

Controlador de acceso de reconocimiento facial y terminal de reconocimiento facial

Manual de usuario



Prefacio

General

Este manual presenta las funciones y operaciones del controlador de acceso de reconocimiento facial y la terminal de reconocimiento facial (en lo sucesivo, el "Dispositivo"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Significado
 DANGER	Indica un peligro de alto 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, reducción del rendimiento o resultados impredecibles.
 TIPS	Proporciona métodos para ayudarlo a resolver un problema o ahorrar tiempo.
 NOTE	Proporciona información adicional como suplemento al texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.1	Actualizado el manual.	marzo 2023
V1.0.0	Primer lanzamiento.	junio 2022

Aviso de protección de privacidad

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

Sobre el Manual

- El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas sufridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y reglamentos de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, use nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Se pueden encontrar 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 dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Por favor

póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.

- Puede haber errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, póngase en contacto con el proveedor o con el servicio de atención al cliente si se produce algún problema durante el uso del dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho de la 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 cuando lo use.

Requisito de transporte



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

Requisito de almacenamiento



Guarde el dispositivo en condiciones de humedad y temperatura permitidas.

requerimientos de instalación



WARNING

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



- El personal que trabaje en alturas 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 en 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 gabinete proporcionada por el fabricante.
- Utilice los cables de alimentación recomendados para la región y cumpla con las especificaciones de potencia nominal.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en el estándar IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de la fuente de alimentación están sujetos a la etiqueta del dispositivo.
- 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 protección a tierra.

Requisitos de operación



- Compruebe si la fuente de alimentación es correcta antes de usar.
- No desconecte el cable de alimentación del lateral del dispositivo mientras el adaptador está encendido.
- Opere el dispositivo dentro del rango nominal de entrada y salida de energía.
- Utilice el dispositivo en 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 en el Dispositivo para evitar que el líquido fluya hacia él.

- No desmonte el dispositivo sin instrucción profesional.

Tabla de contenido

Prefacio.....	I
Medidas de seguridad y advertencias importantes.....	III
1. Introducción.....	1
2 operaciones locales.....	2
2.1 Procedimiento de configuración básica.....	2
2.2 Iconos comunes.....	2
2.3 Inicialización.....	2
2.4 Pantalla de espera.....	3
2.5 Iniciar sesión.....	5
2.6 Red de comunicación.....	6
2.6.1 Configuración de IP.....	6
2.6.2 Registro activo.....	7
2.6.3 Configuración de WiFi.....	8
2.6.4 Configuración del puerto serie.....	8
2.6.5 Configuración de Wiegand.....	9
2.7 Gestión de usuarios.....	10
2.7.1 Adición de nuevos usuarios.....	10
2.7.2 Visualización de la información del usuario.....	12
2.7.3 Configuración de la contraseña de administrador.....	12
2.8 Gestión de acceso.....	13
2.8.1 Configuración de combinaciones de desbloqueo.....	13
2.8.2 Configuración de desbloqueo por período.....	14
2.8.3 Configuración de combinación de grupos.....	15
2.8.4 Desbloqueo por control de temperatura.....	dieciséis
2.8.5 Configuración de alarma.....	17
2.8.6 Configuración del estado de la puerta.....	19
2.8.7 Configuración del tiempo de retención de bloqueo.....	19
2.9 Gestión de períodos.....	19
2.9.1 Período de configuración.....	19
2.9.2 Configuración de grupos de vacaciones.....	19
2.9.3 Configuración del plan de vacaciones.....	20
2.9.4 Configuración del período NO.....	20
2.9.5 Configuración del período NC.....	20
2.9.6 Configuración del período de verificación remota.....	21
2.10 Sistema.....	21
2.10.1 Configuración de la hora.....	21
2.10.2 Configuración de parámetros faciales.....	23
2.10.3 Configuración del modo de imagen.....	26

2.10.4 Configuración del modo de luz de relleno.....	26
2.10.5 Configuración del brillo de la luz de relleno.....	27
2.10.6 Configuración del brillo de la luz IR.....	27
2.10.7 Configuración de parámetros de huellas dactilares.....	27
2.10.8 Configuración del volumen.....	27
2.10.9 Restablecimiento de valores predeterminados de fábrica.....	27
2.10.10 Reiniciar el dispositivo.....	27
2.11 Gestión USB.....	27
2.11.1 Exportando a USB.....	28
2.11.2 Importación desde USB.....	28
2.11.3 Sistema de actualización.....	29
2.12 Configuración de funciones.....	29
2.13 Desbloqueo de la puerta.....	32
2.13.1 Desbloqueo por Tarjetas.....	32
2.13.2 Desbloqueo por Rostro.....	32
2.13.3 Desbloqueo por contraseña de usuario.....	32
2.13.4 Desbloqueo por contraseña de administrador.....	33
2.13.5 Desbloqueo por Huella Dactilar.....	34
2.14 Visualización de registros de desbloqueo.....	34
2.15 Configuración de la autocomprobación.....	34
2.16 Información del sistema.....	36
2.16.1 Visualización de la capacidad de datos.....	36
2.16.2 Visualización de la versión del dispositivo.....	36
3 Operaciones Web.....	37
3.1 Inicialización.....	37
3.2 Iniciar sesión.....	37
3.3 Restablecimiento de la contraseña.....	38
3.4 Configuración de enlace de alarma.....	39
3.4.1 Configuración de enlace de alarma.....	39
3.4.2 Visualización de registros de alarma.....	41
3.5 Configuración del intercomunicador.....	41
3.5.1 Configuración del servidor SIP.....	41
3.5.2 Configuración de parámetros básicos.....	45
3.5.3 Agregar el VTO.....	47
3.5.4 Agregando el VTH.....	48
3.5.5 Adición del VTS.....	49
3.5.6 Visualización del estado del dispositivo.....	50
3.5.7 Visualización de registros de llamadas.....	50
3.6 Capacidad de datos.....	50
3.7 Configuración de vídeo e imagen.....	50

3.7.1 Configuración de vídeo.....	50
3.7.1.1 Configuración del Canal 1.....	51
3.7.1.2 Configuración del Canal 2.....	55
3.7.2 Configuración del volumen.....	57
3.7.3 Configuración de la detección de movimiento.....	57
3.7.4 Configuración de la codificación local.....	58
3.7.5 Configuración del modo de imagen.....	59
3.8 Configuración de la detección de rostros.....	59
3.9 Configuración de red.....	64
3.9.1 Configuración de TCP/IP.....	64
3.9.2 Configuración del puerto.....	sesenta y cinco
3.9.3 Configuración del registro automático.....	66
3.9.4 Configuración de P2P.....	67
3.10 Gestión de la seguridad.....	68
3.10.1 Configuración de la autoridad IP.....	68
3.10.1.1 Acceso a la red.....	68
3.10.1.2 Prohibir PING.....	70
3.10.1.3 Conexión Anti Half.....	71
3.10.2 Configuración del sistema.....	71
3.10.2.1 Crear certificado de servidor.....	73
3.10.2.2 Descarga del certificado raíz.....	74
3.11 Gestión de usuarios.....	78
3.11.1 Adición de usuarios.....	78
3.11.2 Adición de usuarios ONVIF.....	79
3.11.3 Visualización de usuarios en línea.....	80
3.12 Mantenimiento.....	80
3.13 Gestión de la configuración.....	81
3.13.1 Exportación/Importación de archivos de configuración.....	81
3.13.2 Restauración de valores predeterminados de fábrica.....	81
3.14 Sistema de actualización.....	82
3.14.1 Actualización de archivos.....	82
3.14.2 Actualización en línea.....	82
3.15 Ver información de la versión.....	82
3.16 Visualización de registros.....	83
3.16.1 Registros del sistema.....	83
3.16.2 Registros de administración.....	83
3.16.3 Desbloqueo de registros.....	83
4 Configuración inteligente de PSS Lite.....	84
4.1 Instalación e inicio de sesión.....	84
4.2 Adición de dispositivos.....	84

4.2.1 Agregando uno por uno.....	84
4.2.2 Adición de lotes.....	85
4.3 Gestión de usuarios.....	86
4.3.1 Configuración del tipo de tarjeta.....	86
4.3.2 Adición de usuarios.....	87
4.3.2.1 Sumando uno por uno.....	87
4.3.2.2 Adición de lotes.....	88
4.3.3 Asignación de permiso de acceso.....	90
4.4 Gestión de acceso.....	91
4.4.1 Apertura y cierre de puertas a distancia.....	91
4.4.2 Configuración de Siempre abierto y Siempre cerrado.....	92
4.4.3 Supervisión del estado de la puerta.....	92
Apéndice 1 Puntos importantes del funcionamiento del intercomunicador.....	94
Apéndice 2 Puntos importantes de las instrucciones de registro de huellas dactilares.....	95
Apéndice 3 Puntos importantes del registro facial.....	97
Apéndice 4 Recomendaciones sobre ciberseguridad.....	100

1. Introducción

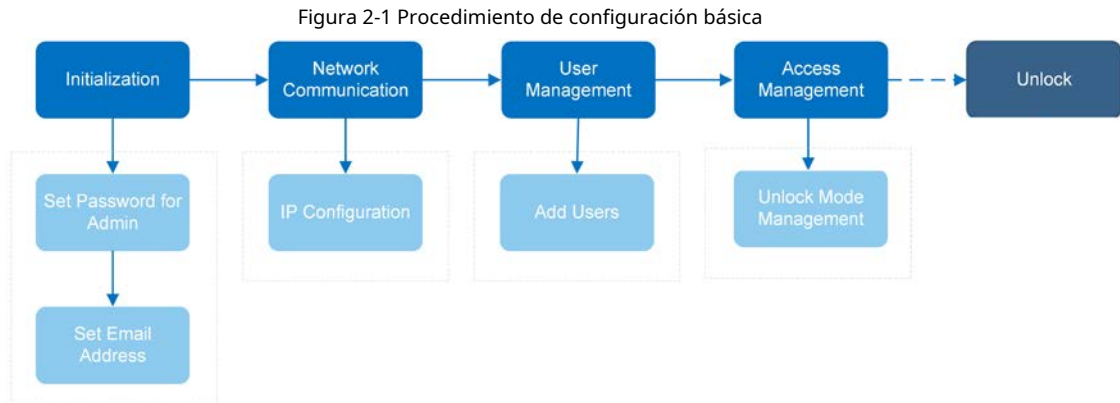
Esta serie de productos es un dispositivo de control de acceso que admite desbloqueo mediante rostros, contraseñas, tarjetas, huellas dactilares y sus combinaciones. Basado en el algoritmo de aprendizaje profundo, presenta un reconocimiento más rápido y una mayor precisión. Puede funcionar con una plataforma de gestión que satisfaga las diversas necesidades de los clientes. También se usa ampliamente en parques, comunidades, centros de negocios y fábricas, y es ideal para lugares como edificios de oficinas, edificios gubernamentales, escuelas y estadios.



Los métodos de desbloqueo pueden diferir según los modelos del producto.

2 operaciones locales

2.1 Procedimiento de configuración básica



2.2 Iconos comunes

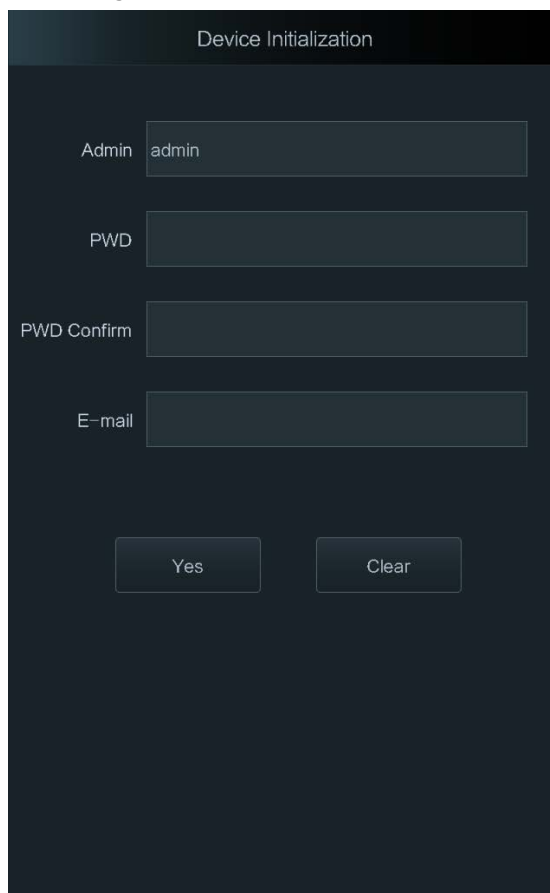
Tabla 2-1 Descripción de los iconos

Icono	Descripción
	Icono del menú principal.
	Confirmar icono.
	Pase a la primera página de la lista.
	Pase a la última página de la lista.
	Vaya a la página anterior de la lista.
	Pase a la página siguiente de la lista.
	Vuelve al menú anterior.
	Encender.
	Apagar.
	Borrar
	Pantalla de inicio
	Buscar

2.3 Inicialización

Para el uso por primera vez o después de restaurar los valores predeterminados de fábrica, debe establecer una contraseña y una dirección de correo electrónico para la cuenta de administrador. Puede utilizar la cuenta de administrador para iniciar sesión en el menú principal del dispositivo y la página web.

Figura 2-2 Inicialización



Device Initialization

Admin admin

PWD

PWD Confirm

E-mail

Yes Clear



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

2.4 Pantalla de espera

Puede desbloquear la puerta a través de rostros, contraseñas, huella digital, tarjeta y sus combinaciones.



- La pantalla de espera a continuación es solo para referencia y puede diferir del producto real.
- Si no hay ninguna operación en 30 segundos, el dispositivo pasará al modo de espera.

Figura 2-3 Página de inicio

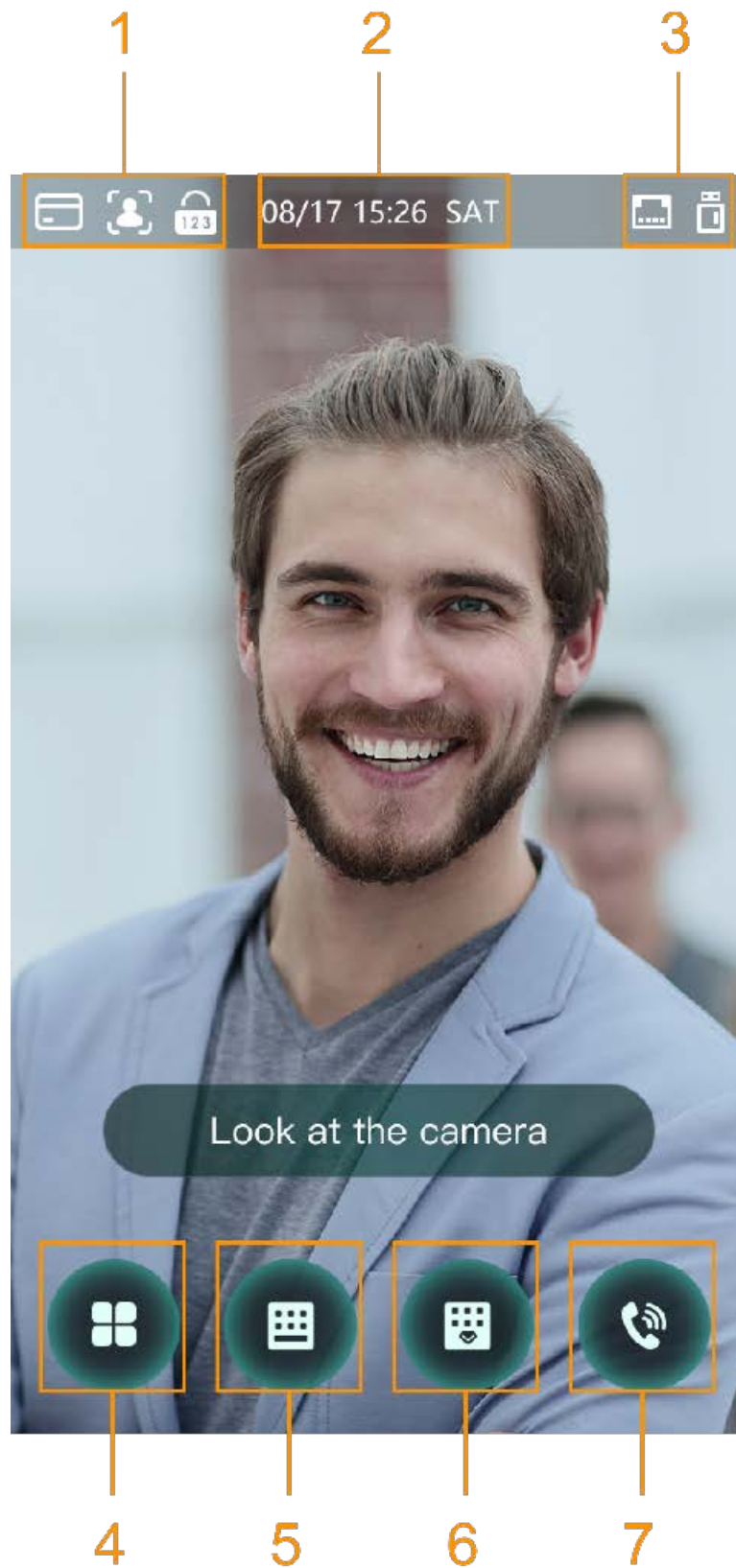


Tabla 2-2 Descripción de la pantalla de inicio

No.	Nombre	Descripción
1	Métodos de desbloqueo	Muestra los métodos de desbloqueo compatibles con Access Controller.
2	Fecha y hora	Fecha y hora actual.
3	Indicación de estado	Muestra el estado de Wi-Fi, red o USB.
4	Icono del menú principal	Inicie sesión en el menú principal del dispositivo. Solo la cuenta de administrador y los usuarios con permiso de administrador pueden ingresar al menú principal.
5/6	Contraseña	Ingrese la contraseña de usuario o la contraseña de administrador para desbloquear la puerta.
7	Intercomunicador	● Cuando el dispositivo funciona como servidor, puede llamar a VTO y VTH. ● Cuando DSS funciona como un servidor, el controlador de acceso puede llamar a VTO, VTS y DSS. Toque el ícono, ingrese el número de la habitación para llamar al propietario de la casa.

2.5 Iniciar sesión

Inicie sesión en el menú principal para configurar el dispositivo. Solo la cuenta de administrador y la cuenta de administrador pueden ingresar al menú principal del dispositivo. Para el uso por primera vez, use la cuenta de administrador para ingresar a la pantalla del menú principal y luego puede crear las otras cuentas de administrador.

Información de contexto

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

Procedimiento

Paso 1 Grifo  en la pantalla de espera.

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

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



El desbloqueo de huellas dactilares solo está disponible en modelos seleccionados.

- Perforación de tarjeta: Ingrese al menú principal deslizando la tarjeta.



La perforación de tarjetas solo está disponible en modelos seleccionados.

- PWD: Introduzca el ID de usuario y la contraseña de la cuenta de administrador.
- admin: Ingrese la contraseña de administrador para ingresar al menú principal.

2.6 Red de comunicación

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



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

2.6.1 Configuración de IP

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

Procedimiento

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

Paso 2 Configurar dirección IP.

Figura 2-4 Configuración de la dirección IP



Las NIC duales (tarjeta de interfaz de red) solo están disponibles en modelos seleccionados.

Tabla 2-3 Parámetros de configuración de IP

Parámetro	Descripción
Dirección IP/Máscara de subred/Dirección de puerta de enlace	La dirección IP, la máscara de subred y la dirección IP de la puerta de enlace deben estar en el mismo segmento de red.
DHCP	Significa Protocolo de configuración dinámica de host. Cuando se activa DHCP, al dispositivo se le asignará automáticamente una dirección IP, una máscara de subred y una puerta de enlace.
P2P	La tecnología P2P (peer-to-peer) permite a los usuarios administrar dispositivos sin solicitar DDNS, configurar el mapeo de puertos o implementar un servidor de tránsito.

2.6.2 Registro activo

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

Procedimiento

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



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

Para evitar la pérdida de datos, mantenga los permisos de la plataforma de gestión correctamente.

Figura 2-5 Registro automático

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

Tabla 2-4 Registro automático

Parámetro	Descripción
Dirección del servidor	La dirección IP de la plataforma de gestión.
Puerto	El número de puerto de la plataforma de gestión.

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

Paso 3 Habilite la función de registro activo.

2.6.3 Configuración de WiFi

Puede conectar el Dispositivo a la red a través de la red Wi-Fi. La función Wi-Fi solo está disponible para ciertos modelos del controlador de acceso.

Procedimiento

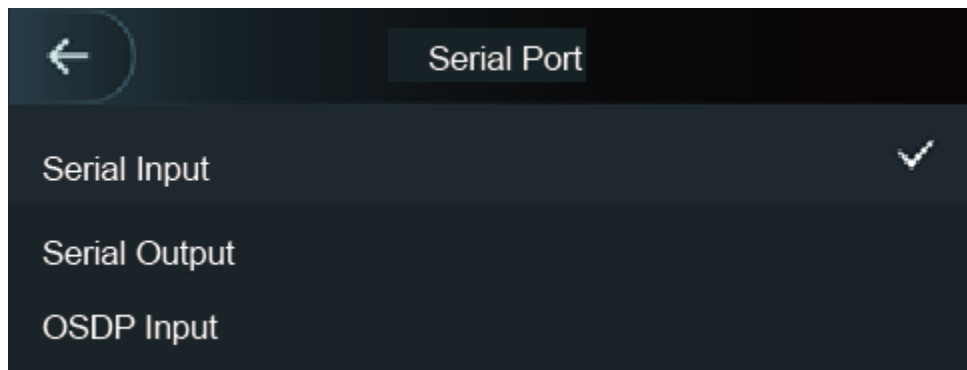
- Paso 1** Sobre el **Menú principal**, seleccionar **Conexión > Red > Wifi**.
- Paso 2** Encienda el wifi.
- Paso 3** Toque  para buscar redes inalámbricas disponibles.
- Etapas 4** Seleccione una red inalámbrica e ingrese la contraseña.
Si no se busca Wi-Fi, toque **SSID** para ingresar el nombre de Wi-Fi.
- Paso 5** Grifo 

2.6.4 Configuración del puerto serie

Procedimiento

- Paso 1** Sobre el **Menú principal**, seleccionar **Conexión > Puerto serial**.
- Paso 2** Seleccione un tipo de puerto.
- Seleccionar **Entrada en serie** cuando el controlador de acceso se conecta a un lector de tarjetas.
 - Seleccionar **Salida en serie** cuando el controlador de acceso funciona como un lector de tarjetas, y el controlador de acceso enviará datos al dispositivo para controlar el acceso.
Tipo de datos de salida:
 - ◇ Tarjeta: emite datos según el número de tarjeta cuando los usuarios deslizan la tarjeta para desbloquear la puerta; genera datos basados en el primer número de tarjeta del usuario cuando utiliza otros métodos de desbloqueo.
 - ◇ No.: genera datos basados en la ID de usuario.
 - Seleccionar **Entrada OSDP** cuando el controlador de acceso está conectado a un lector de tarjetas basado en el protocolo OSDP.
 - Módulo de seguridad: cuando se conecta un módulo de seguridad, el enlace del botón de salida, el bloqueo y la alarma contra incendios no será efectivo.

Figura 2-6 Puerto serie



2.6.5 Configuración de Wiegand

El dispositivo permite el modo de entrada y salida Wiegand.

Procedimiento

- Paso 1** Sobre el **Menú principal**, seleccionar **Conexión>Wiegand**.
- Paso 2** Seleccione un Wiegand.
- Seleccionar **Entrada Wiegand** cuando conecta un lector de tarjetas externo al dispositivo.
 - Seleccionar **Salida Wiegand** cuando el Dispositivo funciona como un lector de tarjetas y necesita conectarlo a un controlador u otro terminal de acceso.

Figura 2-7 Salida Wiegand



Tabla 2-5 Descripción de la salida Wiegand

Parámetro	Descripción
Tipo de salida Wiegand	Seleccione un formato Wiegand para leer números de tarjeta o números de identificación. ● Wiegand26: Lee tres bytes o seis dígitos. ● Wiegand34: Lee cuatro bytes u ocho dígitos. ● Wiegand66: Lee ocho bytes o dieciséis dígitos.
Ancho de pulso	Ingrese el ancho de pulso y el intervalo de pulso de la salida Wiegand.
Intervalo de pulso	

Parámetro	Descripción
Tipo de datos de salida	Seleccione el tipo de datos de salida. ● ID de usuario: genera datos basados en el ID de usuario. ● número de tarjeta: Emite datos basados en el primer número de tarjeta del usuario.

2.7 Gestión de usuarios

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



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

2.7.1 Adición de nuevos usuarios

Procedimiento

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

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



Los parámetros de los nuevos usuarios pueden diferir según los modelos del producto.

Figura 2-8 Nuevo usuario

Field	Value
User ID	1
Name	
FP	0
Face	0
Card	0
PWD	
User Level	User
Period	255-Default
Holiday Plan	255-Default
Valid Date	2037-12-31
User Level	General
Use Time	Unlimited

Tabla 2-6 Descripción de los nuevos parámetros de usuario

Parámetro	Descripción
ID de usuario	Introduzca los ID de usuario. Los ID pueden ser números, letras y sus combinaciones, y la longitud máxima del ID es de 32 caracteres. Cada identificación es única.
Nombre	Ingrese el nombre con un máximo de 32 caracteres (incluidos números, símbolos y letras).
FP	Se pueden registrar como máximo 3 huellas dactilares para cada usuario. Puede configurar una de las huellas dactilares registradas como huella dactilar de coacción. Después de activar la función de coacción, se activará una alarma cuando se use una huella dactilar de coacción para desbloquear la puerta.  No se recomienda que configure la primera huella digital como la huella digital de coacción.
Rostro	Asegúrese de que su rostro esté centrado en el cuadro de captura de imágenes, y se capturará y analizará automáticamente una imagen del rostro.
Tarjeta	Un usuario puede registrar 5 tarjetas como máximo. Ingrese su número de tarjeta o deslice su tarjeta, y luego el dispositivo leerá la información de la tarjeta. Puede habilitar el Tarjeta de coacción función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta.  Solo ciertos modelos admiten el desbloqueo de tarjetas.
PCD	Introduzca la contraseña de usuario. La longitud máxima de la contraseña es de 8 dígitos.
Nivel de usuario	Puede seleccionar un nivel de usuario para los nuevos usuarios. ● Usuario: Los usuarios solo tienen permiso de acceso a la puerta. ● Administración: Los administradores pueden desbloquear la puerta y configurar el controlador de acceso.
Período	Las personas pueden desbloquear la puerta solo durante el período definido.
Plan de vacaciones	Las personas pueden desbloquear la puerta solo durante el plan de vacaciones definido.
Fecha válida	Establezca una fecha en la que caducan los permisos de acceso de la persona.
Tipo de usuario	● General: los usuarios generales pueden desbloquear la puerta. ● Lista de bloqueo: cuando los usuarios de la lista de bloqueo desbloqueen la puerta, el personal de servicio recibirá una notificación. ● Invitado: los invitados pueden desbloquear la puerta dentro de un período definido o por una cierta cantidad de veces. Después de que vence el período definido o se agotan los tiempos de desbloqueo, no pueden desbloquear la puerta. ● Patrulla: los usuarios de Patrulla tendrán un seguimiento de su asistencia, pero no tienen permisos de desbloqueo. ● VIP: cuando VIP desbloquee la puerta, el personal de servicio recibirá un aviso. ● Otros: Cuando abren la puerta, la puerta permanecerá abierta durante 5 segundos más. ● Usuario personalizado 1/Usuario personalizado 2: Lo mismo con los usuarios generales.

Parámetro	Descripción
tiempo de uso	Cuando el nivel de usuario se establece en invitado, puede establecer la cantidad máxima de veces que el usuario puede desbloquear la puerta.

Paso 3 Grifo  para guardar la configuración.

