

Estación de la puerta de la villa

Manual del usuario



Prefacio

General

Este manual presenta la instalación, las funciones y el funcionamiento del videoportero para villa (en adelante, "VTO"). Léalo detenidamente antes de utilizarlo y consérvelo para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

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

Historial de revisiones

Versión	Contenido de la revisión	Fecha de lanzamiento
Versión 1.0.0	Primer lanzamiento.	Noviembre de 2024

Aviso de protección de la privacidad

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

Acerca del manual

- Este manual es solo de referencia. Podrían existir ligeras diferencias entre el manual y el producto.
- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas que no cumplan con el manual.
- El manual se actualizará según las últimas leyes y regulaciones de las jurisdicciones pertinentes. Para obtener información detallada, consulte el manual de usuario impreso, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. Este manual es solo de referencia. Podrían existir ligeras diferencias entre la versión electrónica y la versión impresa.

- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto podrían generar diferencias entre el producto real y el manual. Para obtener el programa más reciente y la documentación complementaria, póngase en contacto con el servicio de atención al cliente.
- Podría haber errores de impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. En caso de duda o controversia, nos reservamos el derecho de ofrecer una explicación definitiva.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de empresas en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta información sobre el manejo adecuado del dispositivo, la prevención de riesgos y la prevención de daños materiales. Lea atentamente antes de usar el dispositivo y siga las instrucciones al usarlo.

Requisitos de instalación



WARNING

- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- No conecte el dispositivo a dos o más tipos de fuentes de alimentación, para evitar dañar el dispositivo.
- Por favor, cumpla con los requisitos eléctricos para alimentar el dispositivo. A continuación,
 - ◇ se detallan los requisitos para seleccionar un adaptador de corriente.
 - La fuente de alimentación debe cumplir con los requisitos de las normas IEC 60950-1 e IEC 62368-1.
 - El voltaje debe cumplir con los requisitos de SELV (voltaje extra bajo de seguridad) y no exceder los estándares ES-1.
 - Cuando la potencia del dispositivo no supere los 100 W, la fuente de alimentación debe cumplir los requisitos de LPS y no ser superior a PS2.
 - ◇ Recomendamos utilizar el adaptador de corriente proporcionado con el dispositivo.
 - ◇ Al seleccionar el adaptador de corriente, los requisitos de suministro de energía (como el voltaje nominal) están sujetos a la etiqueta del dispositivo.



- El personal que trabaja en altura debe tomar todas las medidas necesarias para garantizar su seguridad personal, incluido el uso de casco y cinturones de seguridad.
- No coloque el dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- Instale el dispositivo sobre una superficie estable para evitar que se caiga.
- Instale el dispositivo en un lugar bien ventilado y no bloquee su ventilación.
- Utilice un adaptador o fuente de alimentación de gabinete proporcionado por el fabricante.
- Utilice los cables de alimentación recomendados para la región y que cumplan con las especificaciones de potencia nominal.
- El dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectada a una toma de corriente con conexión a tierra.

Requisitos de operación



DANGER

Precauciones con la batería

Medidas preventivas (incluidas, entre otras):

- No transporte, almacene ni utilice las baterías en altitudes elevadas con baja presión y en entornos con temperaturas extremadamente altas y bajas.
- No arroje las baterías al fuego ni a un horno caliente, ni las aplaste ni las corte mecánicamente para evitar una explosión.

- No deje las baterías en ambientes con temperaturas extremadamente altas para evitar explosiones y fugas de líquidos o gases inflamables.
- No someta las baterías a presiones de aire extremadamente bajas para evitar explosiones y fugas de líquidos o gases inflamables.



- Compruebe si la fuente de alimentación es correcta antes de usarlo.
- No desconecte el cable de alimentación del costado del dispositivo mientras el adaptador esté encendido.
- Utilice el dispositivo dentro del rango nominal de entrada y salida de energía.
- Transporte, utilice y almacene el dispositivo en las condiciones de humedad y temperatura permitidas.
- Si el dispositivo permanece apagado durante más de un mes, debe guardarse en su embalaje original y sellarse. Asegúrese de mantenerlo alejado de la humedad y almacenarlo en las condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquidos sobre el dispositivo y asegúrese de que no haya ningún objeto lleno de líquido sobre el dispositivo que evite que el líquido fluya hacia él.
- No desmonte el dispositivo sin instrucciones profesionales.

Tabla de contenido

Prólogo.....	I
Precauciones y advertencias importantes.....	III 1
Estructura.....	1
1.1 Estación de puerta de villa (varios botones).....	1
1.1.1 Panel frontal.....	1
1.1.2 Panel trasero.....	2
1.2 Estación de puerta de villa (un solo botón).....	3
1.2.1 Serie R.....	3
1.2.2 Serie D.....	5
1.2.3 Serie G.....	8
1.2.4 Serie E.....	9
1.2.5 Serie F.....	15
1.3 Modelo de botón.....	26
1.3.1 Panel frontal.....	26
1.3.2 Panel trasero.....	27
2 Inicialización del VTO.....	29
2.1 Web	29
2.2 Aplicación DMSS.....	29
3 Inicio de sesión y restablecimiento de contraseña.....	33
3.1 Inicio de sesión.....	33
3.2 Restablecimiento de contraseña.....	33
4 Página de inicio.....	35
5 Asistente de configuración.....	36
5.1 Configuración como servidor SIP.....	36
5.2 No configurar como servidor SIP.....	37
6 Configuración del dispositivo local.....	38
6.1 Configuración básica.....	38
6.1.1 Estación de puerta de la villa.....	38
6.1.2 Segunda estación de confirmación.....	41
6.2 Control de acceso.....	43
6.2.1 Configuración.....	43
6.2.2 Función de extensión.....	44
6.3 Control de luz.....	47
6.4 Configuración de la tarjeta.....	48
6.5 Configuración de Wiegand.....	48
6.6 Diseño.....	50
6.6.1 Diseño (varios botones).....	50

6.6.2 Diseño (Múltiples módulos).....	52
6.7 Adición de IPC.....	55
6.7.1 Agregar IPC uno por uno.....	56
6.7.2 Exportación de información de IPC en lotes.....	58
6.7.3 Importación de información de IPC en lotes.....	58
7 Configuración del dispositivo.....	59
7.1 Gestión de VTO.....	59
7.2 Gestión de VTH.....	60
7.3 Gestión de VTS.....	62
Gestión de 8 personas.....	64
9 Configuración de red.....	67
9.1 TCP/IP.....	67
9.2 Puerto.....	68
9.3 Servidor SIP.....	69
9.4 Segunda estación de confirmación en cascada.....	72
9.5 Servicio en la nube.....	73
9.6 UPnP.....	74
9.6.1 Habilitación de servicios UPnP.....	74
9.6.2 Agregar servicios UPnP.....	74
9.7 Wi-Fi.....	76
9.8 Servicios básicos.....	76
9.9 Registro automático.....	78
10 Sistema.....	80
10.1 Alarma.....	80
10.2 Vídeo.....	81
10.3 Audio.....	84
10.4 Tiempo.....	85
10.5 Usuario de ONVIF.....	87
11 Gestión de registros.....	89
11.1 Diagnóstico con un solo clic.....	89
11.2 Información del sistema.....	89
11.2.1 Información de la versión.....	89
11.2.2 Información legal.....	90
11.3 Capacidad de datos.....	90
11.4 Gestión del mantenimiento.....	90
11.4.1 Configuración.....	90
11.4.2 Mantenimiento.....	91
11.5 Actualización.....	91
11.6 Mantenimiento avanzado.....	92
12 Gestión de la seguridad.....	93

12.1 Estado de seguridad.....	93
12.2 Servicio del sistema.....	93
12.3 Defensa de ataque.....	94
12.3.1 Cortafuegos.....	94
12.3.2 Bloqueo de cuenta.....	95
12.3.3 Ataque anti-DoS.....	96
12.4 Certificado CA.....	96
12.5 Cifrado de vídeo.....	97
12.6 Advertencia de seguridad.....	97
Configuración del modelo de 13 botones.....	99
13.1 Conexión del cable.....	99
13.2 Configuración de VTH.....	100
Apéndice 1 Recomendación de seguridad.....	102

1 Estructura

1.1 Estación de puerta de villa (varios botones)

1.1.1 Panel frontal

Figura 1-1 Panel frontal

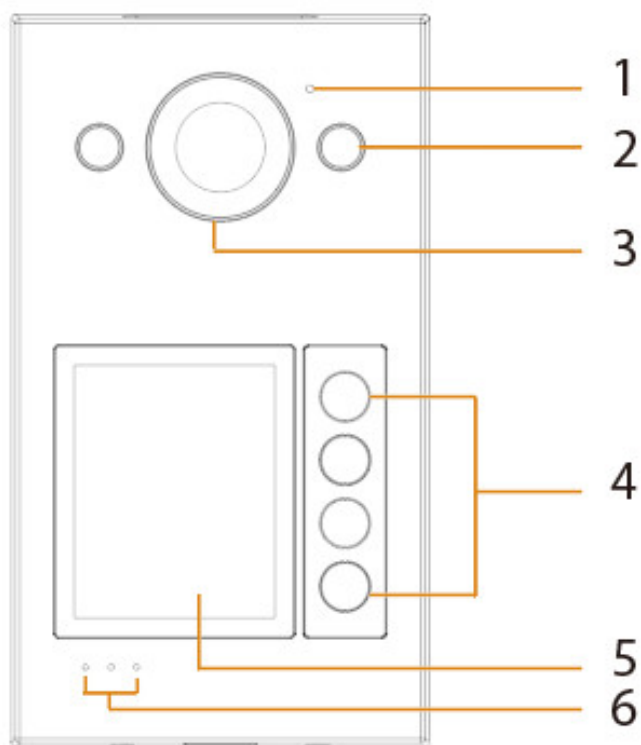


Tabla 1-1 Componentes

No.	Nombre	Función
1	micrófono	Entrada de audio.
2	Iluminador	Proporciona una luz constante para enfocar más fácilmente un sujeto en entornos oscuros.
3	Cámara	Captura imágenes o graba vídeos para el VTO.
4	Botones de llamada	Llama al VTH.
5	Área de deslizamiento de tarjetas	Pase las tarjetas registradas para desbloquear puertas.
6	Indicadores	De izquierda a derecha: ● Anillo: VTO está llamando al VTH. ● Hablando: VTO está en conversación con VTH. ● Desbloqueo: VTO se desbloqueó exitosamente.

1.1.2 Panel trasero



El puerto multifunción puede variar según los modelos reales.

Figura 1-2 Panel trasero

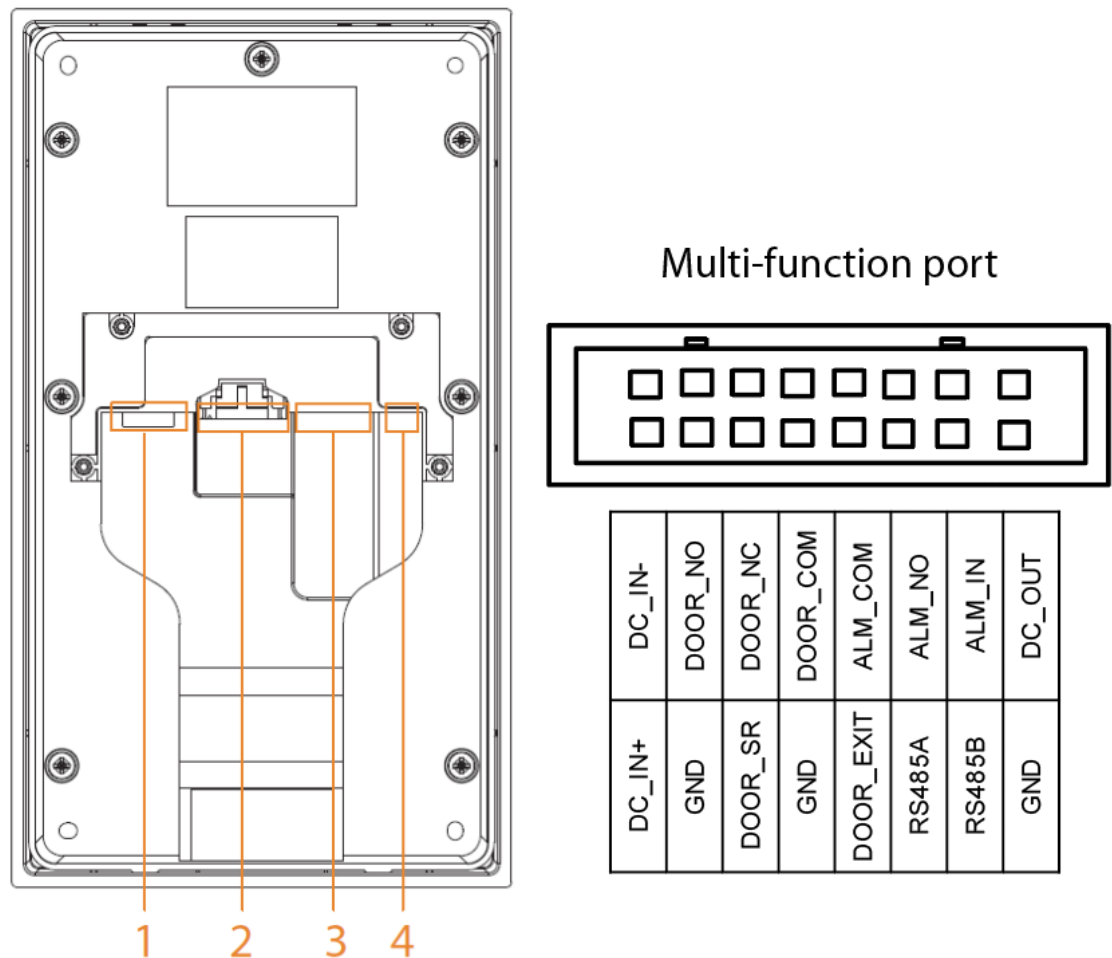


Tabla 1-2 Componentes

No.	Nombre	Función
1	Ranura para tarjeta SD	Se utiliza para insertar una tarjeta SD para poder almacenar información como imágenes y vídeos.
2	Puerto multifunción	Puerto de alarma, puerto de detector de puerta, puerto 485, puerto de alimentación y otros puertos.
3	Puerto de red	Puerto de red RJ-485 para conectarse a la red.
4	Botón de reinicio	Mantenga presionado el botón durante varios segundos para restablecer la configuración de fábrica.

1.2 Estación de puerta de villa (un solo botón)

1.2.1 Serie R

1.2.1.1 Panel frontal

El tamaño y la apariencia pueden variar según los modelos del producto.

