a través de protocolo privado.

Parámetro	Descripción
Versión 1.1 de TLS	<p>TLSv1.1 hace referencia a Transport Layer Security versión 1.1. TLS es un protocolo criptográfico diseñado para proporcionar una comunicación segura y autenticada a través de una red informática.</p>  <p>Pueden presentarse riesgos de seguridad cuando se habilita TLSv1.1. Tenga en cuenta lo siguiente.</p>
LLDP	<p>LLDP es la abreviatura de Link Layer Discovery Protocol (Protocolo de descubrimiento de capa de enlace), que es un protocolo de capa de enlace de datos. Permite que los dispositivos de red, como conmutadores, enrutadores o servidores, intercambien información sobre sus identidades y capacidades entre sí. El protocolo LLDP ayuda a los administradores de red a comprender mejor la topología de la red y proporciona una forma estandarizada de automatizar el descubrimiento y el mapeo de conexiones entre dispositivos de red. Esto facilita la configuración de la red, la resolución de problemas y la optimización del rendimiento.</p>

**Paso 3** Hacer clic **Aplicar**.

### 3.8.1.6 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.

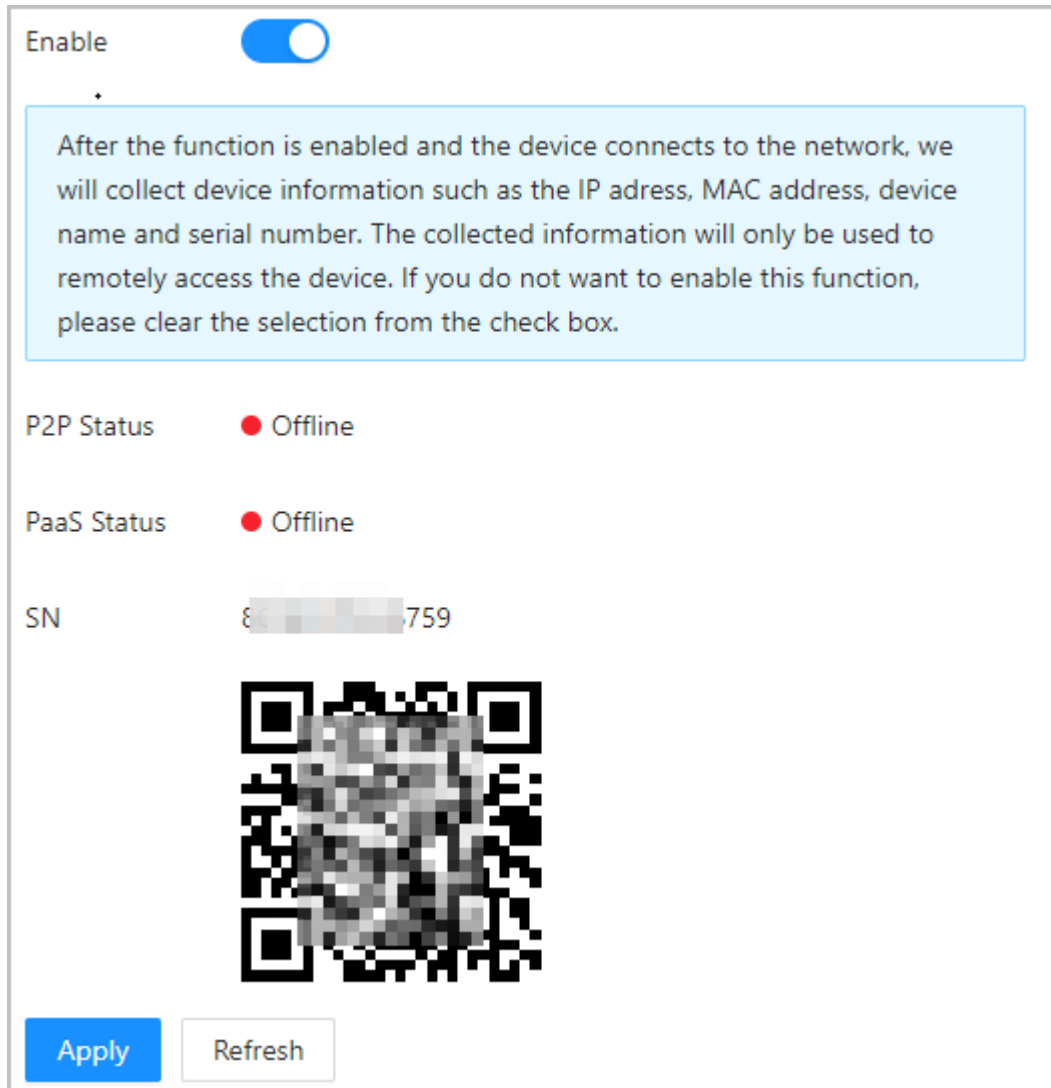
#### Procedimiento

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

**Paso 2** Activar 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 3-38 Servicio en la nube



Paso 3 Hacer clic **Aplicar**.

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

### 3.8.1.7 Configuración del registro automático

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

#### Información de contexto



El registro automático solo es compatible con SDK.

#### Procedimiento

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

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

Figura 3-39 Registro automático

Tabla 3-22 Descripción del registro automático

Parámetro	Descripción
Estado	Muestra el estado de la conexión del registro automático.
Dirección del servidor	La dirección IP o el nombre de dominio del servidor.
Puerto	El puerto del servidor que se utiliza para el registro automático.
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**.

### 3.8.1.8 Configuración del registro automático de CGI

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

#### Información de contexto



Sólo admite IPv4.

#### Procedimiento

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


**Paso 2** Habilite esta función y luego haga clic en  para configurar los parámetros.

Tabla 3-23 Descripción del registro automático

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

**Paso 3** Hacer clic **DE ACUERDO**.

### 3.8.1.9 Configuración de la carga automática

Envía información del usuario y desbloquea registros a través de la plataforma de gestión.

#### Procedimiento

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

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

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

**Paso 3** Habilitar el modo de carga HTTP.

**Paso 4** Hacer clic **Agregar** luego configurar los parámetros.

Figura 3-40 Carga automática

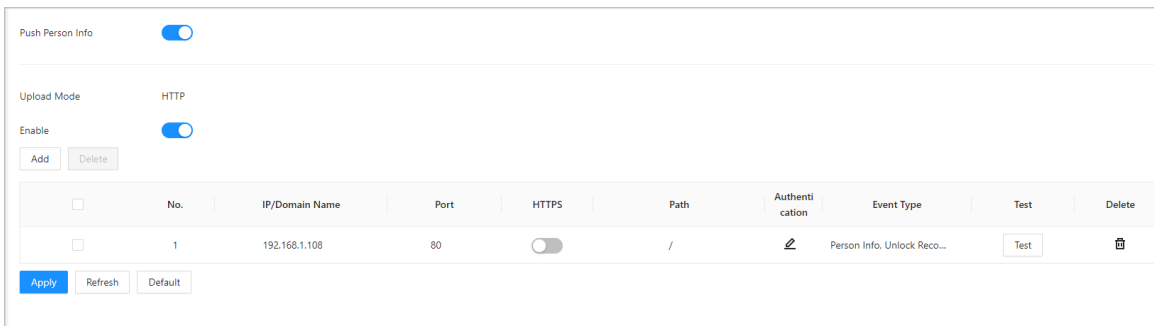



Tabla 3-24 Descripción de parámetros

Parámetro	Descripción
Nombre de dominio/IP	La IP o nombre de dominio de la plataforma de gestión.
Puerto	El puerto de la plataforma de gestión.
HTTPS	Acceda a la plataforma de gestión a través de HTTPS. HTTPS protege la comunicación a través de una red informática.
Autenticación	Habilite la autenticación de la cuenta cuando acceda a la plataforma de administración. Se requiere el nombre de usuario y la contraseña para iniciar sesión.

Parámetro	Descripción
Tipo de evento	<p>Seleccione el tipo de evento que se enviará a la plataforma de administración.</p> <p></p> <ul style="list-style-type: none"> <li>• Antes de utilizar esta función, habilite <b>Introducir información de la persona</b>.</li> <li>• La información personal solo se puede enviar a una plataforma de administración y los registros de desbloqueo se pueden enviar a múltiples plataformas de administración.</li> </ul>

**Paso 5** Hacer clic **Aplicar**.

### 3.8.2 Configuración de RS-485

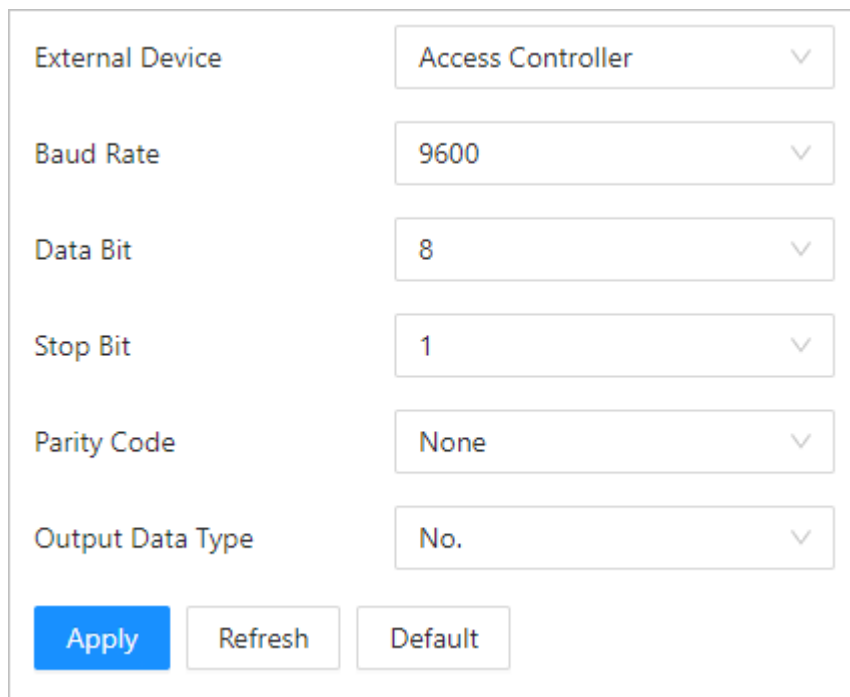
Configure los parámetros RS-485 si conecta un dispositivo externo al puerto RS-485.

Procedimiento

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

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

Figura 3-41 Configurar parámetros



External Device	Access Controller
Baud Rate	9600
Data Bit	8
Stop Bit	1
Parity Code	None
Output Data Type	No.



Tabla 3-25 Descripción de los parámetros RS-485

Parámetro	Descripción
Dispositivo externo	<ul style="list-style-type: none"> <li>● Controlador de acceso Seleccionar <b>Controlador de acceso</b> cuando el dispositivo funciona como un lector de tarjetas y envía datos a otros controladores de acceso externos para controlar el acceso.</li> <li>● Lector de tarjetas: el dispositivo funciona como un controlador de acceso y se conecta a un lector de tarjetas externo.</li> <li>● Lector (OSDP): El dispositivo está conectado a un lector de tarjetas basado en el protocolo OSDP.</li> <li>● 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.</li> </ul>
Tasa de Baud	Seleccione la velocidad en baudios. La predeterminada es 9600.
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.
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.
Tipo de datos de salida	<p>Cuando configura el dispositivo externo como <b>Controlador de acceso</b>.</p> <ul style="list-style-type: none"> <li>● 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.</li> <li>● No.: Genera datos en función del ID del usuario.</li> </ul>

**Paso 3** Hacer clic **Aplicar**.

### 3.8.3 Configuración de Wiegand

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

Procedimiento

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

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

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



Cuando el dispositivo se conecta a un dispositivo de terceros a través del puerto de entrada Wiegand y el número de tarjeta leído por el dispositivo está en orden inverso al número de tarjeta real, en este caso puede activar **Tarjeta N° Inversión** función.

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

Figura 3-42 Salida Wiegand

Tabla 3-26 Descripción de la salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	<p>Seleccione un formato Wiegand para leer números de tarjetas o números de identificación.</p> <ul style="list-style-type: none"> <li>● <b>Wiegand26</b>: Lee 3 bytes o 6 dígitos.</li> <li>● <b>Wiegand34</b>: Lee 4 bytes u 8 dígitos.</li> <li>● <b>Wiegand66</b>: Lee 8 bytes o 16 dígitos.</li> </ul>
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	<p>Seleccione el tipo de datos de salida.</p> <ul style="list-style-type: none"> <li>● <b>No.:</b> Genera datos en función del ID del usuario. El formato de los datos es hexadecimal o decimal.</li> <li>● <b>Número de tarjeta:</b> Genera datos basados en el primer número de tarjeta del usuario.</li> </ul>

Paso 3 Hacer clic **Aplicar**.

### 3.9 Configuración del sistema

## 3.9.1 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.

### 3.9.1.1 Agregar administradores

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

Procedimiento

**Paso 1** En la página de inicio, seleccione **Sistema > Cuenta** 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 puede tener hasta 31 caracteres y solo admite números, letras, guiones bajos, líneas intermedias, puntos o @.
- La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &).

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

Figura 3-43 Agregar administradores

La imagen muestra una ventana de diálogo titulada "Add" con un botón de cerrar "X" en la esquina superior derecha. Dentro de la ventana, hay cuatro campos de entrada:

- \* Username**: un campo de texto vacío.
- \* Password**: un campo de texto vacío con una barra de progreso de fortaleza debajo.
- \* Confirm Password**: un campo de texto vacío.
- Remarks**: un campo de texto vacío.

En la parte inferior derecha de la ventana, hay dos botones: "OK" (en azul) y "Cancel" (en gris).

**Paso 3** Hacer clic **DE ACUERDO**.



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

### 3.9.1.2 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 clic
- Paso 2** en **Agregary** luego configurar los parámetros.

Figura 3-44 Agregar usuario ONVIF

Tabla 3-27 Descripción del usuario de ONVIF

Parámetro	Descripción
Nombre de usuario	El nombre de usuario no puede ser el mismo que el de la cuenta existente. El nombre de usuario puede tener hasta 31 caracteres y solo admite números, letras, guiones bajos, líneas intermedias, puntos o @.
Contraseña	La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &).

Parámetro	Descripción
Grupo	<p>Hay tres grupos de permisos que representan diferentes niveles de permisos.</p> <ul style="list-style-type: none"> <li>● admin: puede ver y administrar otras cuentas de usuario en el Administrador de dispositivos ONVIF.</li> <li>● Operador: no puede ver ni administrar otras cuentas de usuario en el Administrador de dispositivos ONVIF.</li> <li>● Usuario: no puede ver ni administrar otras cuentas de usuario ni registros del sistema en el Administrador de dispositivos ONVIF.</li> </ul>

**Paso 3** Hacer clic **DE ACUERDO**.

### 3.9.1.3 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 3-45 Restablecer contraseña

**Password Reset**

Enable

If you forgot the password, you can receive security codes through the email address left in advance to reset the password.

Email Address

Password Expires in  Days



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

**Paso 4** Hacer clic **Aplicar**.

### 3.9.1.4 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**.

## 3.9.2 Configuración de la hora


Procedimiento

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

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

Figura 3-46 Configuración de fecha

### Time and Time Zone



Date :  
2023-05-30 Tuesday

Time :  
16:18:35

Time  Manually Set  NTP

System Time

Time Format

Time Zone

### DST

Enable

Type  Date  Week

Start Time

End Time

Tabla 3-28 Descripción de la configuración de tiempo

Parámetro	Descripción
Tiempo	<ul style="list-style-type: none"> <li>● Configuración manual: ingrese la hora manualmente o puede hacer clic <b>Sincronizar tiempo</b> para sincronizar la hora con la computadora.</li> <li>● NTP: El dispositivo sincronizará automáticamente la hora con el servidor NTP. <ul style="list-style-type: none"> <li>◇ <b>Servidor:</b> Introduzca el dominio del servidor NTP.</li> <li>◇ <b>Puerto:</b> Introduzca el puerto del servidor NTP.</li> <li>◇ <b>Intervalo:</b> Introduzca su hora con el intervalo de sincronización.</li> </ul> </li> </ul>
Formato de hora	Seleccione el formato de hora.
Huso horario	Introduzca la zona horaria.
Horario de verano	<ol style="list-style-type: none"> <li>1. (Opcional) Habilite el horario de verano.</li> <li>2. Seleccionar <b>Fecha</b> o <b>Semana</b> desde <b>Tipo</b>.</li> <li>3. Configure la hora de inicio y la hora de finalización del horario de verano.</li> </ol>

Paso 3 Hacer clic **Aplicar**.

## 3.10 Centro de mantenimiento

### 3.10.1 Diagnóstico con un solo clic

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

Procedimiento

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

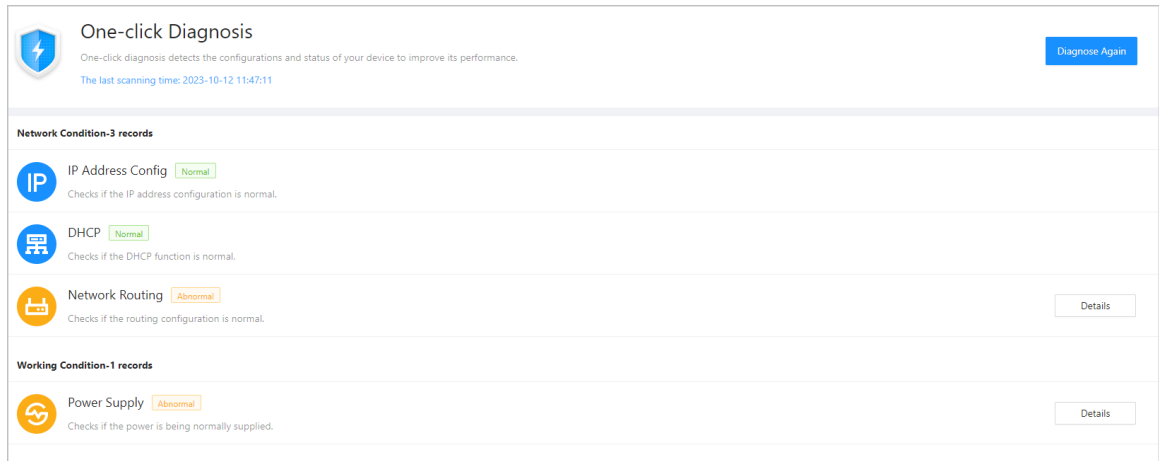
Paso 2 **Diagnosticar**.

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

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

Puede ignorar la anomalía u optimizarla. También puede hacer clic en **Diagnosticar de nuevo** para realizar nuevamente el diagnóstico automático.

Figura 3-47 Diagnóstico con un solo clic



## 3.10.2 Información del sistema

### 3.10.2.1 Visualización de la información de la versión

En la página web, seleccione **Centro de mantenimiento > Información del sistema > Versión**, y podrá ver la información de la versión del dispositivo.

### 3.10.2.2 Visualización de información legal

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

## 3.10.3 Capacidad de datos

Puedes ver cuántos usuarios, tarjetas e imágenes de rostros puede almacenar el dispositivo. Inicia sesión en la página web y selecciona **Capacidad de datos del centro de mantenimiento**.

## 3.10.4 Visualización de registros

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

### 3.10.4.1 Registros del sistema

Ver y buscar registros del sistema.


Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Centro de mantenimiento > 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.

### 3.10.4.2 Desbloquear registros

Busque registros de desbloqueo y expórtelos.

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccione **Centro de mantenimiento > Registro > Desbloquear registros**
- Paso 3** Seleccione el rango de tiempo y el tipo y luego haga clic en **Buscar**.
- Puedes hacer clic **Exportar** para descargar el log.

### 3.10.4.3 Registros de alarmas

Ver registros de alarmas.