2.7.2 Visualización de la información del usuario

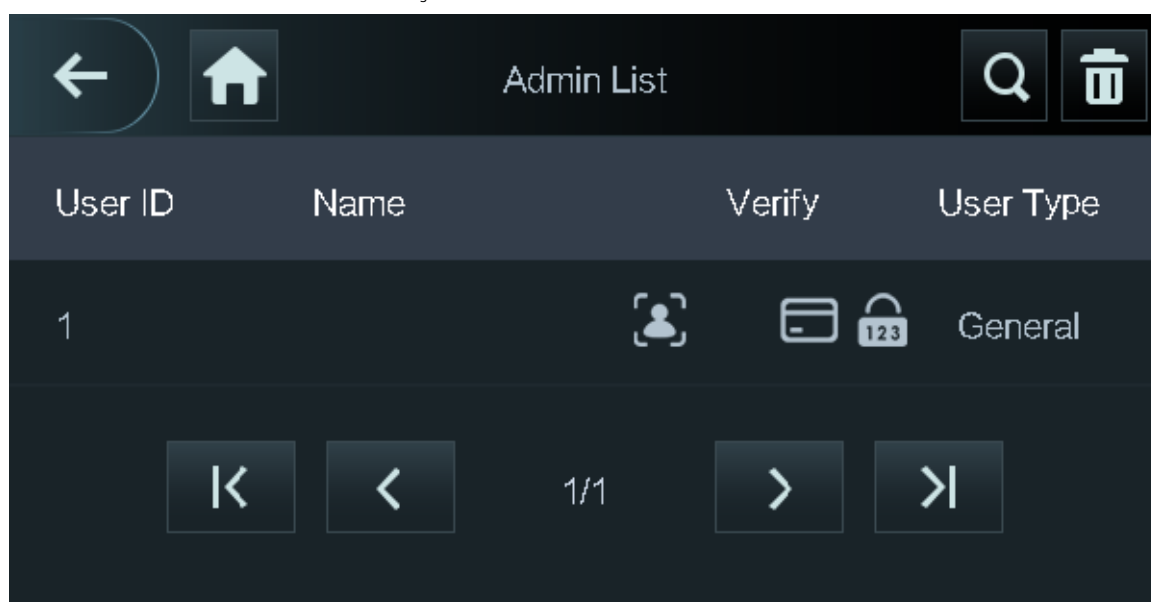
Puede ver la lista de usuarios/administradores y editar la información del usuario.

Procedimiento

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

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

Figura 2-9 Lista de administradores



- : Desbloqueo mediante contraseña.
- : Desbloquear deslizando la tarjeta.
- : Desbloqueo mediante reconocimiento facial.
- : Desbloqueo mediante huella dactilar.

Operaciones relacionadas

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

- Buscar usuarios: toca y luego  ingresa el nombre de usuario.
- Editar usuarios: toque el usuario para editar la información del usuario.
- Eliminar usuarios
 - ◇ Eliminar individualmente: seleccione un usuario y luego toque .
 - ◇ Eliminar en lotes:
 - Sobre el **Lista de usuarios** pantalla, toque  para eliminar todos los usuarios.
 - Sobre el **Lista de administradores** pantalla, toque  para eliminar todos los usuarios administradores.

2.7.3 Configuración de la contraseña de administrador

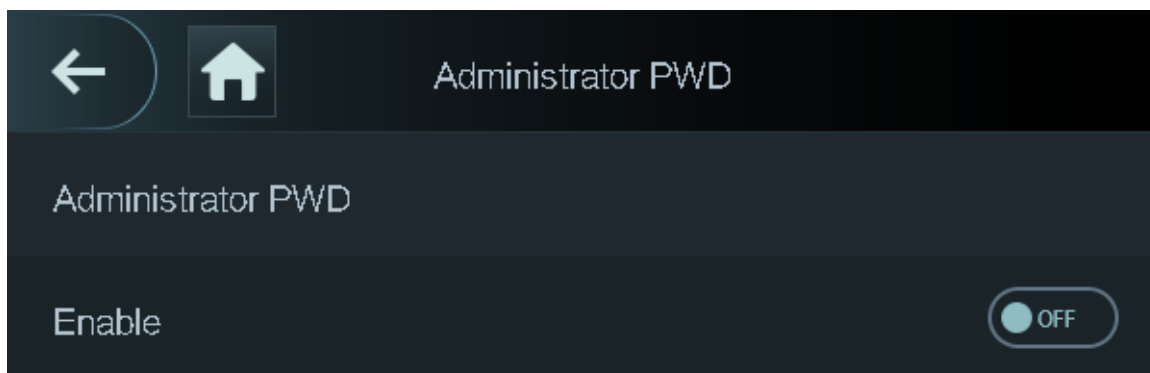
Puede desbloquear la puerta ingresando solo la contraseña de administrador. La contraseña de administrador no está limitada por

tipos de usuario. Solo se permite una contraseña de administrador para un dispositivo.

Procedimiento

Paso 1 Sobre el **Menú principal** pantalla, seleccione **Usuario > PCD del administrador**.

Figura 2-10 Establecer contraseña de administrador



Paso 2 Grifo **PCD del administrador**, a continuación, introduzca la contraseña de administrador.

Paso 3 Grifo .

Etapas 4 Active la función de administrador.

2.8 Gestión de acceso

Puede configurar los parámetros de acceso a las puertas, como los modos de desbloqueo, la vinculación de alarmas, los horarios de las puertas. Los modos de desbloqueo pueden diferir según el producto real.

2.8.1 Configuración de combinaciones de desbloqueo

Use tarjeta, huella digital, cara o contraseña o sus combinaciones para desbloquear la puerta.

Procedimiento

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

Paso 2 Seleccione los métodos de desbloqueo.

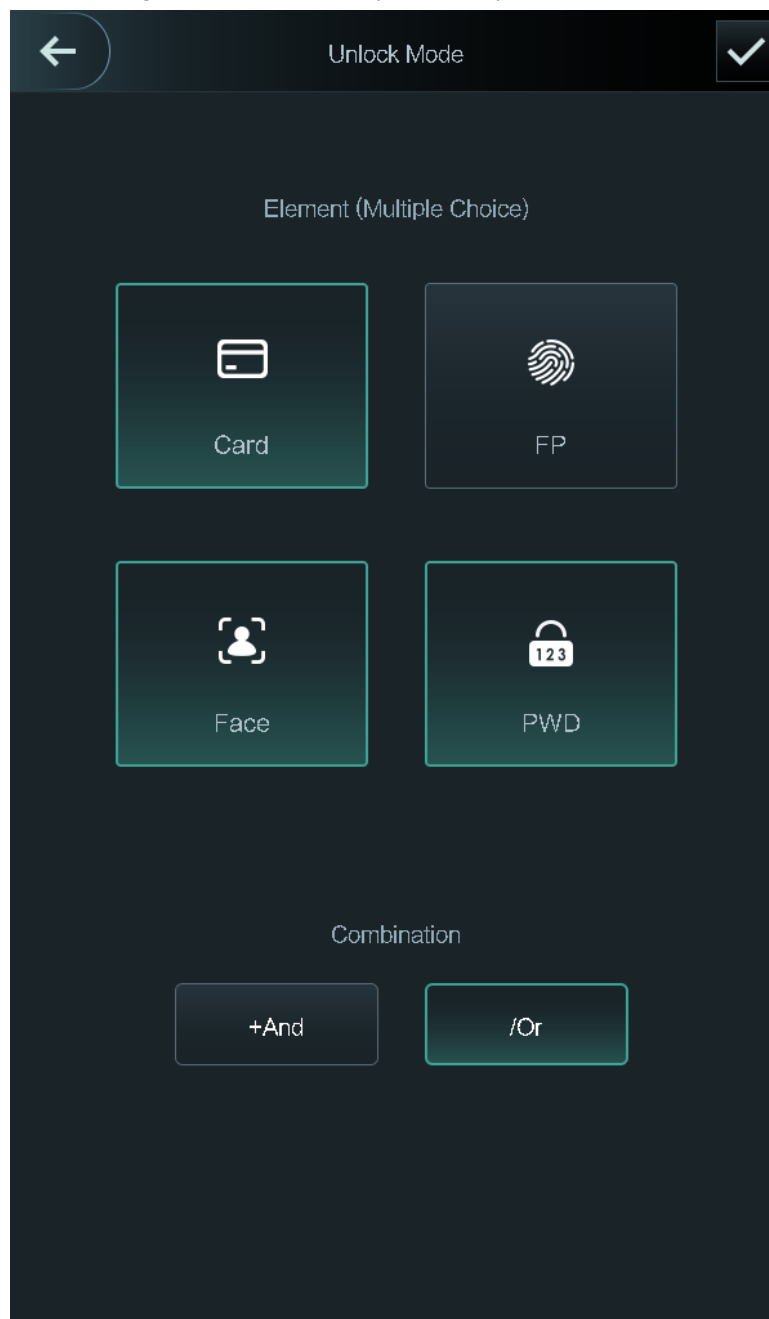


Para cancelar su selección, vuelva a tocar el método seleccionado.

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

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

Figura 2-11 Elemento (opción múltiple)



Etapas 4 Grifo  para guardar los cambios.

2.8.2 Configuración de desbloqueo por período

Las puertas se pueden desbloquear a través de diferentes modos de desbloqueo en diferentes períodos. Por ejemplo, en el período 1, la puerta solo se puede desbloquear con tarjeta; y en el período 2, las puertas solo se pueden cerrar mediante huellas dactilares.

Procedimiento

Paso 1 Seleccionar **Acceso > Modo de desbloqueo > Desbloqueo por período**.

Paso 2 Establezca la hora de inicio y la hora de finalización para un período y luego seleccione un modo de desbloqueo.

Figura 2-12 Desbloqueo por período

Paso 3 Grifo  para guardar los cambios.

Etapas 4 Active la función de desbloqueo por período.

2.8.3 Configuración de combinación de grupos

Las puertas solo pueden ser desbloqueadas por un grupo o grupos que constan de más de dos usuarios si la combinación de grupos está habilitada.

Procedimiento

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

Paso 2 **grupo**  toque para crear un grupo.

Figura 2-13 Agregar grupo

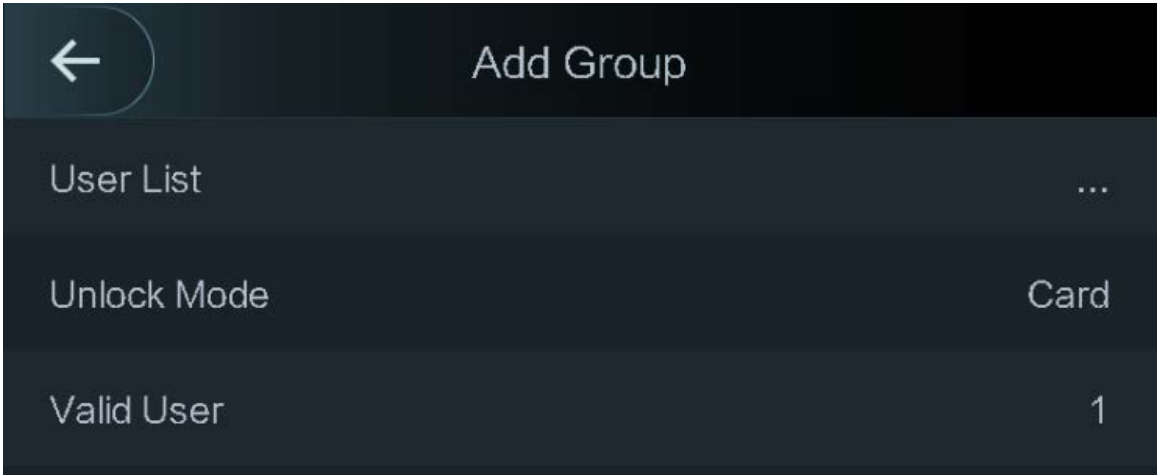


Tabla 2-7 Descripción de la combinación de grupos

Parámetro	Descripción
Lista de usuarios	Agregue usuarios al grupo recién creado. 1. Toque Lista de usuarios . 2. Toca  , a continuación, introduzca un ID de usuario. 3. Toca  para guardar la configuración.
desbloquear Modo	Hay cuatro opciones: Tarjeta, FP, PCDyRostro .
Usuario válido	Los usuarios válidos son los que tienen autorización de desbloqueo. Las puertas se pueden desbloquear solo cuando el número de usuarios para desbloquear las puertas es igual al número de usuario válido. ● Los usuarios válidos no pueden exceder el número total de usuarios en un grupo. ● Si los usuarios válidos son iguales al número total de usuarios en un grupo, solo todos los usuarios del grupo pueden desbloquear las puertas. ● Si los usuarios válidos son menos que el número total de usuarios en un grupo, cualquier usuario cuyo número sea igual al número de usuario válido puede desbloquear las puertas.

Paso 3 Grifo  para volver a la interfaz anterior. para

Etapa 4 Grifo  guardar los cambios.

Paso 5 Encienda la función de combinación de grupo.

2.8.4 Desbloqueo por control de temperatura

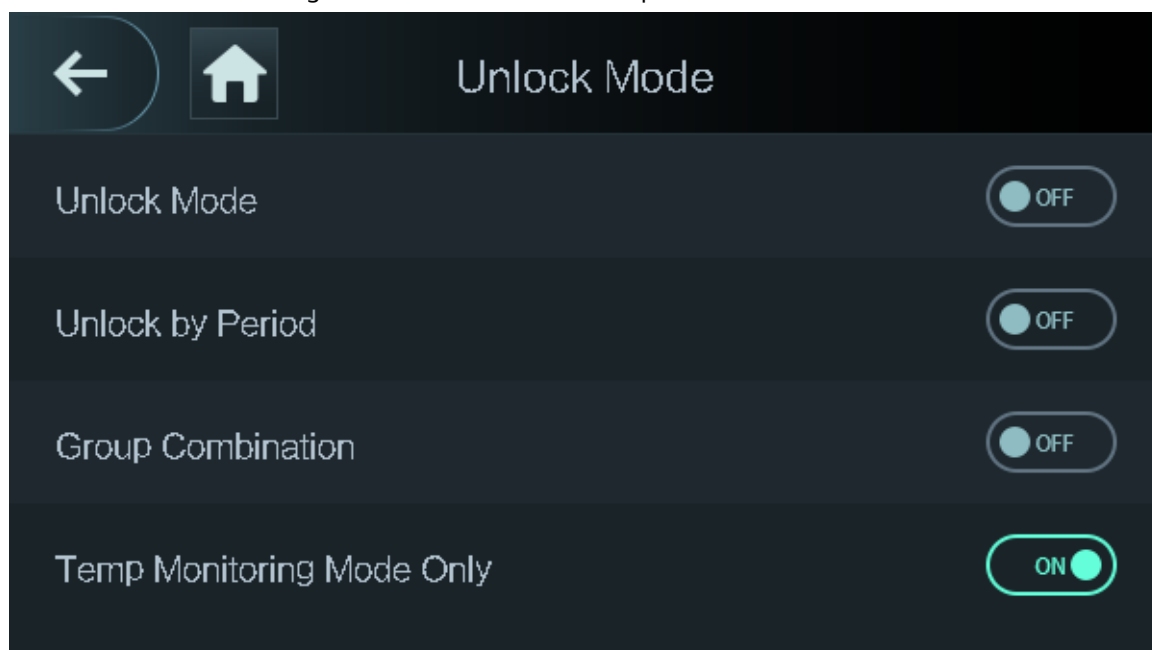
Controle el acceso solo a través del monitoreo de temperatura. Esta función solo está disponible en modelos seleccionados.

Procedimiento

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

Paso 2 **modo de monitoreo de temperatura**.

Figura 2-14 Solo control de temperatura



2.8.5 Configuración de alarma

Se activará una alarma cuando ocurran eventos de acceso anormales.

Procedimiento

Paso 1 Seleccionar **Acceso>Alarma**.

Paso 2 Habilite el tipo de alarma.



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

Figura 2-15 Alarma

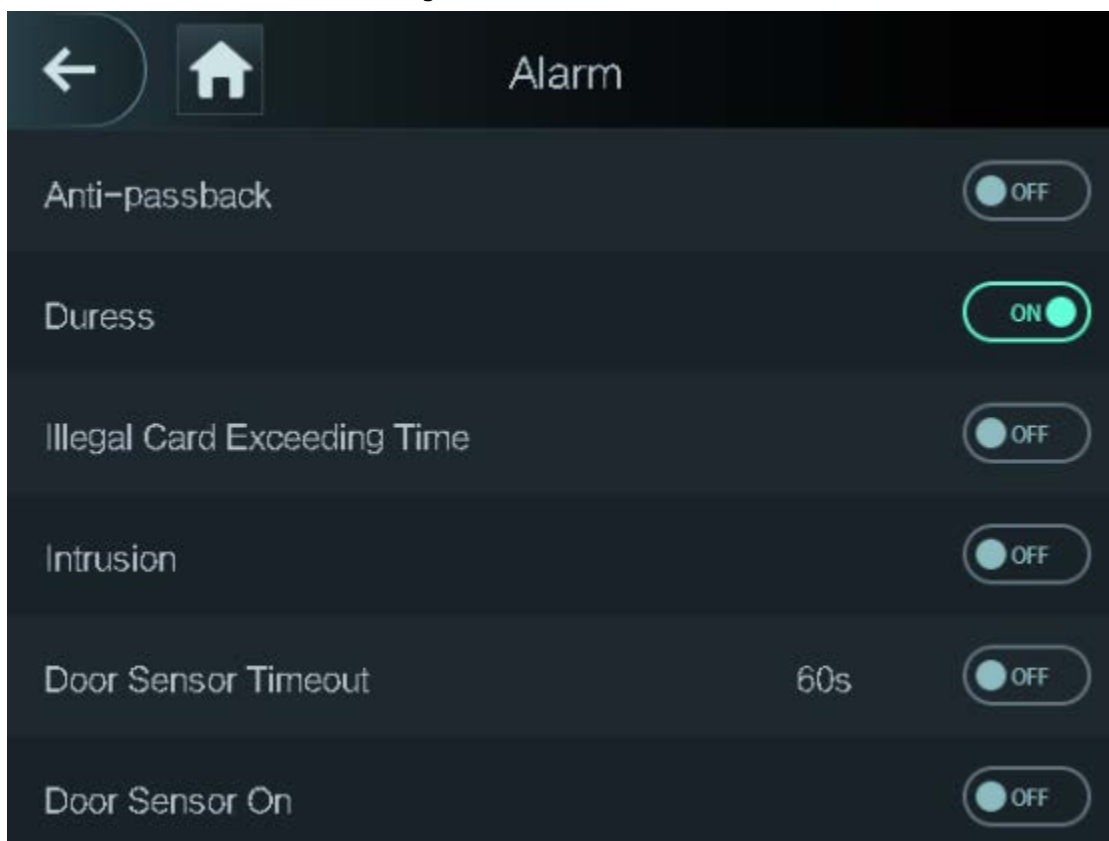


Tabla 2-8 Descripción de los parámetros de alarma

Parámetro	Descripción
Anti-passback	Los usuarios deben verificar sus identidades tanto para la entrada como para la salida; de lo contrario, se activará una alarma. Ayuda a evitar que el titular de la tarjeta le devuelva la tarjeta de acceso a otra persona para que pueda ingresar. Cuando se habilita el antipassback, el titular de la tarjeta debe abandonar el área segura a través de un lector de salida antes de que el sistema permita otra entrada. ● Si una persona ingresa después de la autorización y sale sin autorización, se activará una alarma cuando intente ingresar nuevamente y se negará el acceso al mismo tiempo. ● Si una persona entra sin autorización y sale después de la autorización, se activará una alarma cuando intente entrar de nuevo y se negará el acceso al mismo tiempo.
Coacción	Se activará una alarma cuando se utilice una tarjeta de coacción, una contraseña de coacción o una huella dactilar de coacción para desbloquear la puerta.
Exceso de tarjeta ilegal Tiempo	Después de usar una tarjeta no autorizada para desbloquear la puerta más de 5 veces en 50 segundos, se activará una alarma.
Intrusión	Cuando el sensor de puerta está habilitado, se activará una alarma de intrusión si la puerta se abre de forma anormal.
Tiempo de espera del sensor de puerta	Se activará una alarma de tiempo de espera si la puerta permanece desbloqueada más tiempo que el tiempo de espera del sensor de puerta definido, que oscila entre 1 y 9999 segundos.
Sensor de puerta encendido	Las alarmas de intrusión y tiempo de espera pueden activarse solo después de que el sensor de la puerta esté habilitado.

2.8.6 Configuración del estado de la puerta

Procedimiento

- Paso 1** Sobre el **Menú principal** pantalla, seleccione **Acceso>Estado de la puerta**. Establecer el estado de la puerta.
- Paso 2**
- **NO:** La puerta permanece desbloqueada todo el tiempo.
 - **CAROLINA DEL NORTE:** La puerta permanece bloqueada todo el tiempo.
 - **Normal:** Si **Normal** está seleccionado, la puerta se desbloqueará y bloqueará de acuerdo con su configuración.

2.8.7 Configuración del tiempo de retención de bloqueo

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

Procedimiento

- Paso 1** Sobre el **Menú principal**, seleccionar **Acceso>Tiempo de retención de bloqueo**.
- Paso 2** Introduzca la duración del desbloqueo. Toque para guardar los cambios.
- Paso 3** 

2.9 Gestión de períodos

Puede establecer periodos, periodos de vacaciones, periodos de plan de vacaciones, periodos de puerta normalmente abierta, periodos de puerta normalmente cerrada y periodos de verificación remota.

2.9.1 Periodo de configuración

Puede configurar hasta 128 periodos. En cada período, debe editar los horarios de acceso a la puerta durante una semana completa. Un usuario solo puede desbloquear la puerta durante el tiempo programado.

Procedimiento

- Paso 1** Inicie sesión en el **Menú principal** pantalla. Seleccionar
- Paso 2** **Acceso>Período>Configuración del período**. Toque
- Paso 3** en la  esquina superior derecha.
- Etapa 4** Ingrese el número y el nombre del período.
- **No:** Ingrese un número de sección. Varía entre 0 y 127.
 - **Nombre del período:** Introduzca un nombre para el período. Puede ingresar 10 caracteres chinos o 32 caracteres (que contengan números, caracteres especiales y caracteres ingleses).
- Paso 5** Configure el tiempo para una semana.
- Paso 6** Puede configurar hasta cuatro períodos para un solo día. Toque
- Paso 7** para  guardar los cambios.

2.9.2 Configuración de grupos de vacaciones

Establecer secciones de tiempo para diferentes grupos de vacaciones. Puede configurar hasta 128 grupos de vacaciones (desde

No.0 a No.127), y hasta 16 días festivos para un solo grupo de días festivos.

Procedimiento

- Paso 1** Inicie sesión en el **Menú principal** pantalla.
- Paso 2** Seleccionar **Acceso>Período>Configuración de grupo de**
- Paso 3** **vacaciones**. Toque en la esquina superior derecha.
- Etapas**
- Introduzca un número y un nombre para el grupo de vacaciones.
- **No.:** Introduzca un nombre de período. Va de 0 a 127.
 - **Nombre del grupo de vacaciones:** Introduzca un nombre para cada grupo de vacaciones. Puede ingresar 10 caracteres chinos o 32 caracteres (contiene números, caracteres especiales y caracteres ingleses).
- Paso 5** Grifo **Configuración de grupo** y luego toque .
- Paso 6** Ingrese el número de serie y el nombre del día festivo, y luego seleccione la fecha de inicio y la fecha de finalización. Toque
- Paso 7** para guardar los cambios.

2.9.3 Configuración del plan de vacaciones

Asigne los grupos de vacaciones configurados al plan de vacaciones. Los usuarios solo pueden desbloquear la puerta en las secciones de tiempo definidas en el plan de vacaciones.

Procedimiento

- Paso 1** Inicie sesión en el **Menú principal** pantalla.
- Paso 2** Seleccionar **Acceso>Período>Configuración del plan de**
- Paso 3** **vacaciones**. Toque en la esquina superior derecha.
- Etapas**
- Introduzca un número y un nombre para el plan de vacaciones.
- **No.:** Introduzca un número del plan de vacaciones. Va de 0 a 127.
 - **Nombre del plan de vacaciones:** Ingrese un nombre para cada sección de tiempo. Puede ingresar 10 caracteres chinos o 32 caracteres (contiene números, caracteres especiales y caracteres ingleses).
- Paso 5** Seleccionar **Grupo de vacaciones No.** e ingrese el número de grupo de vacaciones que ha configurado.
- Paso 6** Seleccionar **Período de festivos**, configurar períodos de tiempo para un solo día festivo. Toque para guardar los
- Paso 7** cambios .

2.9.4 Configuración del período NO

Si configura NO período, la puerta permanece abierta en el período definido. El período NO/NC anula otros períodos.

Procedimiento

- Paso 1** Inicie sesión en el **Menú principal** interfaz. Seleccionar
- Paso 2** **Acceso>Período>SIN Período**. Ingrese el número de
- Paso 3** período que ha configurado. Toque para guardar los
- Etapas**
- cambios .

2.9.5 Configuración del período NC

Si configura el período NC, la puerta permanece desbloqueada en el período definido. El período NO/NC

anula otros períodos.

Procedimiento

- Paso 1 Sobre el **Menú principal** pantalla, seleccione **Acceso>Período>SIN Período**.
- Paso 2 Ingrese el número de período que ha configurado.
- Paso 3 Toque  a guardar los cambios.

2.9.6 Configuración del período de verificación remota

Procedimiento

- Paso 1 Inicie sesión en el **Menú principal** pantalla
- Paso 2 Sobre el **Menú principal**, seleccionar **Acceso>Período>Período de verificación remota**.
- Paso 3 Permitir **Período de verificación remota**. Ingrese el número de período que ha configurado.
- Etapas 4 Toque para guardar los cambios.
- Paso 5 

2.10 Sistema

2.10.1 Configuración de la hora

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

Procedimiento

- Paso 1 Sobre el **Menú principal**, seleccionar **Sistema>Tiempo**.
- Paso 2 Configurar la hora del sistema.