Figura 1-3 Panel frontal

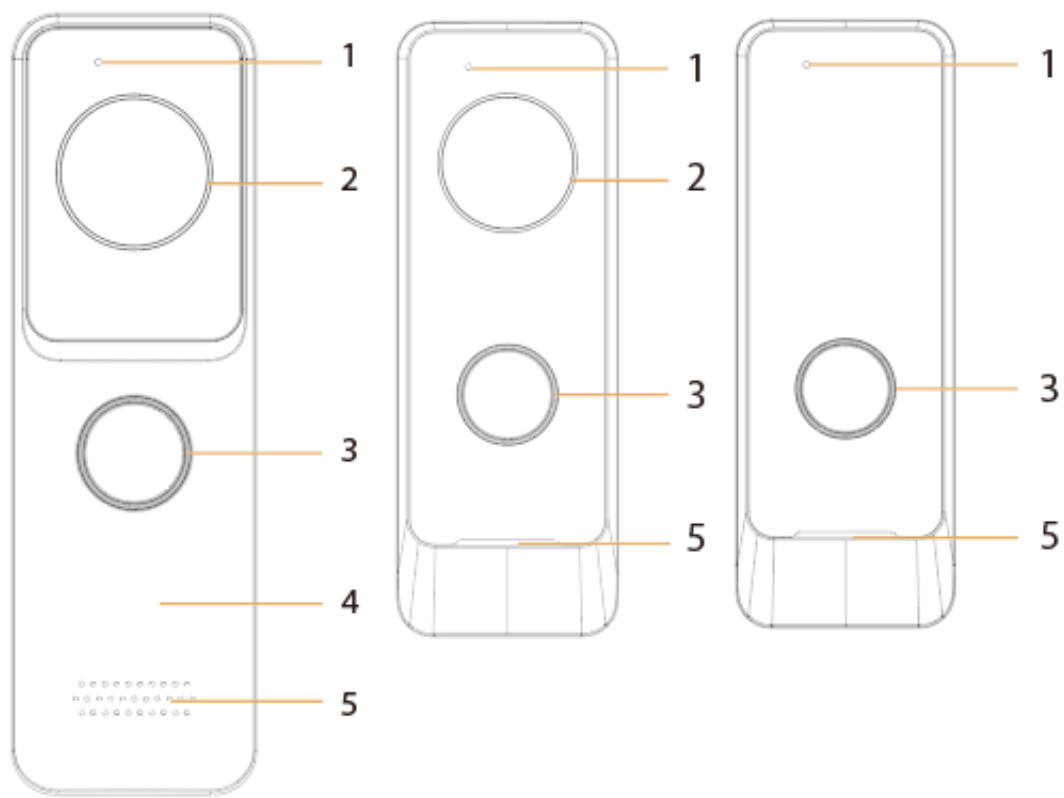


Tabla 1-3 Componentes

No.	Nombre	Función
1	micrófono	Entrada de audio.
2	Cámara	Captura imágenes o graba vídeos para el VTO.
3	Botón de llamada	Llama al VTH.
4	Área de deslizamiento de tarjetas	Pase las tarjetas registradas para desbloquear las puertas. La función de deslizamiento de tarjeta solo está disponible en modelos seleccionados.
5	Vocero	Salida de audio.

1.2.1.2 Panel trasero



El puerto multifunción puede variar según el modelo. A continuación, se muestran dos modelos como ejemplo.

Figura 1-4 Panel trasero (1)

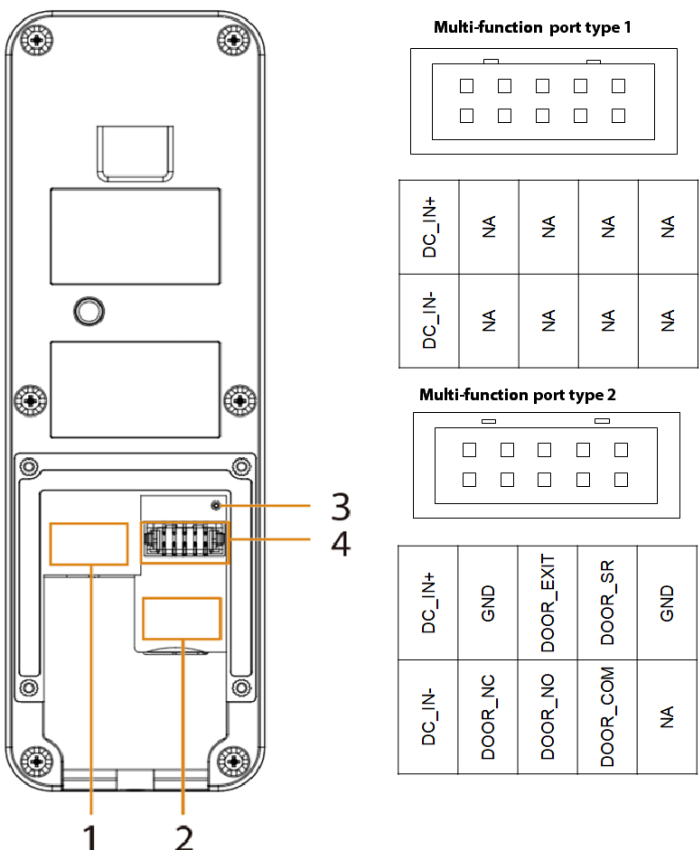


Tabla 1-4 Componentes

No.	Nombre	Función
1	Puerto de red	Se conecta a la red.
2	Ranura para tarjeta SD	Inserte una tarjeta SD para poder almacenar información como imágenes y vídeos.
3	Botón de reinicio	Mantenga presionado el botón durante varios segundos para restablecer la configuración de fábrica.
4	Puerto multifunción	● Tipo 1: El puerto multifunción solo tiene un puerto de entrada de energía para conectarse a la fuente de alimentación. ● Tipo 2: El puerto multifunción incluye un puerto de entrada de energía y un puerto de detector de puerta.

Figura 1-5 Panel trasero (2)

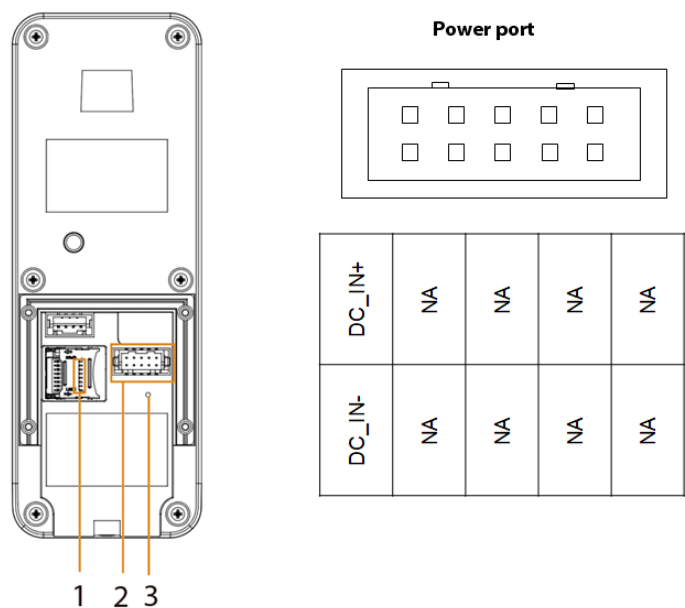


Tabla 1-5 Componentes

No.	Nombre	Función
1	Ranura para tarjeta SD	Inserte una tarjeta SD para poder almacenar información como imágenes y vídeos.
2	Puerto de alimentación	Se conecta a la fuente de alimentación.
3	Botón de reinicio	Mantenga presionado el botón durante varios segundos para restablecer la configuración de fábrica.

1.2.2 Serie D

1.2.2.1 Panel frontal

Figura 1-6 Panel frontal

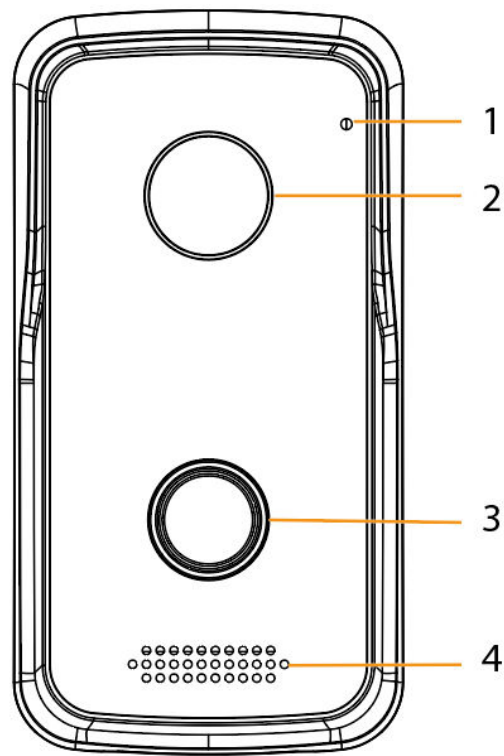


Tabla 1-6 Componentes

No.	Nombre	Función
1	micrófono	Entrada de audio.
2	Cámara	Captura imágenes o graba vídeos para el VTO.
3	Botón de llamada	Llama al VTH.
4	Vocero	Salida de audio.

1.2.2.2 Panel trasero

Figura 1-7 Panel trasero

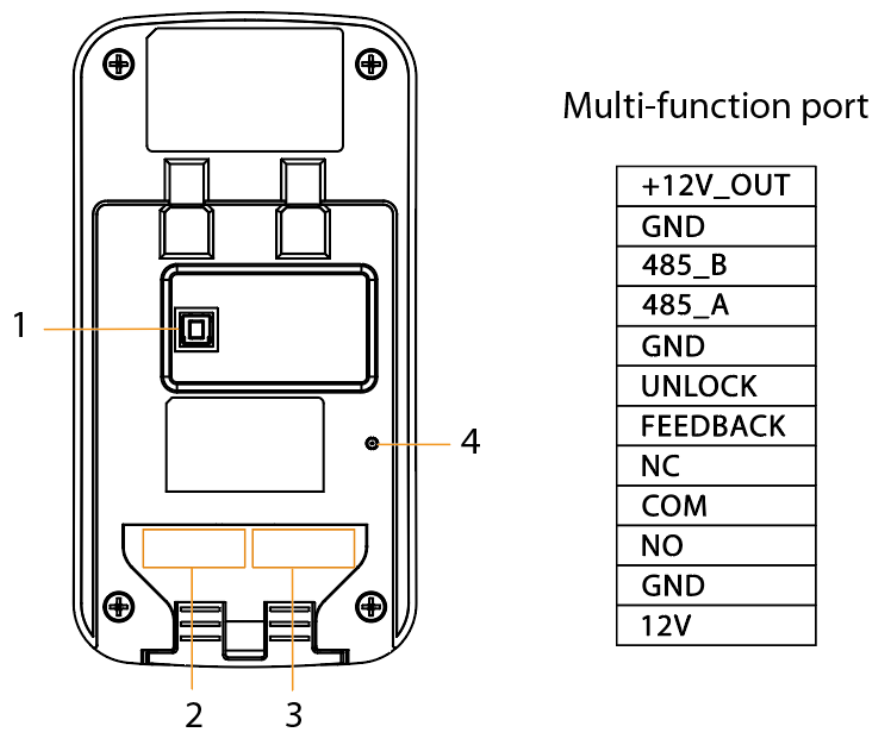


Tabla 1-7 Componentes

No.	Nombre	Función
1	Botón de manipulación	● Una vez que el dispositivo instalado se retira de la pared o de otros lugares, el dispositivo emite un pitido y se genera el registro de alarma. ● Dentro de los 5 minutos posteriores al encendido del dispositivo, si se pulsa el botón de manipulación 5 veces en 8 segundos, el dispositivo emitirá un pitido y eliminará la información de la cuenta. Se generará el registro de la alarma.
2	Puertos multifunción	Puerto de alarma, puerto de detector de puerta, puerto 485, puerto de alimentación y más.
3	Puerto de red	Se conecta a la red.
4	Botón de reinicio	Mantenga presionado el botón durante varios segundos para restablecer la configuración de fábrica.

Serie 1.2.3 G

1.2.3.1 Panel frontal

Figura 1-8 Panel frontal

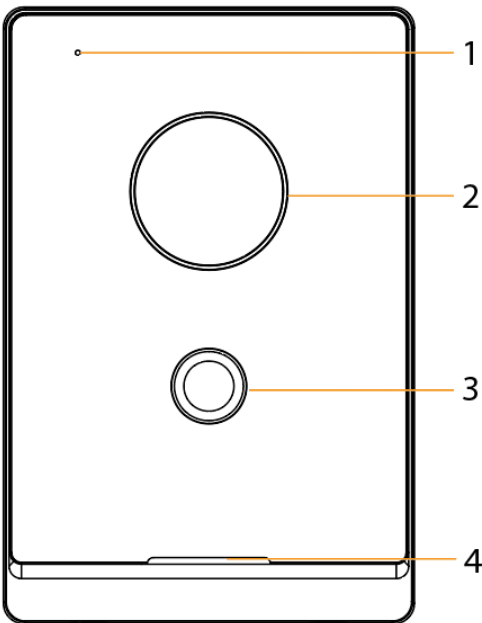


Tabla 1-8 Componentes

No.	Nombre	Función
1	micrófono	Entrada de audio.
2	Cámara	Captura imágenes o graba vídeos para el VTO.
3	Botón de llamada	Llama al VTH. El botón muestra diferentes colores en diferentes estados. ● En espera: Sin luz. ● Llamada no contestada: Verde fijo. ● Llamada contestada: Azul fijo. ● Desbloquear cuando el dispositivo está en estado de espera: Rojo. ● Desbloquear cuando no se responde la llamada: parpadea en verde, amarillo y luego verde. ● Desbloquear después de responder la llamada: parpadea en azul, rosa y luego azul. ● Red desconectada: Luz verde parpadeante.
4	Vocero	Salida de audio.

1.2.3.2 Panel trasero

Figura 1-9 Panel trasero

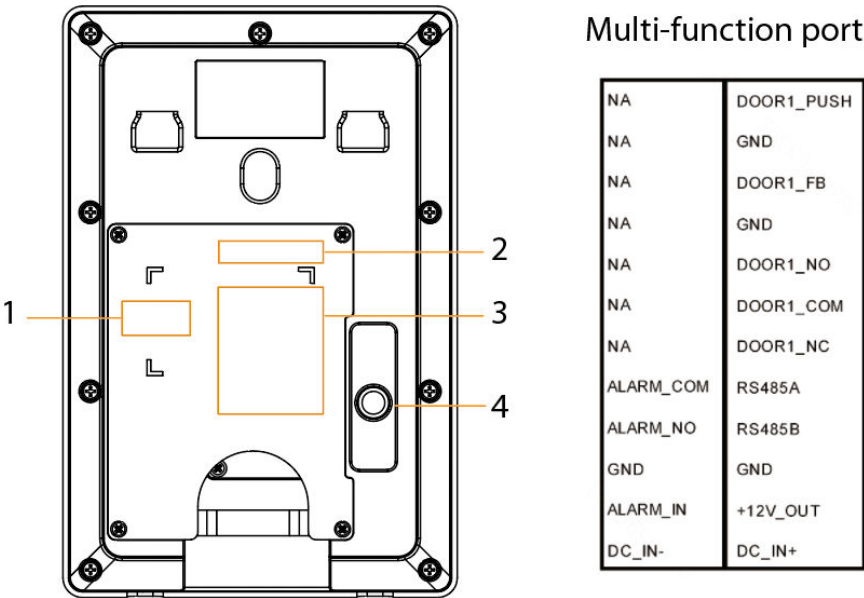


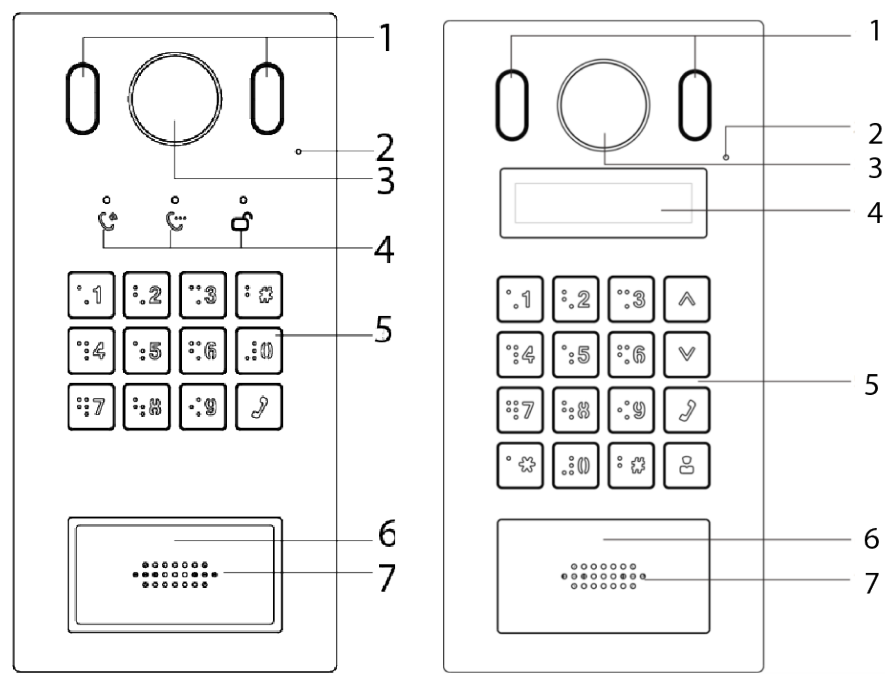
Tabla 1-9 Componentes

No.	Nombre	Función
1	Puerto de red	Se conecta a la red.
2	Puerto multifunción	Puerto de alarma, puerto de detector de puerta, puerto 485, puerto de alimentación y más.
3	Ranura para tarjeta SD	Inserte una tarjeta SD para poder almacenar información como imágenes y vídeos.
4	Botón de manipulación	- Una vez que el dispositivo instalado se retira de la pared o de otros lugares, el dispositivo emite un pitido y se genera el registro de alarma. - Dentro de los 5 minutos posteriores al encendido del dispositivo, si se pulsa el botón de manipulación 5 veces en 8 segundos, el dispositivo emitirá un pitido y eliminará la información de la cuenta. Se generará el registro de la alarma.