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccione **Centro de mantenimiento > Registro > Registros de**
- Paso 3** **alarmas**. Seleccione el tipo y el rango de tiempo.
- Paso 4** Ingrese el ID de administrador y luego haga clic en **Buscar**.

### 3.10.4.4 Registros de administración

Busque registros de administración utilizando el ID de administrador.

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccione **Centro de mantenimiento > Registro > Registros de**
- Paso 3** **administración** Ingrese el ID de administrador y luego haga clic en **Buscar**.
- Hacer clic **Exportar** para exportar registros de administración.

### 3.10.4.5 Gestión USB

Exportar información del usuario desde/hacia USB.

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccione **Centro de mantenimiento > Registro > Gestión USB**.



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

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

## 3.10.5 Gestión del mantenimiento

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

### 3.10.5.1 Exportación e importación de archivos de configuración

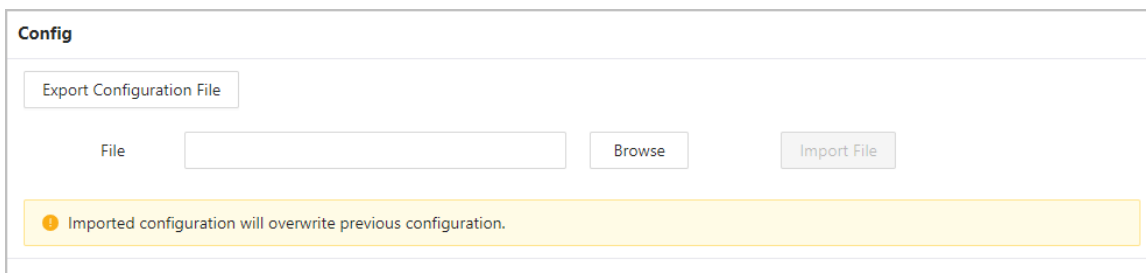
Puede importar y exportar el archivo de configuración del dispositivo. Cuando desee aplicar las mismas configuraciones a varios dispositivos, puede importarles el archivo de configuración.

Procedimiento

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

**Paso 2** Seleccionar **Centro de mantenimiento > Gestión de mantenimiento > Configuración**.

Figura 3-48 Gestión de configuración



The screenshot shows a web interface titled 'Config'. At the top, there is a button labeled 'Export Configuration File'. Below this, there is a 'File' input field, a 'Browse' button, and an 'Import File' button. A yellow warning banner at the bottom of the interface states: 'Imported configuration will overwrite previous configuration.'

**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.

### 3.10.5.2 Configuración del umbral de similitud de huellas dactilares

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

Procedimiento

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

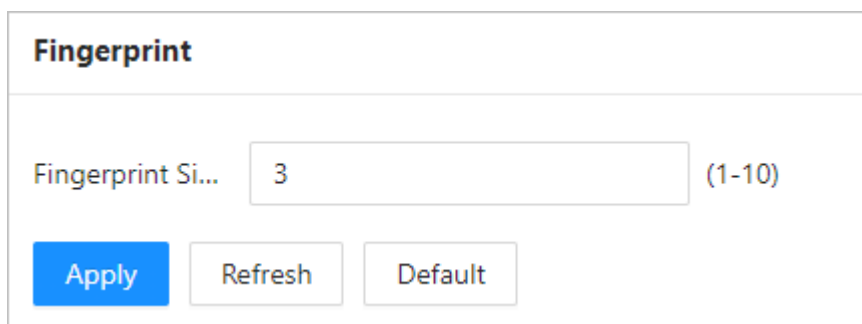
**Paso 2** Seleccionar **Centro de mantenimiento > Gestión de mantenimiento > Configuración**

**Paso 3** Ingrese el umbral de similitud y luego haga clic en **Aplicar**.



- El parámetro está disponible en el controlador de acceso modular con el módulo de huellas dactilares.
- El parámetro está disponible en el controlador de acceso con función de huella dactilar.

Figura 3-49 Umbral de similitud de huellas dactilares



### 3.10.5.3 Restauración de la configuración predeterminada de fábrica

#### Procedimiento

**Paso 1** Seleccionar **Centro de mantenimiento > Gestión de mantenimiento > Configuración**.



Restaurando el **Dispositivo** Si se modifica la configuración predeterminada, se perderán los datos. Tenga en cuenta lo siguiente.

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

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

## 3.10.6 Mantenimiento

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

#### Procedimiento

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

**Paso 2** Seleccionar **Centro de mantenimiento > Gestión de mantenimiento > Mantenimiento**

**Paso 3** Establezca la hora y luego haga clic en **Aplicar**.

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

## 3.10.7 Actualización del sistema



- Utilice el archivo de actualización correcto. Asegúrese de obtener el archivo de actualización correcto del soporte técnico.
- No desconecte la fuente de alimentación ni la red y no reinicie ni apague el dispositivo durante la actualización.
- La actualización a una versión inferior puede ocasionar riesgos potenciales. Tenga en cuenta lo siguiente.
- Si inicia el dispositivo por primera vez o restaura el dispositivo a la configuración predeterminada de fábrica, el dispositivo realiza automáticamente una copia de seguridad de los archivos del sistema dentro de los primeros 10 minutos. No actualice durante este período.

### 3.10.7.1 Actualización de archivos

#### Procedimiento

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

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



El archivo de actualización debe ser un archivo .bin.

**Paso 3** Hacer clic **Actualizar**.

El dispositivo se reiniciará después de finalizar la actualización.

### 3.10.7.2 Actualización en línea

#### Procedimiento

**Paso 1** En la página de inicio, seleccione **Centro de mantenimiento > Actualizar**. En el

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

- Seleccionar **Búsqueda automática de actualizaciones** y el dispositivo 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 dispositivo inmediatamente.

## 3.10.8 Mantenimiento avanzado

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

### 3.10.8.1 Exportación

#### Procedimiento

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

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


### 3.10.8.2 Captura de paquetes

#### Procedimiento

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

Figura 3-50 Captura de paquetes

Packet Capture							
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Backup
eth0	192.168.1.166	Optional	Optional	Optional	Optional	0.00MB	▶
eth2	192.168.1.101	Optional	Optional	Optional	Optional	0.00MB	▶

**Paso 2** Introduzca la dirección IP, haga clic en 

 cambios a 

**Paso 3** Una vez que haya adquirido suficientes datos, haga clic en 

Los paquetes capturados se descargan automáticamente a su computadora local.

## 3.11 Configuración de seguridad (opcional)

### 3.11.1 Estado de seguridad

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

#### Información de contexto

- **Detección de usuarios y servicios:** comprueba si la configuración actual se ajusta a la recomendación.
- **Escanee 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

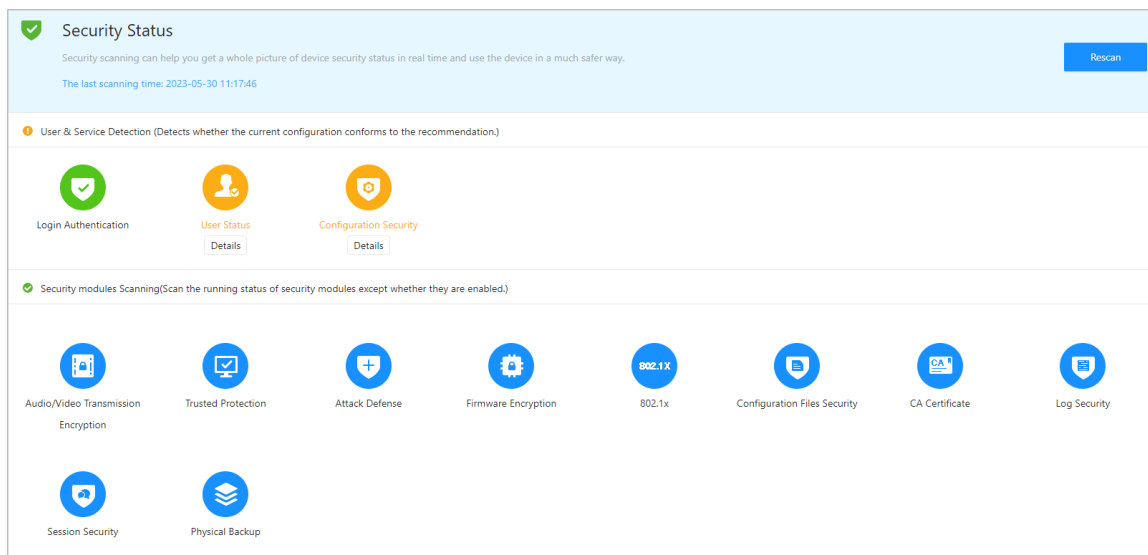
**Paso 1** Seleccionar  > **Estado de seguridad.**

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



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

Figura 3-51 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, no se escaneará. La anomalía que se ignoró se resaltarán en gris.
- Hacer clic **Optimizar** para solucionar la anomalía.

## 3.11.2 Configuración del servicio del sistema

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

Procedimiento

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

**Paso 2** Activar el servicio HTTPS.



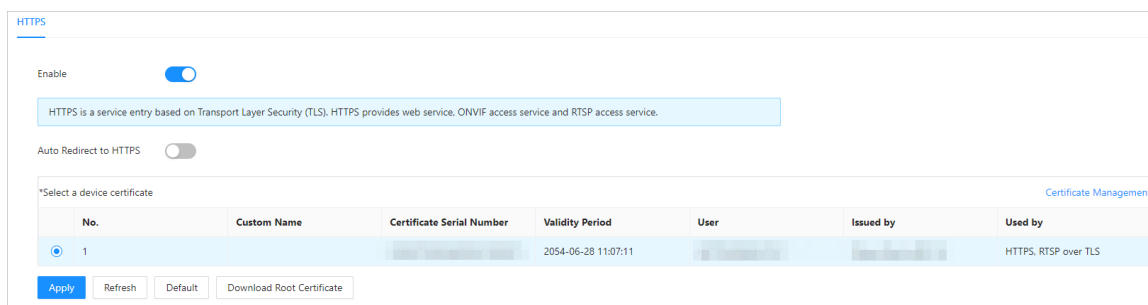
Si activa la compatibilidad con TLS v1.1 y versiones anteriores, pueden producirse riesgos de seguridad. Tenga en cuenta lo siguiente.

**Paso 3** Seleccione el certificado.



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

Figura 3-52 Servicio del sistema



**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.

## 3.11.3 Defensa de ataque

### 3.11.3.1 Configuración del firewall

Configurar el firewall para limitar el acceso al dispositivo.

Procedimiento

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


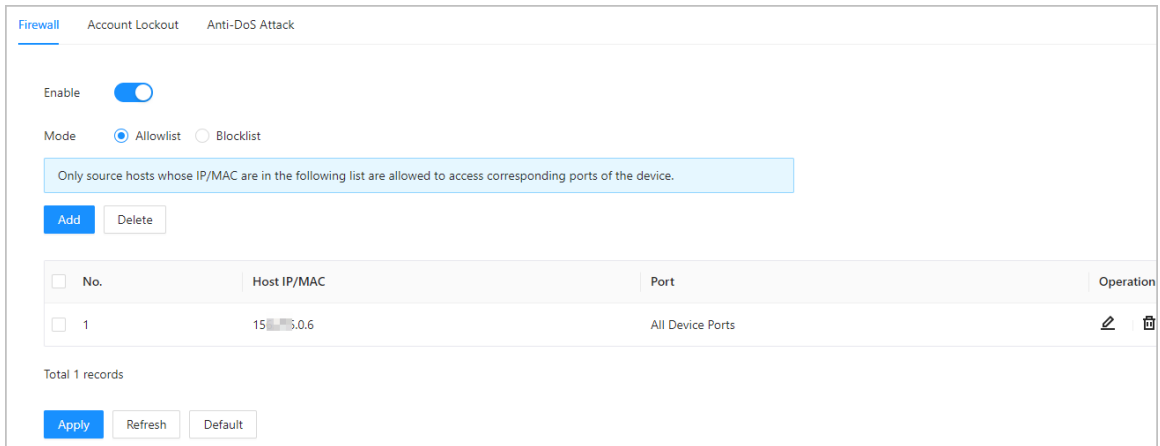
**Paso 2** Hacer clic  para habilitar la función de firewall.

Figura 3-53 Cortafuegos

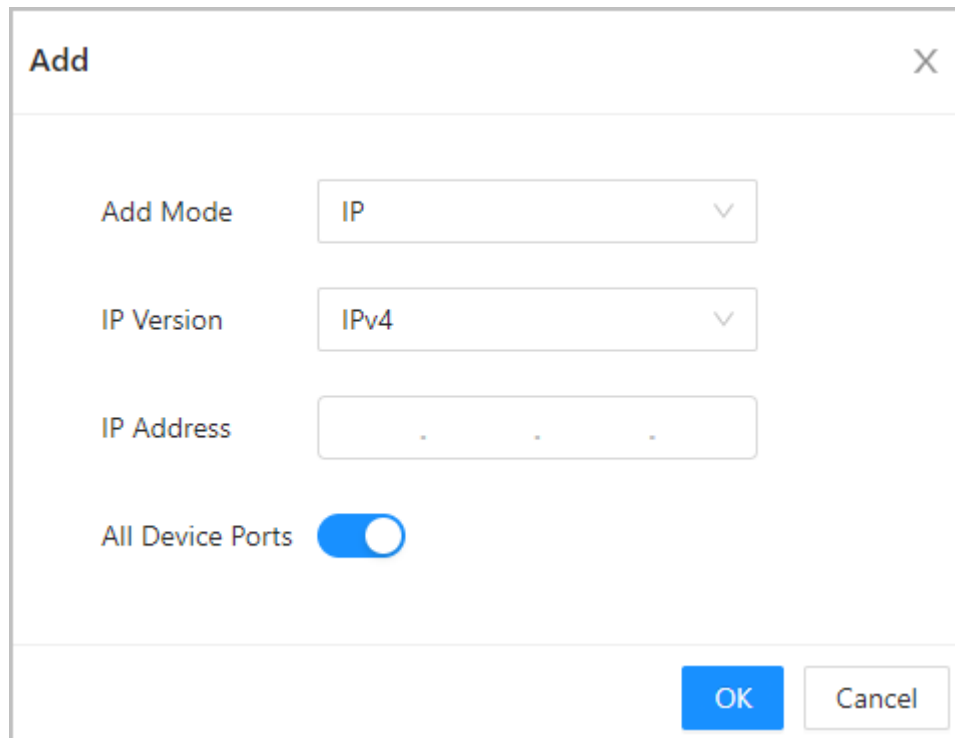


**Paso 3** Seleccione el modo: **Lista de permitidos** y **Lista de bloqueo**.

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



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

Figura 3-54 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.

### 3.11.3.2 Configuración del bloqueo de cuenta

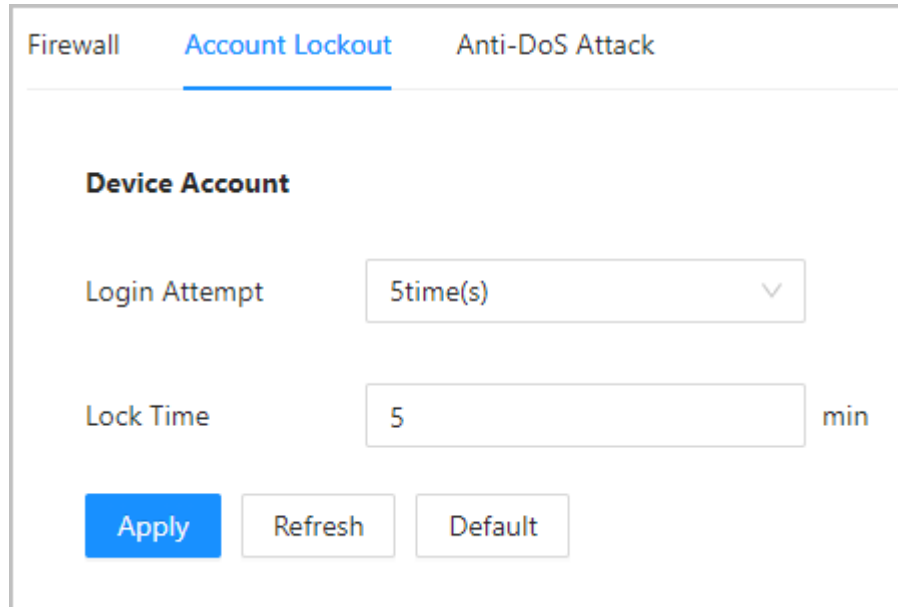
Si se ingresa la contraseña incorrecta un número definido de veces, la cuenta se bloqueará.

Procedimiento

Paso 1 Seleccionar  > **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 3-55 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

Paso 3 en **Aplicar.**

### 3.11.3.3 Configuración de ataques anti-DoS

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

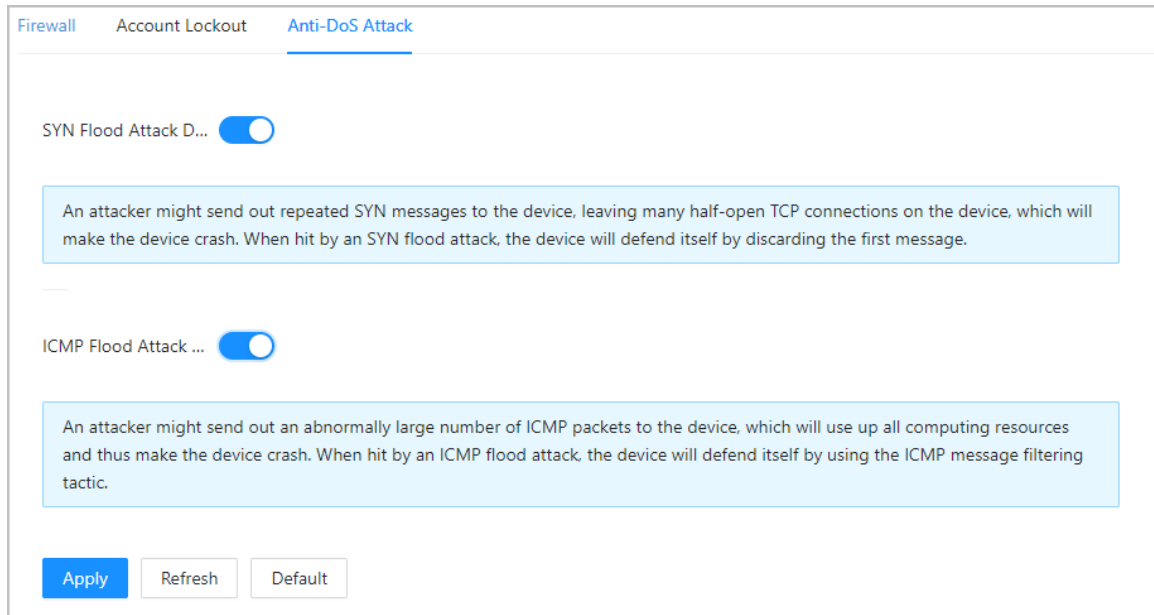
Procedimiento

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

Paso 2 Encender **Defensa contra ataques de inundación SYN** y **Defensa contra ataques de inundación ICMP** para proteger el dispositivo contra ataques DoS.



Figura 3-56 Ataque anti-DoS



**Paso 3** Hacer clic **Aplicar**.

### 3.11.4 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.

#### 3.11.4.1 Creación de certificado

Crear un certificado para el dispositivo.

Procedimiento

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

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

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

**Paso 4** Ingrese la información del certificado.

Figura 3-57 Información del certificado

Step 2: Fill in certificate information. X

Custom Name

\* IP/Domain Name

Organization Unit

Organization

\* Validity Period  Days (1~5000)

\* Region

Province

City Name

Back Create and install certificate Cancel





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.

### 3.11.4.2 Solicitud e importación de un certificado de CA

Importe el certificado CA de terceros al dispositivo.