Figura 2-16 Tiempo

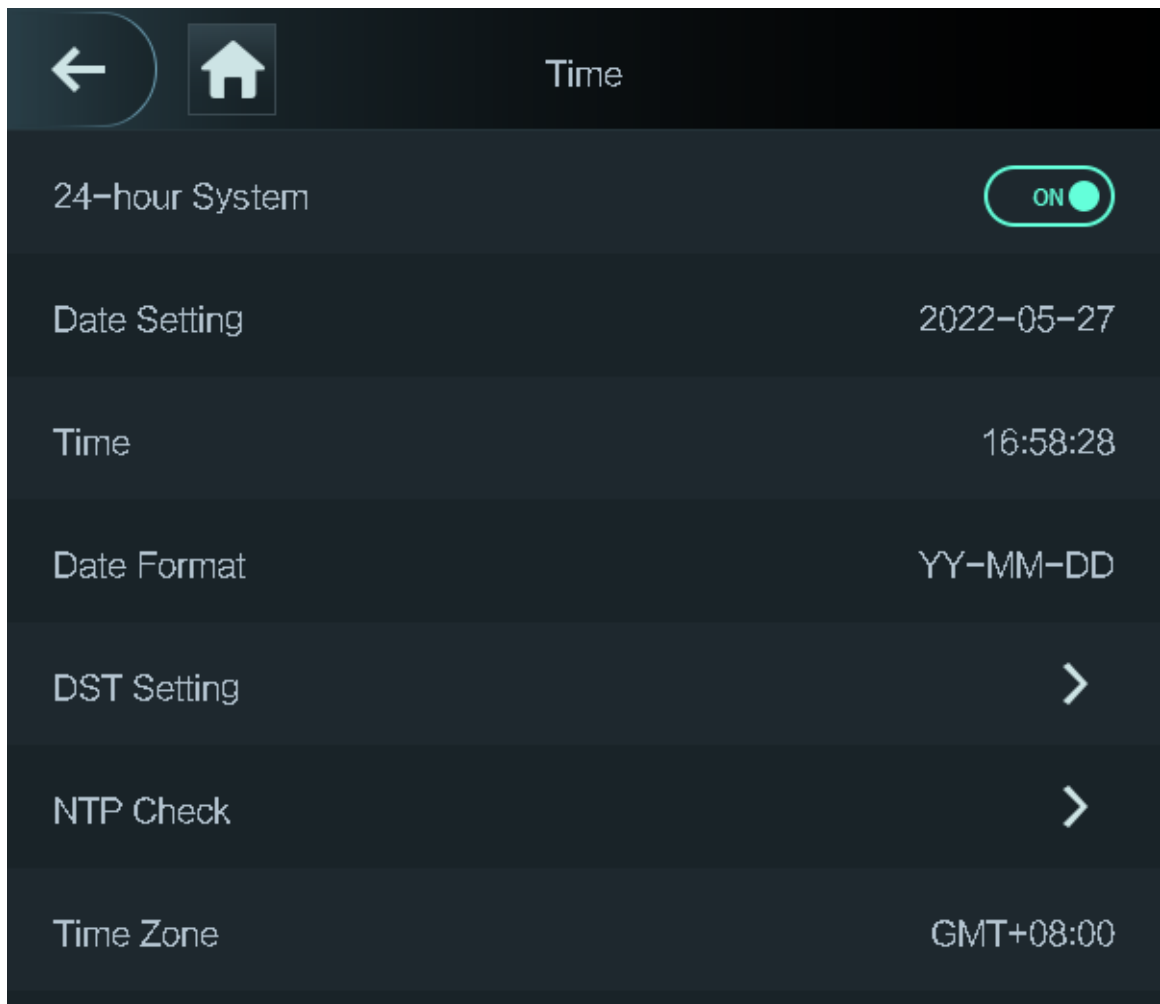


Tabla 2-9 Descripción de los parámetros de tiempo

Parámetro	Descripción
Sistema 24 horas	La hora se muestra en formato de 24 horas.
Configuración de la fecha	Configura la fecha.
Tiempo	Configura el tiempo.
Formato de fecha	Seleccione un formato de fecha.
Configuración de horario de verano	1. Toque Configuración de horario de verano. 2. Habilite el horario de verano. 3. Seleccione Fecha o Semana desde el horario de verano Lista de tipos. 4. Introduzca la hora de inicio y la hora de finalización. 5. Toque

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

2.10.2 Configuración de parámetros faciales

Procedimiento

Paso 1 En el menú principal, seleccione **Sistema > Parámetro de cara**.



DANGER

Recomendamos personal profesional para configurar los parámetros faciales.

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



La imagen a continuación es solo de referencia, y los parámetros de la cara pueden diferir según modelos del producto.

Figura 2-17 Parámetro de cara



Tabla 2-10 Descripción de los parámetros de la cara

Nombre	Descripción
Umbral de cara	Ajuste la precisión del reconocimiento facial. Un umbral más alto significa una mayor precisión.
máx. Ángulo de la cara	Establezca el ángulo máximo de posición de la cara para la detección de rostros. Un valor más grande significa un rango de ángulo de cara más grande. Si el ángulo de la pose del rostro está fuera del rango definido, el cuadro de detección de rostros no aparecerá.
Distancia pupilar	Las imágenes de rostros requieren los píxeles deseados entre los ojos (llamada distancia pupilar) para un reconocimiento exitoso. El píxel predeterminado es 45. El píxel cambia según el tamaño de la cara y la distancia entre las caras y la lente. Si un adulto está a 1,5 metros de la lente, la distancia pupilar puede ser de 50 px-70 px.
Tiempo de espera de reconocimiento (S)	Si se reconoce correctamente el rostro de una persona con permiso de acceso, el dispositivo indicará que el reconocimiento facial se realizó correctamente. Puede introducir el tiempo de intervalo de solicitud.
Intervalo de mensaje de cara no válido (S)	Si una persona sin permiso de acceso intenta desbloquear la puerta varias veces en el intervalo definido, el dispositivo indicará una falla en el reconocimiento de rostros. Puede introducir el tiempo de intervalo de solicitud.

Nombre	Descripción
Parámetros temporales	 Solo el dispositivo con control de temperatura admite esta función. ● Monitoreo de temperatura: habilite o deshabilite esta función. ● Temp Rect: Establezca si mostrar o no el cuadro de control de temperatura. ● Distancia de monitoreo de temperatura (cm): 50 por defecto. Debe controlar su temperatura manteniéndose alejado del Dispositivo a la distancia que defina. ● Duración de corrección de temperatura (ms): Al monitorear la temperatura, el dispositivo tomará el valor de temperatura después del tiempo definido por este parámetro. ● Umbral de alta temperatura: establezca el umbral de temperatura. La temperatura corporal monitoreada se considerará alta si es mayor o igual que el valor establecido. ● Temperatura máxima/mínima: establezca el rango de temperatura que necesita. Si la temperatura monitoreada es inferior al límite inferior, indicará que la temperatura es demasiado baja; si es superior al límite superior, indicará que hay una fuente de calor que interfiere con la función. ● Valor de corrección de temperatura: este parámetro es para realizar pruebas. La diferencia del entorno de monitoreo de temperatura puede causar la desviación de temperatura entre la temperatura monitoreada y la temperatura real. Puede seleccionar múltiples muestras monitoreadas para la prueba y luego corregir la desviación de temperatura por este parámetro de acuerdo con la comparación entre la temperatura monitoreada y la temperatura real. Por ejemplo, si la temperatura monitoreada es 0,5 °C inferior a la temperatura real, el valor de corrección se establece en 0,5 °C; si la temperatura monitoreada es 0,5 °C más alta que la temperatura real, el valor de corrección se establece en -0,5 °C. ● Modo de monitoreo de temperatura: ◇ Automático: utiliza un mapa de calor facial para el reconocimiento facial; si no se encuentran los mapas de calor, cambiará automáticamente al modo de calibración. ◇ Termograma: utiliza solo un mapa de calor para el reconocimiento facial y el control de la temperatura. ◇ Calibración: utiliza una imagen de luz blanca de un rostro para el reconocimiento facial y luego extrae y aplica las coordenadas en el mapa de calor del rostro para monitorear la temperatura. ● Unidad de temperatura: Seleccione ° C o ° F. ● Valor de compensación Evm: este valor se agregará a la temperatura ambiente monitoreada.
Umbral anti-falsificación	Evite el reconocimiento facial falso mediante el uso de una foto, un video, una máscara o un sustituto diferente del rostro de una persona autorizada.

Nombre	Descripción
Parámetros de máscara	● Modo máscara: ◇ Sin detectar: La máscara no se detecta durante el reconocimiento facial. ◇ Recordatorio de máscara: La máscara se detecta durante el reconocimiento facial. Si la persona no lleva mascarilla, el sistema le recordará que la use y se permitirá el acceso. ◇ Intercepción de máscara: La máscara se detecta durante el reconocimiento facial. Si una persona no está usando una máscara, el sistema le recordará que la use y se le negará el acceso. ● Umbral de reconocimiento de máscara: un umbral más alto significa una mayor precisión de detección de máscara.

2.10.3 Configuración del modo de imagen

Configure el modo de imagen según el sitio de instalación.

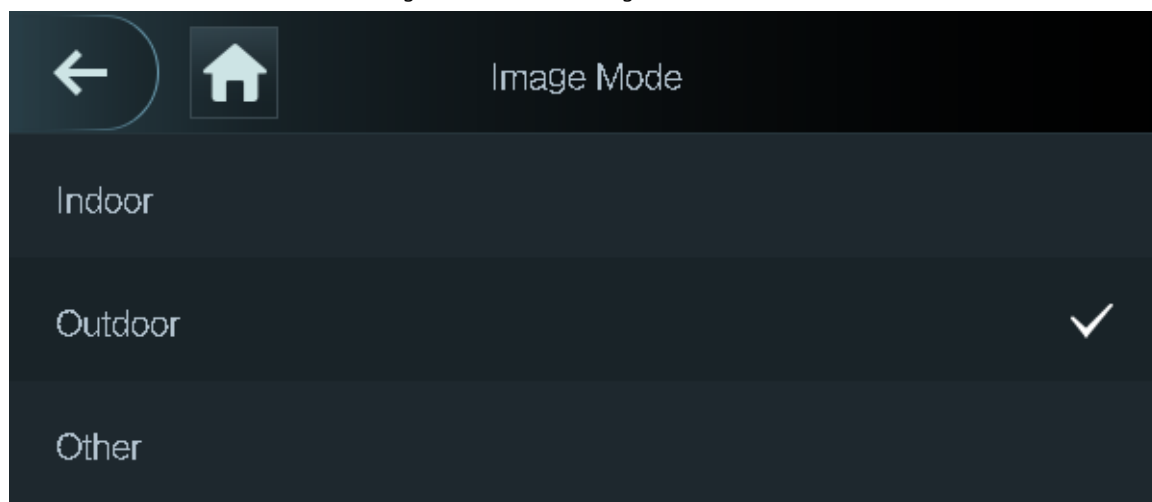
Procedimiento

Paso 1 Sobre el **Menú principal**, seleccionar **Sistema > Modo de imagen**.

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

- Interior: el dispositivo generalmente se instala en interiores, como oficinas. La luz artificial está uniforme al otro lado de la habitación y no hay luz natural.
- Exterior: el dispositivo generalmente se instala al aire libre y la luz del día es brillante y uniforme.
- Otro: cuando el rostro humano está en contraluz, lo que hace que el rostro se oscurezca, le recomendamos que seleccione otro modo para que sea más fácil de detectar para el controlador de acceso.

Figura 2-18 Modo de imagen



2.10.4 Configuración del modo de luz de relleno

Puede seleccionar los modos de la luz de relleno en función del entorno real. Hay tres modos.

- Automático: cuando la luz de relleno se enciende automáticamente cuando el entorno ambiental está oscuro y se apaga automáticamente cuando hay mucha luz.
- NO: La luz de llenado normalmente está abierta.
- NC: La luz de llenado normalmente está cerrada.

2.10.5 Configuración del brillo de la luz de relleno

Puede seleccionar el brillo de la luz de relleno en función del entorno real.

2.10.6 Configuración del brillo de la luz IR

Cuanto mayor sea el valor, más claras serán las imágenes; de lo contrario, menos claras serán las imágenes.

2.10.7 Configuración de parámetros de huellas dactilares

Configure el nivel de precisión de la huella digital. Cuanto mayor sea el nivel, menor será la tasa de reconocimiento falso. Esta función solo está disponible en modelos seleccionados.

2.10.8 Configuración del volumen

Procedimiento

- Paso 1 Sobre el **Menú principal**, seleccionar **Sistema>Volumen**.
- Paso 2 Seleccionar **Volumen del pitido** o **Volumen del micrófono**.
- Paso 3 Toque  para ajustar el volumen.

2.10.9 Restablecimiento de valores predeterminados de fábrica

Procedimiento

- Paso 1 Sobre el **Menú principal**, seleccionar **Sistema>Restaurar Fábrica**. Restaure los
- Paso 2 valores predeterminados de fábrica si es necesario.
 - **Restaurar Fábrica:** Restablece todas las configuraciones excepto las configuraciones de IP y el tipo de módulo de extensión.
 - **Restaurar fábrica (Guardar usuario y registro):** Restablece todas las configuraciones excepto la información del usuario y los registros.

2.10.10 Reiniciar el dispositivo

Sobre el **Menú principal**, seleccionar **Sistema>Reiniciar** y el dispositivo se reiniciará.

2.11 Gestión USB

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



- Asegúrese de que haya un USB insertado en el dispositivo antes de exportar datos o actualizar el sistema. A
Para evitar fallas, no extraiga el USB ni realice ninguna operación del Dispositivo durante el proceso.
- Tienes que usar un USB para exportar la información desde un controlador de acceso a otros dispositivos. Rostro
las imágenes no se pueden importar a través de USB.

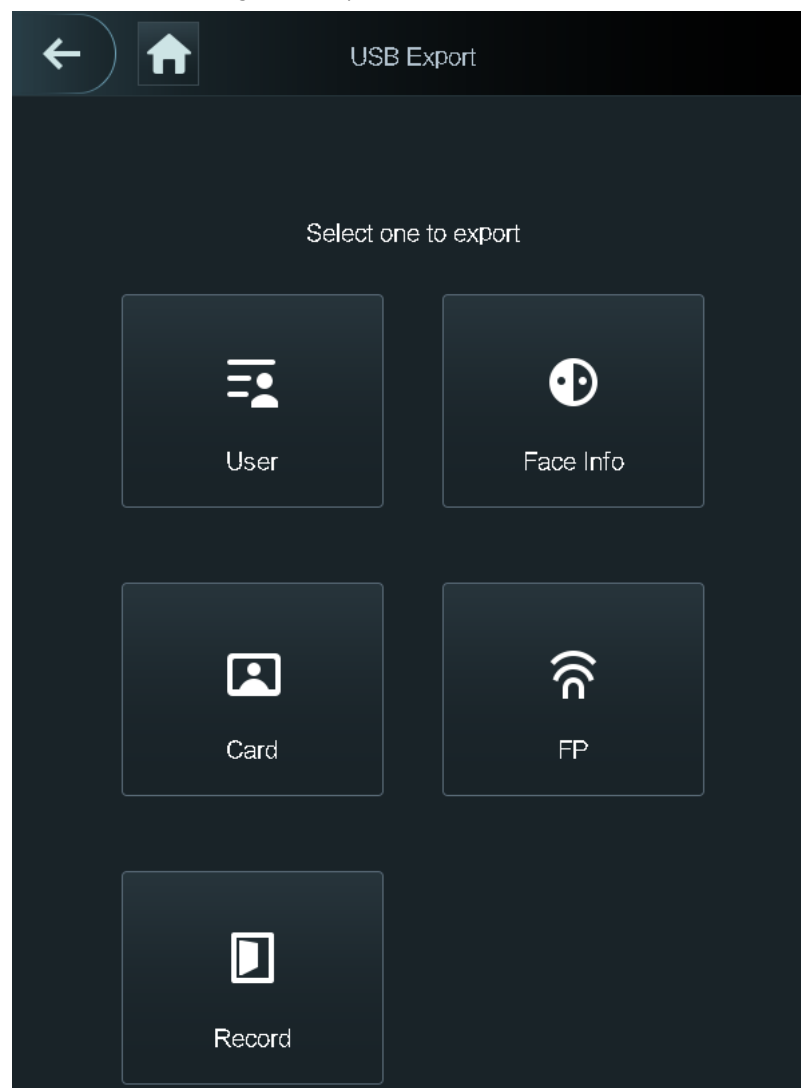
2.11.1 Exportando a USB

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

Procedimiento

- Paso 1 Sobre el **Menú principal**, seleccionar **USB>Exportación USB**.
- Paso 2 Seleccione el tipo de datos que desea exportar y luego toque **DE ACUERDO**.

Figura 2-19 Exportación USB



2.11.2 Importación desde USB

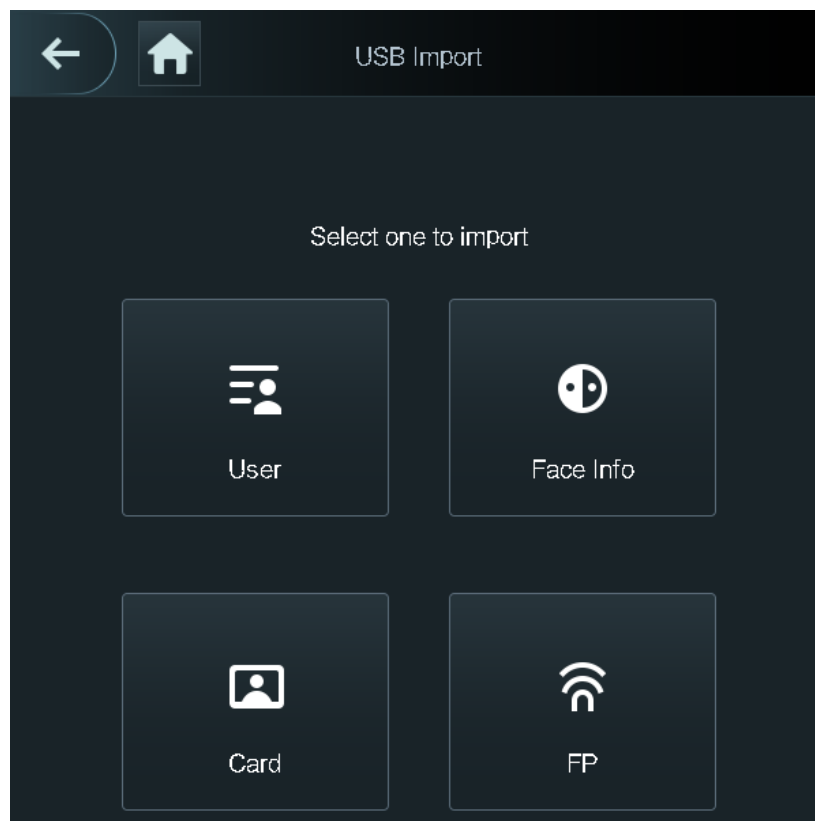
Puede importar datos desde USB al dispositivo.

Procedimiento

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

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

Figura 2-20 Importación USB



2.11.3 Sistema de actualización

Use un USB para actualizar el sistema del Dispositivo.

Procedimiento

- Paso 1** Cambie el nombre del archivo de actualización a "update.bin", colóquelo en el directorio raíz del USB y luego inserte el USB en el dispositivo.
- Paso 2** Sobre el **Menú principal**, seleccionar **USB > Actualización USB**. Grifo **DE**
- Paso 3** **ACUERDO**.
El dispositivo se reiniciará cuando se complete la actualización.

2.12 Configuración de funciones

Sobre el **Menú principal**, grifo **Características**.



Las características pueden diferir según los modelos del producto.

Figura 2-21 Configurar funciones

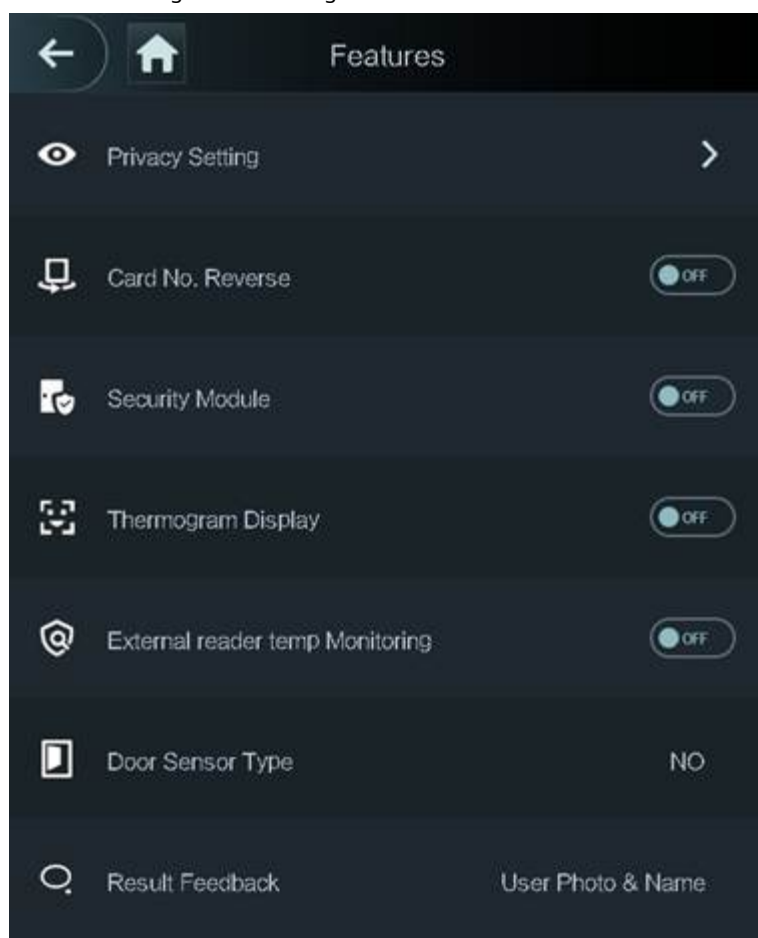


Tabla 2-11 Descripción de características

Parámetro	Descripción
Entorno privado	● PWD Reset Enable: Puede habilitar esta función para restablecer la contraseña. La función Restablecer PWD está habilitada de manera predeterminada. ● HTTPS: Hypertext Transfer Protocol Secure (HTTPS) es un protocolo para la comunicación segura a través de una red informática. Cuando HTTPS está habilitado, HTTPS se utilizará para acceder a los comandos CGI; de lo contrario, se utilizará HTTP.  Cuando HTTPS está habilitado, el dispositivo se reiniciará automáticamente. ● CGI: Common Gateway Interface (CGI) ofrece un protocolo estándar para que los servidores web ejecuten programas de manera similar a las aplicaciones de consola que se ejecutan en un servidor que genera dinámicamente páginas web. El CG I está habilitado por defecto. ● SSH: Secure Shell (SSH) es un protocolo de red criptográfico para operar servicios de red de forma segura en una red no segura. ● Capturar fotos: las imágenes de la cara se capturarán automáticamente cuando las personas abran la puerta. La función está activada por defecto. ● Modo de depuración: habilite este modo para mostrar la temperatura del cuerpo negro en la interfaz de espera. Puede corregir la temperatura del cuerpo negro en consecuencia.  Cuando este modo está habilitado, la puerta no se puede abrir por ningún método. ● Pantalla de temperatura: si está habilitada, la temperatura se mostrará cuando desbloquee la puerta. ● Borrar todas las fotos capturadas: elimina todas las fotos capturadas. ● Face Privacy: establezca diferentes niveles para desenfocar la imagen de la cara en la pantalla de espera.
Número de tarjeta Reverso	Cuando el controlador de acceso se conecta a un dispositivo de terceros a través de la entrada Wiegand, y el número de tarjeta leído por el controlador de acceso está en el orden de reserva del número de tarjeta real, debe encender el Número de tarjeta Reverso función.
Módulo de seguridad	● El módulo de seguridad no viene con el producto y el cliente debe comprarlo por separado. El módulo de seguridad necesita una fuente de alimentación independiente. ● Cuando el módulo de seguridad está encendido, el botón de salida, el control de bloqueo y el enlace de extinción de incendios no serán válidos.
Pantalla de termograma	Muestre un mapa de calor en la esquina superior izquierda.
Temperatura del lector externo Supervisión	Enciéndalo y el lector de tarjetas también controlará la temperatura de una persona.

Parámetro	Descripción
sensor de puerta	NC: cuando la puerta se abre, el circuito del sensor de la puerta está cerrado. NO: Cuando la puerta se abre, el circuito del sensor de puerta está abierto. Las alarmas de intrusión y tiempo extra se activan solo después de que se enciende el detector de puerta.
Comentarios sobre los resultados	● Éxito/Fracaso: solo muestra el éxito o el fracaso en la pantalla de espera. ● Solo nombre: muestra la ID de usuario, el nombre y el tiempo de autorización después de que se otorga el acceso; muestra el mensaje no autorizado y tiempo de autorización después del acceso denegado. ● Foto y nombre: muestra la imagen de la cara registrada del usuario, la identificación del usuario, el nombre y el tiempo de autorización después de que se otorga el acceso; muestra el mensaje no autorizado y el tiempo de autorización después del acceso denegado. ● Fotos y nombre: muestra la imagen de la cara capturada y una imagen de la cara registrada de un usuario, ID de usuario, nombre y tiempo de autorización después de otorgar el acceso; muestra el mensaje no autorizado y el tiempo de autorización después del acceso denegado.

2.13 Desbloqueo de la puerta

Puede desbloquear la puerta a través de caras, contraseñas, tarjetas y más. Los métodos de desbloqueo predeterminados son tarjeta/cara/contraseña.



Los métodos de desbloqueo pueden diferir según los modelos del producto.

2.13.1 Desbloqueo por Tarjetas

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

2.13.2 Desbloqueo por Rostro

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

2.13.3 Desbloqueo por contraseña de usuario

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

Procedimiento

- Paso 1** Grifo  en la pantalla de espera.
- Paso 2** Grifo **Desbloqueo de PCDy**, a continuación, introduzca el ID de usuario y la
- Paso 3** contraseña. Grifo **Sí**.

2.13.4 Desbloqueo por contraseña de administrador

Ingresa solo la contraseña de administrador para desbloquear la puerta. El dispositivo solo permite una contraseña de administrador. Uso de la contraseña de administrador para desbloquear la puerta sin estar sujeto a niveles de usuario, modos de desbloqueo, periodos, planes de vacaciones y anti-passback, excepto para puertas normalmente cerradas. Un dispositivo permite solo una contraseña de administrador.

requisitos previos

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

Información de contexto



La contraseña de administrador no se puede utilizar para desbloquear el estado de la puerta establecido en NC.

Procedimiento

- Paso 1Grifo en la pantalla de espera.
- Paso 2Grifo**PCD del administrador**, a continuación, introduzca la contraseña de administrador.
- Paso 3Grifo

2.13.5 Desbloqueo por Huella Dactilar

Coloque su dedo en el escáner de huellas dactilares. Esta función solo está disponible en modelos seleccionados.

2.14 Visualización de registros de desbloqueo

Puede ver los registros de desbloqueo de puertas.

Figura 2-22 Registros de búsqueda



User ID.	Name	Time	Status	Verify Mode
		09-05 17:21	Failed	Face
1	zxl	09-05 17:19	OK	Face
1	zxl	09-05 17:19	OK	Face
1	zxl	09-05 17:19	OK	Face
1	zxl	09-05 17:19	OK	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face
		09-05 17:18	Failed	Face

2.15 Configuración de la autocomprobación

Cuando usa el dispositivo por primera vez o cuando el dispositivo funciona mal, puede usar la función de prueba automática para verificar si el dispositivo puede funcionar normalmente. Pruebe de acuerdo con las indicaciones de la pantalla. Prueba

los artículos pueden diferir dependiendo de los modelos del producto.