1.2.4 Serie E

1.2.4.1 Panel frontal (3222E y 6222E)

Figura 1-10 Panel frontal



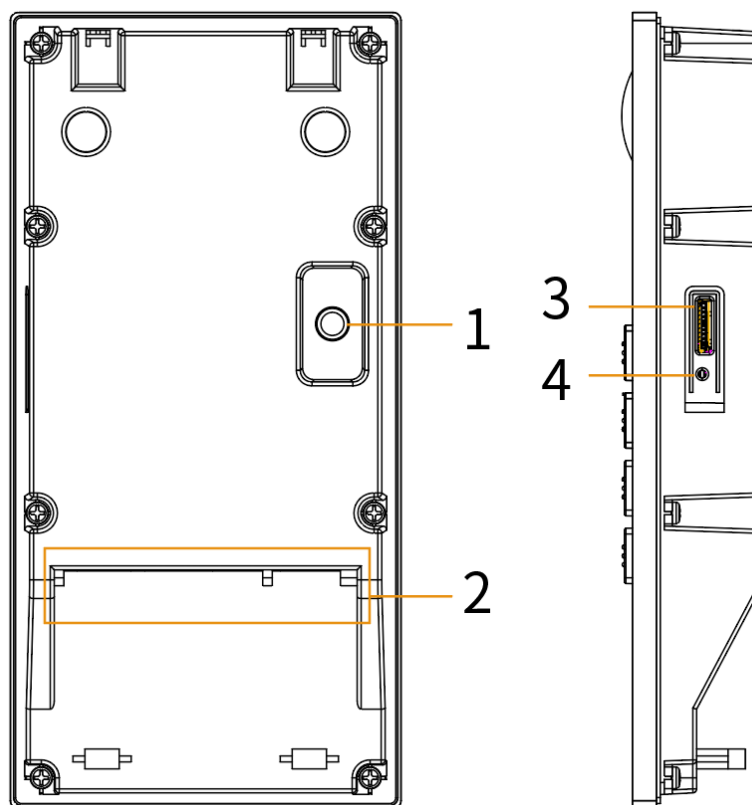
El panel de la izquierda es el modelo 3222E y el de la derecha es el modelo 6222E.

Tabla 1-10 Descripción del panel frontal

No.	Nombre	Descripción
1	Iluminador	Proporciona luz adicional a la cámara cuando está oscuro.
2	Micrófono	Entrada de audio.
3	Cámara	Captura imágenes o graba vídeos para el VTO.
4	Indicadores	Muestra el estado al llamar, hablar y desbloquear.
5	Teclado	—
6	Área de lectura de tarjetas	Pase una tarjeta aquí para desbloquear la puerta.
7	Vocero	Salida de audio.

1.2.4.2 Panel trasero (3222E y 6222E)

Figura 1-11 Panel trasero

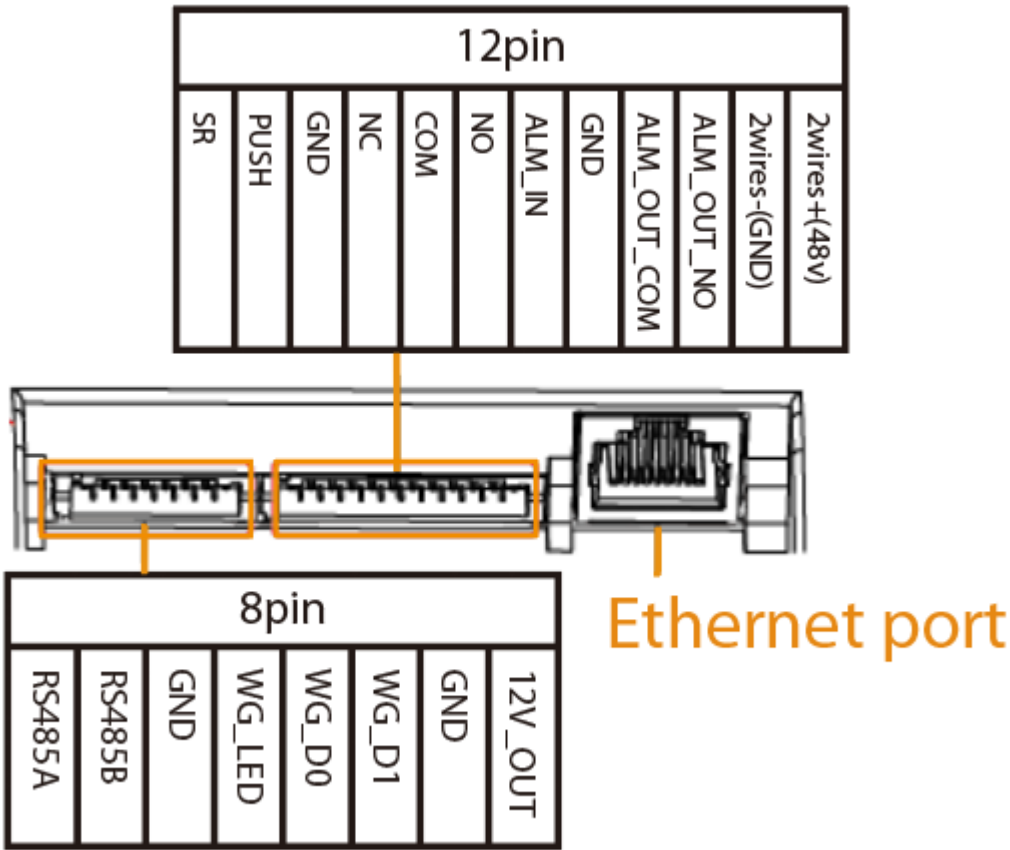


Los paneles traseros del modelo 3222E y 6222E son iguales.

Tabla 1-11 Descripción del panel trasero

No.	Nombre	Descripción
1	Interruptor antimanipulación	Cuando el VTO se retira de la pared por la fuerza, se activará una alarma y la información de la alarma se enviará al centro de administración.
2	Puerto multifunción	Para obtener más detalles, consulte la Figura 1-12.
3	Ranura para tarjeta SD	Conecte la tarjeta SD.
4	Botón de reinicio	Manténgalo presionado durante 10 segundos para restablecer todas las configuraciones.

Figura 1-12 Puerto multifunción



1.2.4.3 Panel frontal (2101E)

Figura 1-13 Panel frontal

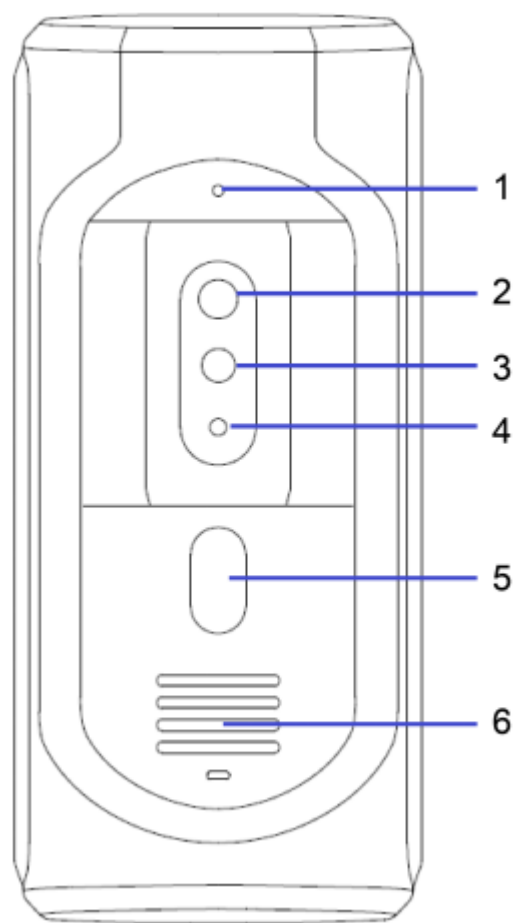


Tabla 1-12 Descripción del panel frontal

No.	Nombre	Descripción
1	Micrófono	—
2	Cámara	—
3	Luz de iluminación infrarroja	Proporciona luz infrarroja adicional para la cámara cuando está oscuro.
4	Sensor de luz	Detecta las condiciones de iluminación ambiental.
5	Botón de llamada	Llamar a VTHs o al centro de gestión.
6	Vocero	—

1.2.4.4 Panel trasero (2101E)

Figura 1-14 Panel trasero

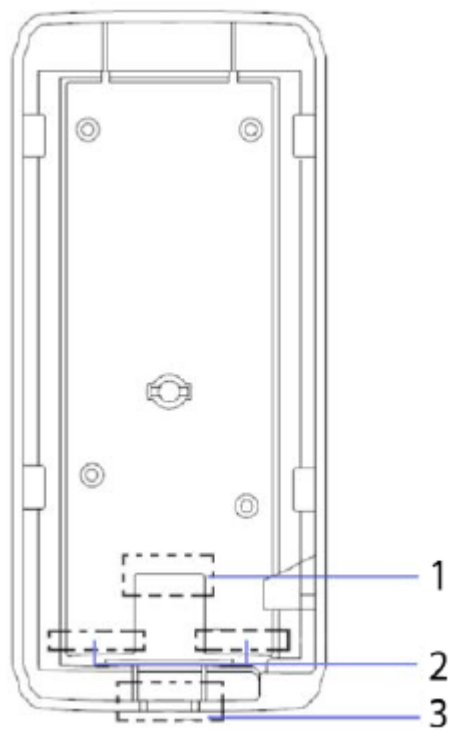


Tabla 1-13 Descripción del panel trasero

No.	Nombre	Descripción
1	Puerto de red	Se conecta al cable de red.
2	Puertos RS-485	Vea la figura y la tabla a continuación.
3	Salida de cable	Pase los cables aquí.

Figura 1-15 Conexión del cable

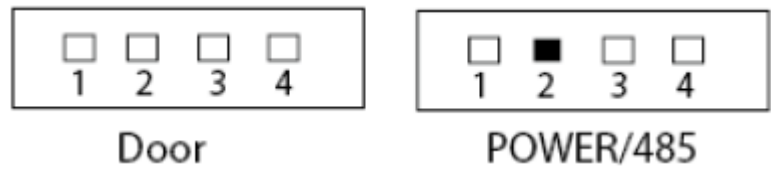


Tabla 1-14 Descripción del puerto

PUERTA		POTENCIA/485	
No.	Nombre	No.	Nombre
1	NO	1	+ 12
2	CAROLINA DEL NORTE	2	Tierra
3	COM	3	RS-485A
4	ALARMA DENTRO o Desbloquear (predeterminado)	4	RS-485B

Serie 1.2.5 F

1.2.5.1 Panel frontal

Figura 1-16 Panel frontal

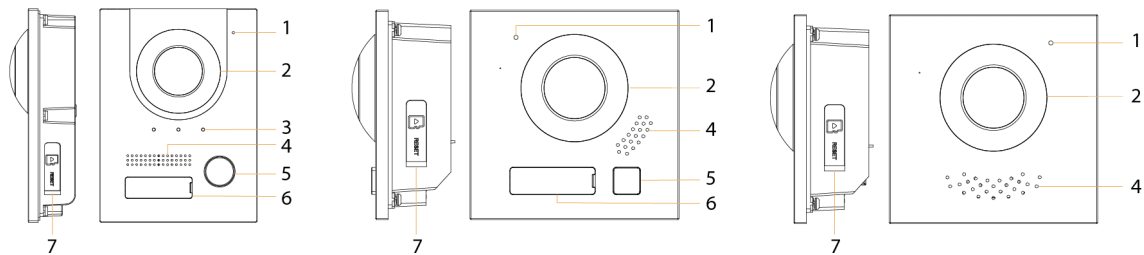


Tabla 1-15 Descripción del panel frontal

No.	Nombre	Descripción
1	Micrófono	Entrada de audio.
2	Cámara	Captura imágenes o graba vídeos para el VTO.
3	Indicadores	Mostrar el estado al llamar, hablar y desbloquear.
4	Vocero	Salida de audio.
5	Botón de llamada	Llamar al VTH y al centro de gestión.
6	Letrero	Muestra la información personalizada.
7	Ranura para tarjeta y botón de reinicio	● Inserte una tarjeta SD para poder almacenar información como imágenes y vídeos. ● Mantenga presionado el botón durante varios segundos para restablecer la configuración de fábrica.

1.2.5.2 Panel trasero

Figura 1-17 Panel trasero

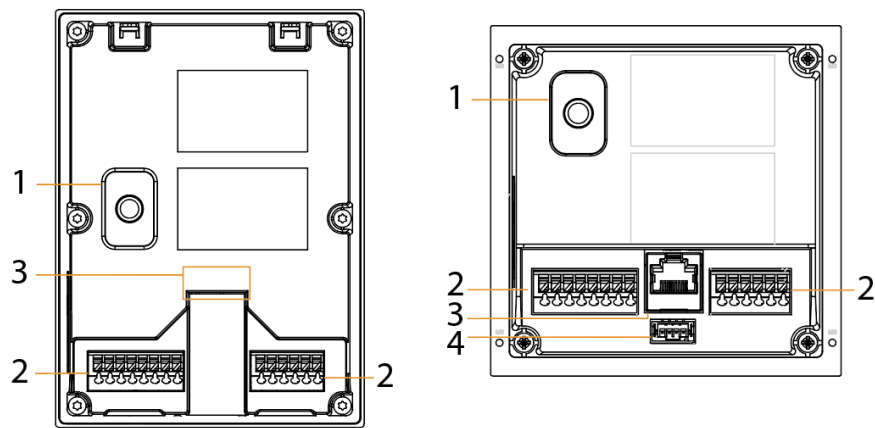


Tabla 1-16 Descripción del panel trasero

No.	Nombre	Función
1	Botón de manipulación	- Una vez que el dispositivo instalado se retira de la pared o de otros lugares, el dispositivo emite un pitido y se genera el registro de alarma. - Dentro de los 5 minutos posteriores al encendido del dispositivo, si se pulsa el botón de manipulación 5 veces en 8 segundos, el dispositivo emitirá un pitido y eliminará la información de la cuenta. Se generará el registro de la alarma.
2	Puertos multifunción	Puerto de alarma, puerto de detector de puerta, puerto 485, puerto de alimentación y más.
3	Puerto de red	Conectarse a la red.
4	Puerto de conexión en cascada	Conectarse a otros módulos.