#### Procedimiento

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

**Paso 2** Hacer clic **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 dispositivo.

- Región: El nombre de la región no debe superar los 3 caracteres. Le recomendamos que introduzca la abreviatura del nombre de la región.

Figura 3-58 Información del certificado (2)

The screenshot shows a web form titled "Step 2: Fill in certificate information." with a close button (X) in the top right corner. The form contains the following fields:

- \* IP/Domain Name: A text input field containing "17[redacted]03".
- Organization Unit: An empty text input field.
- Organization: An empty text input field.
- \* Region: An empty text input field.
- Province: An empty text input field.
- City Name: An empty text input field.

At the bottom of the form, there are three buttons: "Back", "Create and Download" (highlighted in blue), and "Cancel".

**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.

**3.11.4.3 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**.

- Paso 2** Hacer clic **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 3-59 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.

### 3.11.5 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  > **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 3-60 Instalar el certificado de confianza

Install Trusted Certificate



Custom Name

Certificate Path

**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.

## 3.11.6 Cifrado de datos

#### Procedimiento

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

**Paso 2** Configurar los parámetros.

Figura 3-61 Cifrado de datos

Encrypted Transmission

**Private Protocol**

Enable

Stream transmission is encrypted by using private protocol.

\*Please make sure that the corresponding device or software supports video decryption.

Encryption Type: AES256-OFB

Update Period... 12 hr (0-720)

**RTSP over TLS**

Enable

RTSP stream is encrypted by using TLS tunnel before transmission.

\*Please make sure that the corresponding device or software supports video decryption.

\*Select a device certificate [Certificate Management](#)

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
<input checked="" type="radio"/> 1		3930303...343436383232	2053-05-30 11:40:22	8C04F30YA16759	BSC	HTTPS, RTSP over TLS

Tabla 3-29 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	Manténgalo como predeterminado.
	Periodo de actualización de la 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.
	Gestión de certificados	Cree o importe un certificado. Para obtener más información, consulte "3.11.4 Instalación del certificado del dispositivo". Los certificados instalados se muestran en la lista.

### 3.11.7 Advertencia de seguridad

Procedimiento


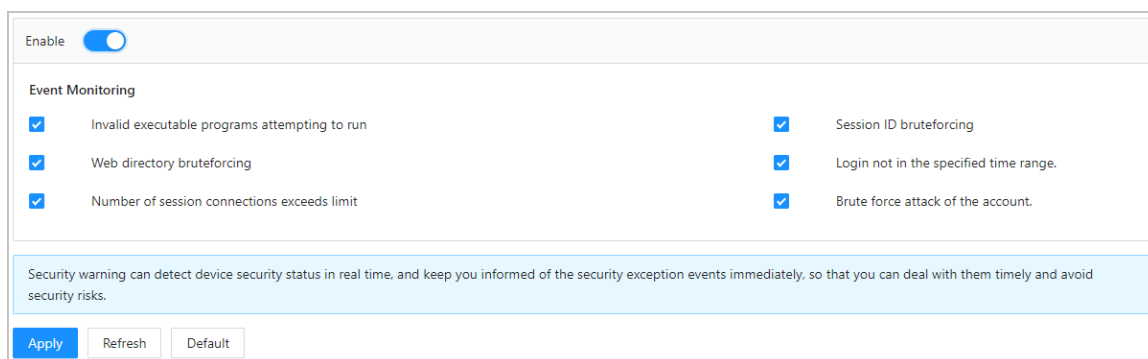
- Paso 1** Seleccionar  > **Advertencia de seguridad.**
- Paso 2** Habilite la función de advertencia de seguridad.
- Paso 3** Seleccione los elementos de monitoreo.

Figura 3-62 Advertencia de seguridad



- Paso 4** Hacer clic **Aplicar.**

### 3.11.8 Autenticación de seguridad

Procedimiento

- Paso 1** Seleccionar **Seguridad** > **Autenticación de seguridad.**
- Paso 2** Seleccione un algoritmo de resumen del mensaje.
- Paso 3** Hacer clic **Aplicar.**

Figura 3-63 Autenticación de seguridad

**Digest Algorithm for Authentication**

---

Digest Algorithm for User Authentication     MD5     SHA256

Digest Algorithm for ONVIF User Authentication     MD5     SHA256

## 4 Operaciones telefónicas

Antes de iniciar sesión en la página web del dispositivo en su teléfono, asegúrese de haber inicializado el dispositivo a través de la página web en la computadora.

Le recomendamos que utilice su teléfono en modo vertical y en modo diurno. Puede iniciar sesión en la página web del dispositivo en su teléfono mediante los siguientes métodos.

- Conecte el dispositivo a la red mediante el cable de red. Asegúrese de que el teléfono y el dispositivo estén en la misma red. Abra el navegador en el teléfono y luego ingrese la dirección IP del dispositivo.
- Conecte el dispositivo y el teléfono a la red a través de la misma red Wi-Fi. Abra el navegador en el teléfono y luego ingrese la dirección IP de acuerdo con la red Wi-Fi conectada.
- Conecte el teléfono a la red a través del Wi-Fi del dispositivo. Abra el navegador en el teléfono y luego ingrese la dirección IP de acuerdo con el punto de acceso Wi-Fi del dispositivo (es 192.168.3.1 por defecto).



El nombre del dispositivo Wi-Fi se muestra en la **Número de serie del dispositivo + Modelo del dispositivo** modo.



- El Wi-Fi y el Wi-Fi AP están disponibles en modelos seleccionados.
- Al iniciar sesión en la página web desde el teléfono, solo se admite el idioma inglés.

### 4.1 Iniciar sesión en la página web

#### Prerrequisitos

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

#### Procedimiento

**Paso 1** Abra un navegador y luego ingrese la dirección IP del dispositivo. Ingrese

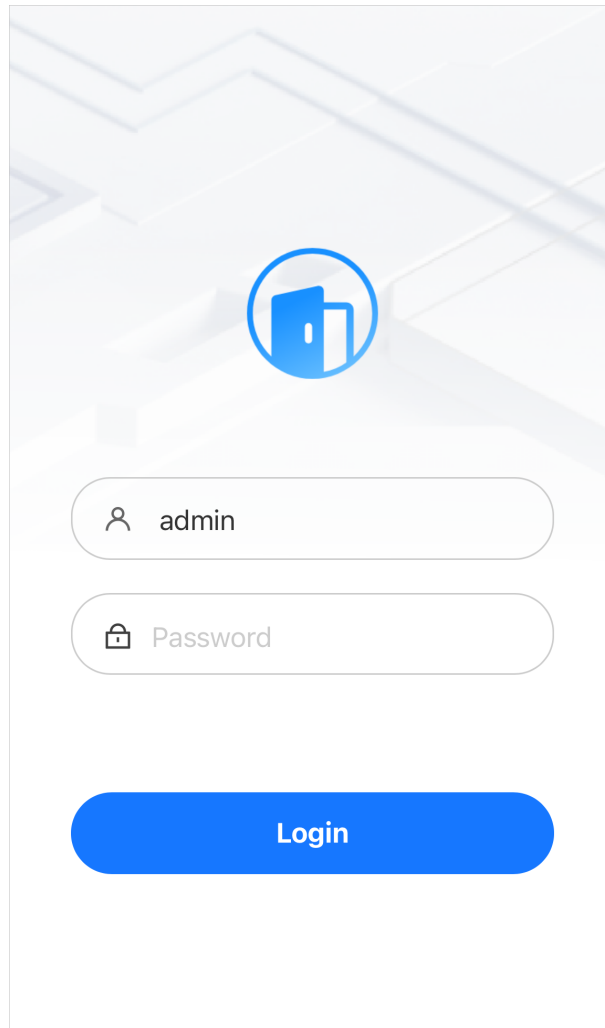
**Paso 2** el nombre de usuario y la contraseña.



- El nombre de administrador predeterminado es admin y la contraseña es la que configuraste durante la inicialización. Te recomendamos cambiar la contraseña de administrador con regularidad para aumentar la seguridad.
- Si olvida la contraseña de inicio de sesión del administrador, puede restablecerla a través de la página web de la computadora. Para obtener más información, consulte "3.2 Restablecimiento de la contraseña".



Figura 4-1 Página de inicio de sesión



The image shows a login interface. At the top, there is a blue circular icon containing a white door symbol. Below this, there are two rounded rectangular input fields. The first field contains a user icon and the text 'admin'. The second field contains a lock icon and the text 'Password'. At the bottom of the form is a large, rounded blue button with the white text 'Login'. The background of the page is light gray with a subtle geometric pattern.

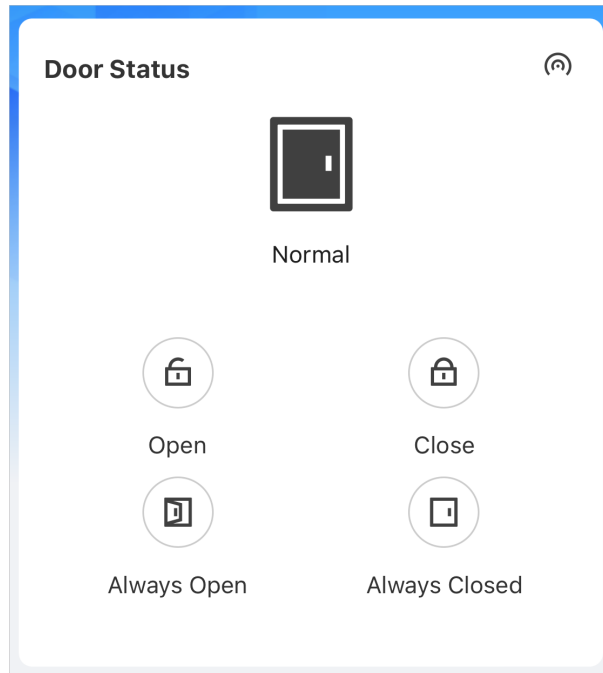
Paso 3 Hacer clic **Acceso**.

## 4.2 Página de inicio

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

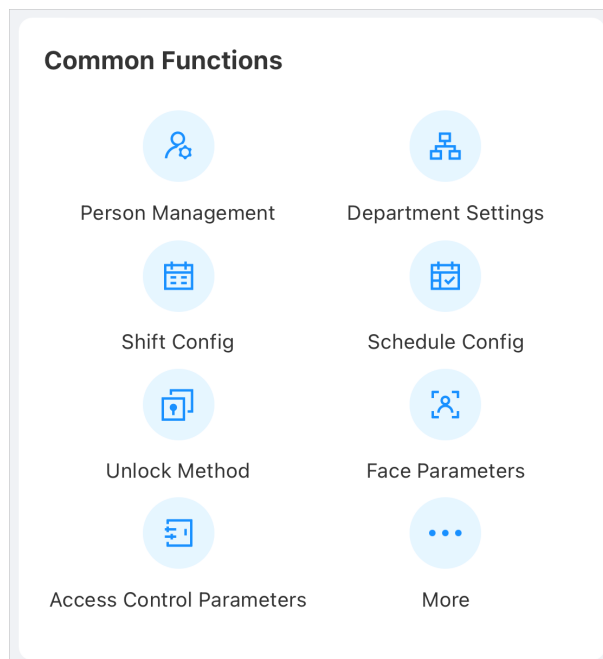
- El **Estado de la puerta**El área muestra el estado de la puerta. Puede abrir o cerrar la puerta de forma remota. También puede configurar el estado de la puerta como **Siempre abierto** o **Siempre cerrado**.

Figura 4-2 Estado de la puerta



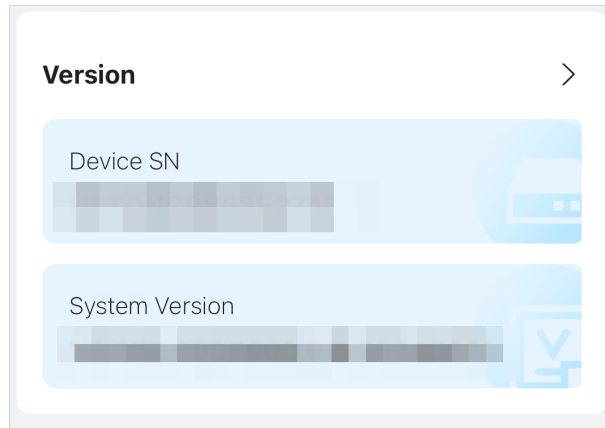
- El **Función común** El área muestra el menú de configuración del dispositivo. Haga clic en **Más** para ver todos los menús de configuración.

Figura 4-3 Funciones comunes



- Ver el número de serie y la información de la versión en el **Versión** Área. Haga clic > para ver los detalles de la versión.

Figura 4-4 Versión



## 4.3 Gestión de personas

Agregue la persona y configure los permisos.

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Hacer clic **Gestión de personas**, y luego haga clic+.
- Paso 3** Configurar la información del usuario.


Figura 4-5 Agregar la persona (1)



Basic Info	
* User ID	
Name	
Verification Mode	
Face	0 >
Password	Not Added >
Card	0 >
Fingerprint	0 >




Figura 4-6 Agregar la persona (2)

Permission	User >
Validity Period	>
2037-12-31 23:59:59	
Period	255-Default >
Holiday Plan	255-Default >
User Type	General User >
Times Used	Unlimited
Department	1-Default >
Schedule Mode	Department Schedule >

Tabla 4-1 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 30 caracteres.
Nombre	El nombre puede tener hasta 32 caracteres (incluidos números, símbolos y letras).
Rostro	<p>Sube una imagen de tu rostro. Cada persona solo puede añadir hasta dos imágenes de tu rostro. Puedes ver o eliminar la imagen de tu rostro después de subirla.</p>  <p>La imagen del rostro está en formato jpg, jpeg, png y debe ser menor a 100 KB.</p>
Contraseña	Configurar la contraseña de usuario. La longitud máxima de la contraseña es de 8 dígitos. La contraseña de coacción es la contraseña de desbloqueo + 1. Por ejemplo, si la contraseña de usuario es 12345, la contraseña de coacción será 12346. Se activará una alarma de coacción cuando se utilice una contraseña de coacción para desbloquear la puerta.

Parámetro	Descripción
Tarjeta	<ul style="list-style-type: none"> <li>● Introduzca el número de tarjeta manualmente.               <ol style="list-style-type: none"> <li>1. Haga clic <b>Agregar</b>.</li> <li>2. Ingrese el número de tarjeta y luego haga clic en <b>Agregar</b>.</li> </ol> </li> <li>● Lee el número automáticamente a través del dispositivo.               <ol style="list-style-type: none"> <li>1. Haga clic <b>Agregar</b>.</li> <li>2. Pase las tarjetas por el lector de tarjetas.                   <p style="margin-left: 20px;">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 <b>Leer tarjeta</b> de nuevo para iniciar una nueva cuenta regresiva.</p> </li> <li>3. Haga clic <b>DE ACUERDO</b>.</li> </ol> </li> </ul> <p>Un usuario puede registrar hasta 5 tarjetas como máximo. Ingrese el número de su tarjeta o deslícela y el dispositivo leerá la información de la tarjeta.</p> <p>Puedes habilitar el <b>Tarjeta de coacción</b> Función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta.</p> <ul style="list-style-type: none"> <li>● <b>Tarjeta de coacción:</b> Haga clic para configurar la tarjeta de coacción.</li> <li>● <b>Cambiar número de tarjeta:</b> Haga clic para cambiar el número de tarjeta.</li> </ul>  <p>Un usuario sólo puede configurar una tarjeta de coacción.</p>
Huella dactilar	<p>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.</p> <p>Inscriba huellas dactilares a través de un lector de inscripción o del Dispositivo.</p> <ol style="list-style-type: none"> <li>1. Haga clic <b>Agregar</b>.</li> <li>2. Presione el dedo sobre el escáner de acuerdo con las instrucciones en pantalla.</li> <li>3. Haga clic <b>DE ACUERDO</b>.</li> </ol>  <ul style="list-style-type: none"> <li>● La función de huella dactilar solo está disponible en modelos seleccionados.</li> <li>● No recomendamos que configure la primera huella digital como huella digital de coacción.</li> <li>● Un usuario solo puede configurar una huella digital de coacción.</li> </ul>
Permiso	<ul style="list-style-type: none"> <li>● <b>Usuario:</b> Los usuarios sólo tienen permisos de acceso a puertas o de control de asistencia.</li> <li>● <b>Administración:</b> Los administradores pueden configurar el dispositivo además del acceso a la puerta y los permisos de asistencia.</li> </ul>
Periodo de validez	<p>Establecer una fecha en la que caducarán los permisos de acceso a la puerta y de asistencia de la persona.</p>

Parámetro	Descripción
Período	<p>Las personas pueden desbloquear la puerta o tomar asistencia durante el período definido.</p>  <p>Puede seleccionar más de un período.</p>
Plan de vacaciones	<p>Las personas pueden desbloquear la puerta o tomar asistencia durante el día festivo definido.</p>  <p>Puede seleccionar más de un día festivo.</p>
Tipo de usuario	<ul style="list-style-type: none"> <li>● <b>Usuario general:</b> Los usuarios generales pueden desbloquear la puerta.</li> <li>● <b>Usuario de la lista negra:</b> Cuando los usuarios de la lista de bloqueo desbloquean la puerta, el personal de servicio recibirá una notificación.</li> <li>● <b>Usuario invitado:</b> Los huéspedes pueden desbloquear la puerta dentro de un período definido o durante un tiempo determinado. Una vez que el período definido o el tiempo de desbloqueo se agoten, no podrán desbloquear la puerta.</li> <li>● <b>Usuario de patrulla:</b> Los usuarios de patrulla pueden tomar asistencia en el dispositivo, pero no tienen permisos de puerta.</li> <li>● <b>Usuario VIP:</b> Cuando el VIP desbloquee la puerta, el personal de servicio recibirá un aviso.</li> <li>● <b>Otro usuario:</b> Cuando desbloqueen la puerta, ésta permanecerá desbloqueada durante 5 segundos más.</li> <li>● Usuario personalizado 1/Usuario personalizado 2: Lo mismo que los usuarios generales.</li> </ul>
Tiempo utilizado	<p>Establezca un límite de desbloqueo para los usuarios invitados. Una vez que se agote el tiempo de desbloqueo, no podrán desbloquear la puerta.</p>
Departamento	<p>Agregar usuarios a un departamento. Si se le asigna un horario de departamento a la persona, esta seguirá el horario de departamento establecido.</p> <ul style="list-style-type: none"> <li>● <b>Horario del departamento:</b> Asigna el horario del departamento al usuario.</li> <li>● <b>Horario personal:</b> Asigna un horario personal al usuario.</li> </ul>
Modo de programación	 <ul style="list-style-type: none"> <li>◇ Esta función solo está disponible en modelos seleccionados.</li> <li>◇ Si aquí configura el modo de programación en programación de departamento, se aplicará la programación personal que haya configurado para el usuario en <b>Asistencia &gt; Configuración de programación &gt; Horario personal</b> no es válido.</li> </ul>

Paso 4 Hacer clic **Agregar**.

## 4.4 Configuración del sistema

#### 4.4.1 Visualización de la información de la versión

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

#### 4.4.2 Mantenimiento

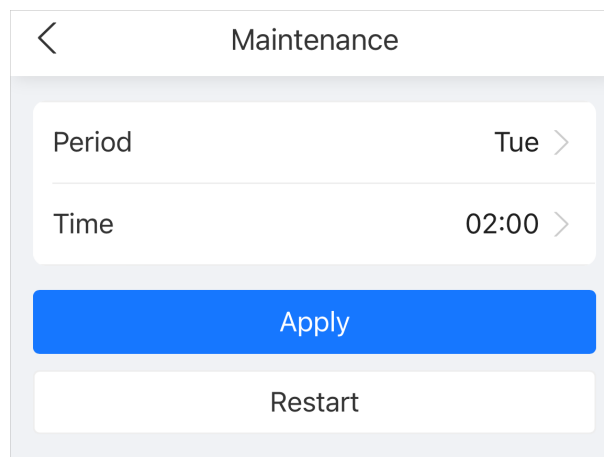
Reinicie periódicamente el dispositivo durante su tiempo de inactividad para mejorar su rendimiento.