Figura 2-23 Autocomprobación

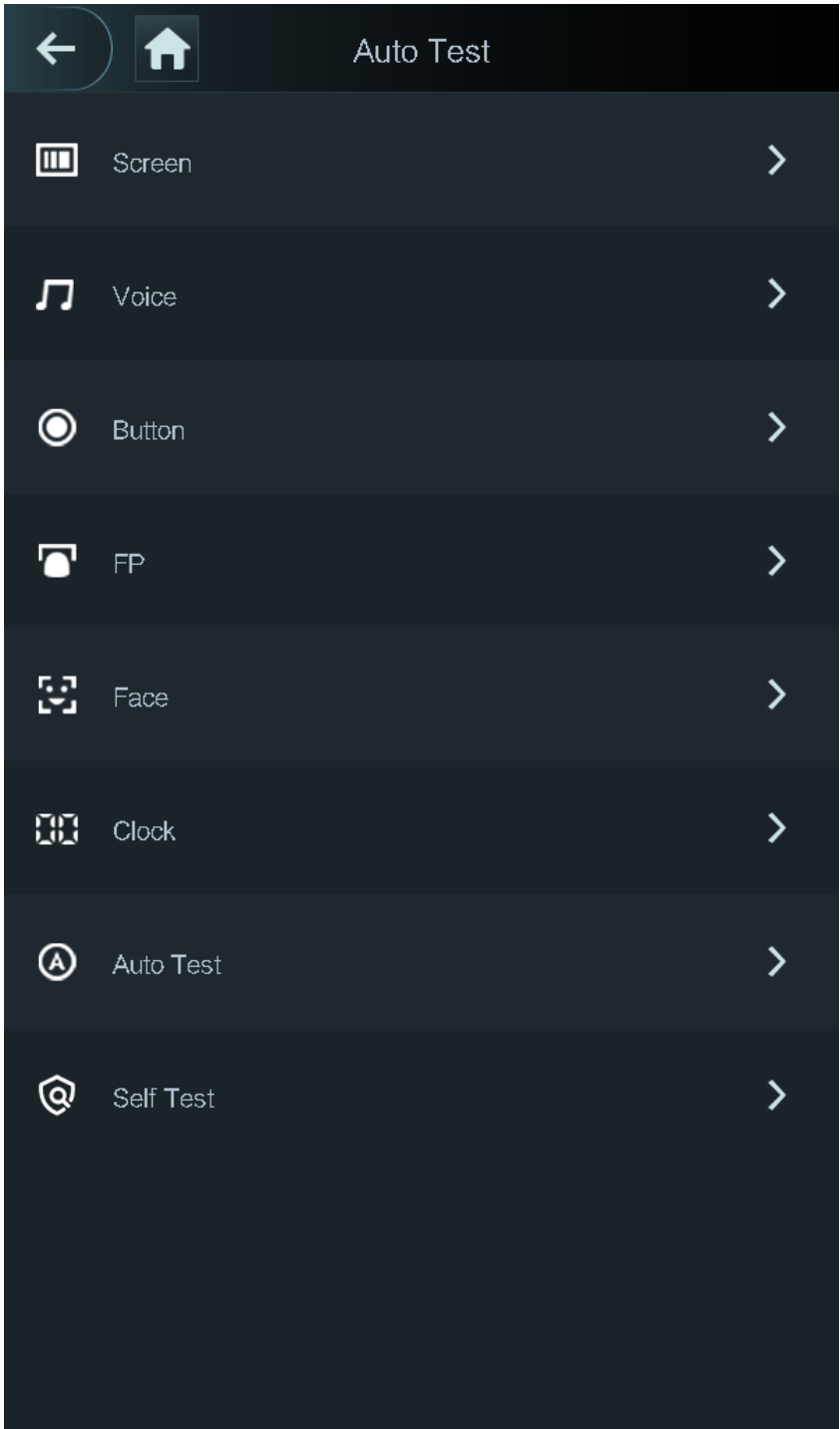


Tabla 2-12 Autodiagnóstico

Parámetro	Descripción
Pantalla	Prueba si la pantalla es normal.
Voz	Prueba si la voz es normal.
Botón	Prueba si la voz es normal.
FP	Pruebe si el reconocimiento de huellas dactilares es normal.
Rostro	Pruebe si el reconocimiento facial es normal.
Reloj	Prueba si el reloj es normal.

Parámetro	Descripción
Auto prueba	Todos los elementos anteriores se probarán automáticamente.
Autotest	El dispositivo prueba automáticamente el reloj RTC, la tarjeta de red, los chips de huellas dactilares y las cámaras, y proporciona los resultados de la prueba.

2.16 Información del sistema

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

2.16.1 Visualización de la capacidad de datos

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

2.16.2 Visualización de la versión del dispositivo

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

3 Operaciones Web

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

requisitos previos

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

Procedimiento

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



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

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



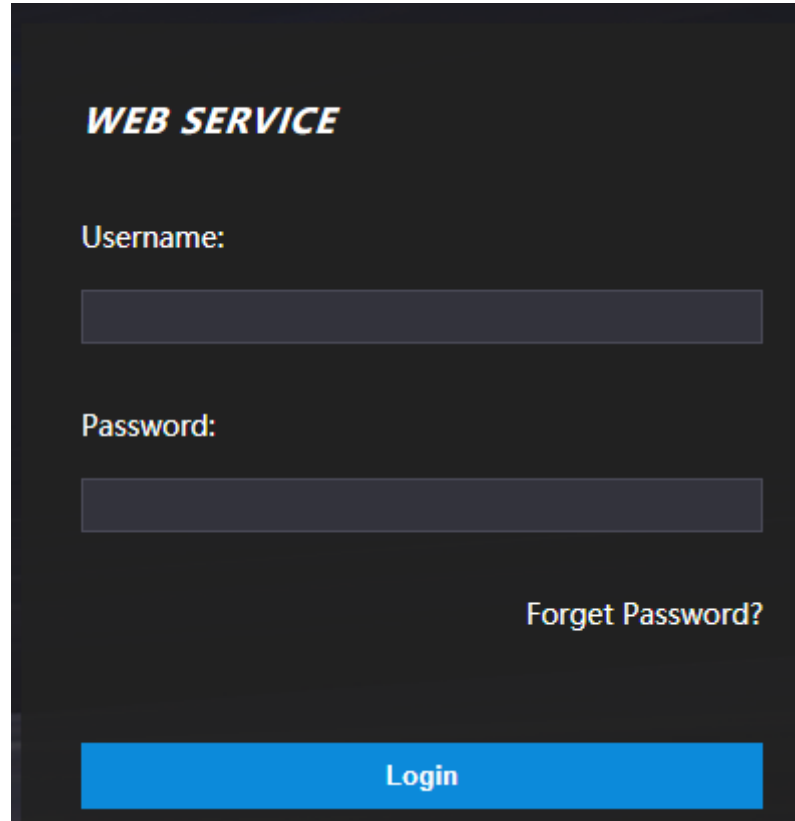
- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y especiales caracteres (excepto ' " ; &). Establezca una contraseña de alta seguridad siguiendo la contraseña indicador de fuerza.
- Mantenga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

3.2 Iniciar sesión

Procedimiento

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

Figura 3-1 Inicio de sesión



Paso 2 Introduzca el nombre de usuario y la contraseña.



- El nombre de administrador predeterminado es admin y la contraseña es la que configuró durante la inicialización. Le recomendamos que cambie la contraseña de administrador con regularidad para aumentar la seguridad.
- Si olvida la contraseña de inicio de sesión del administrador, puede hacer clic en **¿Contraseña olvidada?** Para detalles, consulte "3.3 Restablecimiento de la contraseña".

Paso 3 Hacer clic **Acceso**.

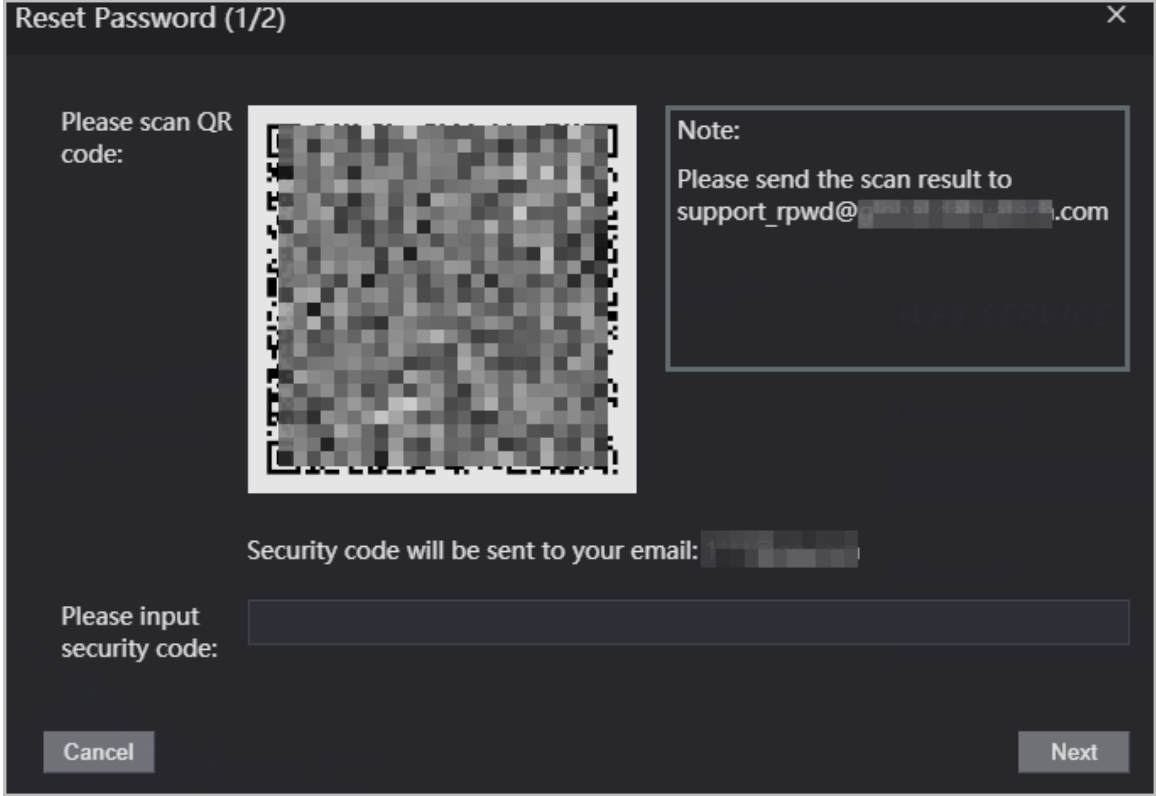
3.3 Restablecimiento de la contraseña

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

Procedimiento

- Paso 1** En la página de inicio de sesión, haga clic en **Has olvidado tu contraseña**.
- Paso 2** Lea atentamente las instrucciones en pantalla y luego haga clic en **DE ACUERDO**. Escanee el código QR y obtendrá el código de seguridad.
- Paso 3**

Figura 3-2 Restablecer contraseña



Reset Password (1/2)

Please scan QR code:

Note:
Please send the scan result to support_rpwd@[redacted].com

Security code will be sent to your email: [redacted]

Please input security code:

Cancel Next



- Se generarán hasta dos códigos de seguridad cuando se escanee el mismo código QR. Si el código de seguridad deja de ser válido, actualice el código QR y vuelva a escanear.
- Después de escanear el código QR, recibirá un código de seguridad en su correo electrónico vinculado DIRECCIÓN. Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, será convertirse en inválido.
- Si se ingresa el código de seguridad incorrecto seguido, la cuenta del administrador se congelará durante 5 minutos.

Etapas 4 Introduzca el código de seguridad.

Paso 5 Hacer clic **Próximo**.

Paso 6 Restablece y confirma la nueva contraseña.



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

Paso 7 Hacer clic **DE ACUERDO**.

3.4 Configuración de enlace de alarma

3.4.1 Configuración de enlace de alarma

Configure el enlace de alarma para activar alarmas cuando ocurran eventos de acceso anormales. Las configuraciones en la página web se sincronizarán con las configuraciones en la plataforma de administración si el

Se le agrega el dispositivo.

Procedimiento

- Paso 1**

Inicie sesión en la página web.
- Paso 2**

Seleccionar**Enlace de alarma>Enlace de alarma.**

Figura 3-3 Enlace de alarma

Alarm Linkage				
Refresh				
Alarm Input	Name	Alarm Input Type	Alarm Output Channel	Modify
1	Zone1	NO	1	
2	Zone2	NO	1	

- Paso 3**

Haga clic en y podrá modificar los parámetros de enlace de alarma.

Figura 3-4 Modificar parámetros de enlace de alarma

Modify

Alarm Input

1

Name

Zone1

Alarm Input Type

NO

Fire Link Enable

☐

Alarm Output Enable

☐

Duration (Sec.)

30

(1~300)

Alarm Output Channel

☒ 1

Access Link Enable

☐

Channel Type

NO

OK

Cancel

Tabla 3-1 Descripción de los parámetros de vinculación de alarmas

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

Parámetro	Descripción
Habilitar enlace de fuego	Si el enlace de incendio está habilitado, se activarán las alarmas de incendio, se producirán eventos de incendio y se vincularán las salidas de alarma y el acceso a la puerta.  Si el enlace de incendio está activado, la salida de alarma se activa mediante por defecto, y la puerta de acceso estará normalmente abierta cuando ocurran eventos de incendio por defecto.
Habilitar salida de alarma	Si la salida de alarma está activada, el relé generará mensajes de alarma.
Duración (seg.)	Duración de la alarma. Va desde 1 s hasta 300 s.
Canal de salida de alarma	Seleccione el canal de salida de alarma de acuerdo con su dispositivo de alarma.
Habilitar enlace de acceso	Después de encender el enlace de control de acceso, la puerta estará normalmente abierta o normalmente cerrada cuando haya señales de alarma de entrada. ● NO: La puerta normalmente está abierta cuando hay señales de alarma de entrada. ● NC: La puerta normalmente está cerrada cuando hay señales de alarma de entrada.
Tipo de canal	

Etapa 4

Hacer clic **DE ACUERDO**.

3.4.2 Visualización de registros de alarma

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Enlace de alarma** > **Registro de alarmas**.
- Paso 3** Seleccione un intervalo de tiempo y un tipo de alarma y, a continuación, haga clic en **Consulta**.

3.5 Configuración del intercomunicador

El dispositivo puede funcionar como una estación de puerta para realizar la función de videoportero.



Solo el dispositivo con intercomunicador admite esta función.

3.5.1 Configuración del servidor SIP

Cuando se conecta al mismo servidor SIP, todos los VTO y VTH pueden llamarse entre sí. Puedes usar el

Dispositivo u otros VTO o la plataforma de gestión como servidor SIP.

Información de contexto



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

Procedimiento

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

Paso 2 Seleccione un tipo de servidor.

- Utilice el dispositivo como servidor SIP. Encender **Servidor SIP** y mantener otros parámetros por defecto.

Figura 3-5 Usar el dispositivo como servidor SIP

SIP Server

SIP Server ☒ Enable

Server Type Express/DSS

IP Address Alternate IP Addr. 0.0.0.0

Port 5080 Alternate Username

Username 8001 Alternate Password

Password Alternate VTS IP Addr. 0.0.0.0

SIP Domain VDP Alternate Server ☐ Enable

SIP Server Username

SIP Server Password

Warning: The device needs reboot after modifying the SIP server enable.

OK Refresh Default

- Utilice otro VTO como servidor SIP:
 1. No habilitar **servidor SIP**. Seleccionar **VTO** desde el **Tipo de servidor**.
 2. Configure los parámetros y luego haga clic en **DE ACUERDO**.

Figura 3-6 Usar VTO como servidor SIP

SIP Server

SIP Server ☐ Enable

Server Type VTO

IP Address 192.168.1.1

Port 5060

Username 8001

Password

SIP Domain VDP

SIP Server Username

SIP Server Password

Warning: The device needs reboot after modifying the SIP server enable.

OK Refresh Default

Tabla 3-2 Configuración del servidor SIP

Parámetro	Descripción
Dirección IP	Dirección IP de la plataforma.
Puerto	● 5060 por defecto cuando VTO funciona como servidor SIP. ● 5080 por defecto cuando la plataforma funciona como servidor SIP.
Nombre de usuario	Déjalos como predeterminados.
Contraseña	
Dominio SIP	VDP.
Nombre de usuario del servidor SIP	El nombre de usuario y la contraseña de inicio de sesión del servidor SIP.
Contraseña del servidor SIP	

- Utilice DSS Express o DSS Pro como servidor SIP. No habilite **servidor SIP**. Seleccionar **Expreso/DSS** desde el **Tipo de servidor**.

Figura 3-7 Usar DSS Express o DSS Pro como servidor SIP

SIP Server

SIP Server ☐ Enable

Server Type Express/DSS

IP Address

Port 5080

Username 8001

Password

SIP Domain VDP

SIP Server Username

SIP Server Password

Alternate IP Addr. 0.0.0.0

Alternate Username

Alternate Password

Alternate VTS IP Addr. 0.0.0.0

Alternate Server ☐ Enable

Warning: The device needs reboot after modifying the SIP server enable.

OK Refresh Default

Tabla 3-3 Configuración del servidor SIP

Parámetro	Descripción
Dirección IP	Dirección IP de la plataforma.
Puerto	● 5060 por defecto cuando VTO funciona como servidor SIP. ● 5080 por defecto cuando la plataforma funciona como servidor SIP.
Nombre de usuario	Déjalos como predeterminados.
Contraseña	
Dominio SIP	Déjalo como predeterminado.
Nombre de usuario del servidor SIP	El nombre de usuario y la contraseña de inicio de sesión de la plataforma.
Contraseña del servidor SIP	
Dirección IP alternativa	El servidor alternativo se utilizará como servidor SIP cuando DSS Express o DSS Pro no respondan. Le recomendamos que configure la dirección IP alternativa. ● Si enciendes el Servidor alternativo función, configurará la Dispositivos del servidor alternativo. ● Si desea que otro VTO funcione como servidor alternativo, debe ingresar la dirección IP, el nombre de usuario y la contraseña del VTO. Hacer no habilitar Servidor alternativo en este caso. ● Le recomendamos que configure el VTO principal como servidor alternativo.
Nombre de usuario alternativo	Se utiliza para iniciar sesión en el servidor alternativo.
Contraseña alternativa	
Dirección IP VTS alternativa	Introduzca la dirección IP del VTS alternativo. Cuando la plataforma de gestión no responde, el VTS alternativo se activará para asegurarse de que VTO, VTH y VTS aún puedan realizar la función de videoportero.

Paso 3

Hacer clic **DE ACUERDO**.

3.5.2 Configuración de parámetros básicos

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

Procedimiento

Paso 1 Seleccionar **Replicar** > **Local**.

Paso 2 Configure los parámetros.

- Utilice el dispositivo como servidor SIP.

Figura 3-8 Parámetro básico

Local

Device Type: Unit Door Station

Centre Call No.: 888888

VTO No.: 8001

Group Call: ☐ Warning: The device will be rebooted after modifying group call enable status.

Transmission Mode: ☒ Mode1 ☐ Mode2

Confirm Refresh Default

Tabla 3-4 Descripción de parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccionar Estación de puerta de la unidad .
VTO No.	El número del VTO, que no se puede configurar.
Llamada de grupo	Cuando enciende la función de llamada grupal, el VTO llama al VTH principal y a las extensiones al mismo tiempo.
Número de llamada del centro	El número de teléfono predeterminado es 888888 + VTS No. cuando el VTO llama al VTS. Puede comprobar el número de VTS desde el Dispositivo pantalla de VTS.
Modo de transmisión	El modo 1 está seleccionado de forma predeterminada.

- Utilice otro VTO como servidor SIP.

Figura 3-9 Parámetro básico

Local

Device Type: Unit Door Station

Centre Call No.: 888888

VTO No.: 8001

Transmission Mode: ☒ Mode1 ☐ Mode2

Confirm Refresh Default

Tabla 3-5 Descripción de parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccionar Estación de puerta de la unidad .

Parámetro	Descripción
VTO No.	El número del VTO.  ● El número debe tener cuatro dígitos. Los primeros dos dígitos son 80, y los dos últimos dígitos comienzan desde 01. Por ejemplo, 8001. ● Si existen varios VTO en una unidad, el número de VTO no se puede repetir.
Número de llamada del centro	El número de teléfono predeterminado para el centro de gestión es 888888. Manténgalo como predeterminado.
Modo de transmisión	El modo 1 está seleccionado de forma predeterminada.

- Utilice la plataforma (DSS Express o DSS Pro) como servidor SIP.

Figura 3-10 Parámetro básico

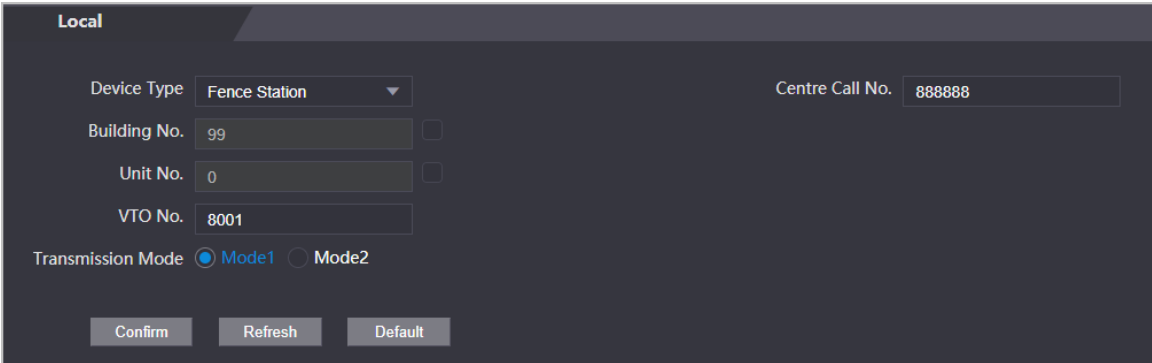


Tabla 3-6 Descripción de parámetros básicos

Parámetro	Descripción	
Tipo de dispositivo	Seleccione el tipo de dispositivo según la posición de instalación.	
Edificio número.	Seleccione la casilla de verificación y luego ingrese el número del edificio donde está instalada la estación de puerta de la unidad.	Si el edificio y la unidad están habilitados en DSS, ingrese el número de edificio y el número de unidad en la página web. El número de edificio, el número de unidad y el número de VTO deben cumplir con los parámetros configurados en DSS.  Tome la habitación 1001, la unidad 2 y el edificio 1 como un ejemplo. Si el número de edificio está habilitado en el DSS y la unidad no está habilitada, la habitación el número es "1#1001". Si el edificio y la unidad son ambos habilitados, el número de habitación es "1#2#1001". Si el edificio no está habilitado y la unidad no está habilitado tampoco, el número de habitación es "1001". Para detalles, consulte el manual de usuario de DSS.
Numero de unidad.	Seleccione la casilla de verificación y luego ingrese el número de la unidad donde se encuentra la estación de puerta de la unidad. instalado.	
VTO No.	El número de la estación de puerta de la unidad.  Si existen varios VTO en una unidad, el VTO No. no se puede repetir	
Número de llamada del centro	El número de teléfono predeterminado es 888888 cuando el VTO llama al VTS. Manténgalo como predeterminado.	
Transmisión Modo	El modo 1 está seleccionado de forma predeterminada.	

Paso 3 Hacer clic **Confirmar**.

3.5.3 Agregar el VTO

Cuando el dispositivo funciona como servidor SIP y tiene otros VTO, debe agregar otros VTO al servidor SIP para asegurarse de que puedan llamarse entre sí.

Procedimiento

- Paso 1

En la página web del dispositivo, seleccione**Configuración de intercomunicación>Gestión de número de**
- Paso 2

VTO. Hacer clic**Agregar** luego configure el VTO.

Figura 3-11 Agregar VTO

Add

Rec No.

Register Password

Build No.

Unit No.

IP Address

Username

Password

OK

Cancel

Tabla 3-7 Agregar configuración de VTO

Parámetro	Descripción
No. de registro	El número del VTO agregado. Puede comprobar el número de la Dispositivo página en la página web de la VTO.
Registro Contraseña	Manténgalo predeterminado.
construir no.	No se puede configurar.
Numero de unidad.	
Dirección IP	La dirección IP del VTO agregado.
Nombre de usuario	El nombre de usuario y la contraseña utilizados para iniciar sesión en la página web del VTO agregado.
Contraseña	

- Paso 3

Hacer clic**DE ACUERDO**.

3.5.4 Agregando el VTH

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

Información de contexto



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

Procedimiento

Paso 1 En la página de inicio, seleccione **Configuración de intercomunicación > Gestión de número de habitación**.

Paso 2 Agregue el VTH.

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

Figura 3-12 Agregar individualmente

Add [Close]

First Name [Text Box]

Last Name [Text Box]

Nick Name [Text Box]

Room No. [Text Box] *

Register Type [public ▼]

Register Password [Text Box] *

[OK] [Cancel]

Tabla 3-8 Información de la habitación

Parámetro	Descripción
Habitación no.	Ingrese el número de habitación del VTH. ● El número de habitación consta de 1 a 5 dígitos y debe coincidir con el número de habitación configurado en el VTH. ● Cuando hay VTH principal y extensiones, el número de habitación del VTH principal termina en -0 y el número de habitación de la extensión termina en -1, -2 o -3. Por ejemplo, el VTH principal es 101-0, y el número de habitación de la extensión es 101-1, 101-2... ● Si la función de llamada de grupo no está activada, no se puede configurar el número de habitación en el formato 9901-xx.
Nombre de pila	Ingrese el nombre del VTH para ayudarlo a diferenciar los VTH.
Apellido	
Apodo	
Tipo de registro	Manténgalos como predeterminados.
Contraseña registrada	

● Añadir en lotes

1. Haga clic en **Agregar lote**
2. Configure los parámetros.

Figura 3-13 Agregar lote

Unit Layer Amount: 5

Room Amount in One Layer: 4

First Floor Number: 101

Second Floor Number: 201

Add

Tabla 3-9 Adición de lotes

Parámetro	Descripción
Cantidad de capa de unidad	El número de pisos del edificio (que va del 1 al 99).
Cantidad de habitación en una capa	El número de habitaciones en cada piso, que va de 1 a 99.
Número del primer piso	La primera habitación en el primer piso.
Número del segundo piso	La primera habitación en el segundo piso, que es igual a la primera habitación en el primer piso más el número de habitaciones en cada piso.

3.5.5 Adición del VTS

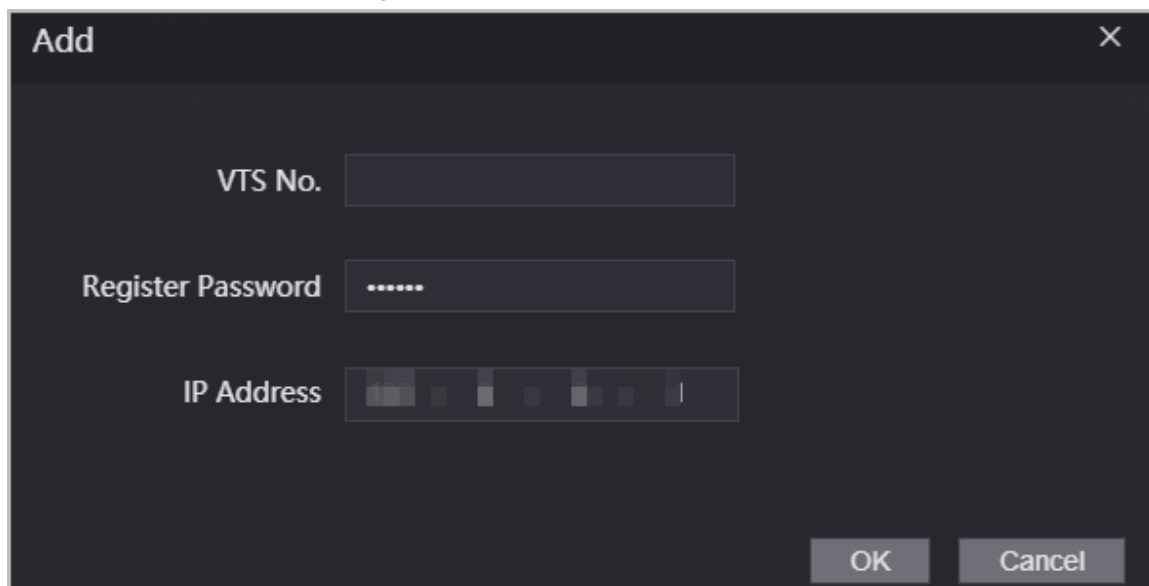
Cuando el dispositivo funciona como servidor SIP, puede agregar VTS al servidor SIP para asegurarse de que

pueden llamarse unos a otros.

Procedimiento

- Paso 1** En la página de inicio, seleccione **Configuración de intercomunicación > Gestión VTS**. Hacer clic **Agregar** establecer parámetros.
- Paso 2**

Figura 3-14 Gestión de VTS



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

3.5.6 Visualización del estado del dispositivo

Cuando el dispositivo funciona como servidor SIP, puede ver el estado de los dispositivos que están conectados al servidor SIP. En la página de inicio, seleccione **Configuración de intercomunicación > Estado**.

3.5.7 Visualización de registros de llamadas

Ver todo el registro de llamadas salientes y llamadas entrantes. En la página de inicio, seleccione **Configuración de intercomunicación > Llamar**.

3.6 Capacidad de datos

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

3.7 Configuración de vídeo e imagen

Configurar parámetros de video e imagen. Los parámetros pueden diferir según los modelos del producto. Le recomendamos que utilice los parámetros predeterminados en esta sección.

3.7.1 Configuración de vídeo

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

exposición.