Figura 1-18 Puertos multifunción

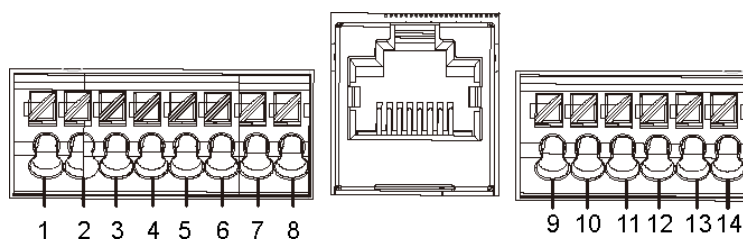


Tabla 1-17 Descripción del puerto

No.	Descripción	No.	Descripción
1	Tierra	8	2 cables (GND) para un módulo de cámara digital de 2 cables - GND para un módulo de cámara digital completo
2	+ 12 V_SALIDA	9	BOTÓN DE LA PUERTA
3	RS-485_B	10	RETROALIMENTACIÓN DE LA PUERTA
4	RS-485_A	11	Tierra
5	ALARMA_NO	12	PUERTA_NC
6	ALARMA_COM	13	PUERTA_COM
7	2 cables + (48 V) para una cámara digital de 2 hilos módulo 12 V_IN para una totalmente digital módulo de cámara	14	PUERTA_NO

1.2.5.3 Módulo Indicador

Figura 1-19 Panel frontal

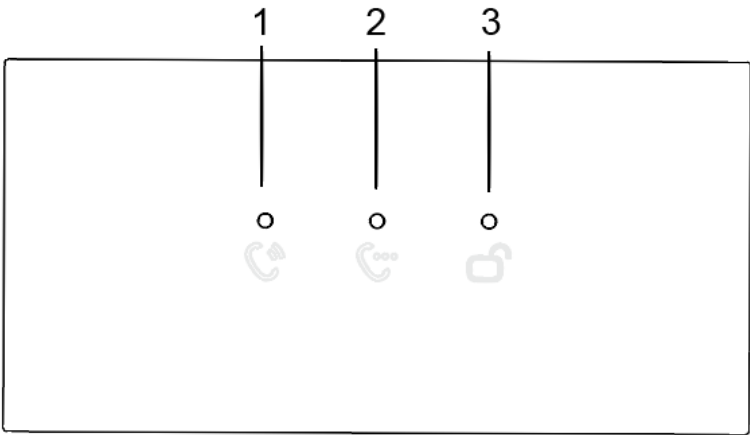


Tabla 1-18 Descripción del panel frontal

No.	Nombre	Descripción
1	Indicador de llamada	Estado de actividad.
2	Indicador de conversación	
3	Indicador de desbloqueo	

Figura 1-20 Panel trasero

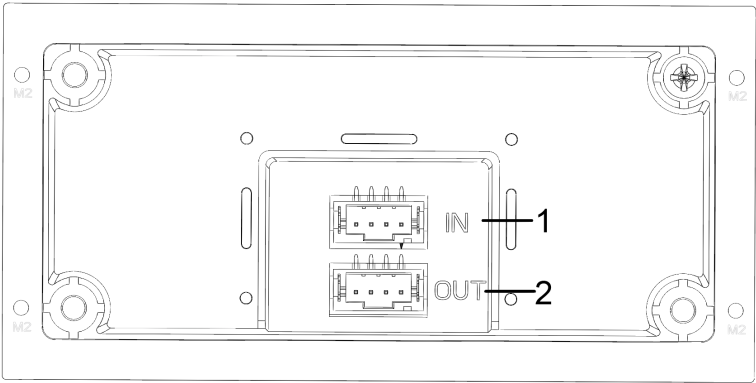


Tabla 1-19 Descripción del panel trasero

No.	Nombre	Descripción
1	Entrada en cascada	Conectarse a otros módulos.
2	Salida en cascada	

1.2.5.4 Módulo de botones

Módulo de 1 botón, módulo de 2 botones y módulo de 5 botones

Los módulos de uno, dos y cinco botones están disponibles con la misma función. Aquí tomamos como ejemplo el módulo de cinco botones.

Figura 1-21 Panel frontal del módulo de cinco botones

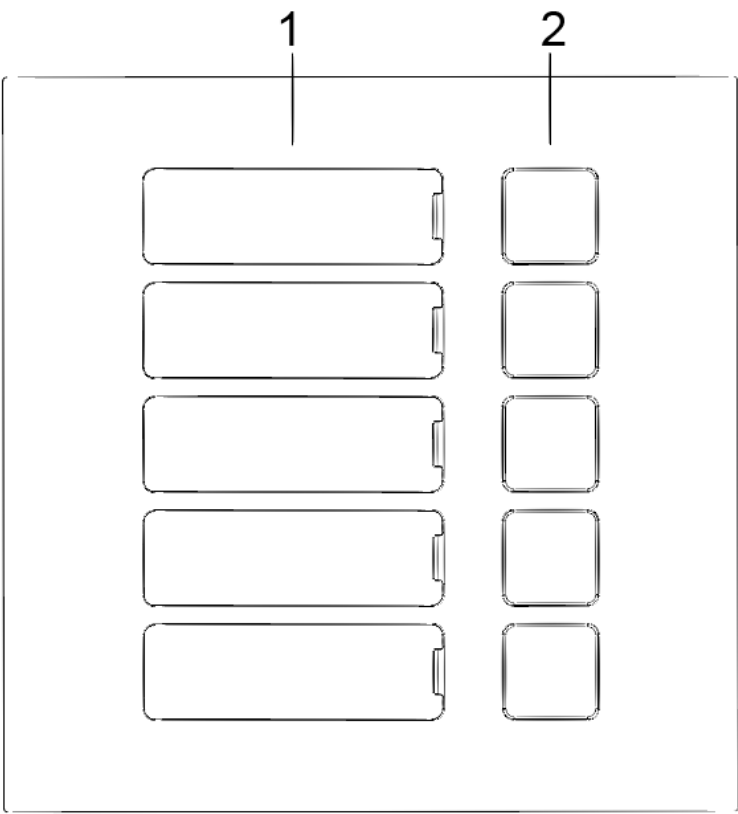


Tabla 1-20 Descripción del panel frontal

No.	Nombre	Descripción
1	Directorio de usuarios	Coloque tarjetas con nombres aquí.
2	Botones de llamada	Llame a otros VTH o al centro de administración.

Figura 1-22 Panel trasero del módulo de cinco botones

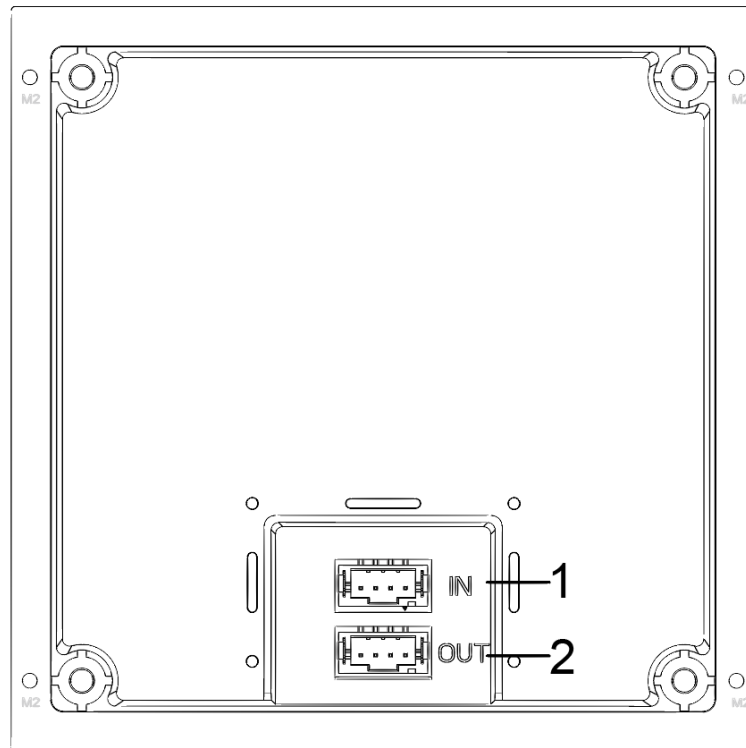


Tabla 1-21 Descripción del panel trasero

No.	Nombre	Descripción
1	Entrada en cascada	Conectarse a otros módulos.
2	Salida en cascada	

Módulo de 2 botones, módulo de 4 botones y módulo de 10 botones

Los módulos de dos, cuatro y diez botones están disponibles con la misma función. Aquí tomamos como ejemplo el módulo de diez botones.

Figura 1-23 Panel frontal del módulo de diez botones

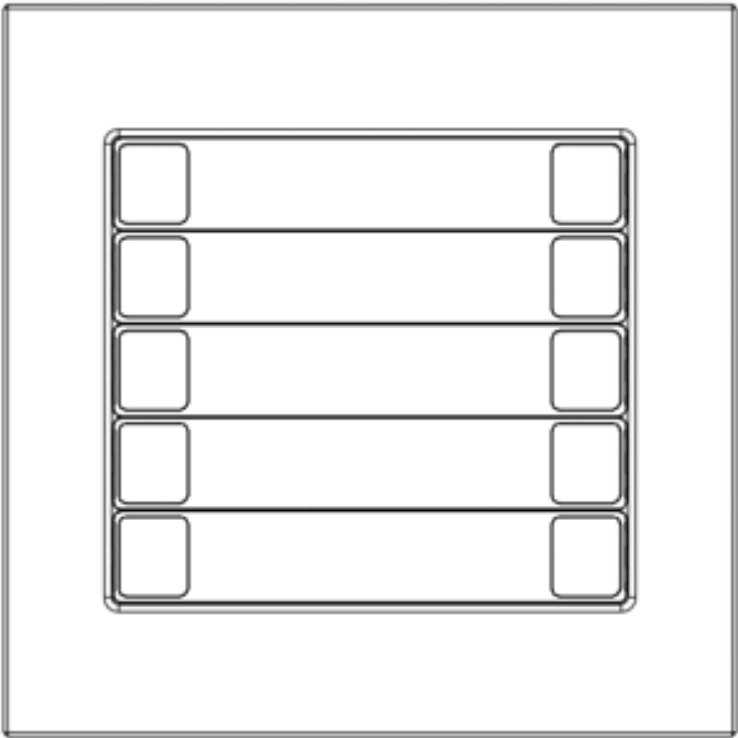


Figura 1-24 Panel trasero del módulo de diez botones

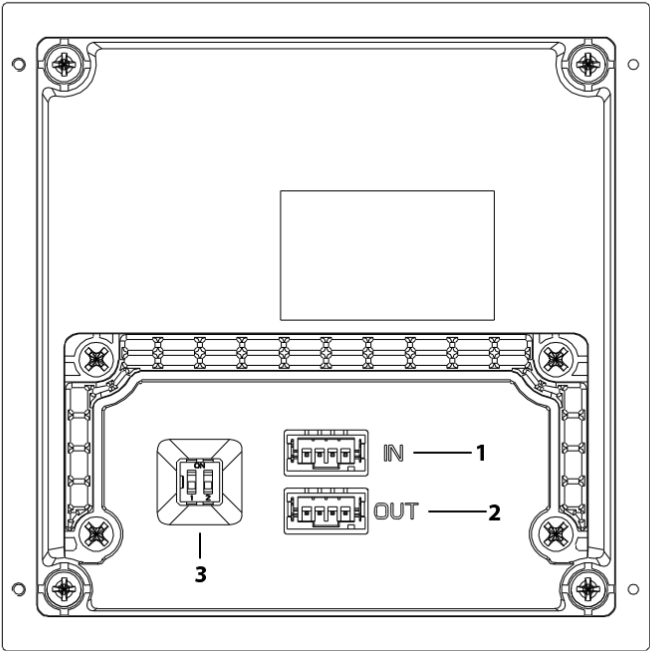


Tabla 1-22 Descripción del panel trasero

No.	Nombre	Descripción
1	Entrada en cascada	Conectarse a otros módulos.
2	Salida en cascada	

No.	Nombre	Descripción
3	Interruptor de modo	● Cambiar entre botones de una sola columna y botones de dos columnas. ● El primer interruptor DIP de la izquierda gira a EN indica los botones de una sola columna, mientras que para 1 indica los botones de dos columnas. ● Tiene efecto después de reiniciar el VTO principal. ● Girar hacia arriba o hacia abajo el segundo interruptor DIP (de izquierda a derecha) no tiene ningún efecto.  Si desea cambiar el modo de botones de dos columnas al modo de botones de una sola columna, saque el accesorio de botones de una sola columna del paquete para reemplazarlo. Para obtener información sobre las configuraciones de números de sala en la WEB, consulte "6.6 Diseño".

1.2.5.5 Módulo de teclado (con Braille)



El panel trasero del módulo del teclado es el mismo que el módulo de botones.

Figura 1-25 Módulo de teclado

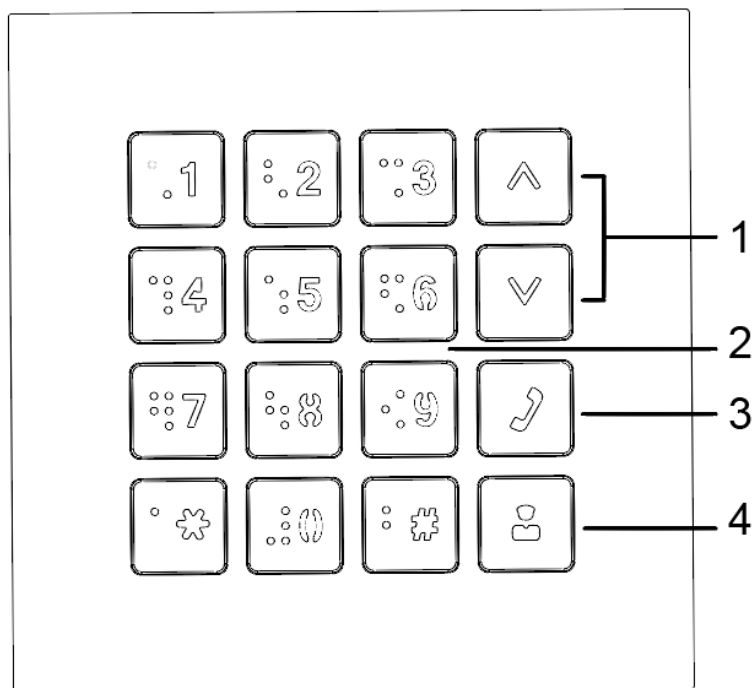


Tabla 1-23 Descripción del módulo de teclado

No.	Nombre	Descripción
1	Selección	Toque el botón para seleccionar el contacto.
2	Números	Introduzca la contraseña o los números VTH.
3	Llamar	Llamar según los números.
4	Centro de gestión de llamadas	Llamar al centro de gestión.

1.2.5.6 Módulo de tarjeta

Hay dos tipos de módulos de tarjeta. Seleccione entre el módulo de tarjeta de identificación y el módulo de tarjeta IC, según sus necesidades.



El panel trasero del módulo de tarjeta es el mismo que el del módulo de botones.

Figura 1-26 Módulo de tarjeta



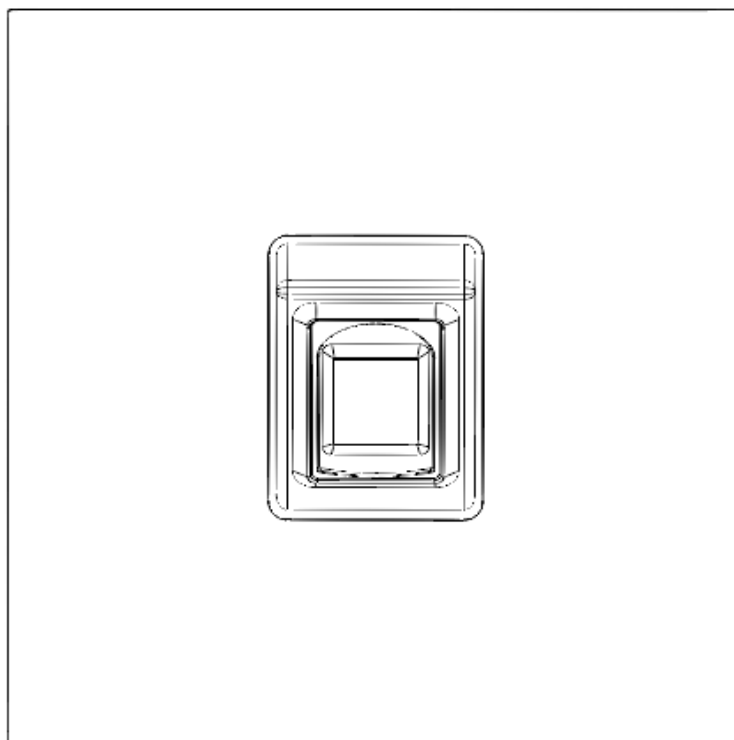
1.2.5.7 Módulo de huellas dactilares

Recoge y verifica huellas dactilares.



- Los paneles traseros del módulo de huellas dactilares y del módulo de botones tienen diferentes posiciones de puertos, pero las funciones de los puertos son las mismas.
- Cuando se accede a un módulo de huellas dactilares y desea agregar un nuevo módulo de huellas dactilares, borre la información de huellas dactilares del módulo de huellas dactilares original.