Procedimiento

- Paso 1 Inicie sesión en la página web.
- Paso 2 Seleccione **Más>Sistema>Mantenimiento**
- Paso 3 Establezca la hora y luego haga clic en **Aplicar**.

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

Figura 4-7 Mantenimiento



#### 4.4.3 Configuración de la hora

Procedimiento

- Paso 1 Inicie sesión en la página web.
- Paso 2 Seleccione **Más>Sistema>Tiempo**.
- Paso 3 Configurar la hora.

Figura 4-8 Configurar los parámetros de tiempo

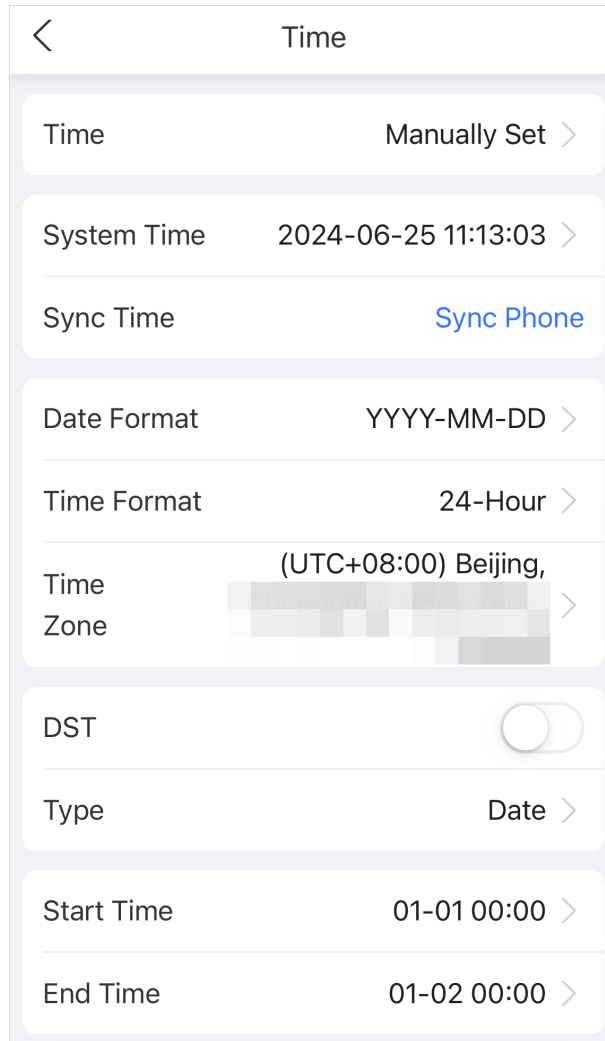


Tabla 4-2 Descripción de la configuración de tiempo

Parámetro	Descripción
Tiempo	<ul style="list-style-type: none"> <li>● Configuración manual: ingrese la hora manualmente o puede hacer clic <b>Sincronizar teléfono</b> para sincronizar la hora con el teléfono.</li> <li>● NTP: El dispositivo sincronizará automáticamente la hora con el servidor NTP. <ul style="list-style-type: none"> <li>◇ <b>Servidor:</b> Introduzca el dominio del servidor NTP.</li> <li>◇ <b>Puerto:</b> Introduzca el puerto del servidor NTP.</li> <li>◇ <b>Intervalo:</b> Introduzca su hora con el intervalo de sincronización.</li> </ul> </li> </ul>
Formato de fecha	Seleccione el formato de fecha y el formato de hora.
Formato de hora	
Huso horario	Seleccione la zona horaria.
Horario de verano	<ol style="list-style-type: none"> <li>1. (Opcional) Habilite el horario de verano.</li> <li>2. Seleccionar <b>Fecha</b> <b>Semana</b> como el <b>Tipo</b>.</li> <li>3. Configure la hora de inicio y la hora de finalización del horario de verano.</li> </ol>



Paso 4 Hacer clic **Aplicar**.

## 4.4.4 Capacidad de datos

Puede ver cuántos usuarios, tarjetas, imágenes faciales, huellas dactilares, registros, registros de desbloqueo y otra información que el dispositivo puede almacenar.

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

## 4.5 Configuración de asistencia

Esta función solo está disponible en modelos seleccionados.

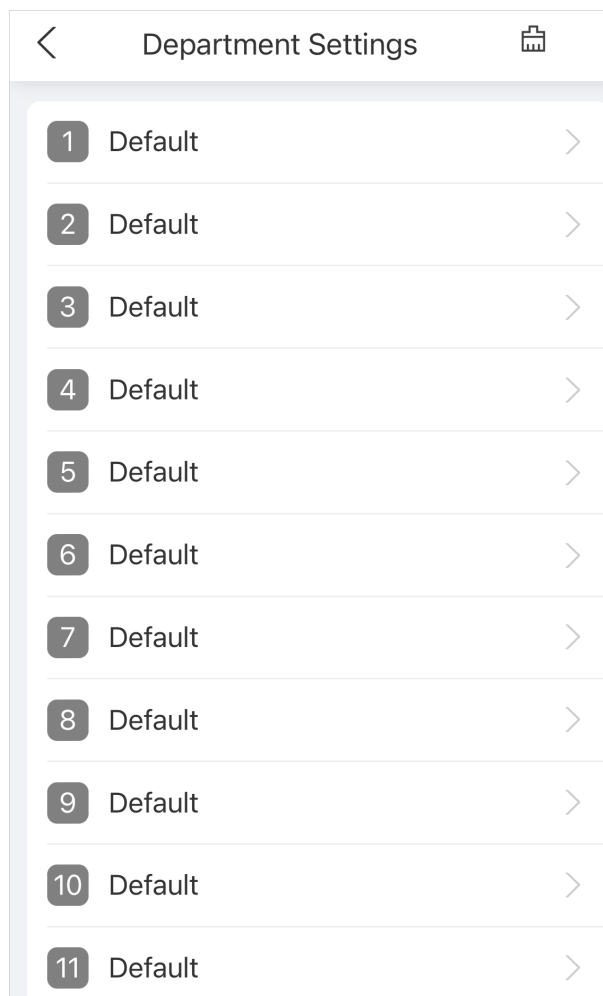
### 4.5.1 Configuración de departamentos

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar **Más> Configuración de asistencia> Configuración del departamento**.

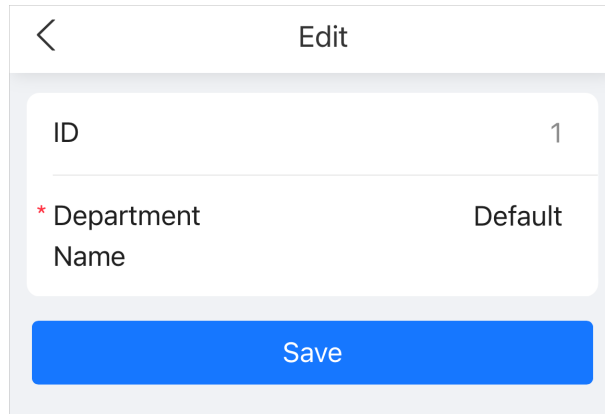
Figura 4-9 Configuración del departamento



Paso 3 Haga clic en el departamento para cambiar el nombre del departamento y luego haga clic en **Ahorrar**.


Hay 20 departamentos predeterminados. Te recomendamos cambiarles el nombre.

Figura 4-10 Cambiar el nombre del departamento



Edit	
ID	1
* Department Name	Default
<a href="#">Save</a>	

#### Operaciones relacionadas

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

## 4.5.2 Configuración de turnos

Configurar turnos para definir reglas de asistencia. Los empleados deben 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 Inicie sesión en la página web.
- Paso 2 Seleccionar **Más**>**Configuración de asistencia**>**Configuración de cambio**>**Cambio**.

Figura 4-11 Lista de turnos

	Shift	Holiday
1	Default 08:00-17:00	00:00-00:00
2	Default 08:00-17:00	00:00-00:00
3	3 08:00-17:00	00:00-00:00
4	4 08:00-17:00	00:00-00:00
5	5 08:00-17:00	00:00-00:00
6	6 08:00-17:00	00:00-00:00
7	7 08:00-17:00	00:00-00:00
8	8 08:00-17:00	00:00-00:00

**Paso 3** Haga clic en el turno para configurar los parámetros del turno y luego haga clic en **Ahorrar**.

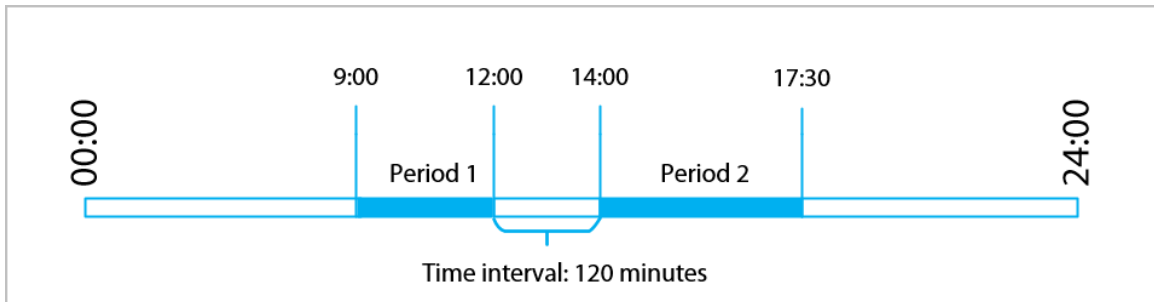
Figura 4-12 Configurar el turno

Tabla 4-3 Descripción de los parámetros de cambio

Parámetro	Descripción
Nombre del turno	Introduzca el nombre del turno.
Periodo 1	<p>Especifique un rango de tiempo en el que las personas pueden registrar su entrada y salida durante la jornada laboral.</p> <p>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.</p> <p>Si establece 2 períodos de asistencia, estos no pueden superponerse. Los empleados deben registrar su entrada y salida en ambos períodos.</p>
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 de trabajo normales.
Límite de llegadas tardías	<p>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.</p>
Límite para salidas anticipadas	

- 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 4-13 Intervalo de tiempo (número par)



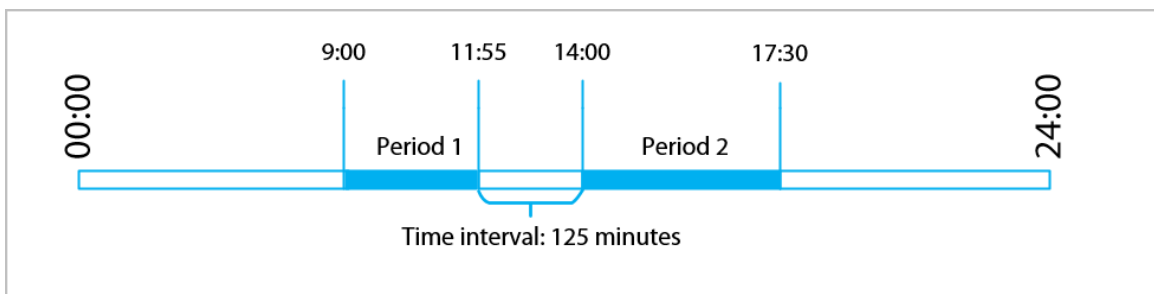
Por ejemplo: si el intervalo es de 120 minutos, entonces la hora de salida para el período 1 es de 12:00 a 12:59, y la hora de entrada para el período 2 es de 13:00 a 14:00.



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

- 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 4-14 Intervalo de tiempo (número impar)



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, será válida la hora más reciente, y si registra su entrada varias veces durante el período 2, será válida la hora más temprana.



Todos los horarios de asistencia son precisos hasta el segundo. Por ejemplo, si la hora de entrada normal está establecida a las 8:05 a. m., el empleado que ingrese a las 8:05:59 a. m. no se considerará que llegó tarde. Sin embargo, el empleado que llegue a las 8:06 a. m. se marcará como que llegó tarde por 1 minuto.

#### Operaciones relacionadas

Puedes hacer clic  para restaurar los turnos a los valores predeterminados de fábrica.

## 4.5.3 Configuración de vacaciones

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

### Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccione **Más** > **Configuración de asistencia** > **Configuración de cambio** > **Día festivo** Haga clic
- Paso 3** en+ para agregar planes de vacaciones.
- Paso 4** Configure los parámetros y luego haga clic en **Ahorrar**.

Figura 4-15 Agregar el día festivo

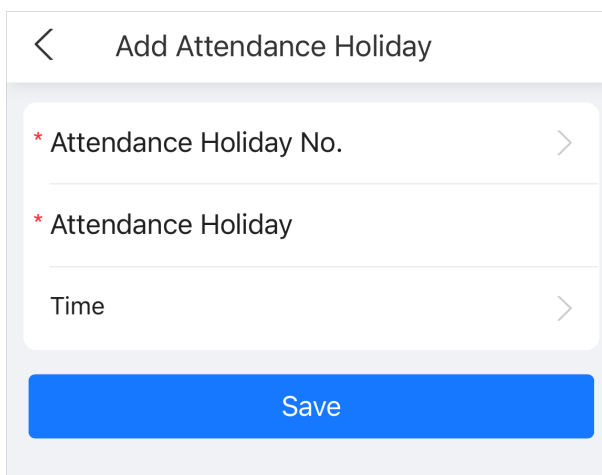


Tabla 4-4 Descripción de parámetros

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

**Paso 5** Hacer clic **DE ACUERDO**.

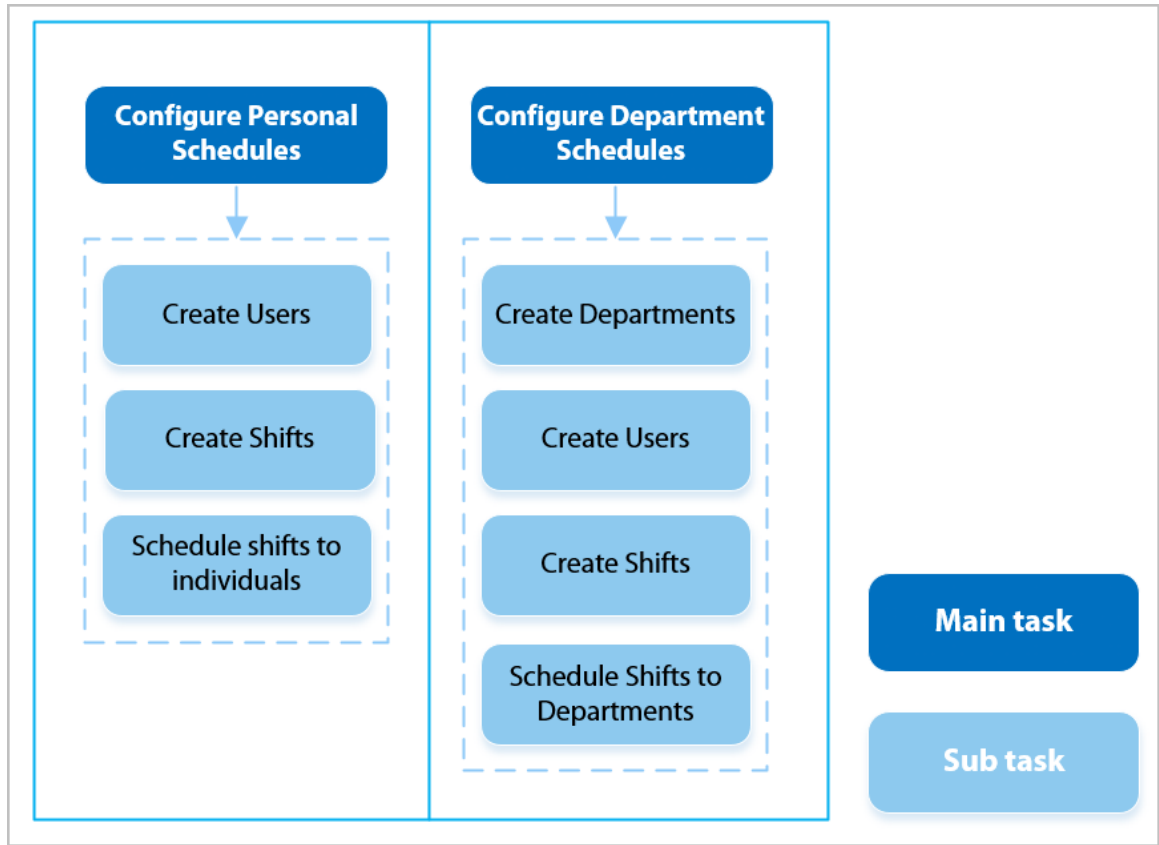
## 4.5.4 Configuración de horarios de trabajo

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 4-16 Configuración de horarios de trabajo



#### Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Más > Configuración de asistencia > Configuración de programación**. Establecer
- Paso 3** horarios de trabajo para personas individuales.

1. Haga clic **Horario personal**.
2. Seleccione una persona en la lista de personas.



Después de configurar el **Modo de programación** como el **Horario personal** Cuando agregas a una persona, esta se muestra en la lista de personas.

3. En el calendario, seleccione un día y luego seleccione un turno.



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

- 0 indica ruptura.
- 1 a 24 indica el número de turnos predefinidos.
- 25 indica viaje de negocios.
- 26 indica licencia de ausencia.

- Paso 4** Establecer horarios de trabajo para los departamentos.

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

Figura 4-17 Horario del departamento

Sun	Mon	Tue	Wed	Thu	Fri	Sat
0	1	1	1	1	1	0

Cancel      Select Shift      OK

0-Rest

1-Default    
08:00:00-17:00:00 00:00:00-00:00:00

2-Default   
08:00:00-17:00:00 00:00:00-00:00:00

3-3   
08:00:00-17:00:00 00:00:00-00:00:00

4-4   
08:00:00-17:00:00 00:00:00-00:00:00

- 0 indica descanso.
- 1 a 24 indica el número de turnos predefinidos.
- 25 indica viaje de negocios.
- 26 indica licencia de ausencia.



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

## 4.5.5 Configuración de modos de asistencia

### Procedimiento

- Paso 1 Inicie sesión en la página web.
- Paso 2 Seleccionar **Más > Configuración de asistencia > Configuración de asistencia**.
- Paso 3 Permitir **Local o remotoy** luego configure el modo de asistencia.