Información de contexto

- Estándar de video: Seleccionar**NTSC**.
- ID de canal: el canal 1 es para configuraciones de imagen de luz visible. El canal 2 es para configuraciones de imagen de luz infrarroja.
- Predeterminado: Restaurar a la configuración predeterminada.
- Capturar: toma una instantánea de la imagen actual.



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

3.7.1.1 Configuración del Canal 1

Procedimiento

- Paso 1 Seleccionar**Configuración de vídeo>Configuración de**
- Paso 2 **vídeo**. Seleccionar**1**desde el**número de canal**lista.
- Paso 3 Configurar la tasa de fecha.

Figura 3-15 Tasa de fecha

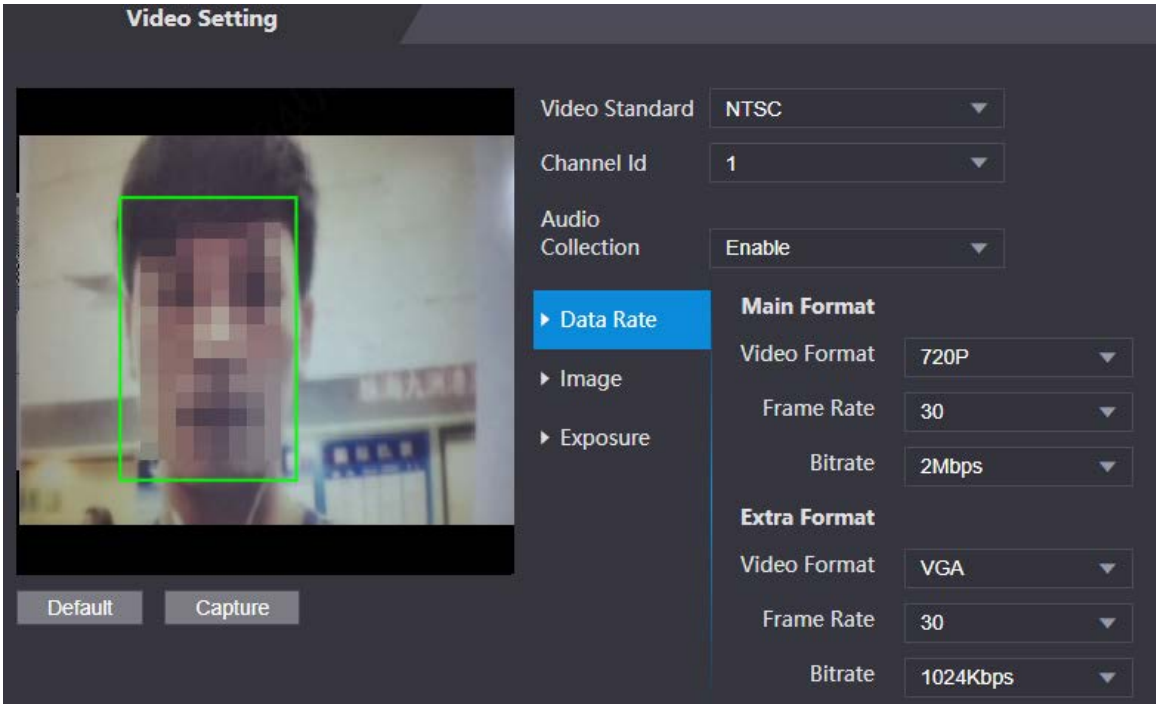


Tabla 3-11 Descripción de tasa de fecha

Parámetro		Descripción
Formato principal	Formato de video	Cuando el dispositivo funciona como un VTO y conecta el VTH, el límite de flujo adquirido de VTH es 720p. Cuando la resolución se cambia a 1080p, la función de llamada y monitoreo puede verse afectada.
	Cuadros por segundo	El número de fotogramas (o imágenes) por segundo. El rango de velocidad de fotogramas es de 1 a 25 fps.

Parámetro		Descripción
	tasa de bits	Indica la cantidad de datos transmitidos a través de una conexión a Internet en un período de tiempo determinado. Seleccione un ancho de banda adecuado según la velocidad de su red.
Transmisión adicional	Formato de video	La transmisión secundaria es compatible con D1, VGA y QVGA.
	Cuadros por segundo	El número de fotogramas (o imágenes) por segundo. El rango de velocidad de fotogramas es de 1 a 25 fps.
	tasa de bits	Indica la cantidad de datos transmitidos a través de una conexión a Internet en un período de tiempo determinado.

Etap 4 Configura la imagen.

Figura 3-16 Imagen

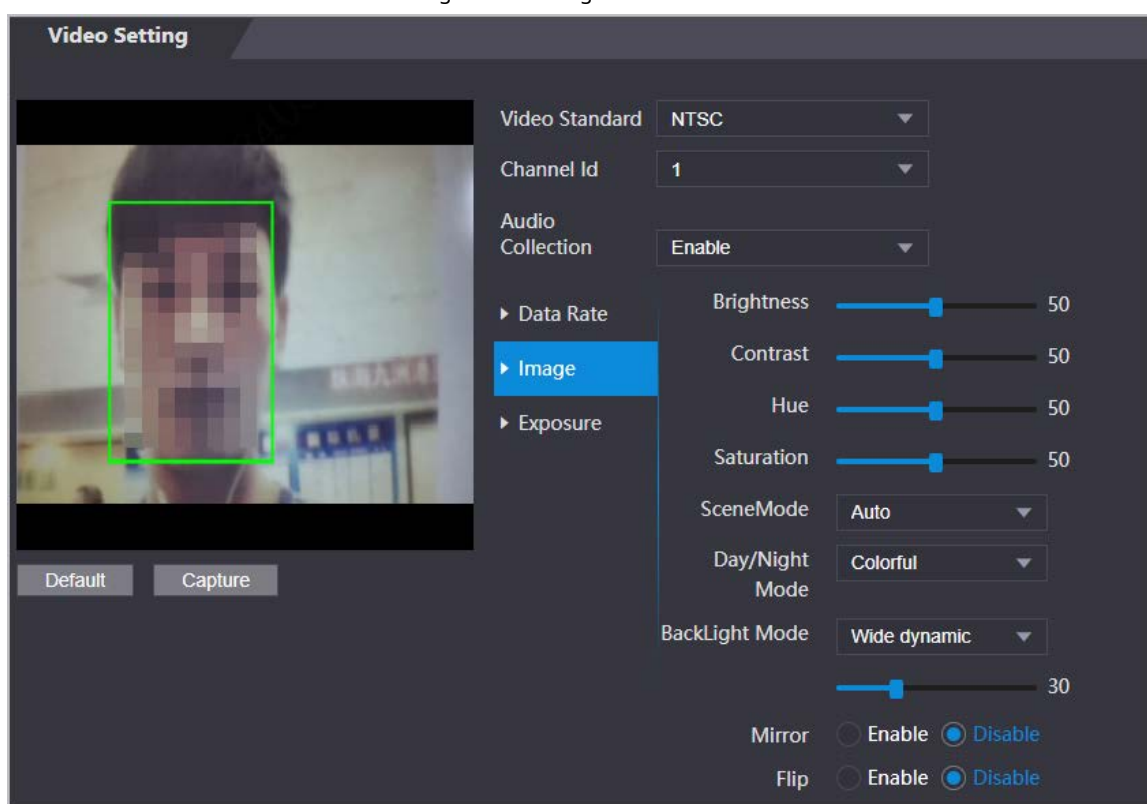


Tabla 3-12 Descripción de la imagen

Parámetro	Descripción
Brillo	El brillo es la claridad u oscuridad relativa de un color en particular. Cuanto mayor sea el valor, más brillante será la imagen.
Contraste	El contraste es la diferencia en la luminancia o el color que hace que un objeto sea distinguible. Cuanto mayor sea el valor de contraste, mayor será el contraste de color.
Matiz	Se refiere a la fuerza o saturación de un color. Describe la intensidad del color, o cuán puro es.

Parámetro	Descripción
Saturación	La saturación de color indica la intensidad del color en una imagen. A medida que aumenta la saturación, el color parece más fuerte, por ejemplo, más rojo o más azul.  El valor de saturación no cambia el brillo de la imagen.
Modo escena	El tono de la imagen es diferente en diferentes modos de escena. ● Cerca: La función del modo de escena está desactivada. ● Auto: El sistema ajusta automáticamente el modo de escena en función de la sensibilidad fotográfica. ● Soleado: En este modo, se reducirá el tono de la imagen. ● Noche: En este modo, se aumentará el tono de la imagen.
Día/Noche	El modo Día/Noche afecta la compensación de luz en diferentes situaciones. ● Auto: El sistema ajusta automáticamente el modo día/noche en función de la sensibilidad fotográfica. ● Vistoso: En este modo, las imágenes son coloridas. ● En blanco y negro: En este modo, las imágenes son en blanco y negro.
Modo de luz de fondo	● Cerca: La compensación de contraluz está desactivada. ● Iluminar desde el fondo: La compensación de contraluz trae automáticamente más luz a las áreas más oscuras de una imagen cuando la luz brillante que brilla desde atrás las oscurece. ● Amplia dinámica: El sistema atenúa las áreas brillantes y compensa las áreas oscuras para crear un equilibrio que mejore la calidad general de la imagen. ● Inhibición: La compensación de altas luces (HLC) es una tecnología utilizada en cámaras de seguridad CCTV/IP para tratar imágenes que están 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 estos puntos para mejorar la calidad general de la imagen.
Espejo	Cuando la función está activada, las imágenes se mostrarán con los lados izquierdo y derecho invertidos.
Voltear	Cuando esta función está activada, las imágenes se pueden voltear.

Paso 5 Configure los parámetros de exposición.

Figura 3-17 Exposición

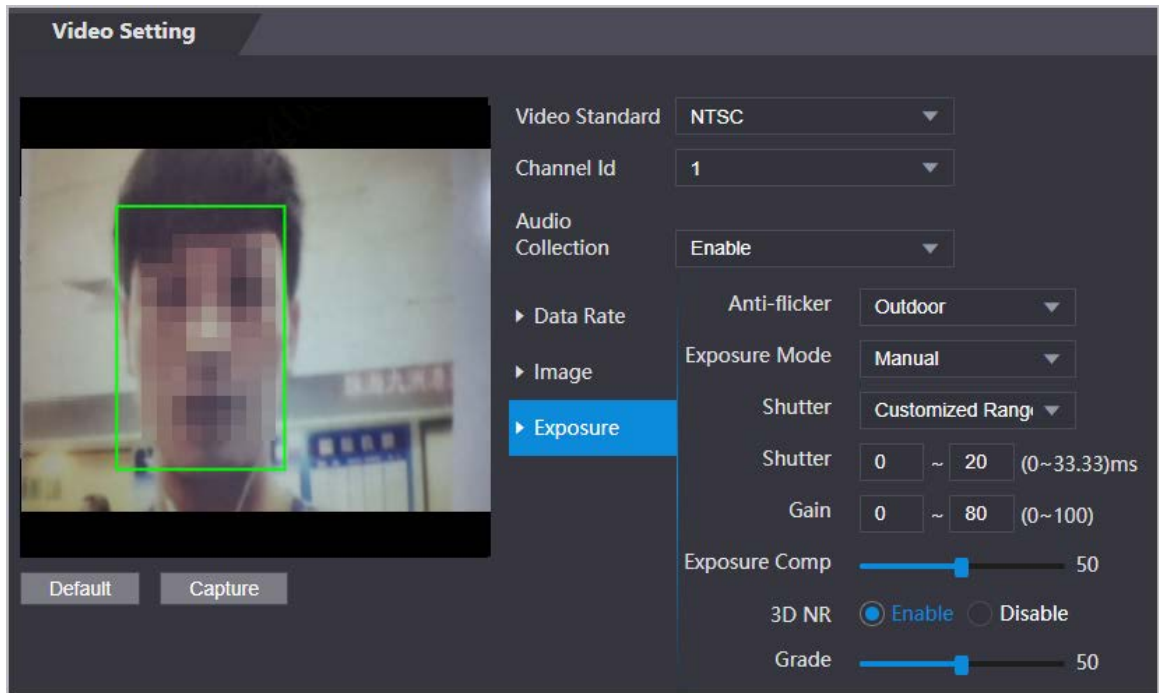


Tabla 3-13 Descripción del parámetro de exposición

Parámetro	Descripción
Contra parpadeo	Establezca antiparpadeo para reducir el parpadeo y los colores o la exposición desiguales. ● 50Hz: Cuando la alimentación de red es de 50 Hz, la exposición se ajusta automáticamente para evitar la aparición de líneas horizontales. ● 60Hz: Cuando la fuente de alimentación principal es de 60 Hz, la exposición se ajusta automáticamente para reducir la aparición de líneas horizontales. ● Exterior: Cuando Exterior está seleccionado, se puede cambiar el modo de exposición.
Modo de exposición	Puede establecer la exposición para ajustar el brillo de la imagen. ● Auto: El dispositivo ajusta automáticamente el brillo de las imágenes. ● Prioridad de obturador: Access Terminal ajustará el brillo de la imagen según el rango de exposición del obturador. Si el brillo de la imagen no es suficiente y el valor del obturador ha alcanzado su límite superior o inferior, el dispositivo ajustará el valor de ganancia automáticamente al nivel de brillo ideal. ● Manual: Puede configurar la ganancia y el valor del obturador manualmente para ajustar el brillo de la imagen.  ◇ cuando seleccionas Exterior desde el Contra parpadeo lista, puedes seleccionar Prioridad de obturador como el modo de exposición. ◇ El modo de exposición puede diferir dependiendo de los diferentes modelos de Dispositivo.
Obturador	La persiana es un componente que permite el paso de la luz durante un tiempo determinado. Cuanto mayor sea la velocidad de obturación, menor será el tiempo de exposición y más oscura la imagen.
Ganar	Cuando se establece el rango de valores de ganancia, se mejorará la calidad del video.

Parámetro	Descripción
Exposición Compensación	Puede hacer una foto más brillante o más oscura ajustando el valor de compensación de exposición.
NR 3D	Cuando la reducción de ruido 3D (RD) está activada, el ruido del video se puede reducir para garantizar videos de alta definición.
Calificación	Puede establecer su calificación cuando esta función está activada.

3.7.1.2 Configuración del Canal 2

Procedimiento

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

Paso 2 **vídeo**. Seleccione 2 de la **número de canal**. Configura el

Paso 3 estado del vídeo.



Recomendamos que encienda la función WDR cuando la cara esté a contraluz.

Figura 3-18 Imagen

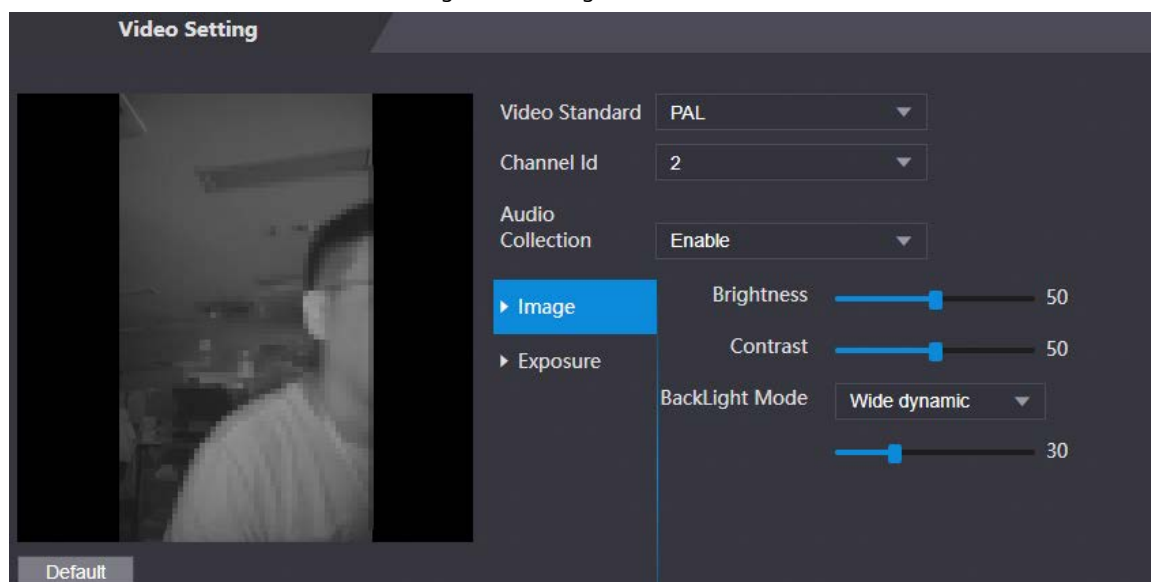


Tabla 3-14 Descripción de la imagen

Parámetro	Descripción
Brillo	El brillo es la claridad u oscuridad relativa de un color en particular. Cuanto mayor sea el valor, más brillante será la imagen.
Contraste	El contraste es la diferencia en la luminancia o el color que hace que un objeto sea distinguible. Cuanto mayor sea el valor de contraste, mayor será el contraste de color.

Parámetro	Descripción
Modo de luz de fondo	● Cerca: La compensación de contraluz está desactivada. ● Iluminar desde el fondo: La compensación de luz negra trae automáticamente más luz a las áreas más oscuras de una imagen cuando la luz brillante que brilla desde atrás las oscurece. ● Amplia dinámica: El sistema atenúa las áreas brillantes y compensa las áreas oscuras para garantizar la creación de un equilibrio que mejore la calidad general de la imagen. ● Inhibición: La compensación de altas luces (HLC) es una tecnología utilizada en cámaras de seguridad CCTV/IP para tratar imágenes que están 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 estos puntos para mejorar la calidad general de la imagen.

Etapas 4 Configure los parámetros de exposición.

Figura 3-19 Parámetro de exposición

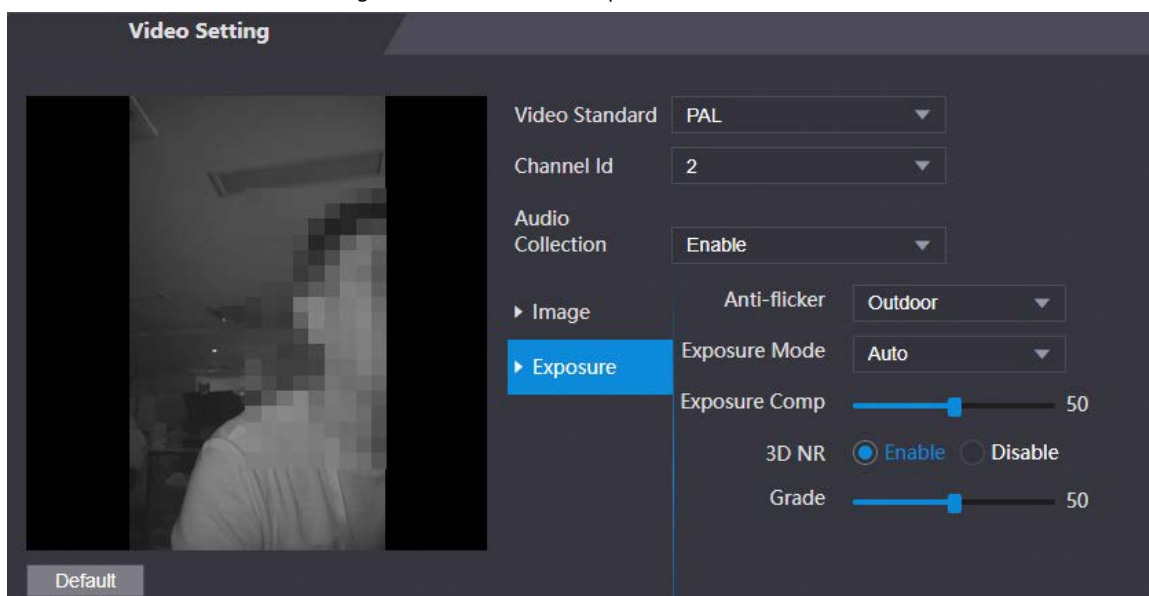


Tabla 3-15 Descripción del parámetro de exposición

Parámetro	Descripción
Contra parpadeo	Configure antiparpadeo para reducir el parpadeo y disminuir o eliminar los colores o la exposición desiguales. ● 50Hz: Cuando la alimentación de red es de 50 Hz, la exposición se ajusta automáticamente para evitar la aparición de líneas horizontales. ● 60 Hz: Cuando la fuente de alimentación principal es de 60 Hz, la exposición se ajusta automáticamente para reducir la aparición de líneas horizontales. ● Exterior: Cuando Exterior está seleccionado, se puede cambiar el modo de exposición.

Parámetro	Descripción
Modo de exposición	Puede establecer la exposición para ajustar el brillo de la imagen. ● Auto: El dispositivo ajusta automáticamente el brillo de las imágenes. ● Prioridad de obturador: Access Terminal ajustará el brillo de la imagen según el rango de exposición del obturador. Si el brillo de la imagen no es suficiente y el valor del obturador ha alcanzado su límite superior o inferior, el dispositivo ajustará el valor de ganancia automáticamente al nivel de brillo ideal. ● Manual: Puede configurar la ganancia y el valor del obturador manualmente para ajustar el brillo de la imagen.  ◇ cuando seleccionas Exterior desde el Contra parpadeo lista, puede seleccionar Prioridad de obturador como el modo de exposición. ◇ El modelo de exposición puede diferir según los diferentes modelos de dispositivo.
Obturador	Obturador es un dispositivo que permite el paso de la luz durante un tiempo determinado. Cuanto mayor sea la velocidad de obturación, menor será el tiempo de exposición y más oscura la imagen.
Ganar	Cuando se establece el rango de valores de ganancia, se mejorará la calidad del video.
Compensación de exposición	Puede hacer una foto más brillante o más oscura ajustando el valor de compensación de exposición.
NR 3D	Cuando la reducción de ruido 3D (RD) está activada, el ruido del video se puede reducir para garantizar videos de alta definición.
Calificación	Puede establecer su calificación cuando esta función está activada.

3.7.2 Configuración del volumen

Puede ajustar el volumen del altavoz.

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Configuración de vídeo** > **Configuración de volumen**.
- Paso 3** Arrastre el control deslizante para ajustar el volumen. Hacer clic **DE**
- Etapas 4** **ACUERDO**.

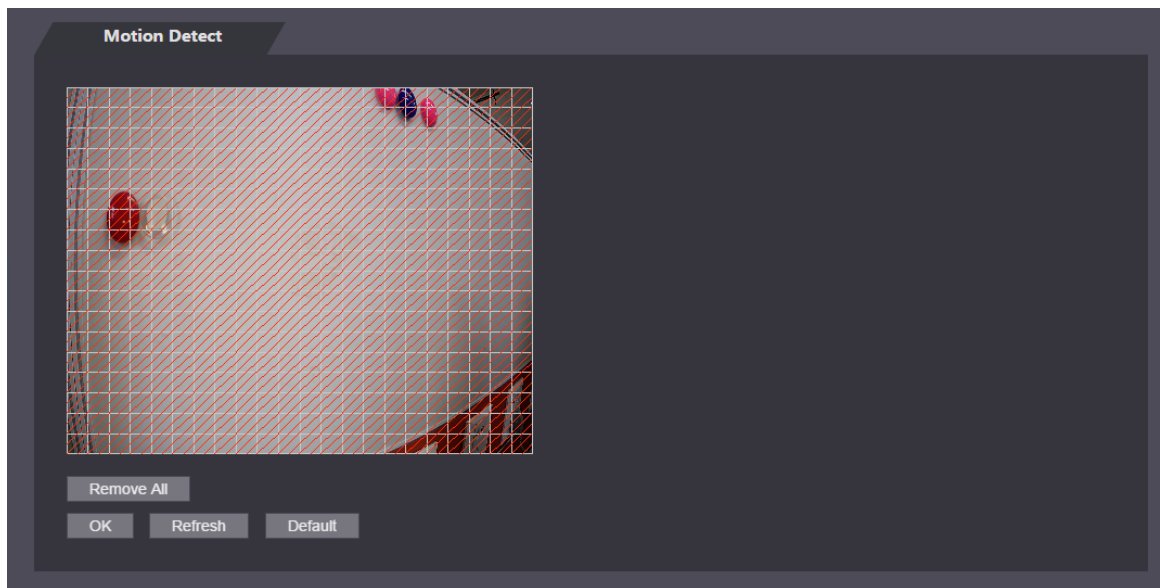
3.7.3 Configuración de la detección de movimiento

Establezca un rango en el que se puedan detectar objetos en movimiento.

Procedimiento

- Paso 1** Seleccionar **Configuración de vídeo** > **Configuración de vídeo** > **Detección de movimiento**.

Figura 3-20 Área de detección de movimiento



Paso 2 Mantenga presionado el botón izquierdo del mouse y luego arrastre el mouse en el área roja.



- Los rectángulos rojos son el área de detección de movimiento. El rango de detección de movimiento predeterminado es todo los rectángulos
- Para dibujar un área de detección de movimiento, debe hacer clic en **Eliminar todo** primero.
- El área de detección de movimiento que dibuje será un área sin detección de movimiento si dibuja el área de detección de movimiento predeterminada.

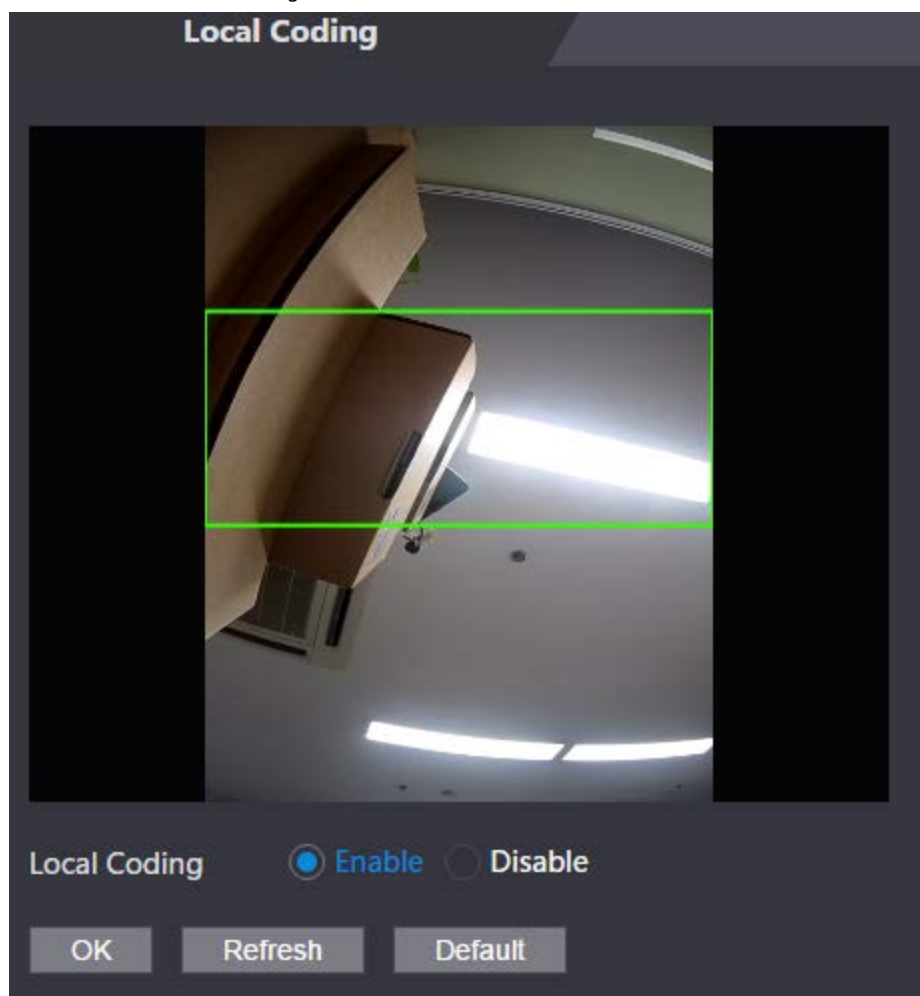
3.7.4 Configuración de la codificación local

Configure el área que se mostrará en los monitores interiores. Esta función solo está disponible en modelos seleccionados.