Figura 1-27 Módulo de huellas dactilares



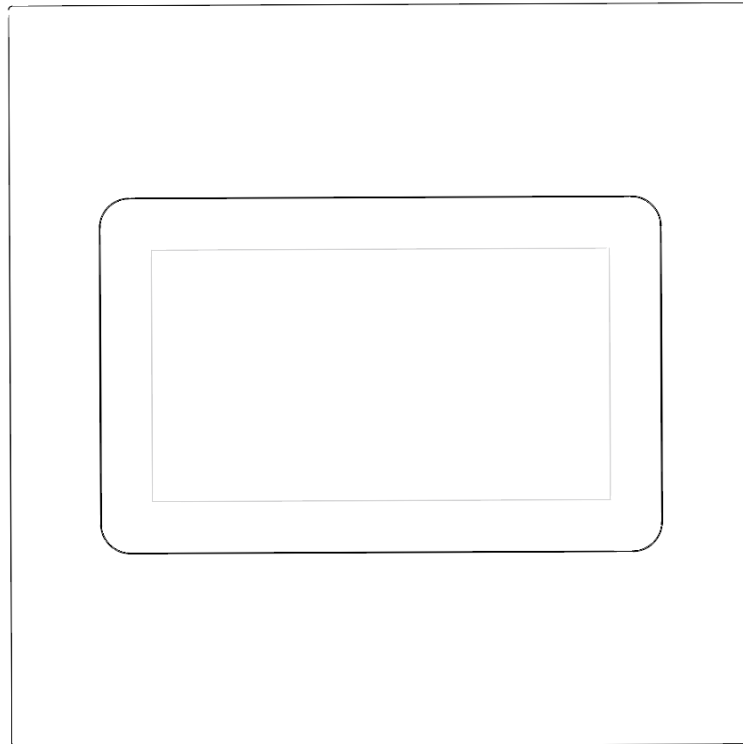
1.2.5.8 Módulo de visualización

Muestra información del usuario.



Los paneles traseros del módulo de pantalla y del módulo de botones tienen diferentes posiciones de puertos, pero las funciones de los puertos son las mismas.

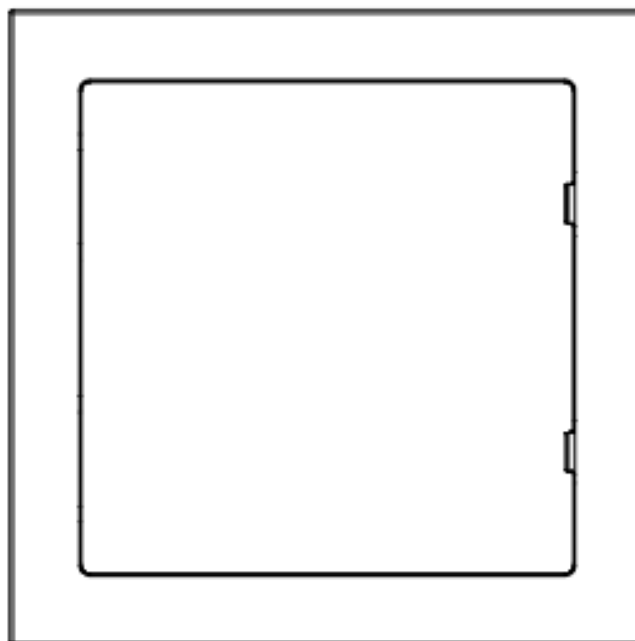
Figura 1-28 Módulo de visualización



1.2.5.9 Módulo de información

Muestra el número de habitación y el mensaje del huésped.

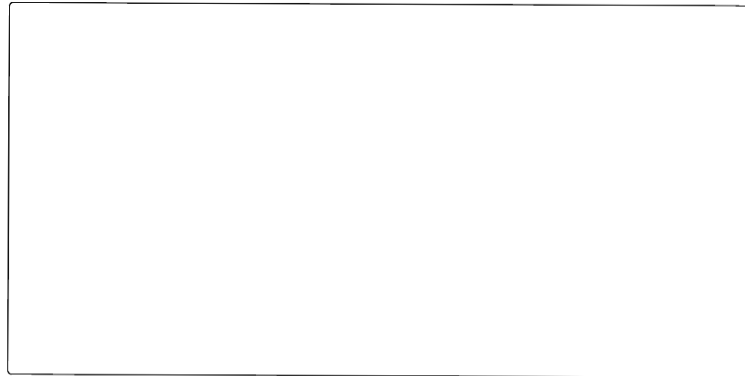
Figura 1-29 Módulo de información



1.2.5.10 Módulo en blanco

Para una mejor apariencia, utilice el módulo en blanco si hay espacio extra al colocar los módulos juntos.

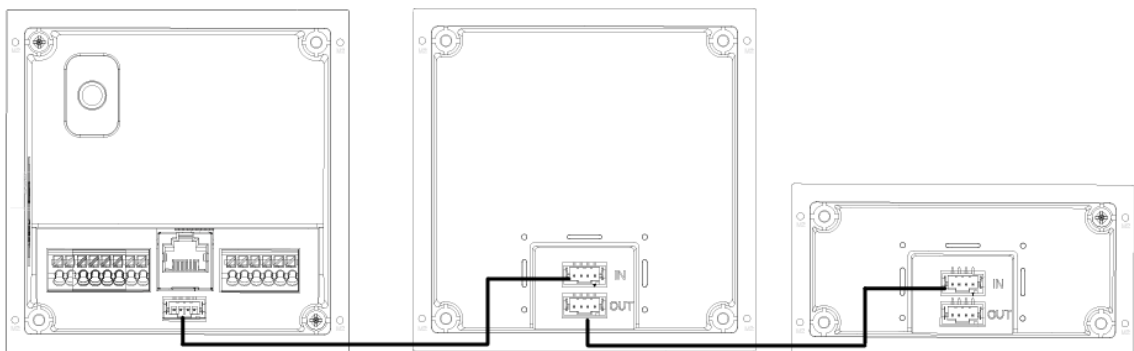
Figura 1-30 Módulo en blanco



1.2.5.11 Conexión en cascada

Se necesita una conexión en cascada para que todos los módulos funcionen juntos.

Figura 1-31 Ejemplo de conexión en cascada



1.3 Modelo de botón

1.3.1 Panel frontal

Figura 1-32 Panel frontal

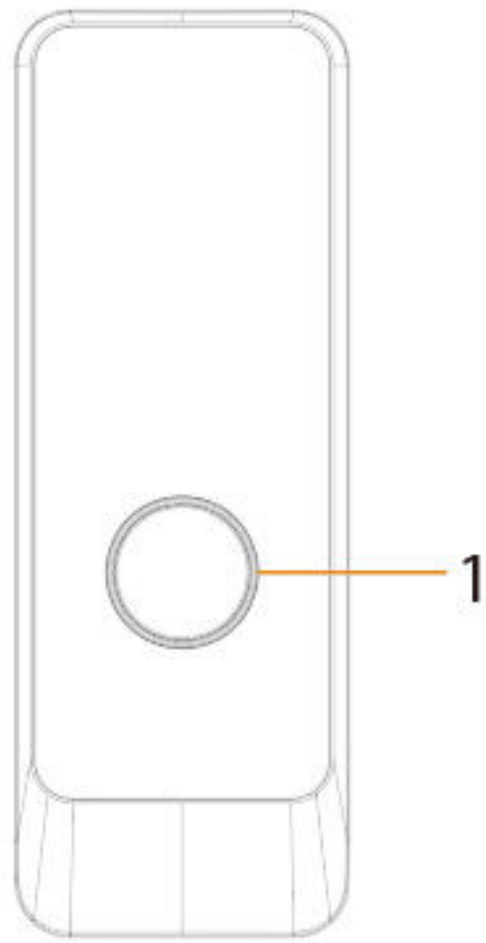


Tabla 1-24 Componentes

No.	Nombre	Función
1	Presione el botón	El modelo de botón se puede conectar al VTH. Al presionarlo, el VTH recibe una señal de alarma.

1.3.2 Panel trasero

Figura 1-33 Panel trasero

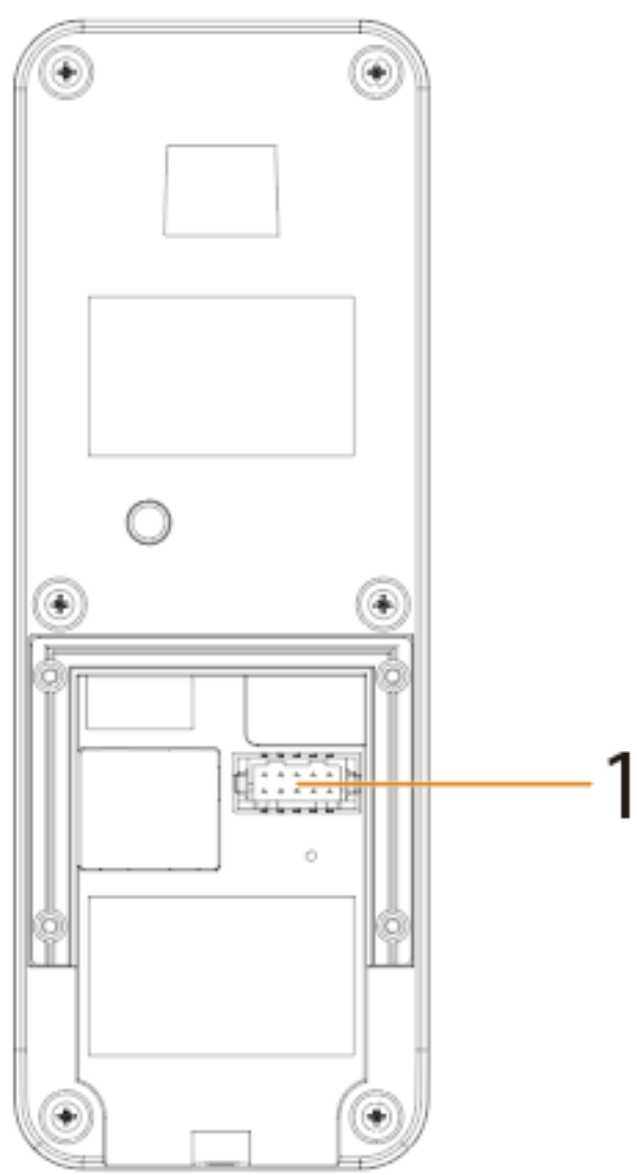
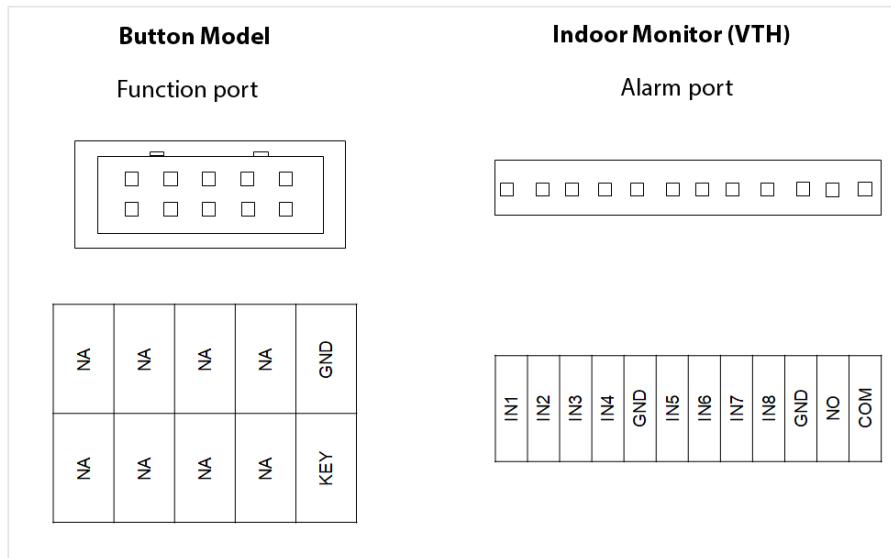


Tabla 1-25 Componentes

No.	Nombre	Función
1	Puerto multifunción	Se utiliza para entrada de alarma.

Figura 1-34 Conexión del cable



Conecte el puerto KEY del modelo de botón a cualquiera de los puertos de entrada de alarma del monitor interior (VTH) con un cable. Después, toque **Configuración>Alarma>Zona cableada** en el VTH y configure el **Tipo** del puerto de entrada de alarma que eligió conectar al puerto KEY como **Timbre de la puerta**.

2 Inicialización del VTO

2.1 Web

Para iniciar sesión por primera vez, debe inicializar el VTO.

Procedimiento

Paso 1 Encienda el VTO.

Paso 2 Vaya a la dirección IP predeterminada (192.168.1.108) del VTO.



Asegúrese de que la dirección IP de su PC esté en el mismo segmento de red que el VTO.

Paso 3 En el **Inicialización del dispositivo** página, ingrese y confirme la contraseña y luego haga clic en **Próximo**.



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

Paso 4 Seleccione el **Correo electrónico** Marque la casilla e ingrese una dirección de correo electrónico para restablecer la contraseña.

Paso 5 Haga clic en **Próximo**.

Paso 6 Hacer clic **DE ACUERDO** para ir a la página de inicio de sesión.

Paso 7 Introduzca el nombre de usuario (admin por defecto) y la contraseña para iniciar sesión en la página web.

2.2 Aplicación DMSS

Si su modelo solo admite conexión Wi-Fi a la red, solo podrá inicializar el VTO en la aplicación DMSS. Para obtener información detallada sobre el funcionamiento de la aplicación, consulte su manual de usuario.

Prerrequisitos

Ha descargado el DMSS en la APP Store (iOS) o Google Play (Android), y ha creado una cuenta y ha iniciado sesión en la aplicación.

Procedimiento

Paso 1 Encienda el VTO.

Paso 2 Habilite el punto de acceso en el VTO presionando y manteniendo presionado el botón de llamada en el VTO hasta que escuche la indicación de voz.



La función de punto de acceso le permite conectar el VTO a la red a través de **Configuración de AP** en la aplicación.

Paso 3 Agregue el VTO a la aplicación DMSS.

1. En el **Hogar** pantalla, toque , y luego seleccione **SN/Escaneo**.

2. Agregue un VTO.

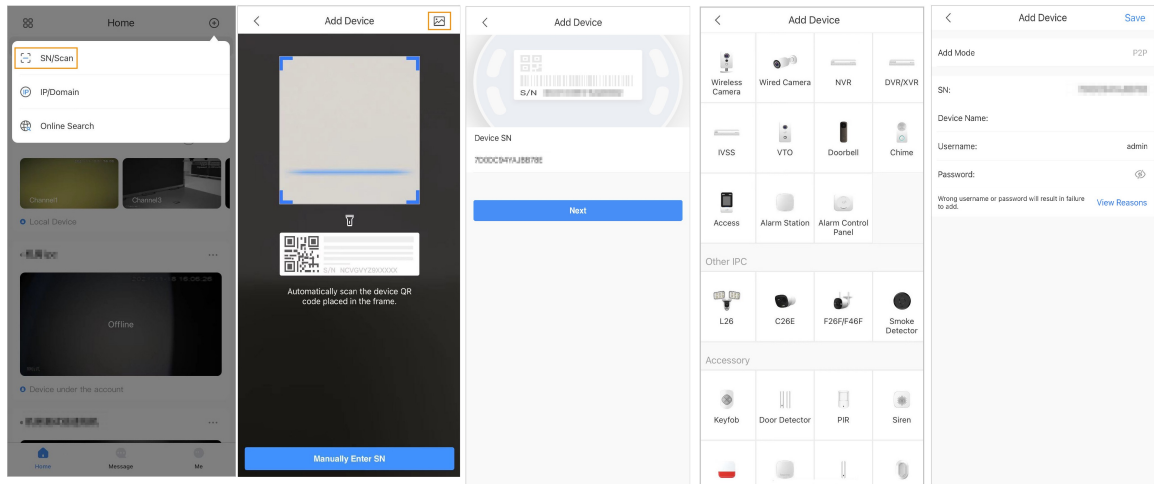
3. Puede agregarlo escaneando el código QR en el panel trasero del VTO.