Figura 4-18 Configuración de asistencia

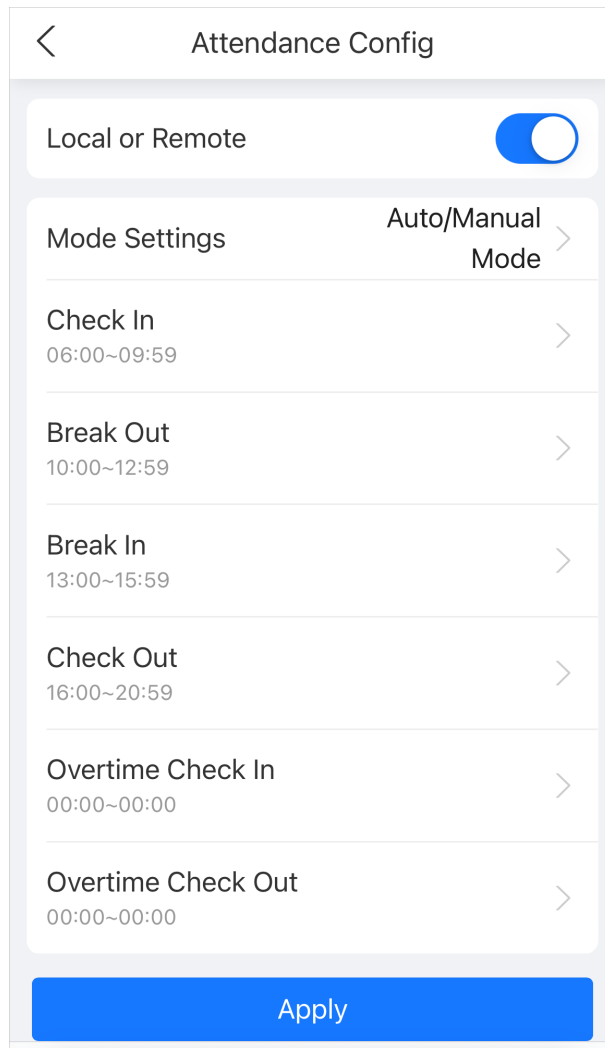


Tabla 4-5 Descripción de los parámetros de asistencia

Parámetro	Descripción
Modo automático/manual	<p>La pantalla muestra el estado de asistencia automáticamente después de registrar su entrada o salida, pero también puede cambiar manualmente su estado de asistencia.</p> <ul style="list-style-type: none"> <li>● Registra tu entrada: registra tu entrada cuando comienza tu jornada laboral normal.</li> <li>● Break Out: Marca tu salida cuando comienza tu descanso.</li> <li>● Break In: Registre su entrada cuando finalice su descanso.</li> <li>● Salida: Marque su salida cuando comience su jornada laboral normal.</li> <li>● Registro de horas extras: Registre su entrada cuando comience su período de horas extras.</li> <li>● Registro de salida de horas extra: Registre su salida cuando finalice su período de horas extra.</li> </ul>

Parámetro	Descripción
Modo automático	<p>La pantalla muestra su estado de asistencia automáticamente después de registrar su entrada o salida.</p> <ul style="list-style-type: none"> <li>● Registra tu entrada: registra tu entrada cuando comienza tu jornada laboral normal.</li> <li>● Break Out: Marca tu salida cuando comienza tu descanso.</li> <li>● Break In: Registre su entrada cuando finalice su descanso.</li> <li>● Salida: Marque su salida cuando comience su jornada laboral normal.</li> <li>● Registro de horas extras: Registre su entrada cuando comience su período de horas extras.</li> <li>● Registro de salida de horas extra: Registre su salida cuando finalice su período de horas extra.</li> </ul>
Modo manual	<p>Seleccione manualmente su estado de asistencia al registrar su entrada o salida.</p>
Modo fijo	<p>Al registrar su entrada o salida, la pantalla mostrará el estado de asistencia definido previamente en todo momento.</p>

**Paso 4** Hacer clic **Aplicar**.

## 4.6 Configuración del control de acceso

### 4.6.1 Configuración de métodos de desbloqueo

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

Procedimiento

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

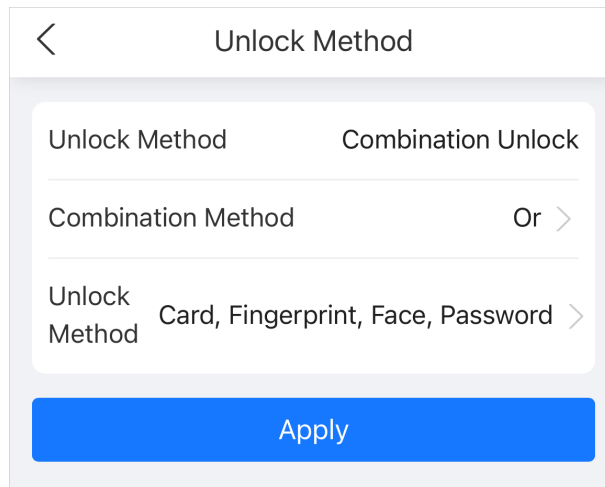
**Paso 2** Hacer clic **Método de desbloqueo** en el menú principal, o seleccione **Más > Control de acceso > Método de desbloqueo**.

**Paso 3** (Opcional) Configure el método de combinación y el método de desbloqueo y luego haga clic en **Aplicar**.

- Método de combinación
  - ◇ 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.
- Método de desbloqueo

Seleccione el método de desbloqueo según las capacidades admitidas del dispositivo.

Figura 4-19 Método de desbloqueo



## 4.6.2 Configuración de parámetros faciales

Configurar los parámetros de detección de rostros. Los parámetros de detección de rostros pueden variar según el modelo del producto.

### Procedimiento

- Paso 1 Inicie sesión en la página web.
- Paso 2 Hacer clic **Parámetros faciales** en el menú principal, o seleccione **Más > Control de acceso > Parámetros faciales**.
- Paso 3 Configure los parámetros y luego haga clic en **Aplicar**.

Figura 4-20 Configurar los parámetros del rostro

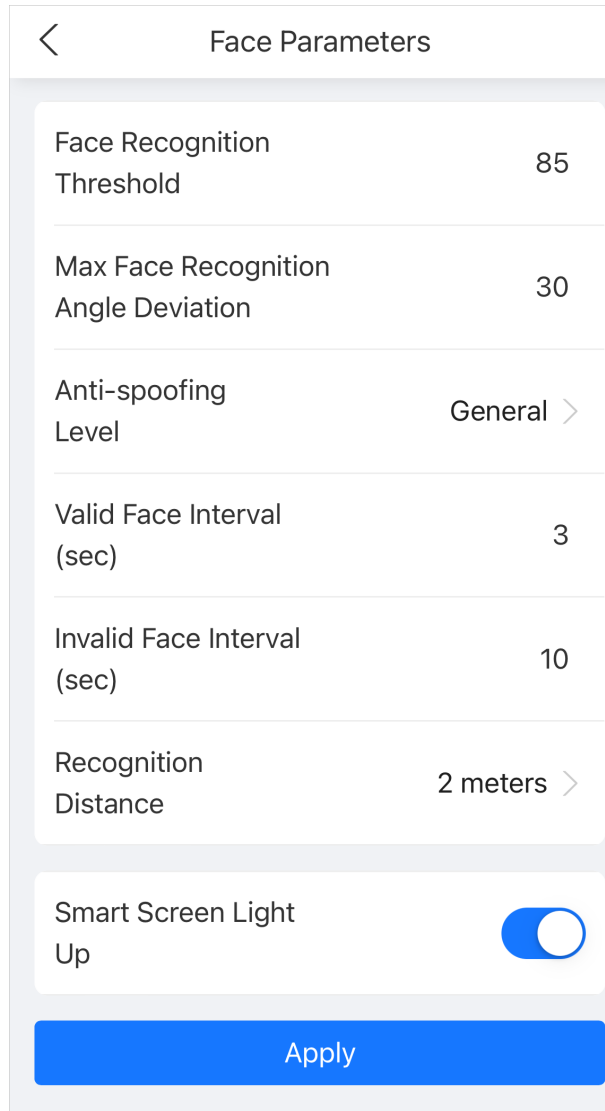



Tabla 4-6 Descripción de los parámetros faciales

Nombre	Descripción
Umbral de reconocimiento facial	<p>Ajuste el nivel de precisión del reconocimiento facial. Un umbral más alto significa mayor precisión y menor tasa de reconocimiento falso.</p> <p></p> <p>Cuando el umbral es demasiado bajo, como 0, la tasa de reconocimiento falso será extremadamente alta. Tenga en cuenta lo siguiente.</p>
Desviación máxima del ángulo de reconocimiento facial	<p>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.</p>
Nivel anti-spoofing	<p>Esto evita que las personas puedan usar fotos, vídeos, máscaras y otros sustitutos para obtener acceso no autorizado.</p>

Nombre	Descripción
Intervalo de cara válido (seg.)	Cuando el mismo rostro permanece frente a la lente después del primer reconocimiento exitoso, el dispositivo realizará nuevamente el reconocimiento del rostro después de un intervalo definido.
Intervalo de rostro no válido (seg.)	Cuando el mismo rostro permanece frente a la lente después del primer reconocimiento fallido, el dispositivo realizará nuevamente el reconocimiento del rostro después de un intervalo definido.
Distancia de reconocimiento	La distancia entre la cara y la lente.
Iluminación de pantalla inteligente	Cuando está habilitado, en el estado de pantalla apagada, la pantalla se iluminará cuando se detecte una cara.

### 4.6.3 Configuración de parámetros de control de acceso

#### Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Hacer clic **Parámetros de control de acceso** en el menú principal, o seleccione **Más>Control de acceso>Parámetros de control de acceso**.
- Paso 3** Configure los parámetros básicos para el control de acceso y luego haga clic en **Aplicar**.

Figura 4-21 Parámetros de control de acceso (1)

Figura 4-22 Parámetros de control de acceso (2)

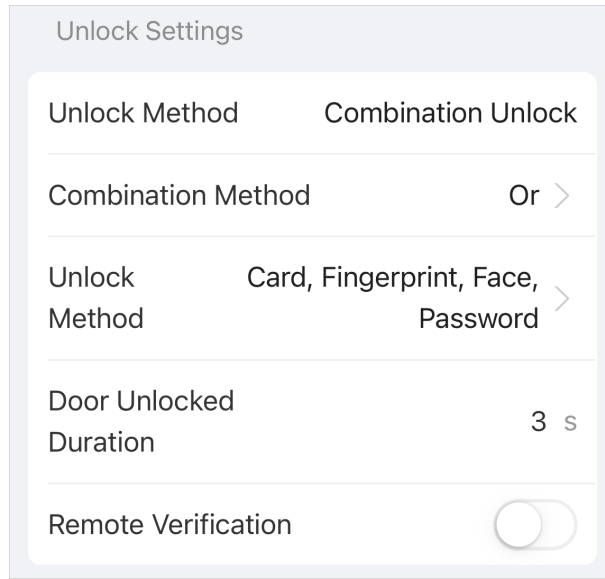



Tabla 4-7 Descripción de los parámetros de control de acceso

Parámetro		Descripción
Configuración básica	Nombre	El nombre de la puerta.
	Estado de la puerta	<p>Establecer el estado de la puerta.</p> <ul style="list-style-type: none"> <li>● Normal: La puerta se desbloqueará y bloqueará según su configuración.</li> <li>● Siempre abierto: la puerta permanece desbloqueada todo el tiempo.</li> <li>● Siempre cerrado: la puerta permanece bloqueada todo el tiempo.</li> </ul>
	Intervalo de verificación	Si verifica su identidad varias veces dentro de un período determinado, solo se considerará válida la verificación más antigua y la puerta no se abrirá después de la segunda o posteriores verificaciones. Desde el momento en que la puerta no se abre, debe esperar el intervalo de tiempo de verificación configurado antes de intentar verificar su identidad nuevamente.
Normalmente abierto Período	Plan de período/vacaciones	<p>Cuando seleccionas <b>Normal</b>, puede seleccionar una plantilla de tiempo de la lista desplegable. La puerta permanece abierta o cerrada durante el tiempo definido.</p> 
Normalmente cerrado Período	Plan de período/vacaciones	<ul style="list-style-type: none"> <li>● Cuando el período normalmente abierto entra en conflicto con período normalmente cerrado, período normalmente abierto tiene prioridad sobre el período normalmente cerrado.</li> <li>● Cuando el período entra en conflicto con el plan de vacaciones, los planes de vacaciones tienen prioridad sobre los períodos.</li> </ul>
Desbloquear configuraciones	Método de desbloqueo	<b>Desbloqueo de combinación</b> por defecto.

Parámetro		Descripción
	Combinación Método	<ul style="list-style-type: none"> <li>● O bien: Utilice uno de los métodos de desbloqueo seleccionados para abrir la puerta.</li> <li>● Y: Utilice todos los métodos de desbloqueo seleccionados para abrir la puerta.</li> </ul>
	Método de desbloqueo	Seleccione el método de desbloqueo según las capacidades admitidas del dispositivo.
	Puerta desbloqueada Duración	Configura el tiempo en el que la puerta se mantiene abierta. Por defecto son 3 segundos. Cuando la puerta se abre por más tiempo del configurado se cierra.
	Verificación remota	Cuando esté habilitado, configure el período y el plan de vacaciones.

Paso 4 Hacer clic **Aplicar**.

## 4.6.4 Configuración de alarmas

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

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar **Más>Control de acceso>Alarma**. Configure los

Paso 3 parámetros de alarma y luego haga clic en **Aplicar**.

Figura 4-23 Configuración de alarma

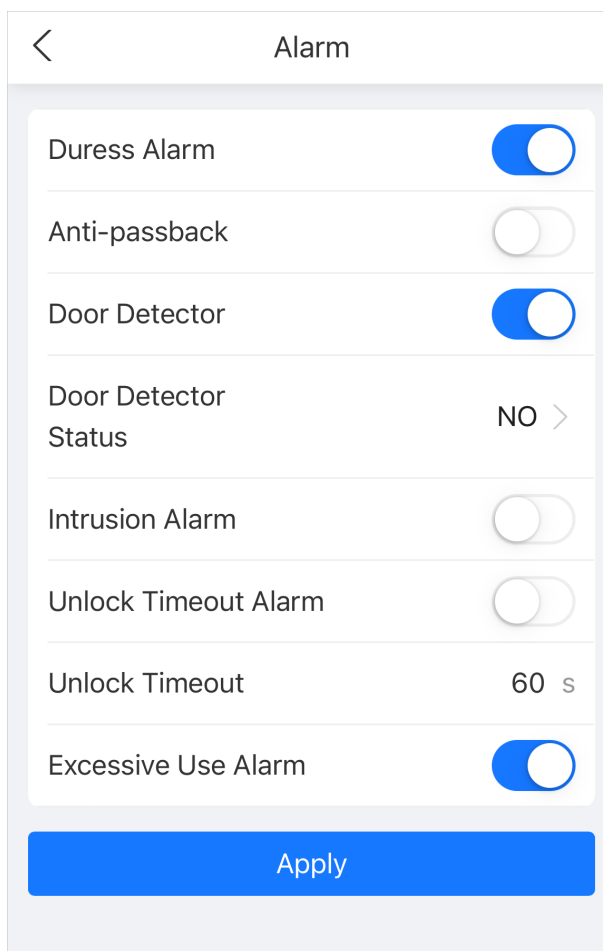





Tabla 4-8 Descripción de los parámetros de alarma

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.



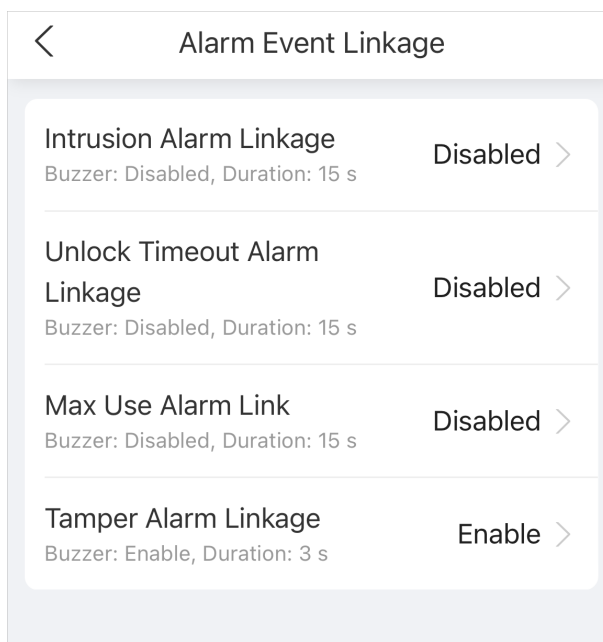
Parámetro	Descripción
Anti-passback	<p>Los usuarios deben verificar su identidad tanto para entrar como para salir; de lo contrario, se activará una alarma. Esto ayuda a evitar que el titular de una tarjeta le pase la tarjeta de acceso a otra persona para poder entrar. Cuando se activa la función antirretorno, 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.</p> <ul style="list-style-type: none"> <li>● 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.</li> <li>● 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.</li> </ul> <p></p> <p>Si el dispositivo solo puede conectar una cerradura, la verificación en el dispositivo significa la dirección de entrada y la verificación en el lector de tarjetas externo significa la dirección de salida de manera predeterminada. Puede modificar la configuración en la plataforma de administración.</p>
Detector de puerta	<p>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.</p> <ul style="list-style-type: none"> <li>● Normalmente cerrado: el sensor está en una posición de cortocircuito cuando la puerta o ventana está cerrada.</li> <li>● Normalmente abierto: se crea un circuito abierto cuando la ventana o puerta está realmente cerrada.</li> </ul>
Alarma de intrusión	<p>Si la puerta se abre de forma anormal, se activará una alarma de intrusión que durará un tiempo definido.</p> <p></p> <p>El detector de puerta y la intrusión deben habilitarse al mismo tiempo.</p>
Alarma de tiempo de espera para desbloqueo	<p>Cuando la puerta permanece desbloqueada durante más tiempo que el tiempo de espera definido, se activará la alarma de tiempo de espera de la puerta y durará el tiempo definido.</p>
Desbloquear tiempo de espera	<p></p> <p>El detector de puerta y la función de tiempo de espera de puerta deben habilitarse al mismo tiempo.</p>
Alarma de uso excesivo	<p>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 un tiempo definido.</p>

## 4.6.5 Configuración de la vinculación de eventos de alarma

### Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Más>Control de acceso>Vinculación de eventos de alarma**.

Figura 4-24 Vinculación de eventos de alarma



- Paso 3** Haga clic en el enlace para configurar el enlace de alarma y luego haga clic en **DE ACUERDO**.

Tabla 4-9 Vinculación de eventos de alarma

Parámetro	Descripción
Vinculación de alarmas de intrusión	Si la puerta se abre de forma anormal, se activará una alarma de intrusión. Timbre: el timbre suena cuando se activa una alarma de intrusión. Puede configurar la duración de la alarma.
Alarma de tiempo de espera para desbloqueo Enlace	Cuando la puerta permanece desbloqueada durante más tiempo que el tiempo de espera definido, se activará la alarma de tiempo de espera de la puerta y durará el tiempo definido. Timbre: el timbre suena cuando se activa la alarma de tiempo de desbloqueo. Puede configurar la duración de la alarma.
Enlace de alarma de uso máximo	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 un tiempo definido. Timbre: el timbre suena cuando se activa la alarma de uso excesivo. Puede configurar la duración de la alarma.

Parámetro	Descripción
Conexión de alarma antimanipulación	La alarma de manipulación se activa cuando alguien intenta dañar físicamente el dispositivo.  Zumbador: el zumbador suena cuando se activa la alarma antimanipulación. Puede configurar la duración de la alarma.

## 4.6.6 Configuración de los ajustes de la tarjeta

### Información de contexto

#### Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Más>Control de acceso>Configuración de la tarjeta**.
- Paso 3** Configure los parámetros de la tarjeta y luego haga clic en **Aplicar**.