Procedimiento

- Paso 1** Inicie sesión en la página web.
- Paso 2** Seleccionar **Audio video** > **Codificación local**.
- Paso 3** Seleccionar **Permitir** para activar la función.
- Etapas 4** Arrastre el cuadro.

Figura 3-21 Codificación local



Paso 5

Hacer clic **DE ACUERDO**.

3.7.5 Configuración del modo de imagen

Seleccione el modo de imagen según el sitio de instalación de Access Controller.

Procedimiento

Paso 1

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

Paso 2

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

- Interior: el dispositivo se instala en interiores, como oficinas. La luz artificial está uniforme al otro lado de la habitación y no hay luz natural.
- Exterior: el dispositivo está instalado al aire libre y la luz del día es brillante y uniforme.
- Otro: El rostro humano está a contraluz, lo que hace que el rostro se oscurezca. Le recomendamos que seleccione otro modo para que sea más fácil de detectar para el controlador de acceso.

Paso 3

Hacer clic **DE ACUERDO**.

3.8 Configuración de la detección de rostros

Puede configurar parámetros faciales para aumentar la precisión del reconocimiento facial.

Procedimiento

Paso 1

Inicie sesión en la página web.

Paso 2 Seleccionar **Detección de rostro**.

Paso 3 Configure los parámetros.



Las siguientes imágenes son solo para referencia. Los parámetros de detección de rostros pueden diferir dependiendo de los modelos del producto.

Figura 3-22 Detección de rostros (con módulo de monitoreo de temperatura)

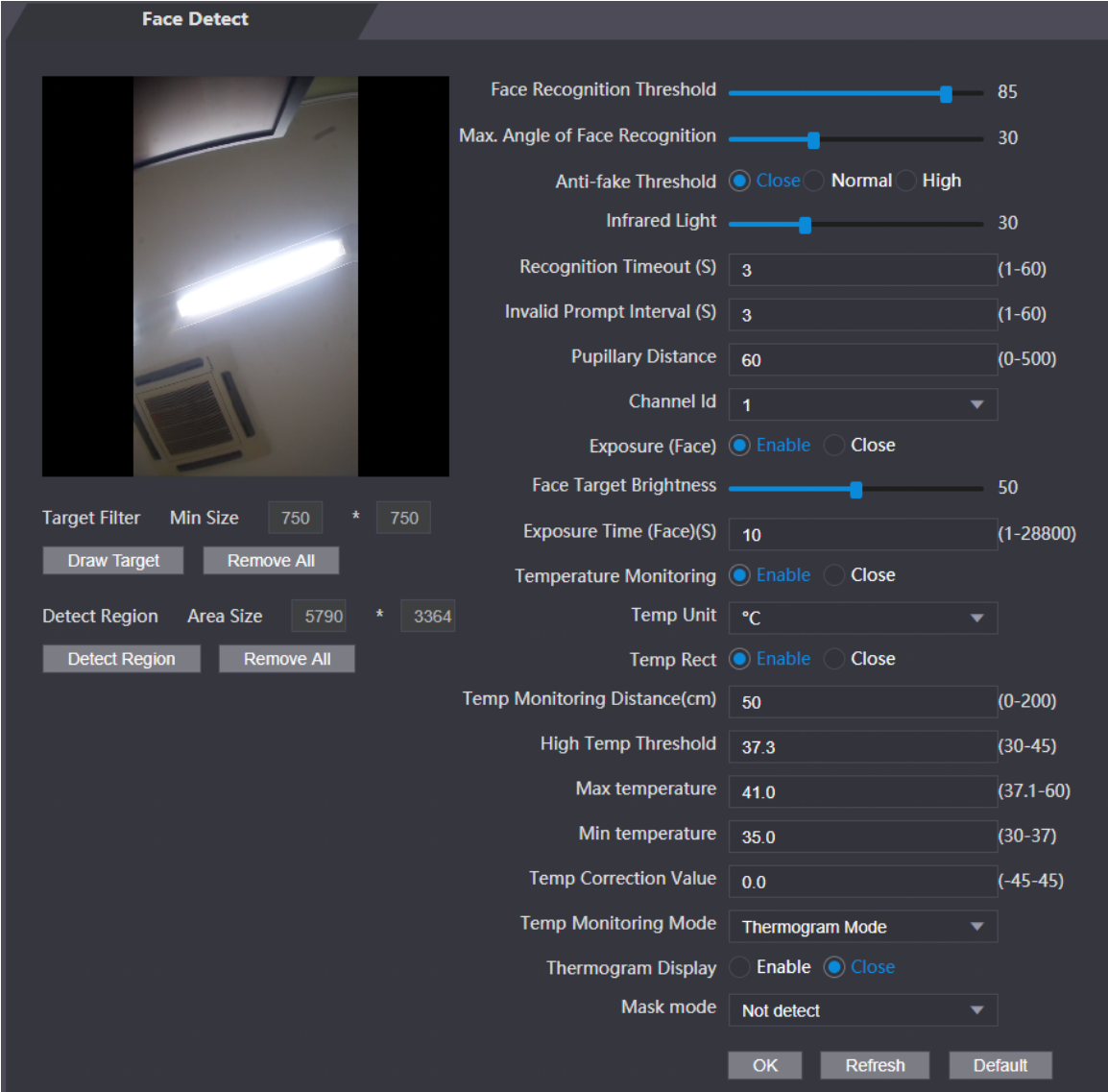


Tabla 3-16 Descripción de los parámetros de detección de rostros (con módulo de monitoreo de temperatura)

Parámetro	Descripción
Umbral de reconocimiento facial	Ajuste la precisión del reconocimiento facial. Un umbral más alto significa una mayor precisión.
máx. Ángulo de reconocimiento facial	Establezca el ángulo máximo de posición de la cara para la detección de rostros. Un valor más grande significa un rango de ángulo de cara más grande. Si el ángulo de la pose del rostro está fuera del rango definido, el cuadro de detección de rostros no aparecerá.
Umbral anti-falsificación	Evite el reconocimiento facial falso cuando las personas usen una foto, un video, una máscara o un sustituto diferente del rostro de una persona autorizada.
Luz infrarroja	Ajuste el brillo de la luz IR.

Parámetro	Descripción
Ajuste de brillo de la luz de relleno	Puede configurar el brillo de la luz de relleno.
Ajuste del modo de luz de relleno	Hay tres modos de luz de relleno. ● NO: La luz de llenado normalmente está abierta. ● NC: La luz de llenado normalmente está cerrada. ● Automático: la luz de relleno se encenderá automáticamente cuando se active un evento de detección de movimiento. Cuando Auto está seleccionado, la luz de relleno no estará encendida incluso si el valor de la luz infrarroja es superior a 19.
Tiempo de espera de reconocimiento (S)	Si se reconoce correctamente el rostro de una persona con permiso de acceso, el dispositivo indicará que el reconocimiento facial se realizó correctamente. Puede introducir el tiempo de intervalo de solicitud.
Intervalo de solicitud no válido (S)	Si una persona sin permiso de acceso intenta desbloquear la puerta varias veces en el intervalo definido, el dispositivo indicará una falla en el reconocimiento de rostros. Puede introducir el tiempo de intervalo de solicitud.
Distancia pupilar	Las imágenes de rostros requieren los píxeles deseados entre los ojos (llamada distancia pupilar) para un reconocimiento exitoso. El píxel predeterminado es 45. El píxel cambia según el tamaño de la cara y la distancia entre las caras y la lente. Si un adulto está a 1,5 metros de la lente, la distancia pupilar puede ser de 50 px a 70 px.
Canal ID	1 es para la cámara de luz blanca y 2 es para la cámara de luz IR.
Exposición (cara)	Una vez habilitada la exposición de rostros, los rostros humanos se verán más claros cuando el dispositivo se instale al aire libre.
Brillo del objetivo de la cara	El valor predeterminado es 50. Ajuste el brillo según sea necesario.
Tiempo de exposición	Después de que se detecta una cara, el dispositivo emitirá luz para iluminar la cara y no volverá a emitir luz hasta que haya transcurrido el intervalo establecido.
Monitoreo de temperatura	Habilite o deshabilite la función de monitoreo de temperatura.
Unidad de temperatura	Seleccione ° C o ° F.
Recto temporal	Establezca si mostrar o no el cuadro de control de temperatura en la pantalla de espera.
Duración de corrección de temperatura (ms)	Al monitorear la temperatura, el Dispositivo tomará el valor de temperatura después del tiempo definido por este parámetro.
Distancia de control de temperatura (cm)	50 por defecto. Puede corregir la temperatura monitoreada según sea necesario de acuerdo con la distancia que establezca.
Umbral de alta temperatura/Umbral de baja temperatura	Establezca el umbral de temperatura. La temperatura corporal monitoreada se considerará como temperatura alta/baja si es mayor/ menor que el valor establecido.
Temperatura máxima	Establezca el rango de temperatura que necesita. Si la temperatura monitoreada es inferior al límite inferior, indicará que la temperatura es demasiado baja; si es superior al límite superior, indicará que hay una fuente de calor que interfiere con la función.
Temperatura mínima	

Parámetro	Descripción
Valor de corrección de temperatura	Este parámetro es para probar. La diferencia del entorno de monitoreo de temperatura puede causar la desviación de temperatura entre la temperatura monitoreada y la temperatura real. Puede seleccionar múltiples muestras monitoreadas para la prueba y luego corregir la desviación de temperatura por este parámetro de acuerdo con la comparación entre la temperatura monitoreada y la temperatura real. Por ejemplo, si la temperatura monitoreada es 0,5 °C inferior a la temperatura real, el valor de corrección se establece en 0,5 °C; si el monitoreado temperatura es 0,5 °C más alta que la temperatura real, el valor de corrección se establece en -0,5 °C.
Modo de monitoreo de temperatura	● Automático: utiliza un mapa de calor facial para el reconocimiento facial; si no se encuentran los mapas de calor, cambiará automáticamente al modo de calibración. ● Termograma: utiliza solo un mapa de calor para el reconocimiento facial y el control de la temperatura. ● Calibración: utiliza una imagen de luz blanca de un rostro para el reconocimiento facial y luego extrae y aplica las coordenadas en el mapa de calor del rostro para monitorear la temperatura. Solo ciertos modelos admiten este parámetro.
Pantalla de termograma	Muestre un mapa de calor en la esquina superior izquierda.
Modo máscara	● Sin detectar: La máscara no se detecta durante el reconocimiento facial. ● Recordatorio de máscara: La máscara se detecta durante el reconocimiento facial. Si la persona no usa una máscara, el sistema le dará un recordatorio para que use máscaras y se le permita el acceso. ● Intercepción de máscara: La máscara se detecta durante el reconocimiento facial. Si una persona no está usando una máscara, el sistema le dará un recordatorio para que use máscaras y se le negará el acceso.

Figura 3-23 Detección de rostros (sin módulo de monitoreo de temperatura)

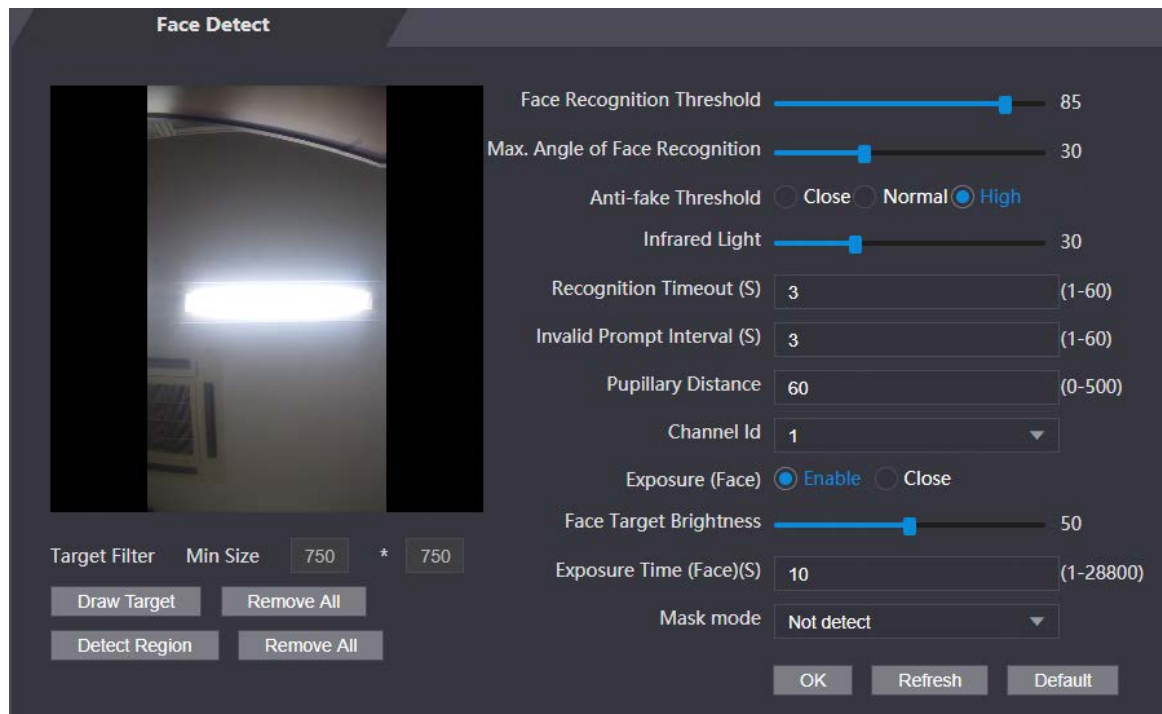


Tabla 3-17 Descripción de los parámetros de detección de rostros (sin módulo de monitoreo de temperatura)

Parámetro	Descripción
Umbral de reconocimiento facial	Ajuste la precisión del reconocimiento facial. Un umbral más alto significa una mayor precisión.
máx. Ángulo de reconocimiento facial	Establezca el ángulo máximo de posición de la cara para la detección de rostros. Un valor más grande significa un rango de ángulo de cara más grande. Si el ángulo de la pose del rostro está fuera del rango definido, el cuadro de detección de rostros no aparecerá.
Umbral anti-falsificación	Evite el reconocimiento facial falso cuando las personas usen una foto, un video, una máscara o un sustituto diferente del rostro de una persona autorizada.
Luz infrarroja	Ajuste el brillo de la luz IR.
Tiempo de espera de reconocimiento (S)	Si se reconoce correctamente el rostro de una persona con permiso de acceso, el dispositivo indicará que el reconocimiento facial se realizó correctamente. Puede introducir el tiempo de intervalo de solicitud.
Intervalo de solicitud no válido (S)	Si una persona sin permiso de acceso intenta desbloquear la puerta varias veces en el intervalo definido, el dispositivo indicará una falla en el reconocimiento de rostros. Puede introducir el tiempo de intervalo de solicitud.
Distancia pupilar	Las imágenes de rostros requieren los píxeles deseados entre los ojos (llamada distancia pupilar) para un reconocimiento exitoso. El píxel predeterminado es 45. El píxel cambia según el tamaño de la cara y la distancia entre las caras y la lente. Si un adulto está a 1,5 metros de la lente, la distancia pupilar puede ser de 50 px a 70 px.
Canal ID	1 es para la cámara de luz blanca y 2 es para la cámara de luz IR.
Exposición (cara)	Una vez habilitada la exposición de rostros, los rostros humanos se verán más claros cuando el dispositivo se instale al aire libre.
Brillo del objetivo de la cara	El valor predeterminado es 50. Ajuste el brillo según sea necesario.

Parámetro	Descripción
Tiempo de exposición (rostro) (S)	Después de que se detecta una cara, el dispositivo emitirá luz para iluminar la cara y no volverá a emitir luz hasta que haya transcurrido el intervalo establecido.
Modo máscara	● Sin detectar: La máscara no se detecta durante el reconocimiento facial. ● Recordatorio de máscara: La máscara se detecta durante el reconocimiento facial. Si la persona no usa una máscara, el sistema le dará un recordatorio para que use máscaras y se le permita el acceso. ● Intercepción de máscara: La máscara se detecta durante el reconocimiento facial. Si una persona no está usando una máscara, el sistema le dará un recordatorio para que use máscaras y se le negará el acceso.

Etapas 4 Dibuja el área de detección de rostros. 1.

Haga clic en **Detectar región**,

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

Se detectará la cara en el área definida. Dibuja el

Paso 5 tamaño objetivo.

1) Haga clic **Dibujar objetivo**.

2) Haga clic derecho para dibujar el cuadro de reconocimiento facial para definir el tamaño mínimo de la cara detectada.

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

Paso 6 Hacer clic **DE ACUERDO**.

3.9 Configuración de red

3.9.1 Configuración de TCP/IP

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

Procedimiento

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

Paso 2 Configurar parámetros.

Figura 3-24 TCP/IP

TCP/IP

IP Version

IPv4

MAC Address

Mode

☒ Static

☐ DHCP

IP Address

Subnet Mask

Default Gateway

Preferred DNS Server

8 . 8 . 8 . 8

Alternate DNS Server

8 . 8 . 4 . 4

OK

Refresh

Default

Tabla 3-18 Descripción de TCP/IP

Parámetro	Descripción
Versión IP	IPv4
Dirección MAC	Dirección MAC del Dispositivo.
Modo	Estático: Introduzca manualmente la dirección IP, la máscara de subred y la puerta de enlace. DHCP: Significa Protocolo de configuración dinámica de host. Cuando se activa DHCP, al dispositivo se le asignará automáticamente una dirección IP, una máscara de subred y una puerta de enlace.
Dirección IP	Si selecciona el modo estático, configure la dirección IP, la máscara de subred y la puerta de enlace. La dirección IP y la puerta de enlace deben estar en el mismo segmento de red.
Máscara de subred	
Puerta de enlace predeterminada	
Servidor DNS preferido	Configure la dirección IP del servidor DNS preferido.
Servidor DNS alternativo	Establezca la dirección IP del servidor DNS alternativo.

Paso 3 Hacer clic **DE ACUERDO**.

3.9.2 Configuración del puerto

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

Procedimiento

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

Paso 2 Configure los números de puerto.

Figura 3-25 Configurar puertos

The screenshot shows a configuration window titled "Port" with a dark background. It contains five rows of settings, each with a label, a text input field, and a range in parentheses:

- Max Connection:** 1000 (1~1000)
- TCP Port:** 3777 (1025~65535)
- HTTP Port:** 80 (1~65535)
- HTTPS Port:** 443 (1~65535)
- RTSP Port:** 554 (1~65535)

At the bottom of the window are three buttons: "OK", "Refresh", and "Default".



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

Tabla 3-19 Descripción de los puertos

Parámetro	Descripción
Conexión máxima	Puede establecer el número máximo de clientes (como web, cliente de escritorio y teléfono) que pueden acceder a la Terminal de acceso al mismo tiempo.
Puerto TCP	El valor predeterminado es 3777.
Puerto HTTP	El valor predeterminado es 80. Si desea cambiar el número de puerto, agregue el nuevo número de puerto después de la dirección IP cuando inicie sesión en la página web.
Puerto HTTPS	El valor predeterminado es 443.
Puerto RTSP	El valor predeterminado es 554.

Paso 3

Hacer clic **DE ACUERDO**.

3.9.3 Configuración del registro automático

El Dispositivo informa su dirección al servidor designado para que pueda acceder al Dispositivo a través de la plataforma de administración.

Procedimiento

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

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

Figura 3-26 Registro

Register

☐ Enable

Host IP

172.16.1.17

Port

7000

Sub-device ID

none

OK

Refresh

Default

Tabla 3-20 Descripción del registro automático

Parámetro	Descripción
IP del anfitrión	La dirección IP o el nombre de dominio del servidor.
Puerto	El puerto del servidor utilizado para el registro automático.
ID de subdispositivo	Introduzca el ID del subdispositivo (definido por el usuario).  Cuando agrega el dispositivo a la plataforma de administración, la ID del subdispositivo en la plataforma de administración debe cumplir con el identificador de subdispositivo definido en el dispositivo.

Paso 3 Hacer clic**Aplicar**.

3.9.4 Configuración de P2P

La computación o redes punto a punto es una arquitectura de aplicación distribuida que divide tareas o cargas de trabajo entre pares. Los usuarios pueden descargar la aplicación móvil escaneando el código QR y luego registrar una cuenta para poder administrar más de un terminal en la aplicación móvil. No necesita aplicar un nombre de dominio dinámico, hacer un mapeo de puertos o no necesita un servidor de tránsito.

Información de contexto



Si va a utilizar P2P, debe conectar el terminal a una red externa; de lo contrario la terminal No puede ser usado.

Procedimiento

- Paso 1

Seleccionar**Configuración de red>P2P**
- Paso 2

Seleccionar**Permitir**para activar la función P2P. Hacer clic**DE**
- Paso 3

ACUERDO.

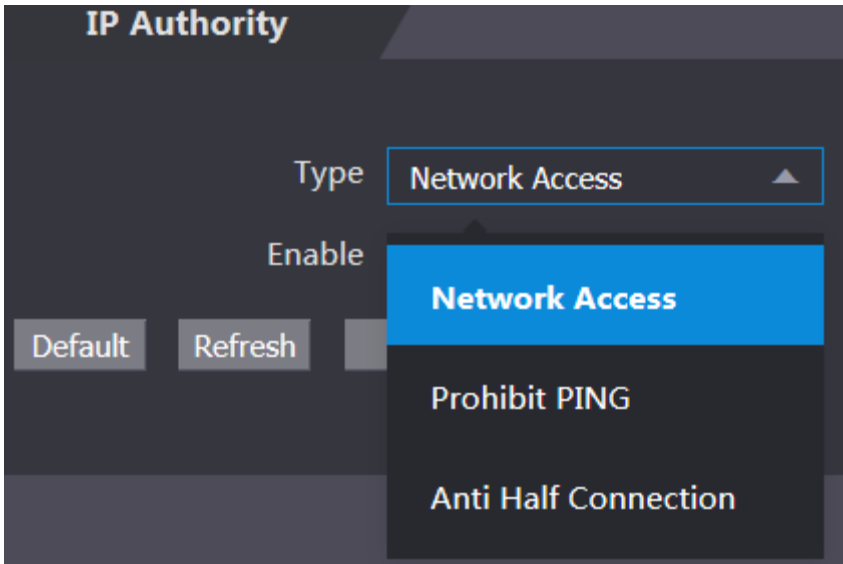
3.10 Gestión de la seguridad

3.10.1 Configuración de la autoridad IP

Procedimiento

- Paso 1
- Inicie sesión en la página web.
- Paso 2
- Hacer clic **Gestión de seguridad**>**Autoridad de PI**.

Figura 3-27 Autoridad IP



- Paso 3
- Seleccione un modo de ciberseguridad de la **Tipolista**.
- **Acceso a la red**: Configure la lista de permitidos y la lista de bloqueados para controlar el acceso al dispositivo.
 - **Prohibir PING**: Permitir **PING prohibido** y el dispositivo no responderá a la solicitud de ping.
 - **Media conexión anti**: Permitir **Media conexión anti** función, y el dispositivo aún puede funcionar correctamente bajo el ataque de la mitad de la conexión.

3.10.1.1 Acceso a la red

Procedimiento

- Paso 1
- Seleccionar **Acceso a la red** desde el **Tipolista**. Selecciona
- Paso 2
- el **Permitir** casilla de verificación

Figura 3-28 Acceso a la red

IP Authority

Type: Network Access

Enable: ☒

Mode: ☒ Allow List ☐ Block List

Allow List Block List

	IP Address	MAC Address	Port	Modify	Delete
No data...					

Only the listed IP addresses/MAC are allowed to visit corresponding ports of the device.

Add

Default Refresh OK

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

Etapas 4 Hacer clic **Agregar**.

Figura 3-29 Agregar IP

Add

Type

IP Address

IP Version

IPv4

IPv4

1.0.0.1

All Ports

☐

Device Start Port

1

Device End Port

1

Save

Cancel

Paso 5 Configurar parámetros.

Tabla 3-21 Descripción de la adición de parámetros IP

Parámetro	Descripción
Tipo	Seleccione el tipo de dirección de laTipolista.
Versión IP	IPv4 por defecto.
Todos los puertos	Seleccionar Todos los puertos marque la casilla y su configuración se aplicará a todos los puertos.
Puerto de inicio del dispositivo	si borras Todos los puertos casilla de verificación, establezca el puerto de inicio del dispositivo y el puerto final del dispositivo.
Puerto final del dispositivo	

Paso 6 Hacer clic**Ahorrar**, y el**Autoridad de PI**se muestra la interfaz. Hacer clic**DE**

Paso 7 **ACUERDO.**

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

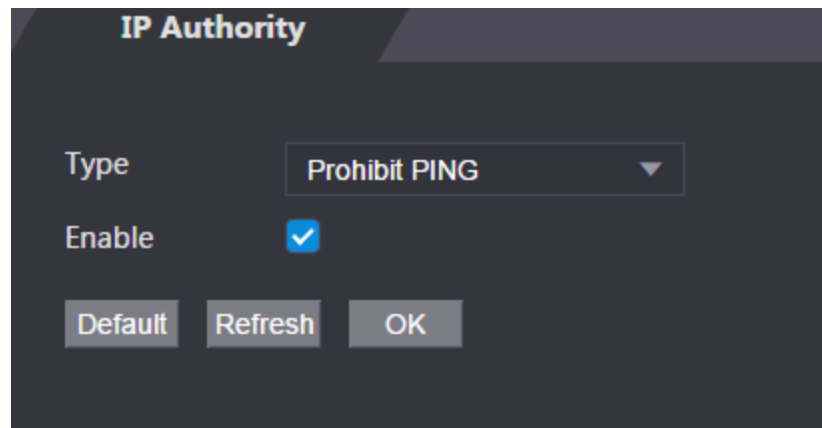
3.10.1.2 Prohibir PING

Procedimiento

Paso 1 Seleccionar**Prohibir PING**desde el**Tipolista**.

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

Figura 3-30 Prohibir PING



Paso 3 Hacer clic **DE ACUERDO**.

3.10.1.3 Conexión Anti Half

Procedimiento

Paso 1 Selecciona el **Media conexión anti** desde el **Tip** lista. Selecciona el **Permitir**

Paso 2 casilla de verificación Hacer clic **DE ACUERDO**.

Paso 3

3.10.2 Configuración del sistema

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar **Gestión de seguridad** > **Servicio del sistema**. Habilite o

Paso 3 deshabilite los servicios del sistema según sea necesario.



Los parámetros del servicio del sistema pueden diferir según los modelos del producto.

Figura 3-31 Servicio del sistema

System Service

- ☒ SSH
- ☒ PWD Reset Enable
- ☒ CGI
- ☒ ONVIF
- ☐ Audio and Video Transmission Encryption
- ☐ RTSP Over TLS
- ☐ HTTPS

Warning: Disabling HTTPS may be at risk

☐ Compatible with TLSv1.1 and earlier versions

☒ Emergency Maintenance

Auth Method ☒ Security Mode (Recommended) ☐ Compatible Mode

Password Expires in **Never**

Create Server Certificate Download Root Certificate

Details Delete

OK Refresh Default

Tabla 3-22 Descripción del servicio del sistema

Parámetro	Descripción
SSH	Secure Shell (SSH) es un protocolo de red criptográfico para operar servicios de red de forma segura en una red no segura. Cuando SSH está habilitado, SSH proporciona un servicio criptográfico para la transmisión de datos.
Habilitar restablecimiento de PWD	Si está habilitado, puede restablecer la contraseña. Esta función está habilitada por defecto.
CGI	Common Gateway Interface (CGI) ofrece un protocolo estándar para que los servidores web ejecuten programas de manera similar a las aplicaciones de consola que se ejecutan en un servidor que genera páginas web dinámicamente. Cuando CGI está habilitado, se pueden usar comandos CGI. El CGI está habilitado de forma predeterminada.
ONVIF	Habilite otros dispositivos para extraer la transmisión de video del VTO a través del protocolo ONVIF.