4. El número SN del VTO aparece automáticamente y luego toque **Próximo**.

5. Seleccione el tipo de dispositivo como **VTO**, y luego aparece la información del dispositivo.

6. Toque **Ver Razones**.

Figura 2-1 Agregar VTO a DMSS



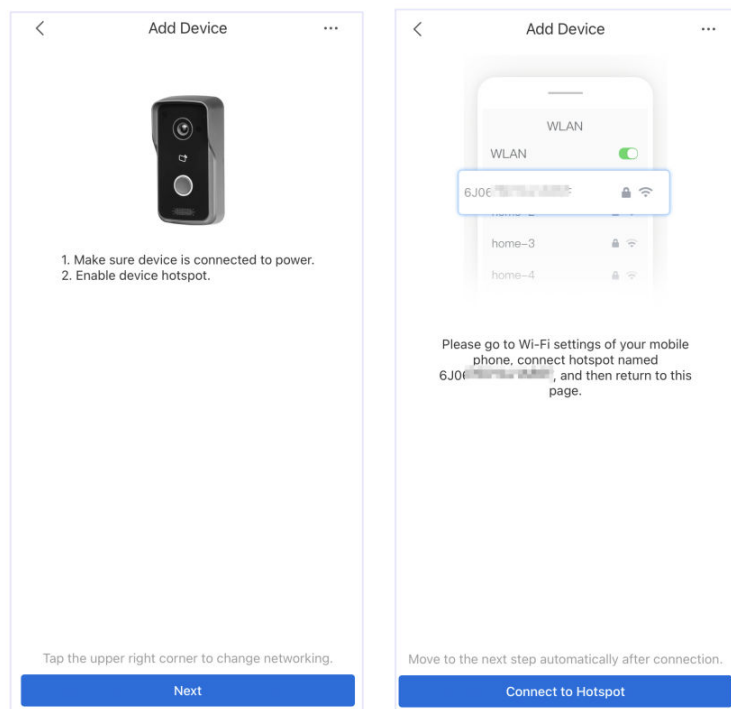
7. Configure la red cambiando la red a **Configuración de AP**, y luego toque **Próximo**.

8. Conecte su teléfono al punto de acceso que acaba de habilitar en el VTO.



- El nombre del punto de acceso es el número SN de su VTO.
- La página actual pasará al siguiente paso automáticamente después de la conexión.

Figura 2-2 Configuración de AP



Paso 4 Inicialización completa según las instrucciones de la aplicación.

1. Ingrese la contraseña que planeó para el VTO, confírmela y luego toque **Próximo**.
2. Seleccionar **Acceso a la nube** y **Comprobación automática**, y luego toque **DE ACUERDO**.

El proceso de inicialización se ha completado.

Figura 2-3 Inicialización

Add Device

To guarantee device safety, please set device password.Usually, it will take 1 – 60s, please wait.

Username
admin

Please enter device password.

Weak Medium Strong

Please confirm the device password

Email (Optional)
The email address is used to receive the default password if you forget the device password.

Next

Cloud Update Configuration

Cloud Access

Register device to Cloud to prepare for you with cloud account to achieve cloud services such as remote monitoring, device recording,talking, alarm, cloud storage, and device management.If P2P is not enabled, you may not properly use functions such as intercom.

Auto-check

The system checks for update once a day automatically. There will be system notification if any update is available. Online update is a service that provides you with firmware updates by cloud. Your device information such as device name, firmware version and device SN will be collected in order to inform you about available firmware updates. All information is only used to inform you firmware updates.

OK

Paso 5 Conecte el VTO a la red a través de Wi-Fi.

1. Seleccione una red Wi-Fi disponible.
2. Ingrese la contraseña y toque **Próximo**. Espere a que el VTO se conecte al enrutador.

Figura 2-4 Conexión Wi-Fi

Add Device

WLAN
home-1 home-2 home-3 home-4
Searching available Wi-Fi nearby ...

Add Device

Please connect to a Wi-Fi hotspot near you or to one that has a strong signal. Refresh

Wi-Fi Network
Wi-Fi Password
Dual band router fails to support 5G Wi-Fi

Next

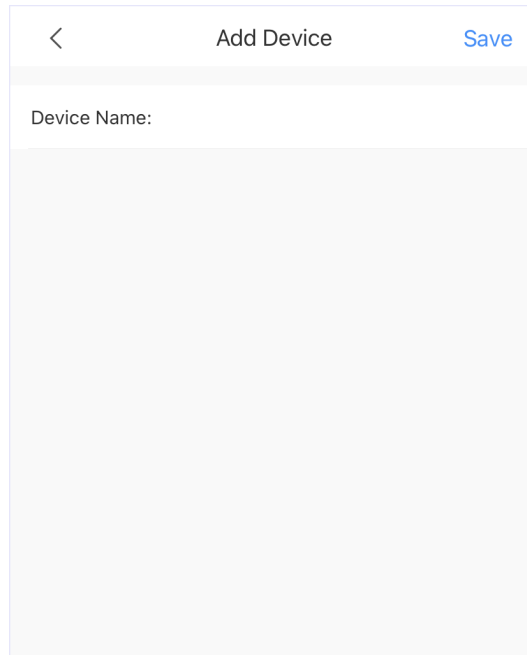
Add Device

Connecting to the router... 58

Cancel Config

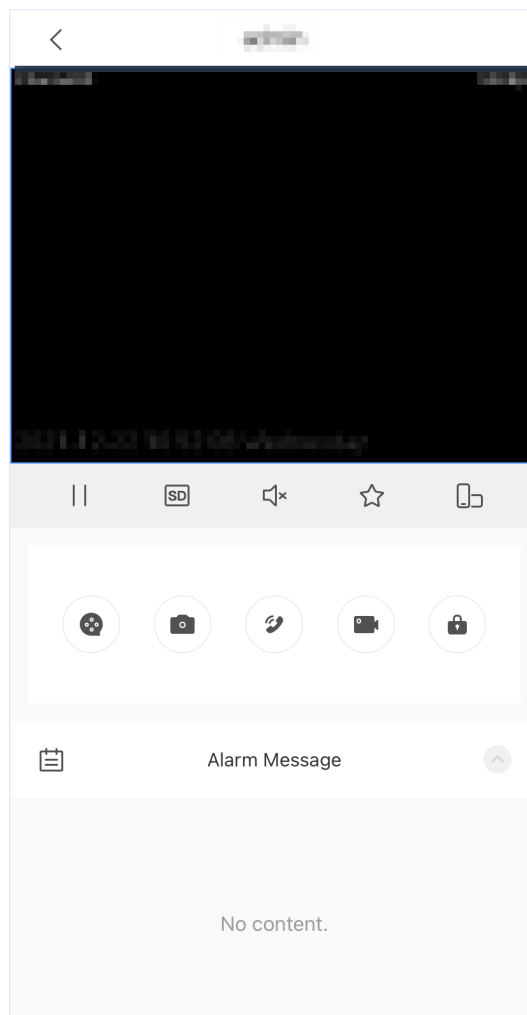
Paso 6 Configure el nombre del dispositivo y luego toque **Ahorrar**.

Figura 2-5 Configurar el nombre del dispositivo



Paso 7 Vea el video de monitoreo de la cámara en el VTO.

Figura 2-6 Monitor



3. Iniciar sesión y restablecer contraseña

3.1 Inicio de sesión

Antes de iniciar sesión, asegúrese de que la computadora esté en el mismo segmento de red que el VTO.

Procedimiento

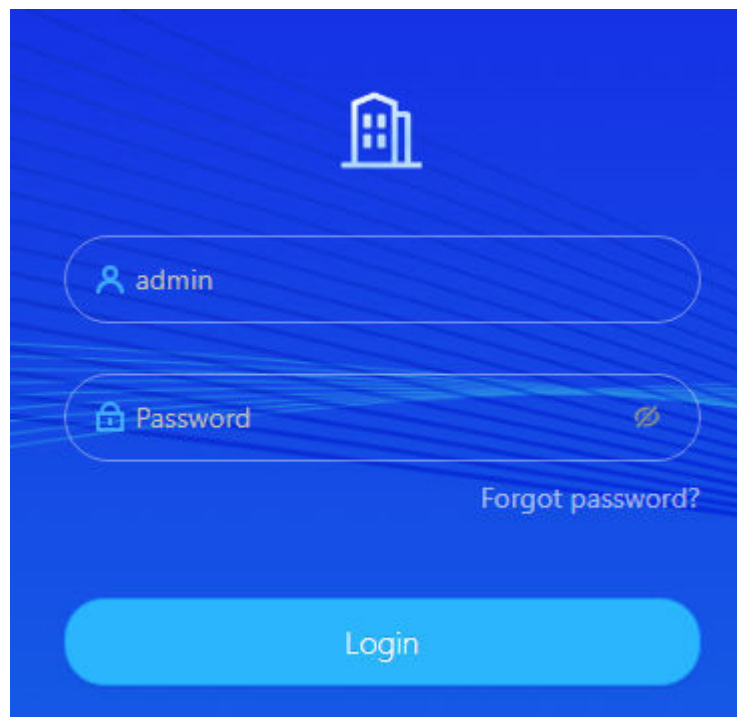
Paso 1 Vaya a la dirección IP del VTO en el navegador.



Para iniciar sesión por primera vez, introduzca la IP predeterminada (192.168.1.108). Si tiene varios VTO, le recomendamos cambiar la dirección IP predeterminada para evitar conflictos.

Paso 2 Ingresar **administración** como nombre de usuario e ingrese la contraseña que estableció durante la inicialización y luego haga clic en **Acceso**.

Figura 3-1 Inicio de sesión



3.2 Restablecimiento de contraseña

Procedimiento

Paso 1 En la página de inicio de sesión, haga clic en **¿Has olvidado tu contraseña?**, y luego haga clic

Paso 2 **Próximo** Escanea el código QR y obtendrás una cadena de números y letras.

Paso 3 Envíe la cadena a la cuenta de correo electrónico que se muestra en la página y luego el código de seguridad se enviará a la dirección de correo electrónico configurada durante la inicialización.

Paso 4 Introduzca el código de seguridad en el cuadro de entrada y luego haga clic en **Próximo**.



- Si no configuró una dirección de correo electrónico durante la inicialización, comuníquese con su proveedor o servicio de atención al cliente para obtener ayuda.

- El código de seguridad será válido solo durante 24 horas a partir de su recepción.
- Si ingresa el código de seguridad incorrecto 5 veces consecutivas, su cuenta se bloqueará durante 5 minutos.

Paso 5

Ingrese y confirme la nueva contraseña y luego haga clic en **DE ACUERDO**.

4 Página de inicio

Figura 4-1 Página de inicio

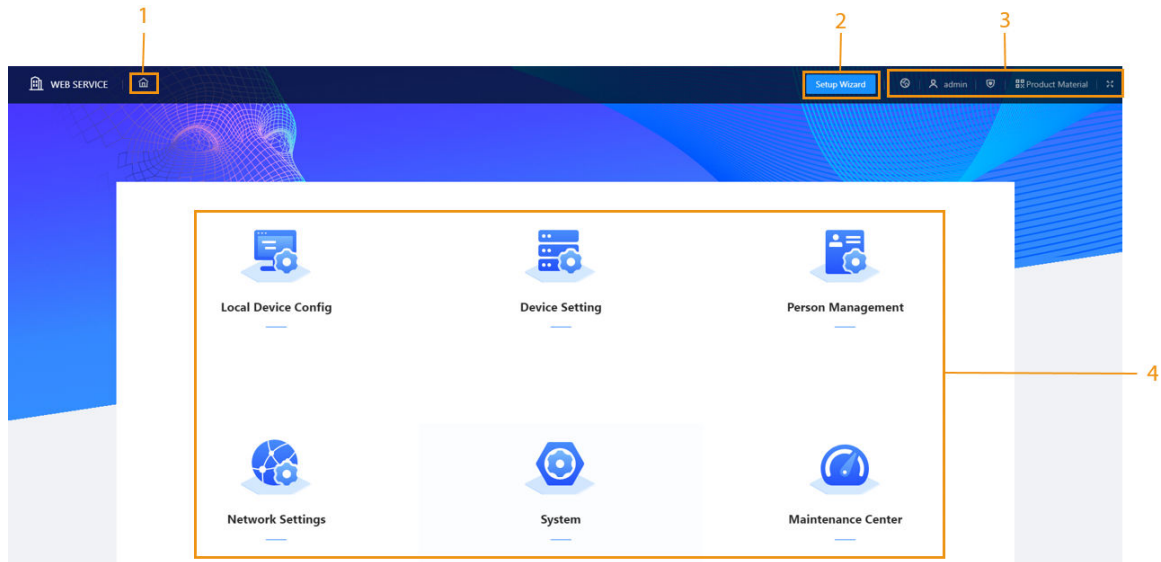


Tabla 4-1 Introducción a la página de inicio

No.	Función	Descripción
1	Botón de inicio	Regresar a la página de inicio.
2	Asistente de configuración	Configurar el servidor SIP VTO.
3	Barra de navegación	:Cambiar el idioma de la página web de la VTO. :Cambiar la contraseña, cerrar la sesión del dispositivo actual, reiniciar el sistema y restaurar el dispositivo a la configuración de fábrica. :Ver y configurar los ajustes de seguridad. :Escanea el código QR para obtener el Material del producto. :Ver la página web en modo de pantalla completa.
4	Función VTO	Diferentes áreas funcionales del VTO.

5 Asistente de configuración

Mediante el asistente de configuración, puede finalizar el proceso de agregar VTO/VTH y especificar cualquier VTO como servidor SIP. También puede cancelar su estado como servidor SIP.

5.1 Configuración como servidor SIP

Establecer el VTO como servidor SIP.

Prerrequisitos

Has añadido VTO en la página web. Si no, puedes añadirlos en **Establecer como servidor SIP** página o en el **Configuración del dispositivo** sección.

Procedimiento

Paso 1 Inicie sesión en la página web de la VTO.

Paso 2 Seleccionar **Asistente de configuración** > **Establecer como servidor SIP**, y luego haga clic en **Próximo**.

Figura 5-1 Establecer como servidor SIP

The screenshot shows a configuration window with a progress bar at the top indicating 'Step 1' and 'Step 2'. The main area contains two options: 'Set as SIP Server' (highlighted with a blue border and a blue icon) and 'Do not Set as SIP Server' (with a grey border and a grey icon). At the bottom, there are 'Exit' and 'Next' buttons.

Paso 3 Seleccione el VTO que se configurará como servidor SIP y luego haga clic en **DE ACUERDO**.

También puedes hacer clic **Agregar** para agregar VTO si no tienes uno que funcione como servidor SIP.

Figura 5-2 Seleccione el servidor SIP

The screenshot shows a table with 11 records. The table has columns for Device Type, SIP No., IP Address, Online Status, and Operation. The first record is a VTO (8001, 127.0.0.1, Online) and the rest are VTHs (990140 to 990148, all Offline). There are 'Add', 'Delete', 'Clear', and 'Refresh' buttons at the top left, and a search bar at the top right. At the bottom, there are 'Exit', 'Back', and 'OK' buttons, along with pagination controls showing '11 records' and '10 / page'.

Device Type	SIP No.	IP Address	Online Status	Operation
☐ VTO	8001	127.0.0.1	Online	
☐ VTH	990140		Offline	
☐ VTH	990141		Offline	
☐ VTH	990142		Offline	
☐ VTH	990143		Offline	
☐ VTH	990144		Offline	
☐ VTH	990145		Offline	
☐ VTH	990146		Offline	
☐ VTH	990147		Offline	
☐ VTH	990148		Offline	

5.2 No configurar como servidor SIP

Si desea cambiar el servidor SIP, deberá eliminar el actual de la lista.

Procedimiento

- Paso 1** Inicie sesión en la página web de la VTO.
- Paso 2** Seleccionar **Asistente de configuración** > **No establecer como servidor SIP**, y luego haga clic en **Próximo**.