Figura 4-25 Configuración de la tarjeta (1)

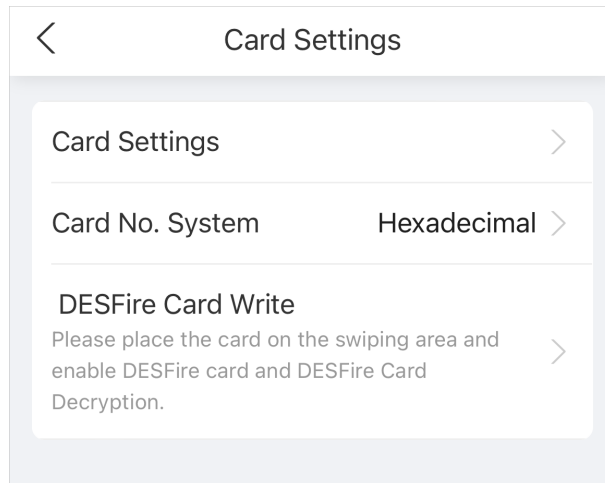


Figura 4-26 Configuración de la tarjeta (2)

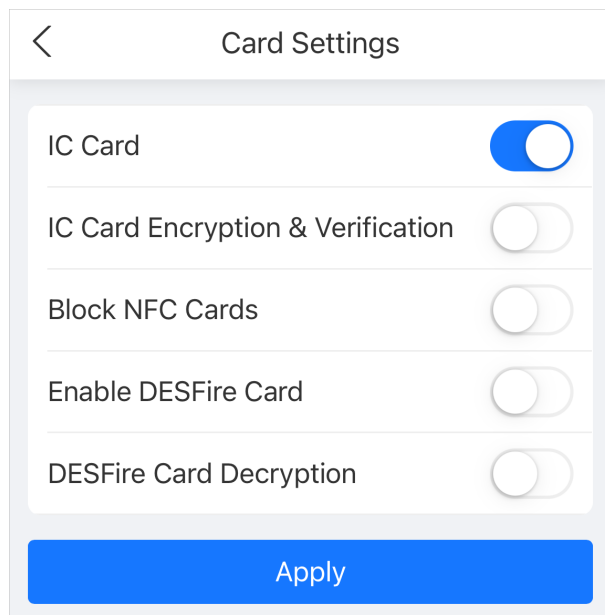








Tabla 4-10 Descripción de los parámetros de la tarjeta

Artículo	Parámetro	Descripción
Configuración de la tarjeta	Tarjeta IC	<p>La tarjeta IC se puede leer cuando esta función está habilitada.</p>  <p>Esta función solo está disponible en modelos seleccionados.</p>
	Cifrado y verificación de tarjetas IC	<p>La tarjeta cifrada se puede leer cuando esta función está habilitada.</p>  <p>Cerciorarse <b>Tarjeta IC</b> está habilitado.</p>
	Bloquear tarjetas NFC	<p>Evitar el desbloqueo mediante tarjeta NFC duplicada después de habilitar esta función.</p>  <ul style="list-style-type: none"> <li>● Esta función sólo está disponible en modelos que admiten tarjetas IC.</li> <li>● Cerciorarse <b>Tarjeta IC</b> está habilitado.</li> <li>● La función NFC solo está disponible en algunos modelos de teléfonos.</li> </ul>
	Habilitar tarjeta Desfire	<p>El dispositivo puede leer el número de tarjeta de la tarjeta Desfire cuando esta función está habilitada.</p>  <ul style="list-style-type: none"> <li>● Esta función sólo está disponible en modelos que admiten tarjetas IC.</li> <li>● Sólo admite formato hexadecimal.</li> </ul>
	Descifrado de la tarjeta Desfire	<p>La información de la tarjeta Desfire se puede leer cuando <b>Habilitar tarjeta Desfire</b> y <b>Descifrado de la tarjeta Desfire</b> se habilitan al mismo tiempo.</p>  <ul style="list-style-type: none"> <li>● Esta función sólo está disponible en modelos que admiten tarjetas IC.</li> <li>● Asegúrese de que la tarjeta Desfire esté habilitada.</li> </ul>
Sistema de Nro. de Tarjeta	Sistema de Nro. de Tarjeta	<p>Seleccione el formato decimal o hexadecimal para el número de tarjeta cuando esté conectado el lector de tarjetas Wiegand. El sistema de número de tarjeta es el mismo tanto para la entrada como para la salida del número de tarjeta.</p>

Artículo	Parámetro	Descripción
Escritura de tarjeta DESFire	Número de tarjeta	<p>Coloque la tarjeta en el lector, ingrese el número de tarjeta y luego haga clic <b>Escribir</b> para escribir el número de tarjeta en la tarjeta.</p>  <ul style="list-style-type: none"> <li>● La función de tarjeta Desfire debe estar habilitada.</li> <li>● Sólo admite formato hexadecimal.</li> <li>● Admite hasta 8 caracteres.</li> </ul>

**Paso 4** Hacer clic **Aplicar**.

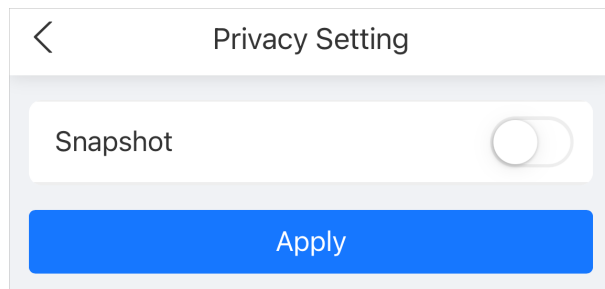
## 4.6.7 Configuración de privacidad

### Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Más>Control de acceso>Configuración de privacidad**
- Paso 3** Habilitar la función de instantánea.

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

Figura 4-27 Habilitar instantánea



**Paso 4** Hacer clic **Aplicar**.

## 4.7 Configuración de comunicación

### 4.7.1 Configuración de TCP/IP

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

### Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Más>Configuración de comunicación>Configuración de red>Protocolo TCP/IP**.
- Paso 3** Configure los parámetros y luego haga clic en **Aplicar**.

Figura 4-28 TCP/IP

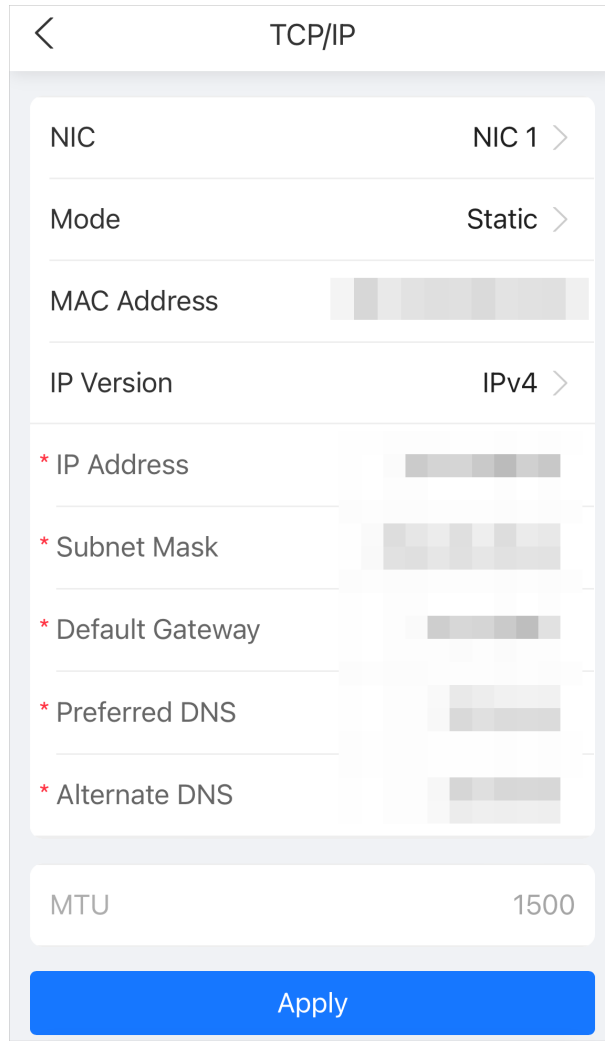



Tabla 4-11 Descripción de TCP/IP

Parámetro	Descripción
Modo	<ul style="list-style-type: none"> <li>● Estático: ingrese manualmente la dirección IP, la máscara de subred y la puerta de enlace.</li> <li>● DHCP: Significa Protocolo de configuración dinámica de host. Cuando se activa el DHCP, se le asignará automáticamente al dispositivo una dirección IP, una máscara de subred y una puerta de enlace.</li> </ul>
Dirección MAC	Dirección MAC del dispositivo.
Versión IP	IPv4 o IPv6.
Dirección IP	Si configura el modo en <b>Estático</b> , configure la dirección IP, la máscara de subred y la puerta de enlace.
Máscara de subred	
Puerta de enlace predeterminada	 <ul style="list-style-type: none"> <li>● La dirección IPv6 se representa en hexadecimal.</li> <li>● La versión IPv6 no requiere configurar máscaras de subred.</li> <li>● La dirección IP y la puerta de enlace predeterminada deben estar en el mismo segmento de red.</li> </ul>

Parámetro	Descripción
DNS preferido	Establezca la dirección IP del servidor DNS preferido.
DNS alternativo	Establecer la dirección IP del servidor DNS alternativo.
Unidad de medida máxima	<p>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:</p> <ul style="list-style-type: none"> <li>● 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.</li> <li>● 1492: Valor óptimo para PPPoE</li> <li>● 1468: Valor óptimo para DHCP.</li> <li>● 1450: Valor óptimo para VPN.</li> </ul>

## 4.7.2 Configuración de Wi-Fi

### Procedimiento

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

**Paso 2** Seleccionar **Más > Configuración de comunicación > Wifi**.

**Paso 3** Encienda el Wi-Fi.

Se muestran todas las conexiones WiFi disponibles.



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

**Paso 4** Haga clic en Wi-Fi y luego ingrese la contraseña.

El wifi está conectado.

### Operaciones relacionadas

- DHCP: Seleccione el **DHCP** modo y haga clic **Aplicar**, al dispositivo se le asignará automáticamente una dirección Wi-Fi.
- Estático: Seleccione el **Estático** modo, ingrese manualmente una dirección Wi-Fi y luego haga clic en **Aplicar**, el dispositivo se conectará al Wi-Fi.

## 4.7.3 Configuración del punto de acceso Wi-Fi

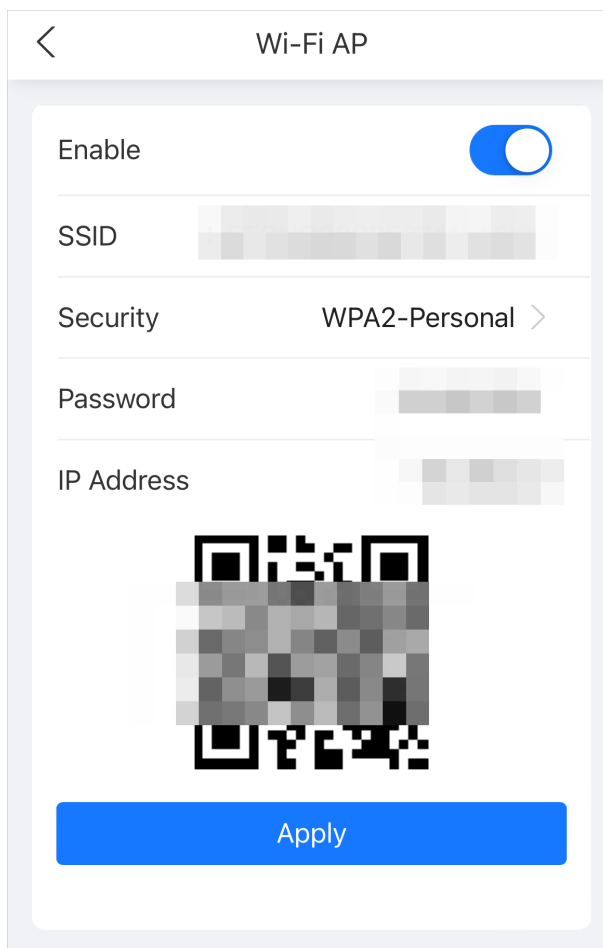


- La función Wi-Fi está disponible en modelos seleccionados.
- No se pueden habilitar Wi-Fi y Wi-Fi AP al mismo tiempo.

## Procedimiento

- Paso 1 Inicie sesión en la página web.
- Paso 2 Seleccionar **Más**>**Configuración de comunicación**>**Punto de acceso**
- Paso 3 **wifi**Habilite la función y luego haga clic en**Aplicar**.

Figura 4-29 Punto de acceso Wi-Fi



## 4.7.4 Configuración del servicio en la nube

### Procedimiento

- Paso 1 Inicie sesión en la página web.
- Paso 2 Seleccionar **Más**>**Configuración de comunicación**>**Servicio en la nube**.
- Paso 3 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. Haga clic**Aplicar**.
- Paso 4 clic**Aplicar**.

## 4.7.5 Configuración del registro automático

### Procedimiento

- Paso 1 Inicie sesión en la página web.
- Paso 2 Seleccionar **Más**>**Configuración de red**>**Registro automático**.



**Paso 3** Habilite la función de registro automático, configure los parámetros y luego haga clic en **Aplicar**.

Figura 4-30 Registro automático

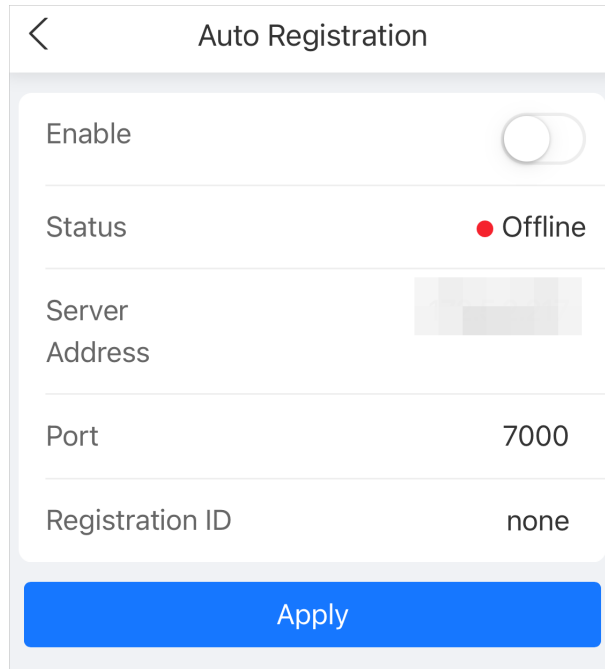


Tabla 4-12 Descripción del registro automático

Parámetro	Descripción
Estado	Muestra el estado de la conexión del registro automático.
Dirección del servidor	La dirección IP o el nombre de dominio del servidor.
Puerto	El puerto del servidor que se utiliza para el registro automático.
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.

## 4.7.6 Configuración de Wiegand

### Procedimiento

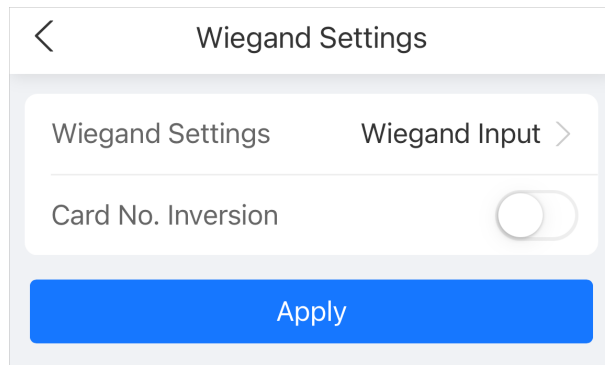
- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Más > Configuración de comunicación > Wiegand**.
- Paso 3** Seleccione un tipo de Wiegand, configure los parámetros y luego haga clic en **Aplicar**.

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



Cuando el dispositivo se conecta a un dispositivo de terceros a través del puerto de entrada Wiegand y el número de tarjeta leído por el dispositivo está en orden inverso al número de tarjeta real, en este caso puede activar **Tarjeta N° Inversión** función.

Figura 4-31 Entrada Wiegand



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

Figura 4-32 Salida Wiegand

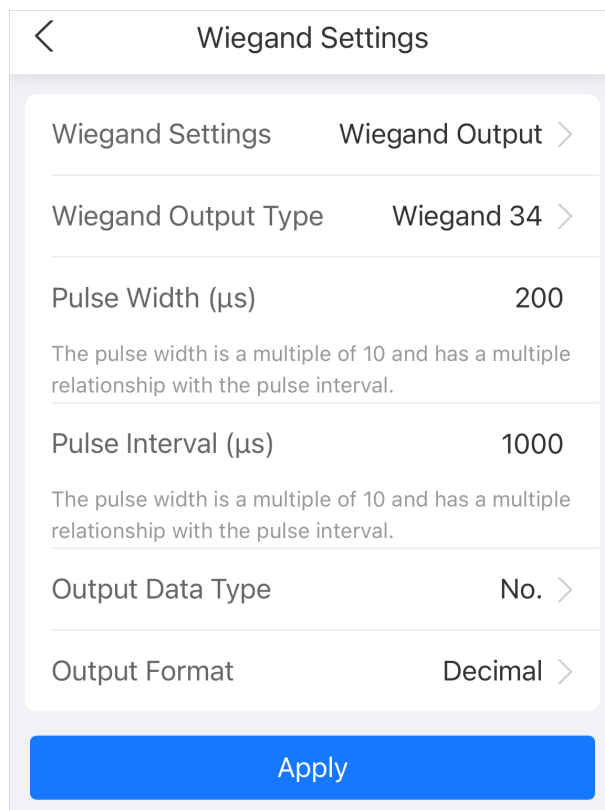


Tabla 4-13 Descripción de la salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	Seleccione un formato Wiegand para leer números de tarjetas o números de identificación. <ul style="list-style-type: none"> <li>◇ <b>Wiegand26:</b> Lee 3 bytes o 6 dígitos.</li> <li>◇ <b>Wiegand34:</b> Lee 4 bytes u 8 dígitos.</li> <li>◇ <b>Wiegand66:</b> Lee 8 bytes o 16 dígitos.</li> </ul>
Ancho de pulso	Introduzca el ancho de pulso y el intervalo de pulso de la salida Wiegand.
Intervalo de pulso	

Parámetro	Descripción
Tipo de datos de salida	<p>Seleccione el tipo de datos de salida.</p> <ul style="list-style-type: none"> <li>◇ <b>No.:</b> Genera datos en función del ID del usuario. El formato de los datos es hexadecimal o decimal.</li> <li>◇ <b>Número de tarjeta:</b> Genera datos basados en el primer número de tarjeta del usuario.</li> </ul>

## 4.7.7 Configuración de RS-485

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

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Más > Configuración de comunicación > Configuración RS-485**.
- Paso 3** Configure los parámetros y luego haga clic en **Aplicar**.

Figura 4-33 Configuración RS-485

The screenshot shows the 'RS-485 Settings' interface. It features a list of configuration items, each with a right-pointing chevron indicating it is a dropdown menu. The settings are: External Device (Access Controller), Baud Rate (9600), Data Bit (8), Stop Bit (1), Parity Code (None), and Output Data Type (No.). At the bottom of the screen is a blue 'Apply' button.

Tabla 4-14 Descripción de los parámetros RS-485

Parámetro	Descripción
Dispositivo externo	<ul style="list-style-type: none"> <li>● Controlador de acceso Seleccionar <b>Controlador de acceso</b> cuando el dispositivo funciona como un lector de tarjetas y envía datos a otros controladores de acceso externos para controlar el acceso.</li> <li>● Lector de tarjetas: el dispositivo funciona como un controlador de acceso y se conecta a un lector de tarjetas externo.</li> <li>● Lector (OSDP): El dispositivo está conectado a un lector de tarjetas basado en el protocolo OSDP.</li> <li>● 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.</li> </ul>
Tasa de Baud	Seleccione la velocidad en baudios. La predeterminada es 9600.
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.
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.
Tipo de datos de salida	<p>Cuando configura el dispositivo externo como <b>Controlador de acceso</b>.</p> <ul style="list-style-type: none"> <li>● 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.</li> <li>● No.: Genera datos en función del ID del usuario.</li> </ul>

## 4.8 Configuración de indicaciones de audio

Establecer indicaciones de audio durante la verificación de identidad.

### Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Más > Configuración de audio y video > Audio**.
- Paso 3** Configure los parámetros de audio y luego haga clic en **Aplicar**.