Parámetro	Descripción
Audio y video Transmisión Cifrado	Si esta función está habilitada, la transmisión de audio y video se cifra automáticamente.
RTSP sobre TLS	Si esta función está habilitada, la transmisión de audio y video se cifra a través del protocolo RTSP.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) es un protocolo para la comunicación segura a través de una red informática. Cuando HTTPS está habilitado, HTTPS se utilizará para acceder a los comandos CGI; de lo contrario, se utilizará HTTP.
Compatible con TLSv1.1 y anteriores versiones	Habilite esta función si su navegador utiliza TLS V1.1 o versiones anteriores.
Emergencia Mantenimiento	Habilítelo para análisis de fallas y mantenimiento.
La contraseña caduca en	Establecer la fecha de caducidad de la contraseña.

Etapa 4

Hacer clic **DE ACUERDO**.

3.10.2.1 Crear certificado de servidor

Información de contexto

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

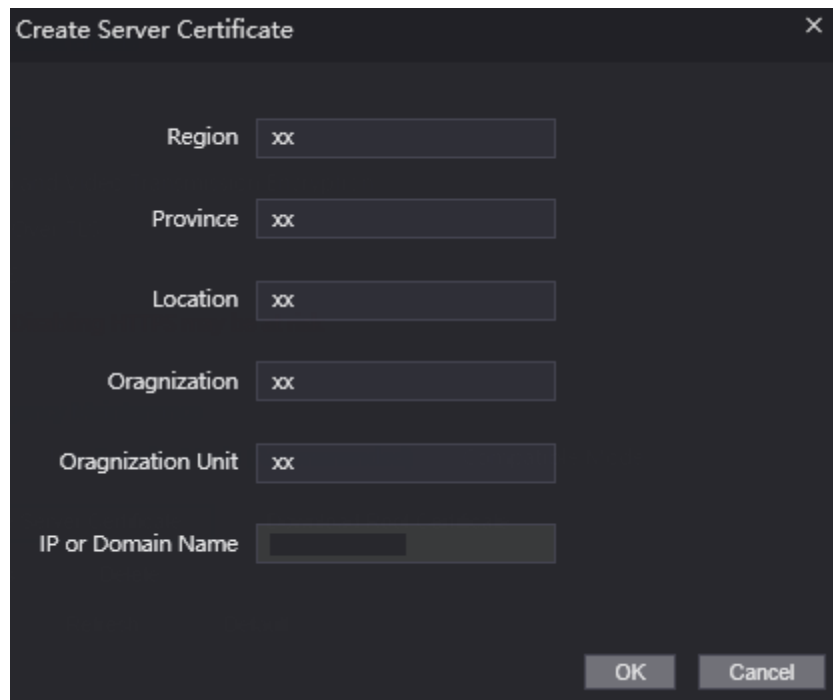


- Si usa HTTPS por primera vez o se cambia la dirección IP del controlador de acceso, cree un certificado de servidor e instale un certificado raíz.
- Si usa otra computadora para iniciar sesión en la página web del controlador de acceso, debe descargar e instale el certificado raíz nuevamente en la nueva computadora o copie el certificado raíz al eso.

Procedimiento

- Paso 1 Sobre el **Servicio del sistema** página, haga clic **Crear certificado de servidor**.
- Paso 2 Ingrese la información y haz clic **DE ACUERDO**. El dispositivo se reiniciará.

Figura 3-32 Crear certificado de servidor



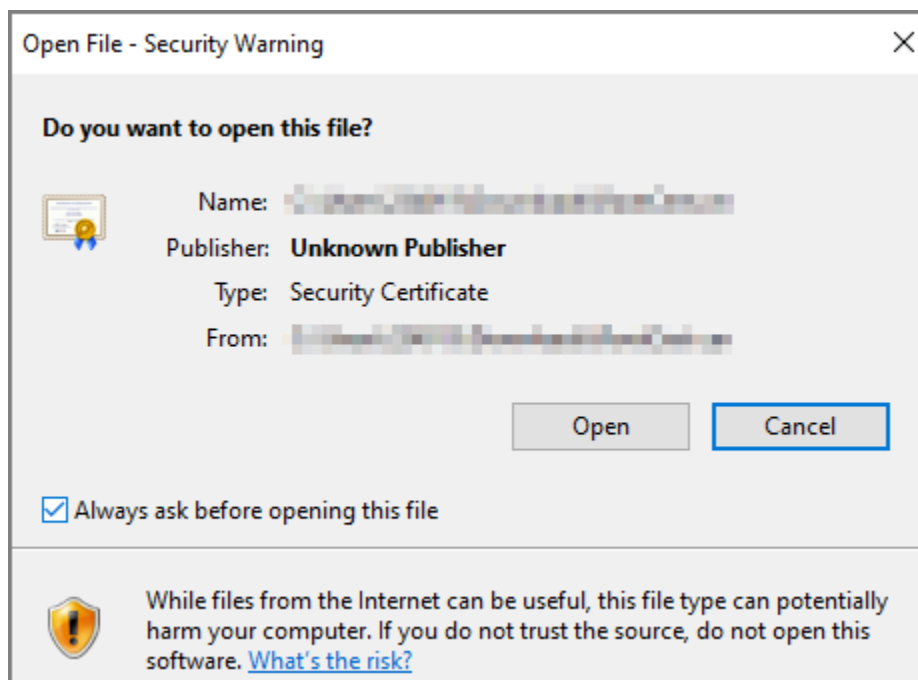
A dialog box titled "Create Server Certificate" with a close button (X) in the top right corner. It contains six text input fields, each with "xx" as a placeholder: "Region", "Province", "Location", "Oragnization" (note the typo), "Oragnization Unit" (note the typo), and "IP or Domain Name". At the bottom right are "OK" and "Cancel" buttons.

3.10.2.2 Descarga del certificado raíz

Procedimiento

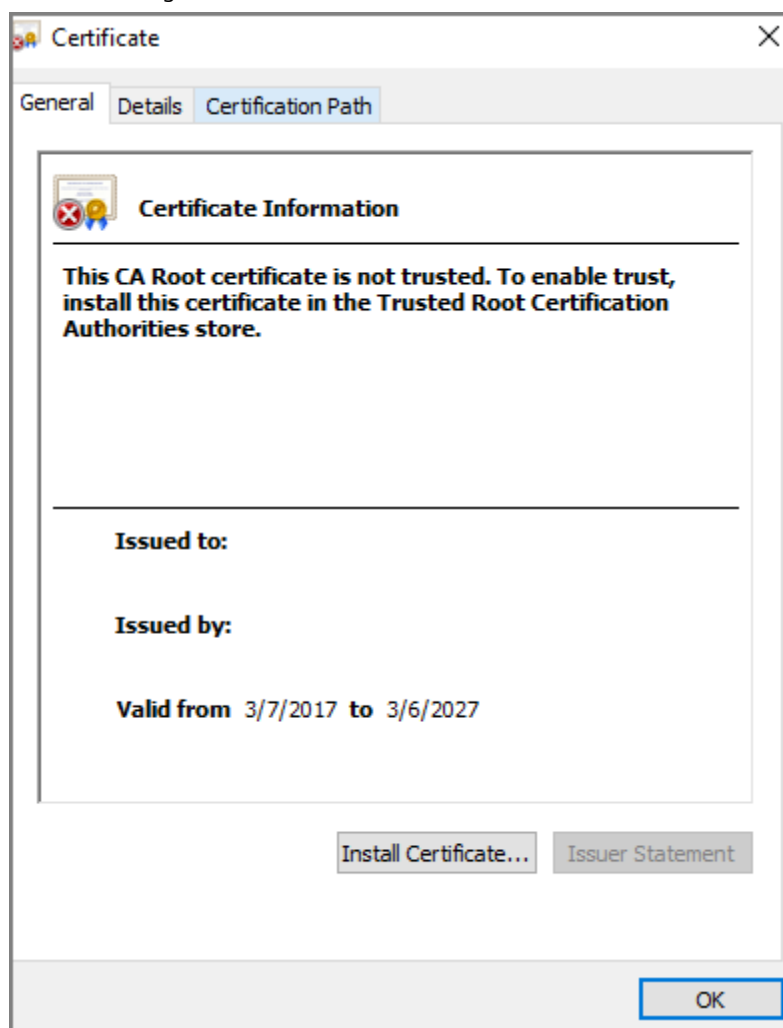
- Paso 1 Sobre el **Servicio del sistema** página, haga clic **Descargar certificado raíz**. Haga
- Paso 2 doble clic en el archivo que ha descargado y luego haga clic en **Abierto**.

Figura 3-33 Descarga de archivos



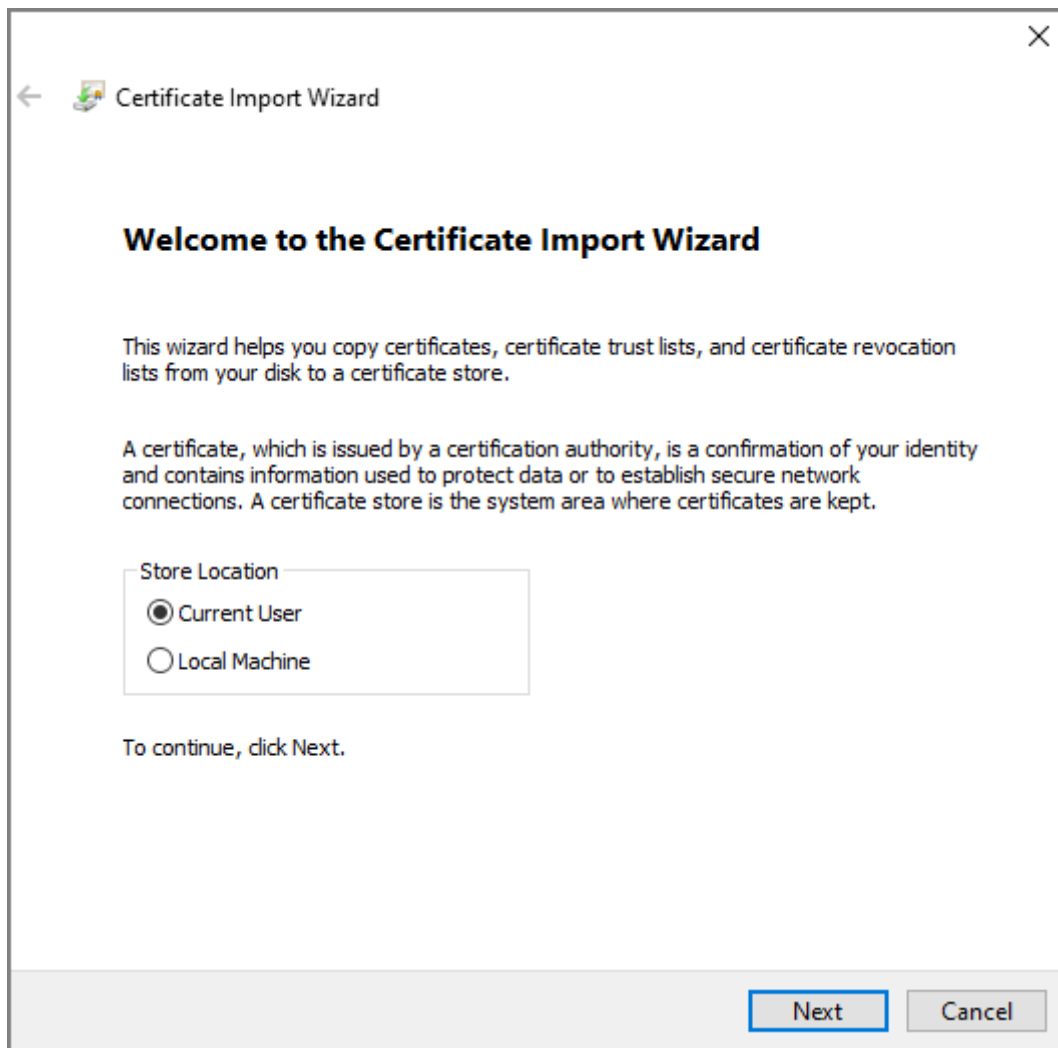
- Paso 3 Hacer clic **Instalar certificado**.

Figura 3-34 Información del certificado



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

Figura 3-35 Asistente de importación de certificados (1)

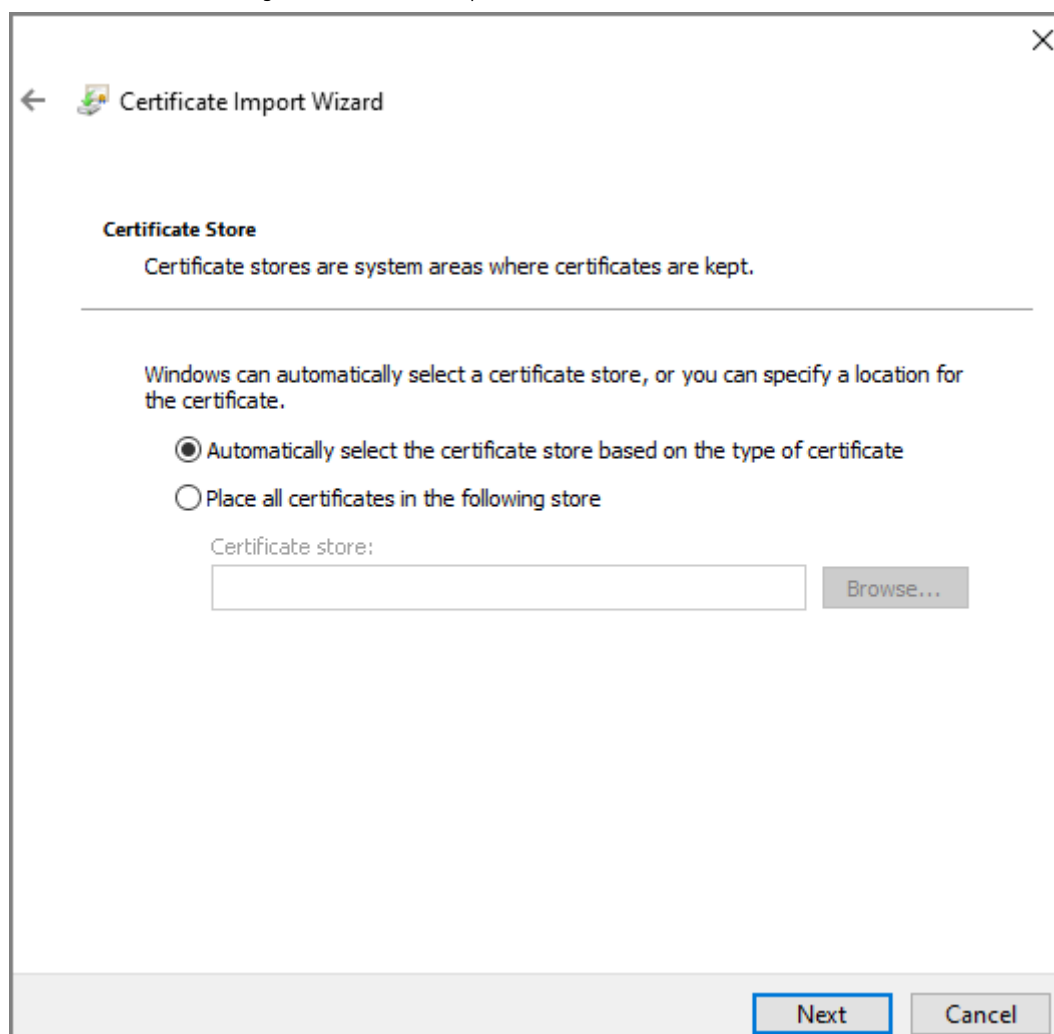


Paso 5

Seleccione la ubicación de almacenamiento adecuada.

- 1) Seleccionar **Coloque todos los certificados en la siguiente tienda**.
- 2) Haga clic **Navegar** para importar el certificado al **Autoridades de certificación raíz de confianza** almacenar y luego haga clic en **Próximo**.

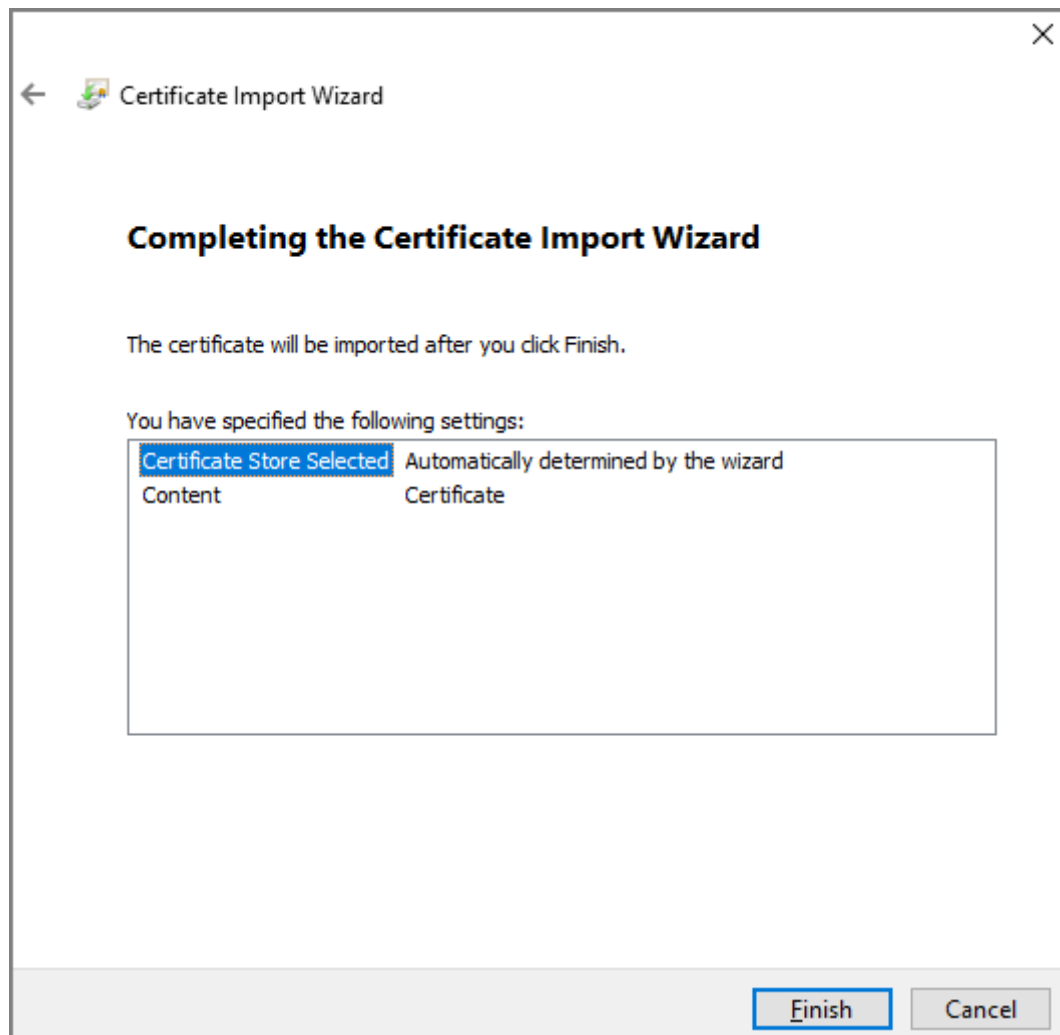
Figura 3-36 Asistente de importación de certificados (2)



Paso 6

Hacer clic **Finalizar**.

Figura 3-37 Asistente de importación de certificados (3)



3.11 Gestión de usuarios

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

3.11.1 Adición de usuarios

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

Procedimiento

- Paso 1 En la página de inicio, seleccione **Gestión de usuarios** > **Gestión de usuarios**.
- Paso 2 Hacer clic **Agregar** ingrese la información del usuario.



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

Figura 3-38 Agregar usuario

Add [X]

Username []

Password [] Low Medium High

Confirm Password []

Remark []

[OK] [Cancel]

Paso 3

Hacer clic **DE ACUERDO**.



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

3.11.2 Adición de usuarios ONVIF

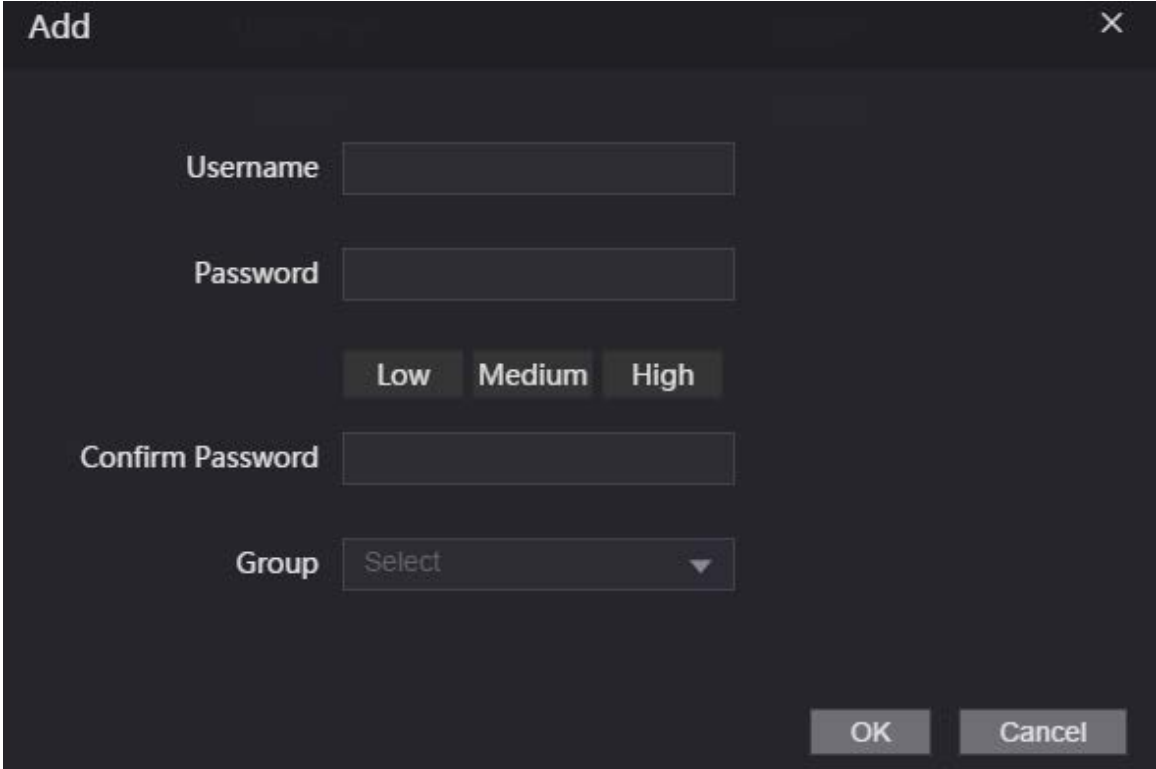
Información de contexto

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

Procedimiento

- Paso 1** En la página de inicio, seleccione **Gestión de usuarios** > **Usuario Onvif**.
- Paso 2** Hacer clic **Agregar** y luego configure los parámetros.

Figura 3-39 Agregar usuario ONVIF



Paso 3 Hacer clic **DE ACUERDO**.

3.11.3 Visualización de usuarios en línea

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

3.12 Mantenimiento

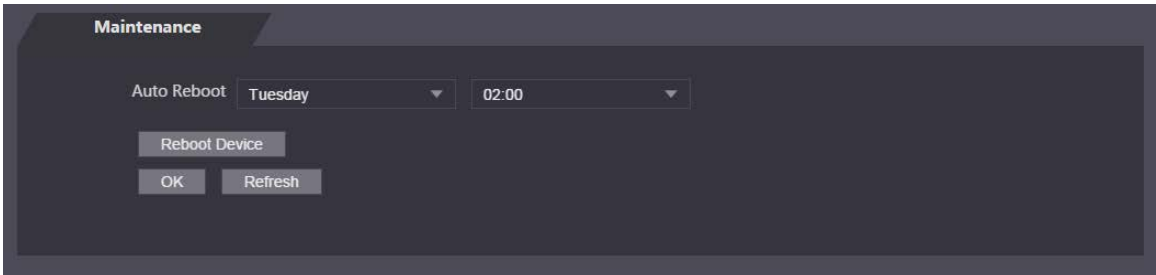
Puede reiniciar regularmente el dispositivo durante el tiempo de inactividad para mejorar su rendimiento.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar **Mantenimiento**.

Figura 3-40 Mantenimiento



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

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

3.13 Gestión de la configuración

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

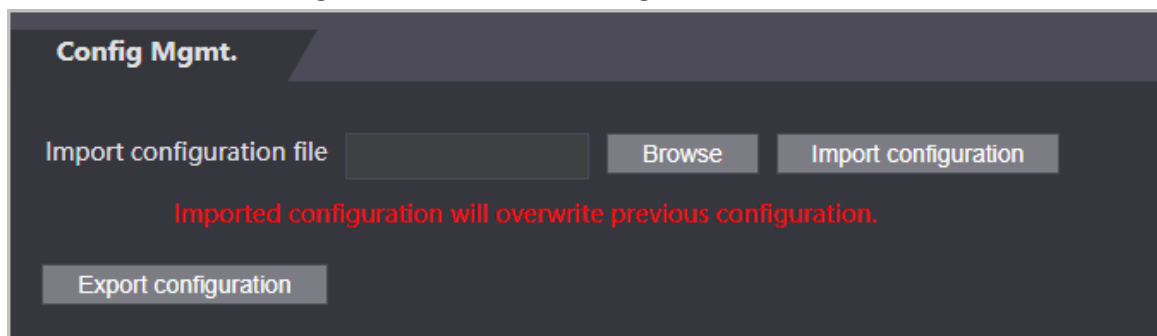
3.13.1 Exportación/Importación de archivos de configuración

Puede importar o 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** Seleccione **Gestión de configuración** > **Gestión de configuración**.

Figura 3-41 Gestión de la configuración



- Paso 3** Exportar o importar archivos de configuración.
- Exportar archivo de configuración. Haga clic en **Exportar configuración** para descargar el archivo al local.



La IP no se exportará.

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



El archivo de configuración solo se puede importar al dispositivo con el mismo modelo.

3.13.2 Restauración de valores predeterminados de fábrica

Procedimiento

- Paso 1** Seleccione **Gestión de configuración** > **Por defecto** Restaure los
- Paso 2** valores predeterminados de fábrica si es necesario.



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

- **Restaurar Fábrica:** Restablece las configuraciones del Dispositivo y elimina todos los datos.
- **Restaurar fábrica (Guardar usuario y registro):** restablece las configuraciones del dispositivo y elimina todos los datos excepto la información del usuario y los registros.

3.14 Sistema de actualización

Información de contexto



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

3.14.1 Actualización de archivos

Procedimiento

- Paso 1 En la página de inicio, seleccione **Mejora**.
- Paso 2 En el **Actualización de archivo** área, haga clic **Navegar**, a continuación, 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 que se complete la actualización.

3.14.2 Actualización en línea

Procedimiento

- Paso 1 En la página de inicio, seleccione **Mejora**.
- Paso 2 En el **Actualización en línea** área, seleccione un método de actualización.
- Seleccionar **Verificación automática**, el dispositivo comprobará automáticamente si su última versión está disponible.
 - Seleccionar **Comprobación manual** puede verificar inmediatamente si la última versión está disponible.
- Paso 3 Actualice el dispositivo cuando esté disponible la última versión.

3.15 Ver información de la versión

Información de contexto

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

3.16 Visualización de registros

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

3.16.1 Registros del sistema

Ver y buscar registros del sistema.

Procedimiento

- Paso 1 Inicie sesión en la página web. Seleccione **Registro**
- Paso 2 **del sistema>Registro del sistema.**
- Paso 3 Seleccione el intervalo de tiempo y el tipo de registro y, a continuación, haga clic en **Consulta.**
Hacer clic **Respaldar** para descargar el registro del sistema.

3.16.2 Registros de administración

Busque registros de administrador mediante el ID de administrador.