Figura 5-3 No configurar como servidor SIP

The screenshot shows a configuration window with a progress bar at the top indicating 'Step 1' and 'Step 2'. In the center, there are two buttons: 'Set as SIP Server' (with a server icon) and 'Do not Set as SIP Server' (with a checkmark icon). The 'Do not Set as SIP Server' button is highlighted with a blue border. At the bottom, there are 'Exit' and 'Next' buttons.

- Paso 3** Configure la información del VTO que no desea configurar como servidor SIP y luego haga clic en **DE ACUERDO**.

Figura 5-4 Configurar información

The screenshot shows a configuration window with a progress bar at the top indicating 'Step 1' and 'Step 2'. The 'Step 1' indicator is active. The form contains the following fields:

- * VTO ID: 8002
- Building No.: 0
- Unit No.: 0
- Server Type: Device
- Server Address: [Redacted]
- Port: 5060
- SIP No.: 8001
- Registration Password: [Redacted]
- SIP Domain: VDP
- SIP Server Username: admin
- SIP Server Password: [Redacted]

At the bottom, there are 'Exit', 'Back', and 'OK' buttons.

6 Configuración del dispositivo local

Este capítulo presenta la configuración detallada del VTO.



Pueden encontrarse ligeras diferencias en distintos modelos.

6.1 Configuración básica

Configurar ajustes básicos del dispositivo.

6.1.1 Estación de puerta de la villa

Procedimiento

Paso 1 Seleccionar **Configuración del dispositivo local** > **Configuración**

Paso 2 **básica**. Configure los parámetros.

Figura 6-1 Configuración básica (estación de villa)

Local Device Config

Device Type

Villa Station

Device Name

11111111

Villa Room No.

101

VTO ID

8001

Group Call

☒

Management Center

888888

Call Period

Setting

Calling by Period Mode

Enable

☐

Functions

Storage Method

SD Card

SD Card Usage

0M/0M

Format SD Card

ⓘ If the SD card cannot be recognized, you can format it.

Auto Capture while Unlocking

☒

Auto Capture during Call

☒

Upload Messages and Videos

☒

Auto Record while Calling

☒

ⓘ Please regularly perform backups to avoid data loss.

Apply

Refresh

Default

Figura 6-2 Configuración básica (apartamento pequeño)

Local Device Config

Device Type

Small Apartment

Device Name

VTO ID

8001

Group Call

☐

Management Center

888888

Apply

Refresh

Default

Tabla 6-1 Descripción de parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccione de Estación de Villay Apartamento pequeño.  El apartamento pequeño está disponible en modelos seleccionados.
Nombre del dispositivo	Cuando otros dispositivos estén monitoreando este VTO, el nombre del dispositivo aparecerá en la imagen de monitoreo.
Habitación Villa No.	Número de habitación VTH. Se utiliza para llamar a los VTH.
Identificación de VTO	Se utiliza para diferenciar cada VTO y le recomendamos que lo configure según el número de unidad o edificio, y luego puede agregar VTO al servidor SIP usando sus números.  El número no se puede cambiar cuando el VTO actúa como servidor SIP.
Llamada grupal	Habilítelo en el VTO que funciona como servidor SIP y, cuando un VTH principal recibe una llamada, todos los VTH de extensión también recibirán la llamada.
Centro de gestión	888888 por defecto.
Período de llamada	El período de tiempo en el que el VTO puede llamar a otros dispositivos es ilimitado. Haga clic en Configuración para configurar el período de llamada en un día/semana.

Parámetro	Descripción
Llamada por modo de período	● Si habilita la Llamada por modo de período Se puede llamar al número especificado en el período especificado y al número predeterminado en otro período. ● Hacer clic Configuración para establecer el plan de tiempo para llamar.  Esta función solo está disponible cuando el modo es estación de puerta de villa.
Método de almacenamiento	Tarjeta SD por defecto.
Uso de la tarjeta SD	Muestra la capacidad total y utilizada de la tarjeta SD. Puedes hacer clic en Formatear tarjeta SD para borrar todos los datos de la tarjeta SD.
Captura automática al desbloquear	Tome una instantánea y guárdela en la tarjeta SD del VTO cuando el VTO se desbloquee.  Si el VTO se desbloquea a través del botón de desbloqueo local, no se tomará la instantánea.
Captura automática durante la llamada	Tome una instantánea y guárdela en la tarjeta SD del VTO cuando el VTO esté llamando.
Subir mensajes y vídeos	Cuando está habilitado: ● Si se inserta una tarjeta SD tanto en el VTH como en el VTO, el mensaje de vídeo se guardará tanto en las tarjetas SD del VTH como en el VTO. ● Si solo se inserta una tarjeta SD en el VTH o el VTO, el mensaje de video se guardará solo en la tarjeta SD del VTH o el VTO. ● Si no se inserta ninguna tarjeta SD en el VTH o VTO, no se guardará ningún mensaje de video.
Grabación automática durante la llamada	Tome una grabación cuando el VTO esté en una llamada y guarde la grabación en la tarjeta SD del VTO.  ● Cuando el tiempo de llamada sea inferior a 5 segundos, no se generará ningún archivo de vídeo. ● Si existe un conflicto entre Grabación automática durante la llamada y Dejar videos, Dejar videos prevalece.

Paso 3 Hacer clic **Aplicar**.

6.1.2 Segunda estación de confirmación



La configuración de la segunda estación de confirmación está disponible en modelos seleccionados.

Procedimiento

Paso 1 Seleccionar **Configuración del dispositivo local** > **Configuración básica**.

Paso 2 Configurar los parámetros.

Figura 6-3 Configuración básica (Segunda estación de confirmación)

Local Device Config

Device Type

Second Confirmation Station ▾

Device Name

Villa Room No.

9901

* VTO ID

8002

Management Center

888888

Management Center Call Peri...

00:00:00 ⌚

-

23:59:59 ⌚

☐

Call Period

Setting

Apply

Refresh

Default

Tabla 6-2 Descripción de parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccionar Segunda Estación de Confirmación .
Nombre del dispositivo	Cuando otros dispositivos estén monitoreando este VTO, el nombre del dispositivo aparecerá en la imagen de monitoreo.
Habitación Villa No.	Número de habitación VTH. Se utiliza para llamar a los VTH.
Identificación de VTO	Se utiliza para diferenciar cada VTO y le recomendamos que lo configure según el número de unidad o edificio, y luego puede agregar VTO al servidor SIP usando sus números.  El número no se puede cambiar cuando el VTO actúa como servidor SIP.
Centro de gestión	888888 por defecto.
Periodo de llamada del Centro de Gestión	Configure el horario si solo desea recibir llamadas de VTH durante un período específico y luego habilite la función.
Periodo de llamada	Hacer clic Configuración para configurar el periodo de llamada en un día/semana.

Paso 3 Hacer clic**Aplicar**.

6.2 Control de acceso



Las distintas series de modelos tienen distintas funciones de control de acceso. A continuación, se muestra un ejemplo de configuración de la serie E.

6.2.1 Configuración

Procedimiento

- Paso 1** Seleccionar **Configuración del dispositivo local > Control de acceso >**
- Paso 2** **Configuración.** Configure los parámetros.

Figura 6-4 Control de acceso

Interval between Consecutive...	5	s (1-20)
Door Unlocked Duration	2	s (1-20)
Alarm Input/Door Detector	☐ Alarm Input ☒ Door Detector	
Check Door Detector Signal ...	☐	
Door Detector Alarm Thresh...	30	s (1-9999)
Door Detector Status	☒ NC ☐ NO	
Door Detector Alarm Sound	☐	
Unlock Code	123	
☐ Lock Linkage		
New Duress Password		
Confirm New Duress Password		
Public Password	Setting	
Apply Refresh Default		

Tabla 6-3 Descripción de los parámetros de control de acceso

Parámetro	Descripción
Intervalo entre desbloques consecutivos	La puerta sólo podrá desbloquearse nuevamente después del intervalo.
Duración de la puerta desbloqueada	El tiempo durante el cual el bloqueo permanece desbloqueado.
Entrada de alarma/Detector de puerta	Seleccione uno de ellos.
Compruebe la señal del detector de puerta antes de bloquearla	Habilite la función según sus necesidades.
Umbral de alarma del detector de puerta	El tiempo umbral en el que se activa la alarma del detector de puerta.
Estado del detector de puerta	● CAROLINA DEL NORTE: Normalmente cerrado. ● NO: Normalmente abierto.
Sonido de alarma del detector de puerta	Está deshabilitado por defecto. Cuando está habilitado: ● Estado del detector de puerta es CAROLINA DEL NORTE: Si el tiempo de apertura de la puerta supera el umbral de alarma de detección de puerta establecido, el VTO emitirá un pitido. Cuando el detector de puerta se cierra, el VTO no vuelve a emitir un pitido. ● Estado del detector de puerta es NO: Si el tiempo de cierre de la puerta supera el umbral de alarma de detección de puerta establecido, el VTO emitirá un pitido. Si el detector de puerta está abierto, el VTO no volverá a emitir un pitido.
Código de desbloqueo	Puede conectar un teléfono de terceros, como un teléfono SIP, al VTO y usar el código para abrir la puerta de forma remota.
Enlace de bloqueo	Habilitar el Enlace de bloqueo y luego seleccione el bloqueo de vínculo de la lista desplegable.
Nueva contraseña de coacción	Configure la contraseña de coacción. Si la introduce al ser forzado, se enviará una alarma al centro de administración.
Confirmar nueva contraseña de coacción	
Contraseña pública	Hacer clic Configuración para establecer la contraseña pública. - Haga clic Agregar para agregar una contraseña pública. - Ingrese el nombre de usuario y la contraseña. Luego haga clic en DE ACUERDO.  La contraseña debe constar de 4 a 6 dígitos.

Paso 3 Hacer clic **Aplicar**.

6.2.2 Función de extensión

6.2.2.1 RS-485

Procedimiento

Paso 1 Seleccionar **Configuración del dispositivo local** > **Control de acceso** > **Función de extensión** > **RS-485**.

Paso 2 Configurar los parámetros de la cerradura conectada a través del puerto RS-485.

Figura 6-5 RS-485

RS-485

Port Type

Lock

Interval between C...

15

s (1-20)

Unlock Duration

2

s (1-20)

Unlock Code

456

☒ Lock Linkage

Apply

Refresh

Default

Tabla 6-4 Descripción de RS-485

Parámetro	Descripción
Tipo de puerto	Cerrar por defecto. Se pueden conectar lectores de tarjetas que sólo admitan tarjetas flash compactas.
Intervalo entre desbloques consecutivos	La puerta sólo podrá desbloquearse nuevamente después del intervalo.
Duración del desbloqueo	El tiempo durante el cual el bloqueo permanece desbloqueado.
Código de desbloqueo	Puede conectar un teléfono externo, como un teléfono SIP, al VTO y usar el comando para abrir la puerta remotamente. El comando predeterminado es 456.
Enlace de bloqueo	Habilitar el Enlace de bloqueo y luego seleccione el bloqueo de vínculo de la lista desplegable.

Paso 3 Hacer clic **Aplicar**.



- Cuando el módulo 485 del VTO conectado al módulo de seguridad (DEE1010B) se conecta al lector de tarjetas, este tiene un límite de longitud para la contraseña introducida (10 dígitos). Por lo tanto, el número de habitación (6 dígitos) y la contraseña personal (6 dígitos) no permiten desbloquear la puerta.

- Cuando el módulo 485 de VTO vinculado con el módulo de seguridad (DEE1010B) se conecta al lector de tarjetas QR, el código QR no puede desbloquear la puerta porque el RS-485 de VTO no admite la transmisión del código QR.
- Cuando el módulo 485 de VTO vinculado con el módulo de seguridad (DEE1010B) se conecta al lector de tarjetas, no se pueden emitir tarjetas a través del módulo 485 y el módulo de seguridad DEE1010B, porque el módulo 485 no admite la interacción de comandos bidireccionales.

6.2.2.2 Control de elevación de red

La cerradura se puede conectar al control del ascensor de red.



Esta función solo está disponible cuando **Tipo de dispositivo** se selecciona como **Apartamento pequeño**.

Procedimiento

- Paso 1** Seleccionar **Configuración del dispositivo local** > **Control de acceso** > **Función de extensión** > **Control de elevación de red**.
- Paso 2** Habilite el control de elevación de red.
- Paso 3** Configure el control de elevación.

Figura 6-6 Control de elevación de red

Lift Name	Enable	Lift Control Duration (sec)	IP Address	Port	Username	Password	Connection Status	Operation
Lift 1	☐	0	192.168.0.2	5000	admin	*****	Test	Edit
Lift 2	☐	0	192.168.0.2	5000	admin	*****	Test	Edit
Lift 3	☐	0	192.168.0.2	5000	admin	*****	Test	Edit
Lift 4	☐	0	192.168.0.2	5000	admin	*****	Test	Edit
Lift 5	☐	0	192.168.0.2	5000	admin	*****	Test	Edit
Lift 6	☐	0	192.168.0.2	5000	admin	*****	Test	Edit
Lift 7	☐	0	192.168.0.2	5000	admin	*****	Test	Edit
Lift 8	☐	0	192.168.0.2	5000	admin	*****	Test	Edit

Tabla 6-5 Descripción del control de elevación de red

Parámetro	Descripción
Modo de control de elevación	● Con controlador de ascensor: se pueden agregar hasta 8 ascensores. ● Sin controlador de ascensor: se pueden agregar hasta 6 ascensores.
Método de verificación	Se habilita cuando el Modo de control de elevación se establece como Con controlador de ascensor. ● Verificación Remota: La verificación se realiza de forma remota. ● Verificación local: La verificación se realiza localmente.
Piso VTO	Cada ascensor controla hasta 128 pisos.

- Paso 4** Hacer clic **Editar** Para editar la información del ascensor. Y luego haga clic en **DE ACUERDO**.

Figura 6-7 Establecer información del elevador

Tabla 6-6 Descripción del control de elevación de red

Parámetro	Descripción
Duración del control de elevación	Establezca la duración del control del ascensor entre 0 y 999 segundos.
Dirección IP	Configure la dirección IP del dispositivo, el puerto, el nombre de usuario y la contraseña.
Puerto	
Nombre de usuario	
Contraseña	

Paso 5 Hacer clic **Aplicar**.

Operaciones relacionadas

Hacer clic **Probar** para probar el estado de conexión de los ascensores.

6.3 Control de luz

Configure el iluminador según sea necesario.

Procedimiento

Paso 1 Seleccionar **Configuración del dispositivo local > Control de luz**.

Paso 2 Configure los modos de iluminación y de luz del dispositivo entre los siguientes modos.

- **NO**: El iluminador está abierto todo el tiempo.
- **CAROLINA DEL NORTE**: El iluminador está cerrado todo el tiempo.
- **Autoadaptativo**: El iluminador se adaptará al entorno y luego establecerá un valor adecuado.

- **Período:**El iluminador estará abierto durante el período de definición.



Apagar el iluminador afectará la detección de movimiento en entornos oscuros.

Paso 3 Hacer clic **Aplicar**.

6.4 Configuración de la tarjeta

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar **Configuración del dispositivo local** > **Configuración de la tarjeta**.

Figura 6-8 Configuración de la tarjeta

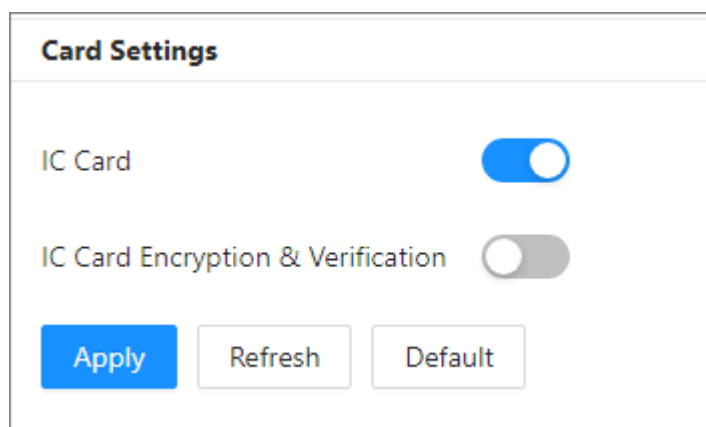


Tabla 6-7 Descripción de los parámetros de la tarjeta

Parámetro	Descripción
Tarjeta IC	Cuando está habilitada, se puede utilizar la tarjeta IC para abrir la puerta.
Cifrado y verificación de tarjetas IC	Al activarse, la tarjeta IC se cifra. Deslice la tarjeta correcta con detección de cifrado correcta para abrir la puerta.