Figura 4-34 Configurar los parámetros de audio

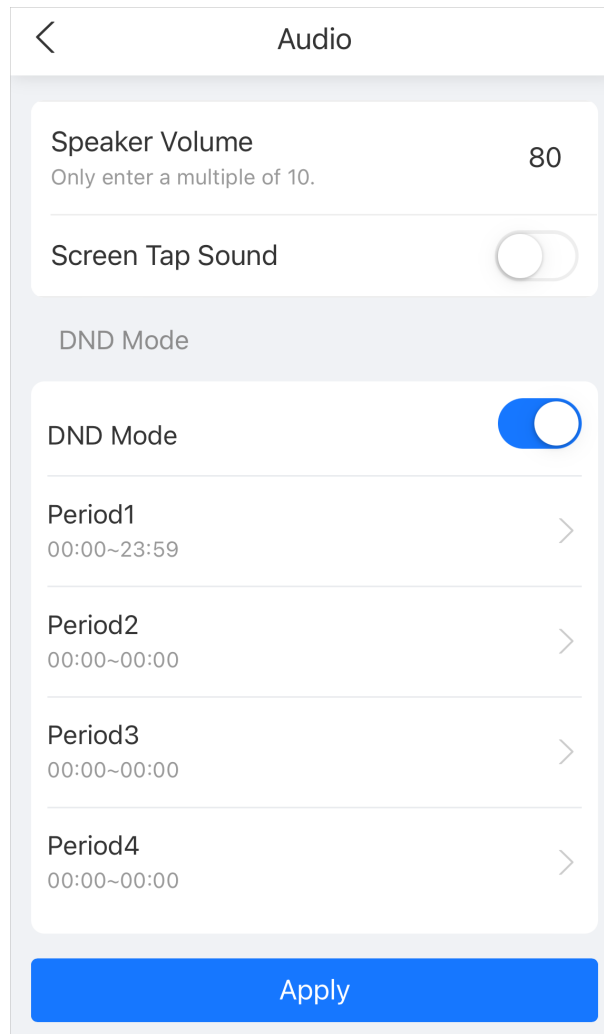


Tabla 4-15 Descripción de parámetros

Parámetros	Descripción
Volumen del altavoz	Configurar el volumen del altavoz.
Sonido al tocar la pantalla	Cuando esta función está habilitada, el dispositivo producirá sonido al presionar el botón.
Modo DND	No se escucharán mensajes de voz durante el tiempo establecido cuando verifique su identidad en el dispositivo. Puede configurar hasta 4 períodos.

## 4.9 Visualización de registros

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

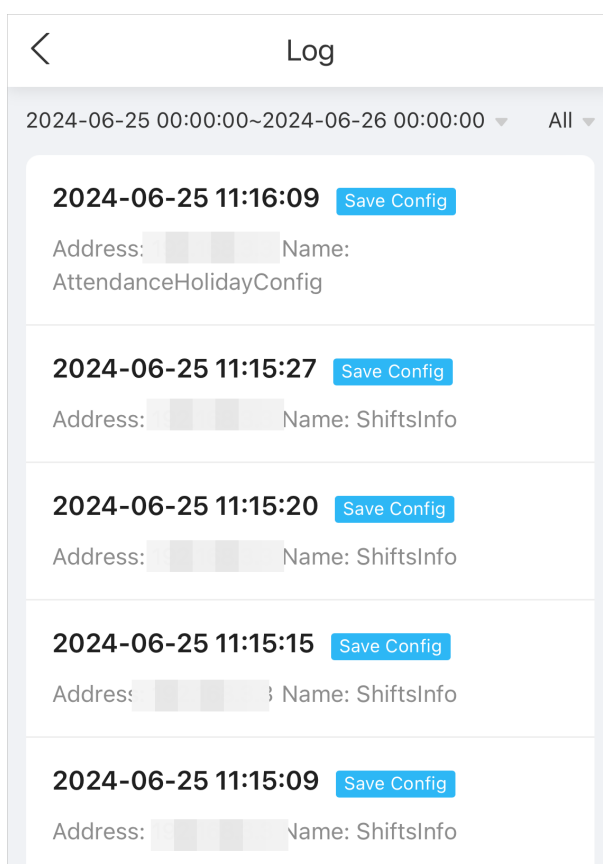
### 4.9.1 Registros del sistema

Ver y buscar registros del sistema.

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccione **Más>Registro>Registro**.

Figura 4-35 Registros



### 4.9.2 Desbloquear registros

Buscar registros de desbloqueo.

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Más>Registro>Desbloquear registros**.
- Paso 3** Haga clic en el registro para ver los detalles.

### 4.9.3 Registros de alarmas

Ver registros de alarmas.

#### Procedimiento

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

Paso 2 **Registro**>**Registro de alarmas**.

## 5. Configuración inteligente de PSS Lite

En esta sección se explica cómo administrar y configurar el dispositivo a través de Smart PSS Lite. Para obtener más información, consulte el manual del usuario de Smart PSS Lite.

### 5.1 Instalación e inicio de sesión

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

#### Procedimiento

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

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



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

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

### 5.2 Agregar dispositivos

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

#### 5.2.1 Agregar dispositivos uno por uno

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

#### Procedimiento

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

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



Figura 5-1 Agregar dispositivos

Tabla 5-1 Parámetros de adición de IP

Parámetro	Descripción
Nombre del dispositivo	Le recomendamos que nombre los dispositivos con el área de monitoreo para una fácil identificación.
Método para agregar	<p>Seleccionar <b>IP/Dominio</b>.</p> <ul style="list-style-type: none"> <li>● IP/Dominio: Ingrese la dirección IP o el nombre de dominio del dispositivo.</li> <li>● SN: Ingrese el número de serie del dispositivo.</li> </ul>
Puerto	Ingrese el número de puerto. El número de puerto predeterminado es 37777. El número de puerto real puede variar según los distintos modelos.
Nombre de usuario	Introduzca el nombre de usuario del dispositivo.
Contraseña	Introduzca la contraseña del dispositivo.

**Paso 3** Hacer clic **Agregar**.

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

## 5.2.2 Agregar dispositivos en lotes

### Información de contexto



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

## Procedimiento

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

**Paso 2** Seleccione un método de búsqueda.

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



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

Figura 5-2 Búsqueda de dispositivos

The screenshot shows the 'Auto Search' window with the following details:

- Search Method:** Auto Search (selected), Device Segment: 10.0.0.1 - 10.0.0.255
- Search Device Number:** 59
- Table of Found Devices:**

No.	IP	Device Type	MAC Address	Port	Initialization Status
1	10.0.0.5	...	3c:e3:...:d3	37777	Initialized
2	10.0.0.5	...	e4:24:...:41	37777	Initialized
3	10.0.0.0	...	3c:e3:...:df	37777	Initialized
4	10.0.0.3	...	fc:b6:...:60	37777	Initialized
5	10.0.0.4	...	f4:b1:...:24	37777	Initialized
6	10.0.0.6	...	3c:e3:...:38	37777	Initialized
7	10.0.0.8	...	c0:39:...:61	37777	Initialized
8	10.0.0.1	...	c0:39:...:7fc	37777	Initialized
- Buttons:** Add, Cancel

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

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

## Resultados

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

Figura 5-3 Dispositivos añadidos

The screenshot shows the 'All Device' list with the following data:

No.	Name	IP	Device Type	Device Model	Port	Channel Number	Online Status	SN	Operation
1	10.0.0.73	10.0.0.3	N/A	N/A	37777	0/0/0/0	Offline (Ca...	N/A	[Edit] [Refresh] [Delete]
2	10.0.0.07	10.0.0.7	VTO	...	37777	2/0/10/2	Online	8D0...C74	[Edit] [Refresh] [Delete]
3	10.0.0.08	10.0.0.8	Apartment VTO	...S2	37777	1/0/5/1	Offline	9B0...CEB	[Edit] [Refresh] [Delete]
4	10.0.0.11	10.0.0.11	VTS	...	37777	0/0/10/2	Offline	8D0...E1D	[Edit] [Refresh] [Delete]
5	10.0.0.15	10.0.0.15	IPC	D...HR	37777	1/0/2/1	Online	8M0...7FAB	[Edit] [Refresh] [Delete]

## 5.3 Gestión de usuarios

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

### 5.3.1 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** luego seleccione un tipo de tarjeta.



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

**Paso 4** Hacer clic **DE ACUERDO**.

### 5.3.2 Agregar usuarios

#### 5.3.2.1 Agregar usuarios uno por uno

Procedimiento

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

**Paso 2** Ingrese información básica del personal.

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



- El número de tarjeta se puede leer automáticamente o completar manualmente. Para leer automáticamente el número de tarjeta, seleccione el lector de tarjetas junto a **Tarjeta Nro.**, y luego coloque la tarjeta en el lector de tarjetas. El número de tarjeta se leerá automáticamente.

- Puede seleccionar varias cámaras USB para tomar fotografías.

- Establecer contraseña


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

- Configurar tarjeta

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

b. Agregar tarjetas.

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

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



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

- Configurar huella digital


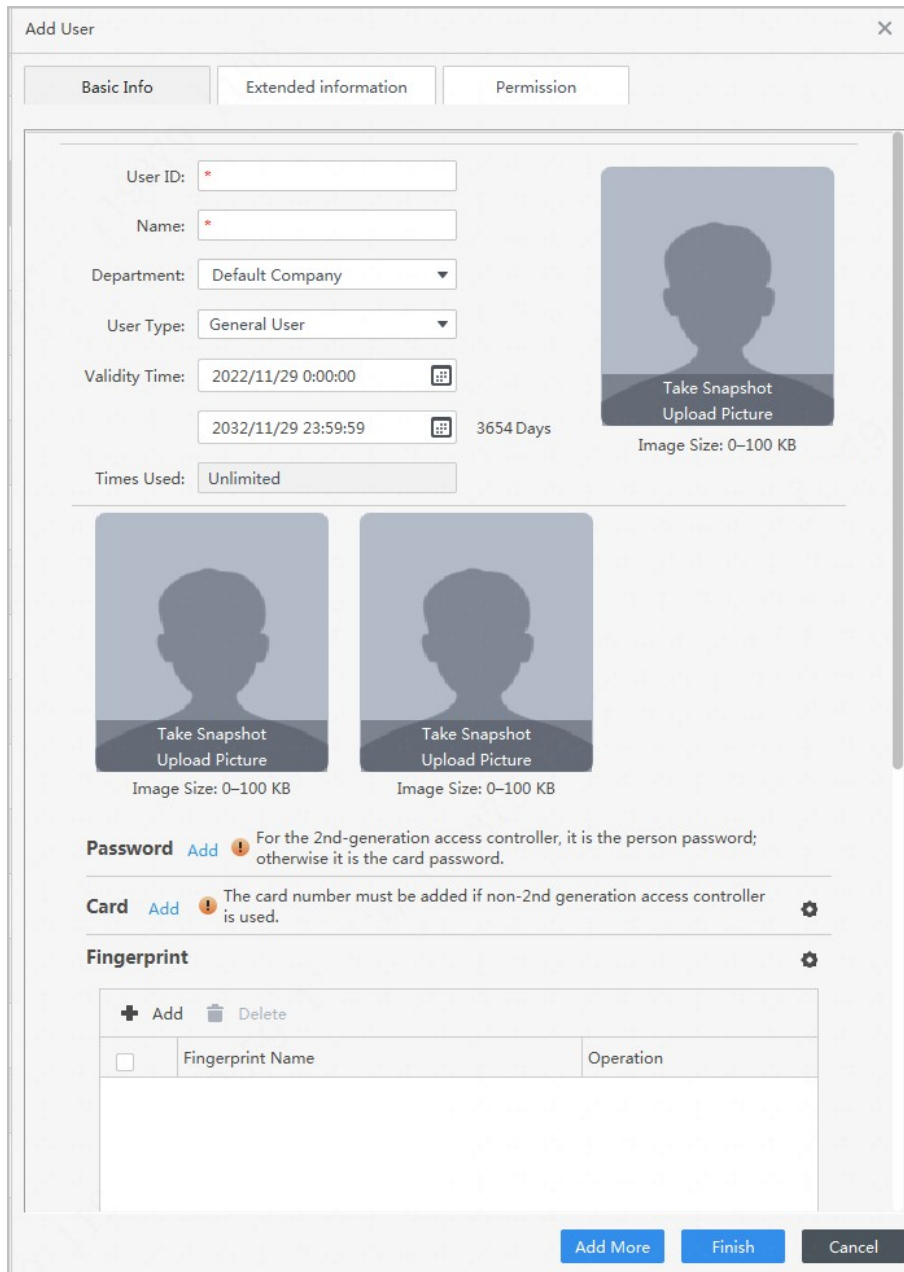
- a. Haga clic  para seleccionar **Dispositivo Escáner de huellas dactilares** como recolector de huellas dactilares.
- b. Agregar huella digital. Seleccionar **Agregar > Agregar huella digital** y luego presione el dedo sobre el escáner tres veces seguidas.

Figura 5-4 Agregar información básica



The screenshot shows the 'Add User' dialog box with the following fields and options:

- User ID:** \* (required)
- Name:** \* (required)
- Department:** Default Company (dropdown)
- User Type:** General User (dropdown)
- Validity Time:** 2022/11/29 0:00:00 to 2032/11/29 23:59:59 (3654 Days)
- Times Used:** Unlimited
- Image Upload:** One large image slot and two smaller slots, each with 'Take Snapshot' and 'Upload Picture' buttons. Image size limit: 0-100 KB.
- Password:** Add (warning icon) For the 2nd-generation access controller, it is the person password; otherwise it is the card password.
- Card:** Add (warning icon) The card number must be added if non-2nd generation access controller is used.
- Fingerprint:** Add (warning icon)
- Fingerprint Table:**

<input type="checkbox"/>	Fingerprint Name	Operation

Buttons at the bottom: Add More, Finish, Cancel.

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



Figura 5-5 Agregar información extendida

The screenshot shows a software window titled "Add User" with a close button (X) in the top right corner. The window has three tabs: "Basic Info", "Extended information" (which is selected), and "Permission". Under the "Extended information" tab, there is a "Details" section with the following fields and controls:

- Gender: Radio buttons for "Male" (selected) and "Female".
- Title: A dropdown menu showing "Mr".
- Date of Birth: A date picker showing "1985/3/15".
- Tel: An empty text input field.
- Email: An empty text input field.
- Mailing Address: An empty text input field.
- Administrator: A toggle switch currently turned off.
- Remark: A large empty text area.
- ID Type: A dropdown menu showing "ID".
- ID No.: An empty text input field.
- Company: An empty text input field.
- Occupation: An empty text input field.
- Employment Date: A date-time picker showing "2022/11/28 19:38:45".
- Termination Date: A date-time picker showing "2032/11/29 19:38:45".

At the bottom right of the window, there are three buttons: "Add More" (blue), "Finish" (blue), and "Cancel" (grey).

**Paso 4** Configurar permisos.

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

**Paso 5** Configurar permisos. Para obtener más información, consulte "5.3.3 Asignación de permisos de acceso".

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

Figura 5-6 Configurar grupos de permisos

Add Permission Group

Basic Info

Group Name: Permission Group4

Remark:

Time Templ...: Full-day Time Te

Verification Method:  Card  Fingerprint  Password  Face

All Device

Selected (1)

Search..

- Default Group
  - 172.16.0.140
    - Door 1

172.16.0.140-Door 1

OK Cancel

**Paso 6** Hacer clic **Finalizar**.



Después de completar la adición, puede hacer clic en el



Para modificar información o agregar detalles en la lista

personal.

### 5.3.2.2 Agregar usuarios en lotes

Procedimiento

- Paso 1 Hacer clic **Gerente de personal** > **Actualización por lotes** > **Agregar por lotes**.
- Paso 2 Seleccionar **Emisor de la tarjeta** o **Dispositivo** desde **Dispositivo** lista y luego configure los parámetros.

Figura 5-7 Agregar usuarios en lotes

Batch Add

Device: Card Issuer Read C...

Start No.: \* 3789 Quantity: \* 20

Department: Default Company

Validity Period: 2023/9/25 0:00:00 Expiration Time: 2029/9/25 23:59:59

Issue Card

ID	Card No.
3789	
3790	
3791	
3792	
3793	
3794	
3795	
3796	
3797	
3798	
3799	

OK Cancel

Tabla 5-2 Parámetros para agregar usuarios en lotes

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

**Paso 3** Hacer clic **Leer la tarjeta n.º** y pase las tarjetas por el lector de tarjetas.

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

**Paso 4 ACUERDO.**

### 5.3.3 Asignación de permisos de acceso

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

Procedimiento

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

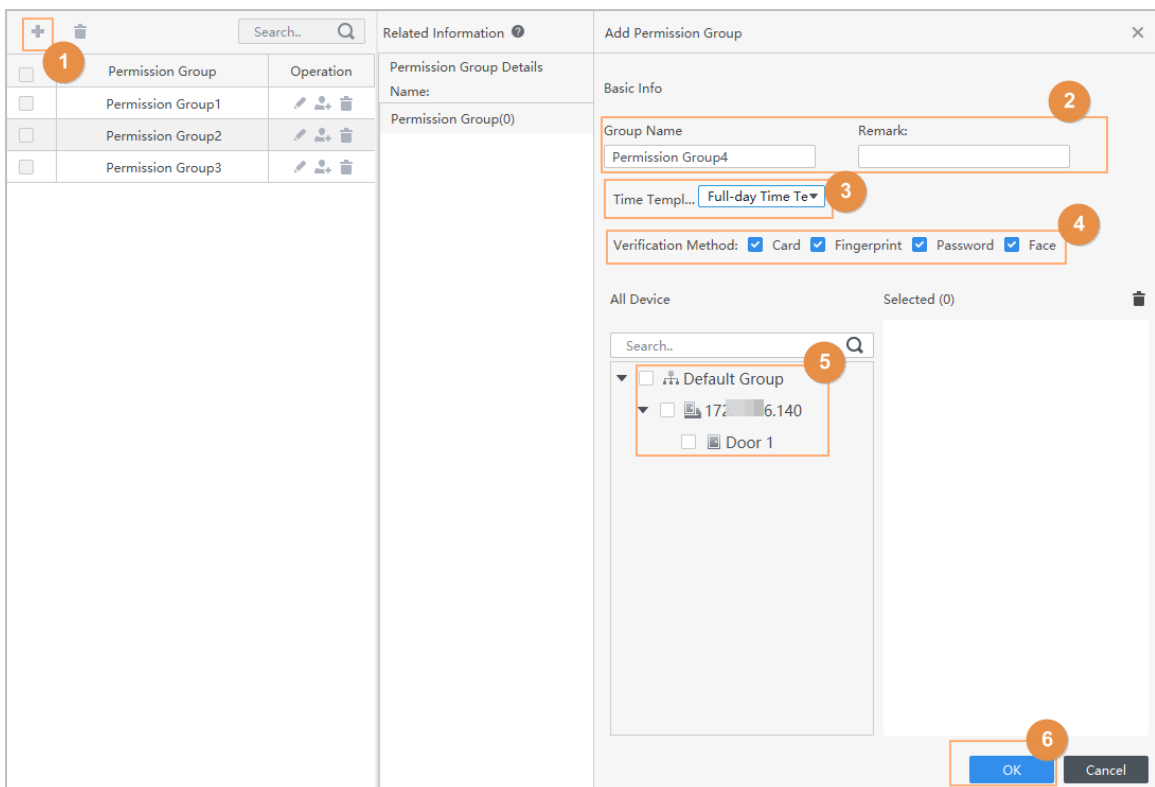
**Paso 2** Haga clic **en**.