Procedimiento

- Paso 1 Inicie sesión en la página web. Seleccione **Registro del sistema>Registro de**
- Paso 2 **administración.** Ingrese la identificación del administrador y luego haga clic
- Paso 3 en **Consulta.**

3.16.3 Desbloqueo de registros

Busque registros de desbloqueo y expórtelos.

Procedimiento

- Paso 1 Inicie sesión en la página web.
- Paso 2 Seleccione **Registro del sistema>Registros de búsqueda.**
- Paso 3 Seleccione el intervalo de tiempo y el tipo de registro y, a continuación, haga clic en **Consulta.** Puedes hacer clic **Exportar datos** para descargar el registro.

4 Configuración inteligente de PSS Lite

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

4.1 Instalación e inicio de sesión

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

Procedimiento

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

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



Configure la contraseña para el primer uso y luego configure las preguntas de seguridad para restablecer su contraseña cuando la olvidó.

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

4.2 Adición de dispositivos

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

4.2.1 Agregando uno por uno

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

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

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

Figura 4-1 Información del dispositivo

The screenshot shows a configuration window titled 'Add and Continue'. It has two columns of input fields. The first column contains 'Device Name' with the value 'Access Terminal', 'IP' with a masked value, 'User Name' with the value 'admin', and 'Password' with a masked value. The second column contains 'Method to add' with a dropdown menu set to 'IP', and 'Port' with the value '37777'. At the bottom, there are three buttons: 'Add and Continue' (highlighted in blue), 'Add', and 'Cancel'.

Tabla 4-1 Parámetros del dispositivo Descripción

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

Etapas

Hacer clic **Agregar**.

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

4.2.2 Adición de lotes

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

Procedimiento

Paso 1

Inicie sesión en Smart PSS Lite.

Paso 2

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

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

Figura 4-2 Búsqueda automática

Se mostrará una lista de dispositivos.



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

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

Etapas 4 Introduzca el nombre de usuario y la contraseña del controlador de acceso.

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



El controlador de acceso inicia sesión automáticamente en Smart PSS Lite después de agregarlo. **En línea** se muestra después de un inicio de sesión exitoso.

4.3 Gestión de usuarios

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

4.3.1 Configuración del tipo de tarjeta

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

Procedimiento

Paso 1 Inicie sesión en Smart PSS Lite.

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

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



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

Etapas 4 Hacer clic **DE ACUERDO**.

4.3.2 Adición de usuarios

4.3.2.1 Sumando uno por uno

Puede agregar usuarios uno por uno.

Procedimiento

- Paso 1** Inicie sesión en Smart PSS Lite.
- Paso 2** Hacer clic **Solución de acceso>Gerente de Personal>Usuario>Agregar**.
- Paso 3** Hacer clic **Información básica** pestaña e ingrese la información básica del usuario, y luego importe la imagen de la cara.

Figura 4-3 Agregar información básica

Etapa 4 Haga clic en el **Certificación** pestaña para agregar información de certificación del usuario.

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

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

2. Haga clic en **Agregar**, deslice una tarjeta en el lector de tarjetas. Se muestra el número de tarjeta.

3. Haga clic en **DE ACUERDO**.

Después de agregar una tarjeta, puede configurar la tarjeta como tarjeta principal o tarjeta de coacción, o reemplazar la

tarjeta con una nueva, o elimine la tarjeta.

- Configurar huella dactilar.

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

Figura 4-4 Agregar contraseña, tarjeta y huella digital

Add User

Basic Info Certification Permission configuration

Password Add ⚠ For the 2nd-generation access controller, it is the personnel password; otherwise it is card password.

Card Add ⚠ The card number must be added if not the 2nd generation access controller is used.

Fingerprint

+ Add - Delete

☐	Fingerprint Name	Operation
--------------------------	------------------	-----------

Continue Finish Cancel

- Paso 5 Configurar permisos para el usuario. Para obtener más información, consulte "4.3.3 Asignación de permisos de acceso". Hacer clic
- Paso 6 Finalizar.

4.3.2.2 Adición de lotes

Puede agregar usuarios en lotes.

Procedimiento

- Paso 1 Inicie sesión en Smart PSS Lite.
- Paso 2 Hacer clic **Gerente de Personal** > **Usuario** > **Agregar lote**.
- Paso 3 Seleccionar **Emisor de la tarjeta** desde el **Dispositivo** list, y luego configure los parámetros.

Figura 4-5 Agregar usuarios en lotes

Device

Card issuer

Issue

Start No.:

* 1

Quantity:

* 30

Department:

Default Company

Effective Time:

2022/4/1 0:00:00

Expired Time:

2032/4/1 23:59:59

Issue Card

ID	Card No.
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	

OK

Cancel

Tabla 4-2 Parámetros de agregar usuarios en lotes

Parámetro	Descripción
Nº de inicio	El ID de usuario comienza con el número que 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.

Etapas 4 Hacer clic **Asunto**.
El número de tarjeta se leerá automáticamente. Hacer clic **DE**

Paso 5 **ACUERDO**.

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

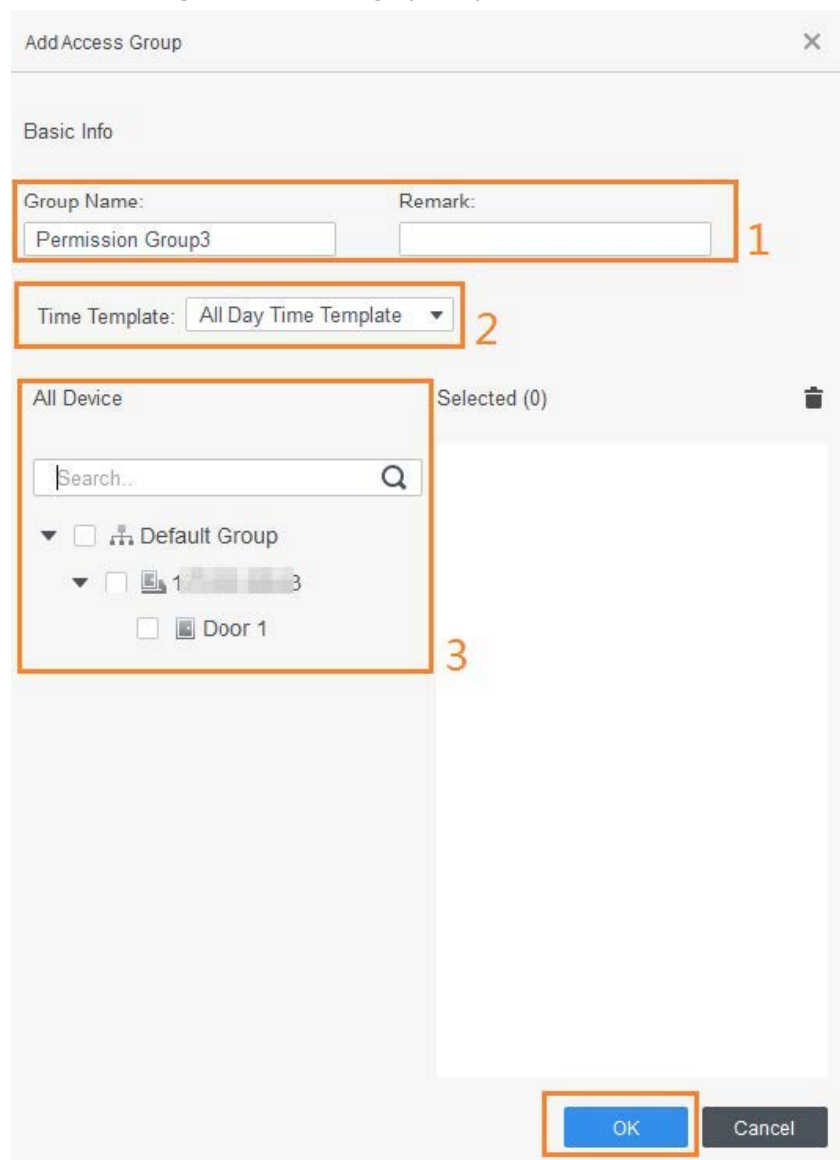
4.3.3 Asignación de permiso de acceso

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

Procedimiento

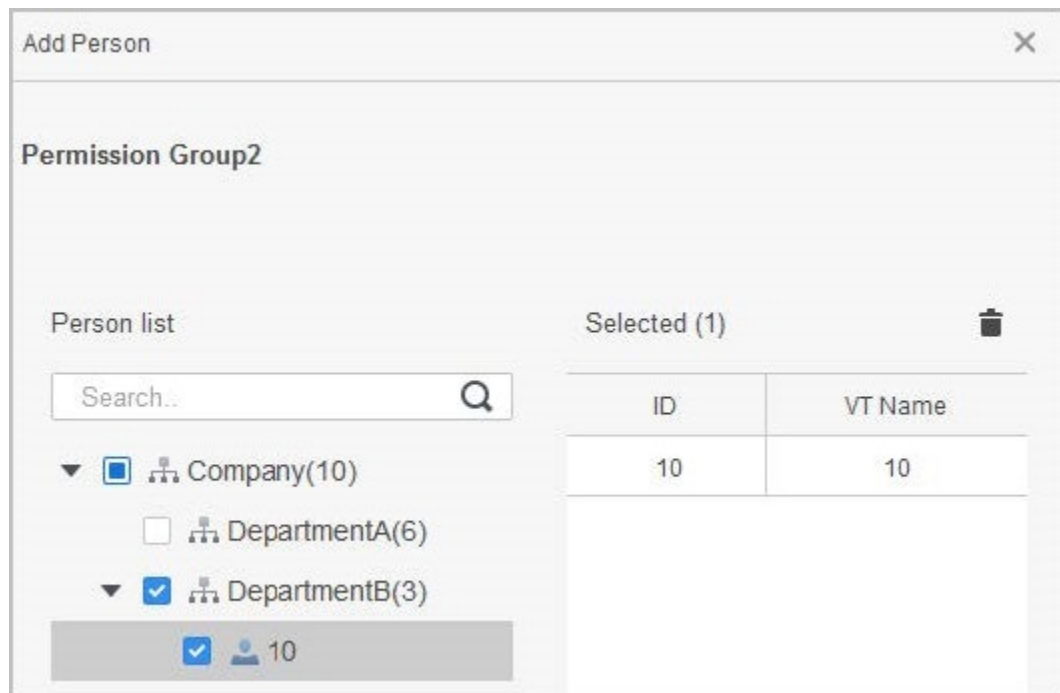
- Paso 1** Inicie sesión en Smart PSS Lite.
- Paso 2** Hacer clic **Solución de acceso>Gerente de Personal>Configuración de permisos**. Haga clic
- Paso 3** en . 
- Etapas 4** Ingrese el nombre del grupo, comentarios (opcional) y seleccione una plantilla de tiempo.
- Paso 5** Seleccione el dispositivo de control de acceso.
- Paso 6** Hacer clic **DE ACUERDO**.

Figura 4-6 Crear un grupo de permisos



- Paso 7** Hacer clic  del grupo de permisos que agregó.
- Paso 8** Seleccione usuarios para asociarlos con el grupo de permisos.

Figura 4-7 Agregar usuarios a un grupo de permisos



Paso 9

Hacer clic **DE ACUERDO**.

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

4.4 Gestión de acceso

4.4.1 Apertura y cierre de puertas a distancia

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

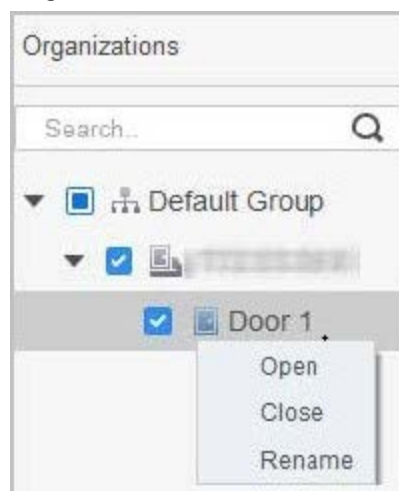
Procedimiento

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

Paso 2 Controlar remotamente la puerta.

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

Figura 4-8 Puerta abierta



- Hacer clic o para abrir o cerrar la puerta.

Operaciones relacionadas

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

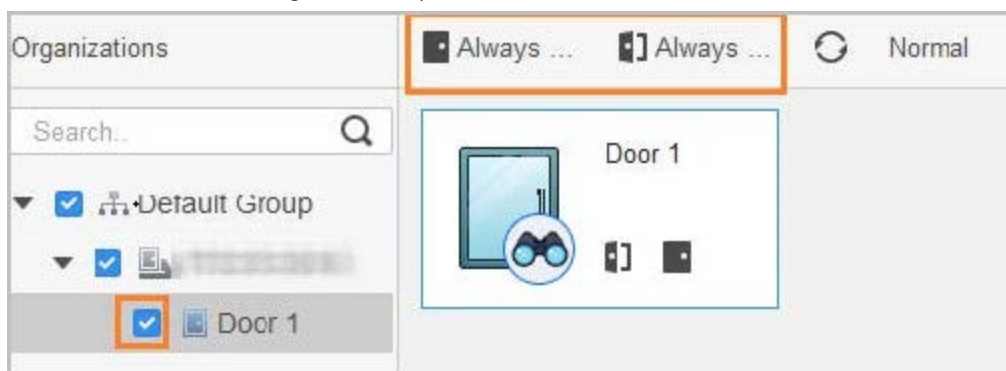
4.4.2 Configuración de Siempre abierto y Siempre cerrado

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

Procedimiento

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

Figura 4-9 Siempre abierto o cerrado



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

4.4.3 Supervisión del estado de la puerta

Procedimiento

- Paso 1** Hacer clic **Solución de acceso** > **Administrador de acceso** en la página de inicio.
- Paso 2** Seleccione el controlador de acceso en el árbol de dispositivos y haga clic derecho en el controlador de acceso y luego seleccione **Iniciar monitoreo de eventos en tiempo real**.
- Los eventos de control de acceso en tiempo real se mostrarán en la lista de eventos.



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

Figura 4-10 Supervisar el estado de la puerta

Organizations

Search...

1 Group

2 Door 1

Start Real-time Event Monitoring

Show All Doors

Reboot

Details

Event Info

All Alarm Abnormal Normal

Event History

Event Configuration

Time	Event	Description
2022-04-08 17:37:36	111/Door 1	Door is locked
2022-04-08 17:37:33	111/Door 1	E731FC4A Card Unlock
2022-04-08 17:37:33	111/Door 1	Door is unlocked
2022-04-07 11:11:50	111	Tamper Alarm

IP: 192.168.243.100

Device Type: Access Standalone

Device Model: E731FC4A...

Status: Online

Operaciones relacionadas

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

Apéndice 1 Puntos importantes de Intercom Operación

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

requisitos previos

La función de intercomunicación está configurada en el Dispositivo y VTO.

Procedimiento

Paso 1 En la pantalla de espera, toque Ingresar 

Paso 2 número de la habitación y luego toque .

Apéndice 2 Puntos importantes de la huella digital

Instrucciones de registro

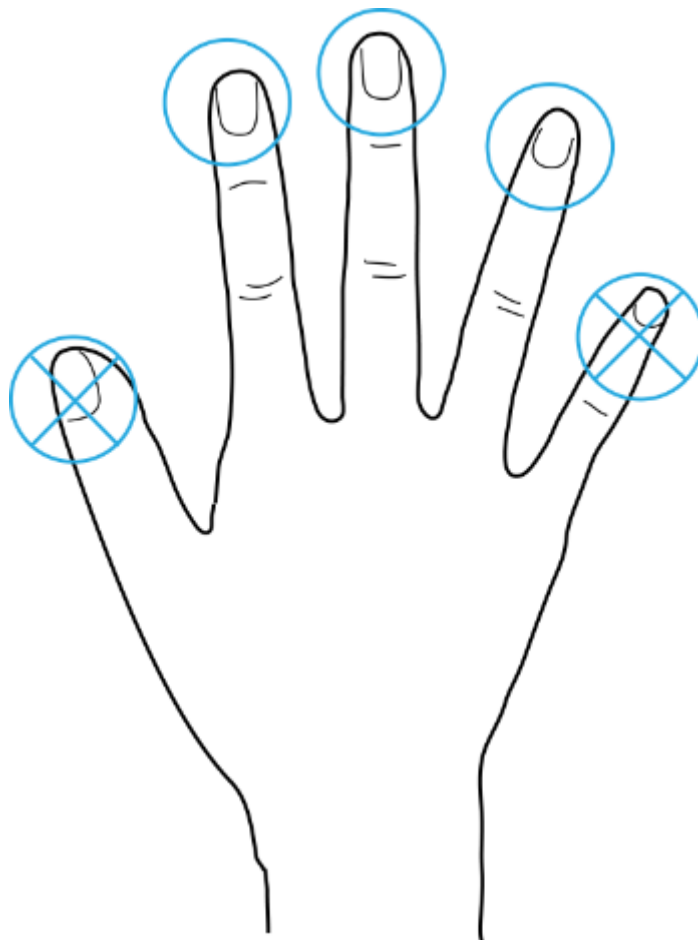
Cuando registre la huella digital, preste atención a los siguientes puntos:

- Asegúrese de que sus dedos y la superficie del escáner estén limpios y secos.
- Presione su dedo en el centro del escáner de huellas 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.

Dedos recomendados

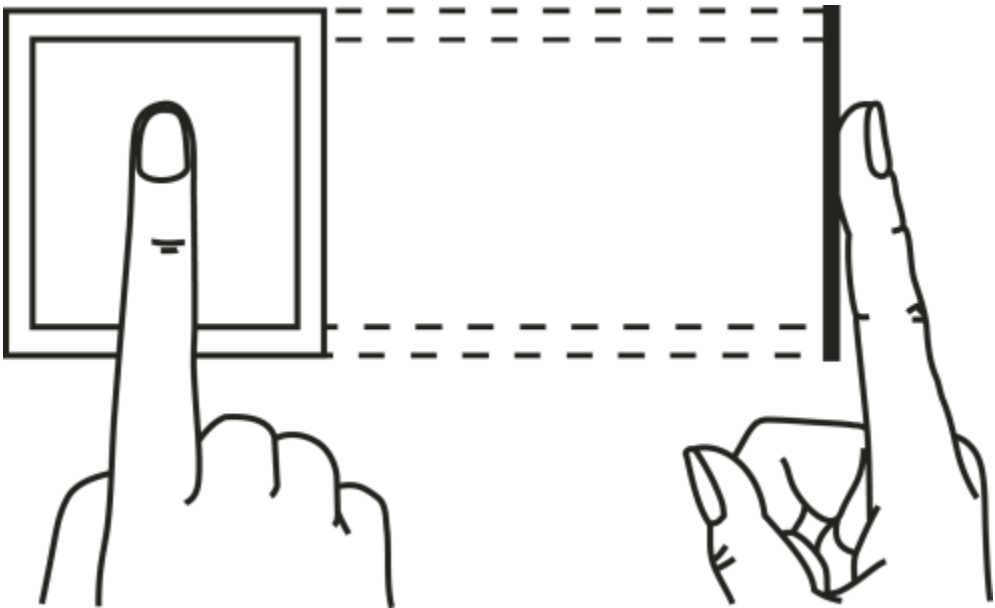
Se recomiendan los dedos índice, medio y anular. Los pulgares y los meñiques no se pueden colocar fácilmente en el centro de grabación.

Apéndice Figura 2-1 Dedos recomendados

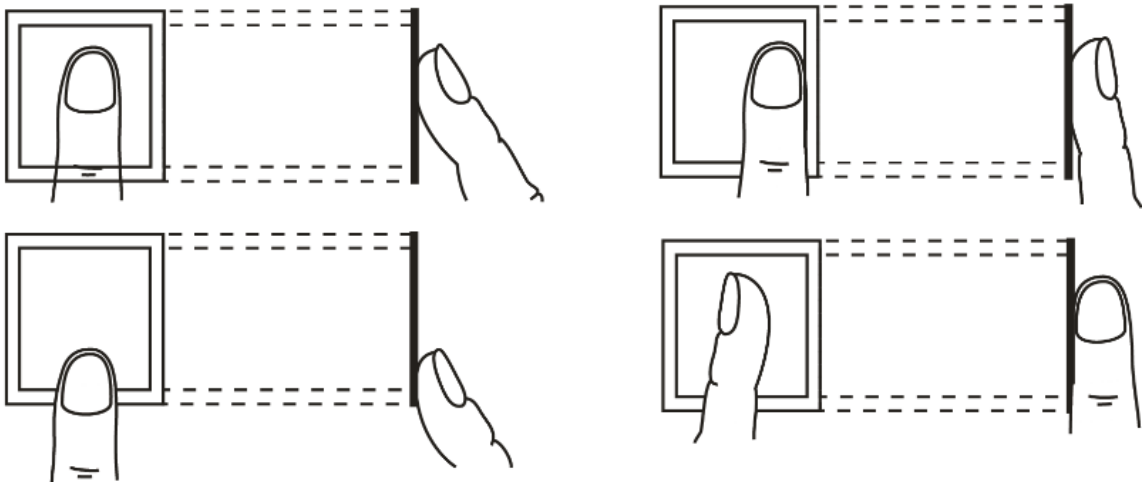


Cómo presionar su huella digital en el escáner

Apéndice Figura 2-2 Colocación correcta



Apéndice Figura 2-3 Colocación incorrecta



Apéndice 3 Puntos importantes de la cara

Registro

Antes del registro

- Las gafas, los sombreros y la barba pueden influir en el rendimiento del reconocimiento facial.
- No cubra sus cejas cuando use sombreros.
- 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 dos metros de la fuente de luz y al menos a tres metros de ventanas o puertas; de lo contrario, la luz de fondo y la luz solar directa podrían influir en el rendimiento del reconocimiento facial del controlador de acceso.

Durante el registro

- Puede registrar rostros a través del Dispositivo o a través de la plataforma. Para el registro a través de la plataforma, consulte el manual de usuario de la plataforma.
- Haga que su cabeza se centre en el marco de captura de fotos. La imagen de la cara se capturará automáticamente.

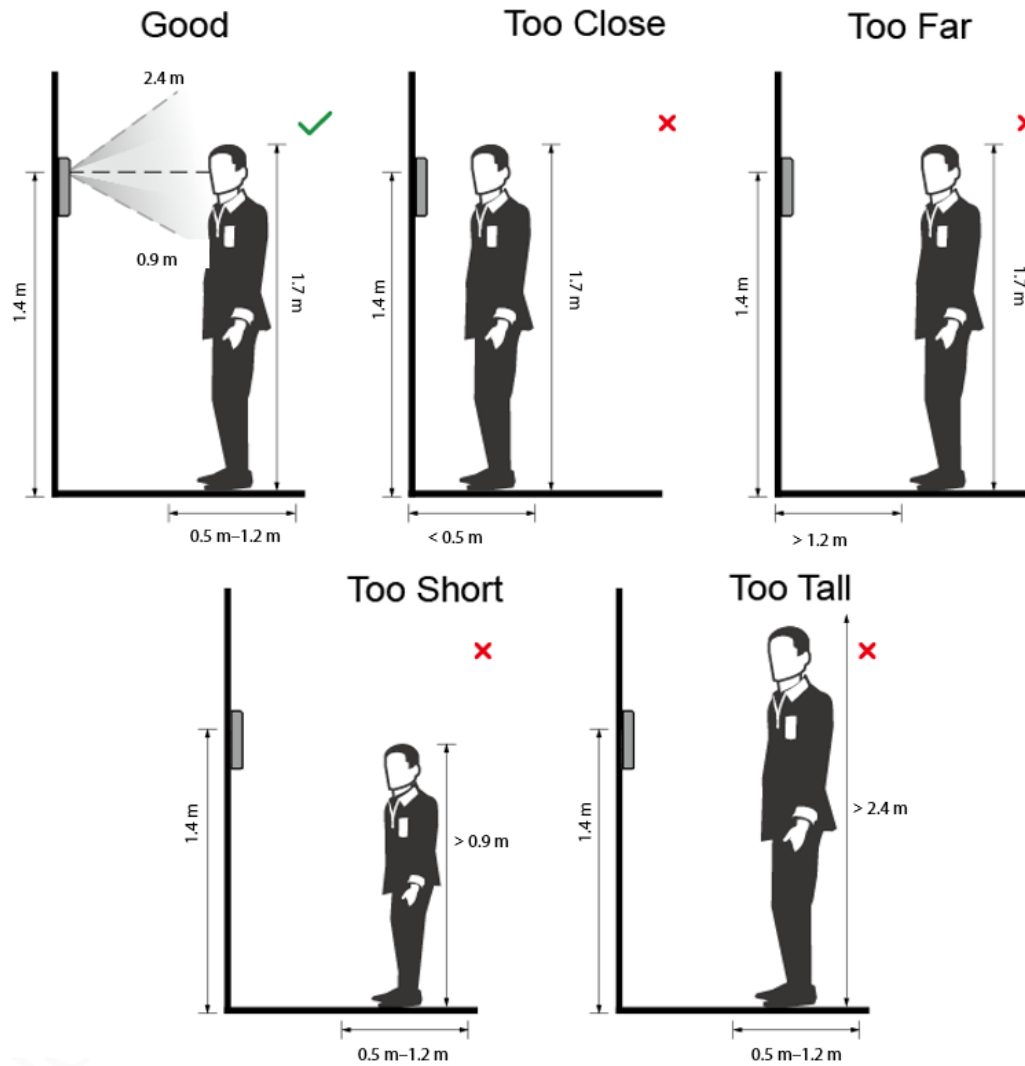


- No sacuda la cabeza o el cuerpo, de lo contrario, el registro podría fallar.
- Evite que aparezcan dos rostros en el cuadro de captura al mismo tiempo.

Posición de la cara

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

Apéndice Figura 3-1 Posición adecuada de la cara



Requisitos de las caras

- Asegúrese de que la cara esté limpia y que la frente no esté cubierta por pelo.
- No use anteojos, sombreros, barbas pobladas u otros adornos faciales que influyan en la grabación de imágenes faciales.
- Con los ojos abiertos, sin expresiones faciales, y coloca tu rostro hacia el centro de la cámara.
- Cuando grabe su rostro o durante el reconocimiento facial, no mantenga su rostro demasiado cerca o demasiado lejos de la cámara.

Apéndice Figura 3-2 Posición de la cabeza





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

Apéndice 4 Recomendaciones sobre ciberseguridad

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

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

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

Recomendaciones "agradables de tener" para mejorar la seguridad de la red de su equipo:

1. Protección Física

Le sugerimos que realice protección física a los equipos, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en un gabinete y una sala de computadoras especiales, e implemente una administración de claves y permisos de control de acceso bien hechos para evitar que personal no autorizado realice contactos físicos, como dañar el hardware, conexión no autorizada de equipos extraíbles (como un disco flash USB, puerto), etc

2. Cambie las contraseñas regularmente

Le sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinadas o descifradas.

3. Establecer y actualizar contraseñas Restablecer información a tiempo

El dispositivo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluido el buzón del usuario final y las preguntas de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección de contraseña, se sugiere no utilizar aquellas que se pueden adivinar fácilmente.

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilitar HTTPS

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

7. Enlace de dirección MAC

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

8. Asigne cuentas y privilegios de manera razonable

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

conjunto mínimo de permisos para ellos.

9. Deshabilite los servicios innecesarios y elija modos seguros

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

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

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

10 Transmisión encriptada de audio y video

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

Recordatorio: la transmisión encriptada causará cierta pérdida en la eficiencia de la transmisión.

11 Auditoría segura

- **Verifique a los usuarios en línea:** le sugerimos que verifique a los usuarios en línea regularmente para ver si el dispositivo está conectado sin autorización.
- **Verifique el registro del equipo:** al ver los registros, puede conocer las direcciones IP que se usaron para iniciar sesión en sus dispositivos y sus operaciones clave.

12 Registro de red

Debido a la limitada capacidad de almacenamiento del equipo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, se recomienda habilitar la función de registro de red para asegurarse de que los registros críticos se sincronizan con el servidor de registro de red para su seguimiento.

13 Construir un entorno de red seguro

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

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