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

**Paso 4** Seleccione los métodos de verificación y las puertas.

**Paso 5** Hacer clic **DE ACUERDO.**

Figura 5-8 Crear un grupo de permisos

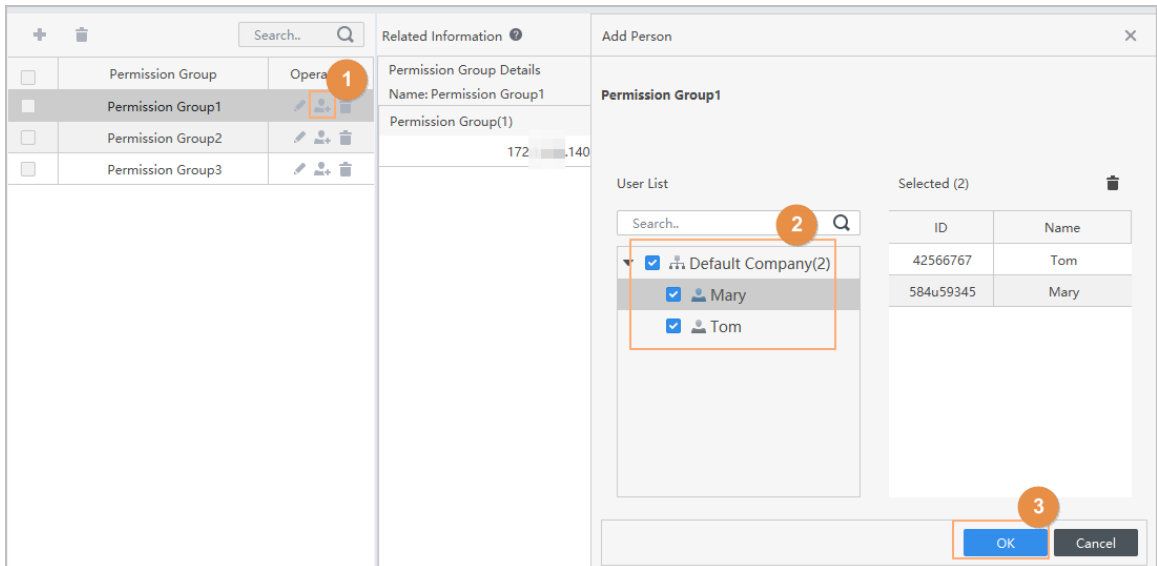


**Paso 6** Hacer clic **del grupo de permisos.**



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

Figura 5-9 Agregar usuarios a un grupo de permisos



**Paso 8** Hacer clic **DE ACUERDO**.

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

## 5.3.4 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**.

**Paso 3** Haga clic 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 5-10 Crear un grupo de permisos

Add Access Group

Basic Info

Group Name: Remark:

Permission Group3

Time Template: All Day Time Template

All Device Selected (0)

Search..

Default Group

1 3


Door 1

OK Cancel



- El control de tiempo y asistencia permite el registro de entrada y salida mediante contraseña, reconocimiento facial, tarjeta y huella digital.
- La asistencia con tarjeta y huella digital está disponible en modelos selectos.

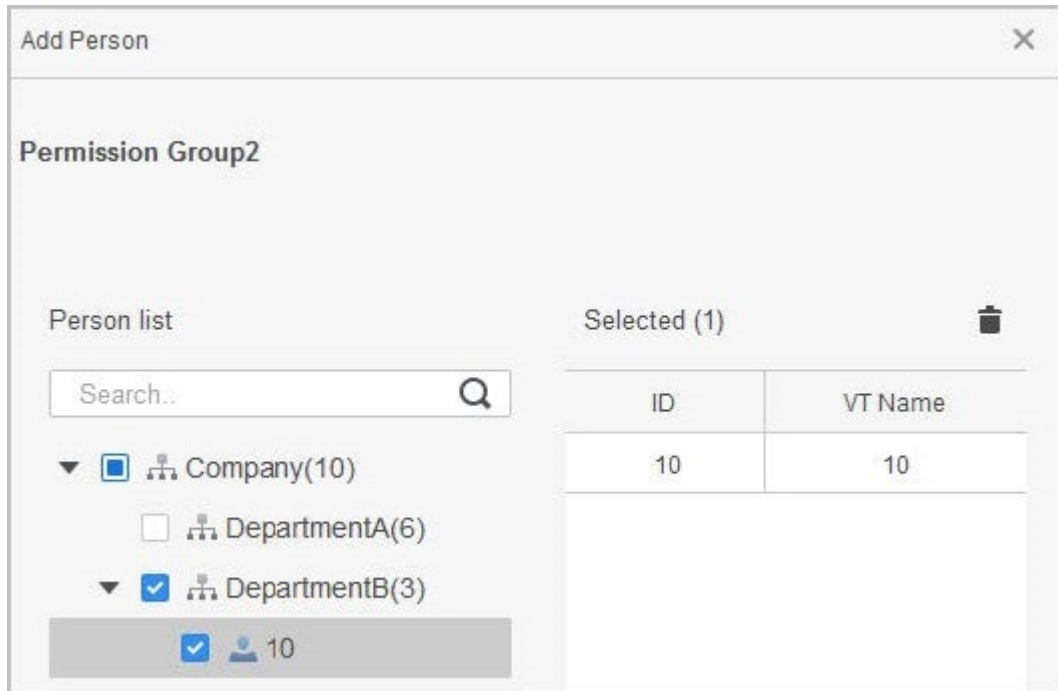
**Paso 7**

Hacer clic  del grupo de permisos que agregó.

**Paso 8**

Seleccione usuarios para asociarlos con el grupo de permisos.

Figura 5-11 Agregar usuarios a un grupo de permisos



**Paso 9** Hacer clic **DE ACUERDO**.

## 5.4 Gestión de acceso

### 5.4.1 Apertura y cierre remoto de la puerta

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

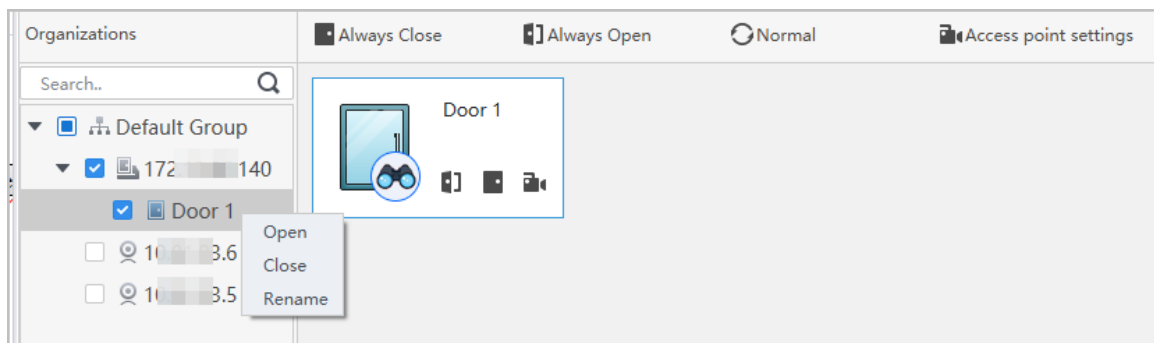
Procedimiento

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

**Paso 2** Controla la puerta de forma remota.

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

Figura 5-12 Puerta abierta



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

## Operaciones relacionadas

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

## 5.4.2 Configuración de Siempre abierto y Siempre cerrado

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

### Procedimiento

- Paso 1** Hacer clic **Solución de acceso > Administrador de acceso** En la página de inicio, haga clic en **Siempre abierto** o **Siempre cerca** para abrir o cerrar la puerta.
- Paso 2**

Figura 5-13 Siempre abierto o cerrado



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

## 5.4.3 Monitoreo del estado de la puerta

### Procedimiento

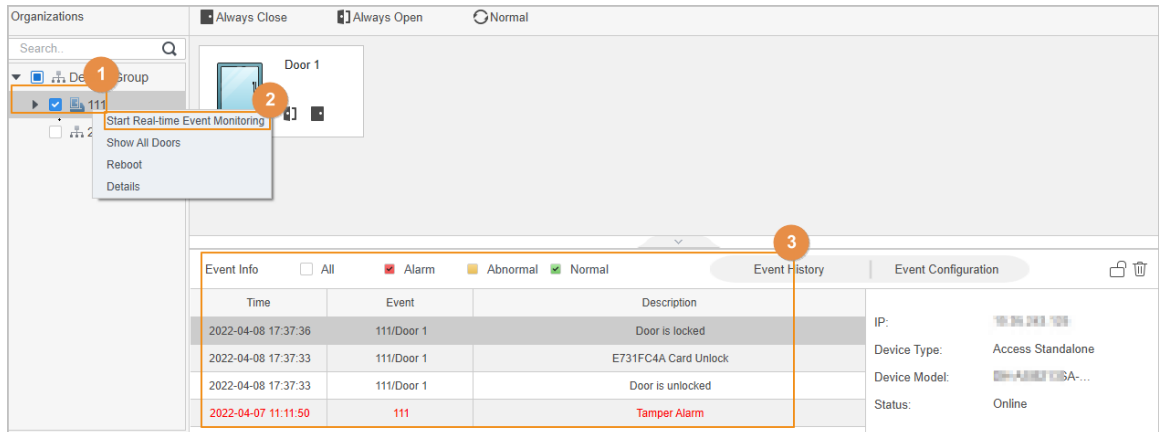
- Paso 1** Hacer clic **Solución de acceso > Administrador de acceso** en la página de inicio.
- Paso 2** Seleccione el dispositivo en el árbol de dispositivos, haga clic derecho en el dispositivo y luego seleccione **Iniciar el monitoreo de eventos en tiempo real**.

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



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

Figura 5-14 Estado de la puerta del monitor



### Operaciones relacionadas

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

# Apéndice 1 Puntos importantes del rostro

## Registro

### Antes de la inscripción

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

### Durante el registro

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



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

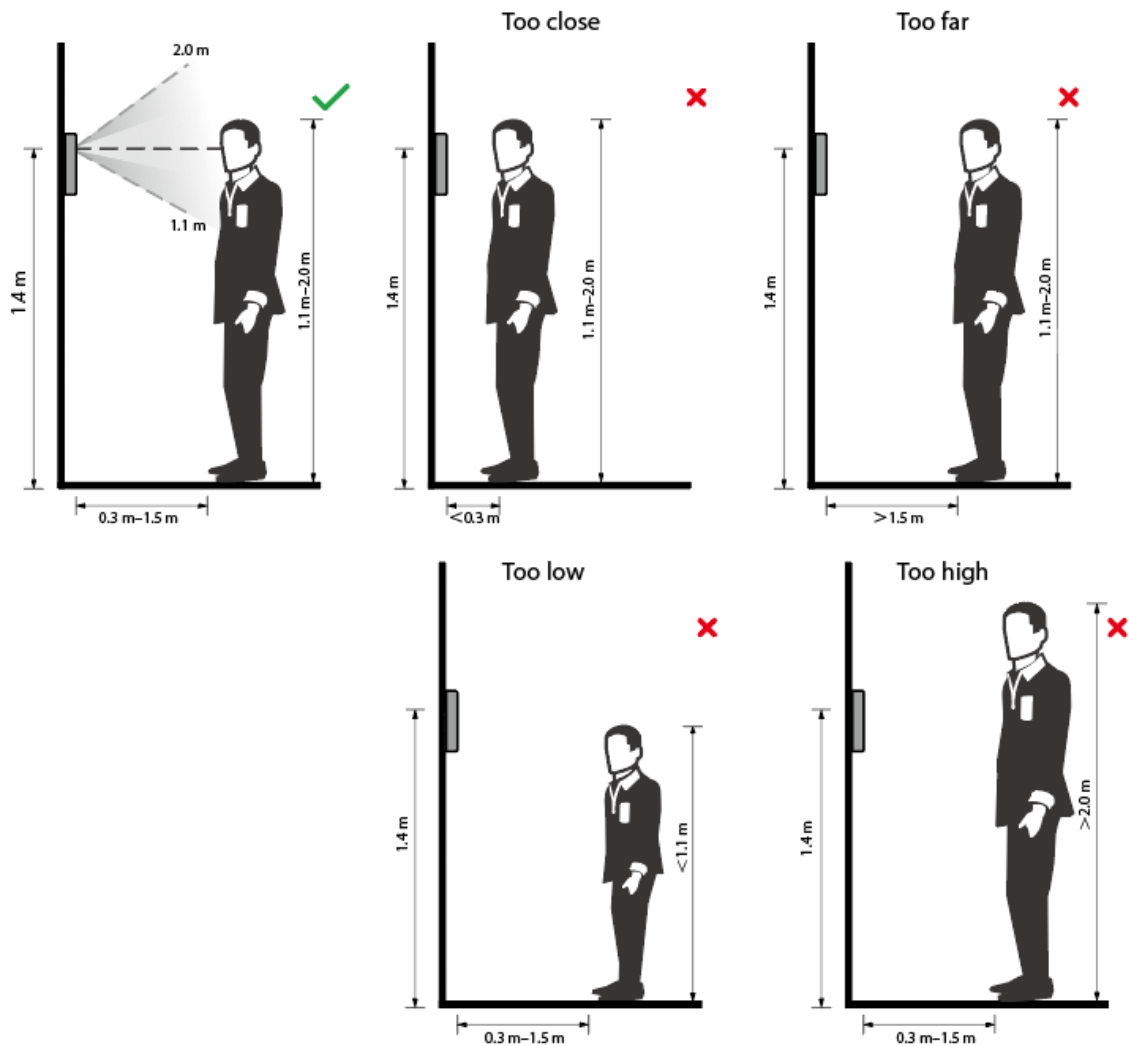
### Posición de la cara

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



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

Apéndice Figura 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 mascarillas, gafas, sombreros, barbas pobladas u 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 use mascarillas y no mantenga su rostro demasiado cerca o demasiado lejos de la cámara.

Apéndice Figura 1-2 Posición de la cabeza





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



## Apéndice 2 Puntos importantes de la toma de huellas dactilares

# Instrucciones de registro

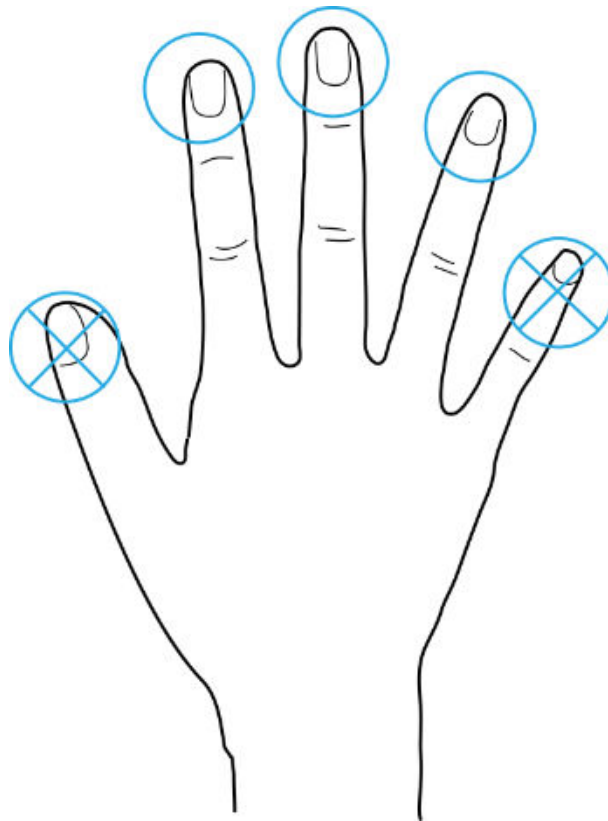
Al registrar la huella dactilar, preste atención a los siguientes puntos:

- 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

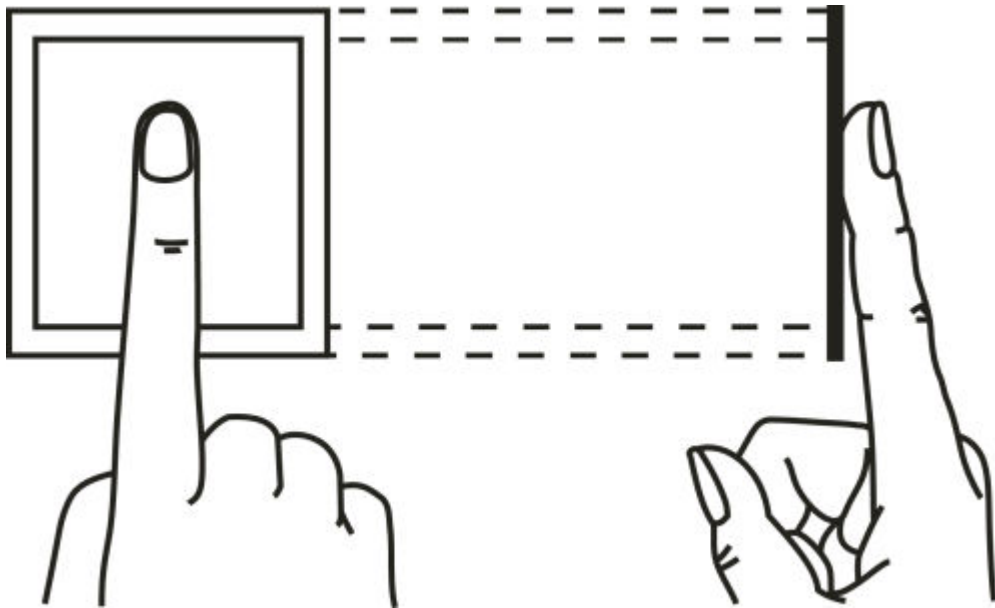
Se recomiendan los dedos índice, medio y anular. Los pulgares y meñiques no se pueden colocar fácilmente en el centro de la grabación.

Apéndice Figura 2-1 Dedos recomendados

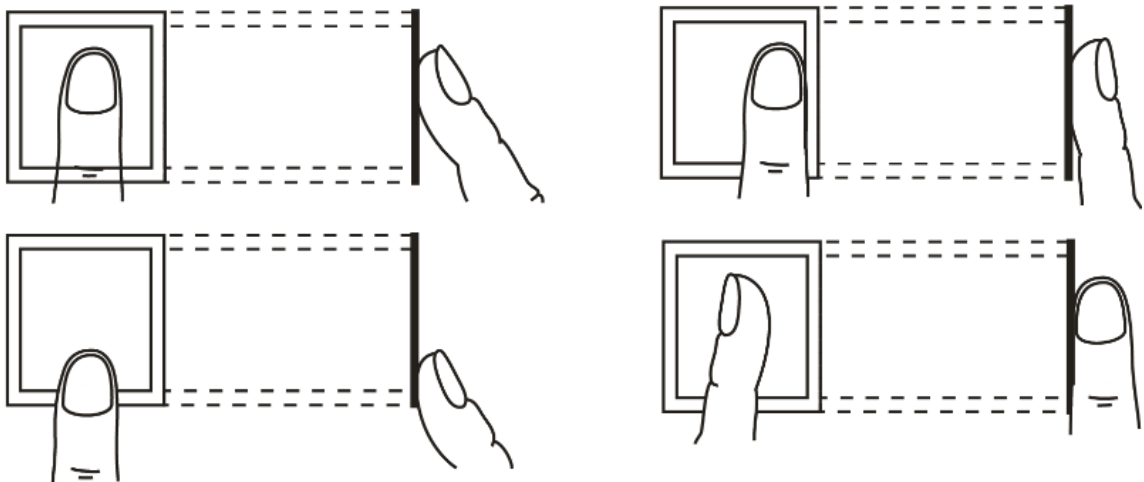


# Cómo presionar su huella digital en el escáner

Apéndice Figura 2-2 Colocación correcta



Apéndice Figura 2-3 Colocación incorrecta



# Apéndice 3 Recomendaciones de seguridad

## Gestión de cuentas

### 1. Utilice contraseñas complejas

Consulte las siguientes sugerencias para establecer contraseñas:

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

### 2. Cambie las contraseñas periódicamente

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

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

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

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

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

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

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

## Configuración del servicio

### 1. Habilitar HTTPS

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

### 2. Transmisión cifrada de audio y vídeo

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

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

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

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

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

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

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

## Configuración de red

### 1. Habilitar lista de permitidos

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

### 2. Vinculación de dirección MAC

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

### 3. Construir un entorno de red seguro

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

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

## Auditoría de seguridad

### 1. Comprobar usuarios en línea

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

### 2. Comprobar el registro del dispositivo

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

### 3. Configurar el registro de red

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

## Seguridad del software

### 1. Actualizar el firmware a tiempo

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

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

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

## Protección física

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

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