Los lectores de tarjetas externos no admiten tarjetas IC cifradas.

Paso 3 Hacer clic **Aplicar**.

6.5 Configuración de Wiegand

Compatible con dispositivos Wiegand. Configure el modo y el modo de transmisión según sus dispositivos.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar **Configuración del dispositivo local** > **Configuración de**

Wiegand. Configure los parámetros Wiegand.

Figura 6-9 Entrada Wiegand

Wiegand Settings
☒ Wiegand Input
☐ Wiegand Output

Card No. Inversion
☐

Input Door Channel
Local Lock

Apply Refresh Default

Figura 6-10 Salida Wiegand

Wiegand Settings
☐ Wiegand Input
☒ Wiegand Output

Wiegand Output Type
Wiegand 34

Pulse Width (µs)
200
(20-200)

Pulse Interval (µs)
1000
(200-5000)

The pulse width is a multiple of 10 and has a multiple relationship with the pulse interval.

Output Data Type
☐ Card Number
☒ No.

Output Format
Hexadecimal

Apply Refresh Default

Tabla 6-8 Descripción de los parámetros de Wiegand

Parámetro		Descripción
Configuración de Wiegand		● Seleccionar Entrada Wiegand cuando se conectan otros dispositivos de reconocimiento. ● Seleccionar Salida Wiegand Cuando el VTO funciona como dispositivo de reconocimiento, se puede conectar el controlador de acceso u otros dispositivos al VTO.
Entrada Wiegand	Tarjeta n.º Inversión	Cuando se conectan dispositivos de terceros, si el orden del número de tarjeta reconocido por el dispositivo es diferente del número de tarjeta real, habilite esta función para corregirlo.

Parámetro		Descripción
	Canal de puerta de entrada	Seleccione el canal de Bloqueo localy Bloqueo externo.
Salida Wiegand	Tipo de salida Wiegand	Seleccione un formato Wiegand para leer números de tarjeta o números de identificación. ● Wiegand26: Lee tres bytes o seis dígitos. ● Wiegand34: Lee cuatro bytes u ocho dígitos. ● Wiegand66: Lee ocho bytes o dieciséis dígitos.
	Ancho de pulso	Introduzca el ancho de pulso y el intervalo de pulso de la salida Wiegand.
	Intervalo de pulso	
	Tipo de datos de salida	Seleccione el tipo de datos de salida. ● Número de tarjeta: Genera datos basados en el primer número de tarjeta del usuario. ● No.: Genera datos basados en el ID del usuario.
	Formato de salida	Cuando el tipo de datos de salida esté configurado como número, seleccione entre Decimaly Hexadecimal.

Paso 4 Hacer clic **Aplicar**.

6.6 Diseño

6.6.1 Diseño (varios botones)

Esta función solo está disponible en algunos modelos con varios botones (1, 2 y 4). A continuación, se muestra un ejemplo de configuración para el VTO con un botón instalado.

Procedimiento

- Paso 1 Inicie sesión en la página web de la VTO. Seleccione
- Paso 2 **Configuración del dispositivo local>Disposición.**
- Paso 3 Haga clic en las placas de identificación junto a donde haya instalado los botones y luego seleccione los números de habitación en la lista. **Habitación N°** que desea vincular. Por ejemplo, 9901, 9902, 9903 y 9904.



- Primero debe configurar el número de habitación. De lo contrario, no tendrá ningún número de habitación para seleccionar en la lista de módulos. Los números de habitación VTH se configuran en **Configuración del dispositivo** Para más detalles, consulte "7.2 Gestión de VTH".
- Debe configurar el número de habitación según la posición de instalación de los botones. Por ejemplo, si solo instaló un botón junto a la primera placa, deberá hacer clic en el módulo de la primera placa para configurar el número de habitación en la página web. Si instaló un botón junto a la cuarta placa, deberá hacer clic en el módulo de la cuarta placa para configurar el número de habitación en

La página web. Mantenga la regla de configuración anterior al instalar 2 o 4 botones en el VTO y configure los números de habitación correspondientes en la página web.

Figura 6-11 Instalación del cuarto botón

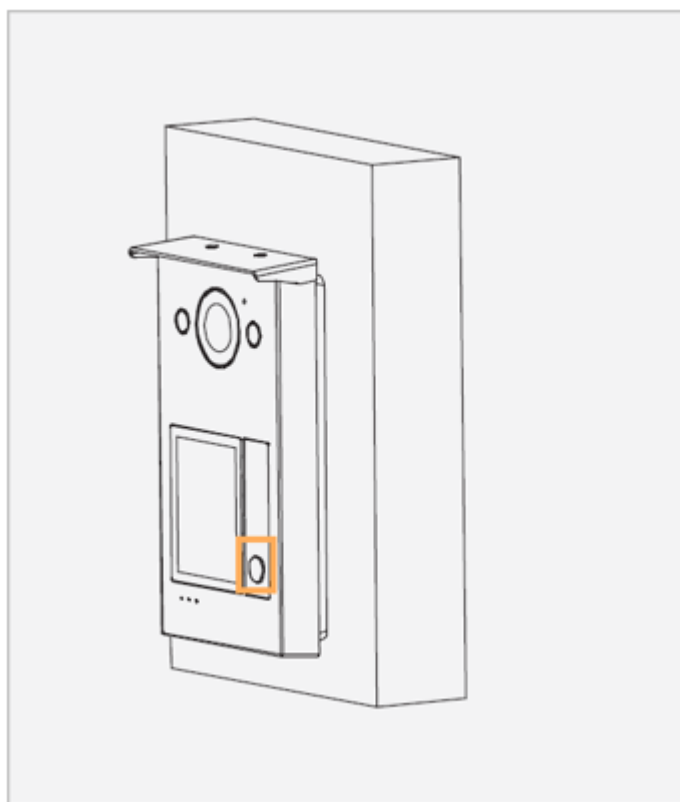


Figura 6-12 Configure la cuarta placa de identificación para el número de habitación (1)

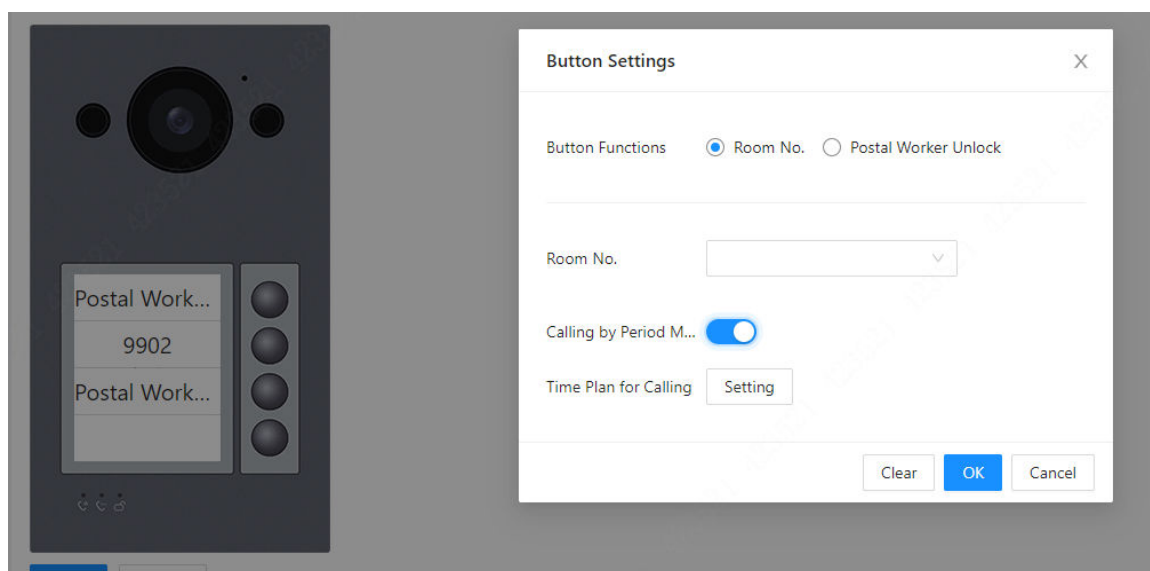
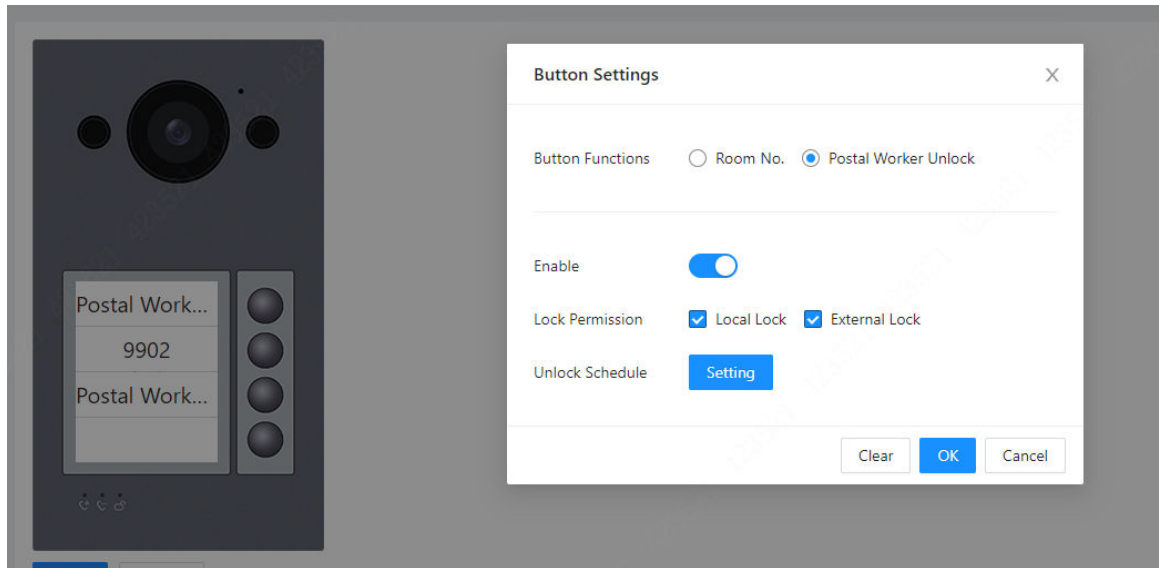


Figura 6-13 Configure la cuarta placa de identificación para el desbloqueo del trabajador postal (2)



Paso 4 Hacer clic **Aplicar** para guardar el número de habitación seleccionado.

Paso 5 Si desea vincular números de habitaciones cuando instala 2 botones o 4 botones para el VTO, repita el Paso 3 al Paso 4 hasta que haya configurado todos los números de habitaciones.

6.6.2 Diseño (Múltiples módulos)

Esta función solo está disponible para modelos seleccionados con múltiples módulos.

Procedimiento

Paso 1 Inicie sesión en la página web de la VTO. Seleccione

Paso 2 Configuración del dispositivo local > Disposición.

Paso 3 Haga clic  para agregar módulos.

Paso 4 Haga clic en el botón del módulo correspondiente para configurar los parámetros relacionados.



Primero debe configurar el número de habitación. De lo contrario, no tendrá ningún número de habitación para seleccionar en la lista de módulos. Los números de habitación VTH se configuran en **Configuración del dispositivo** Para más detalles, consulte "7.2 Gestión de VTH".

Figura 6-14 Configurar el diseño

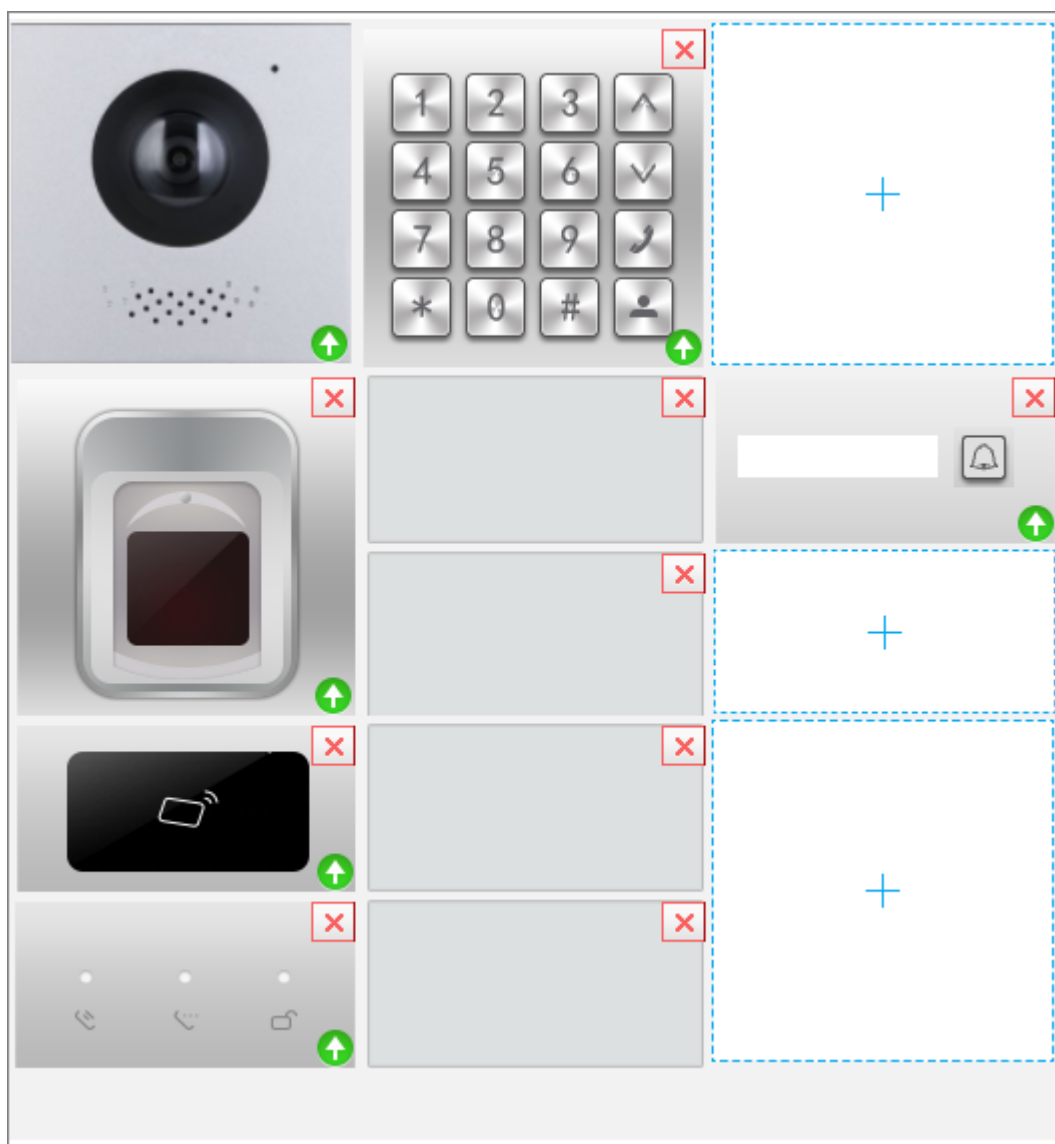


Figura 6-15 Configurar el número de habitación

Button Settings [X]

Button Functions ☒ Room No. ☐ Postal Worker Unlock

Room No. 103 [v]

[Clear] [OK] [Cancel]

Figura 6-16 Configurar el desbloqueo del trabajador postal

Button Settings [X]

Button Functions ☐ Room No. ☒ Postal Worker Unlock

Enable ☒

Lock Permission ☒ Local Lock ☐ External Lock

Unlock Schedule Setting

[Clear] [OK] [Cancel]

Tabla 6-9 Descripción de los parámetros de los botones

Parámetro	Descripción
Habitación N°	Seleccione el número de habitación de la lista desplegable.

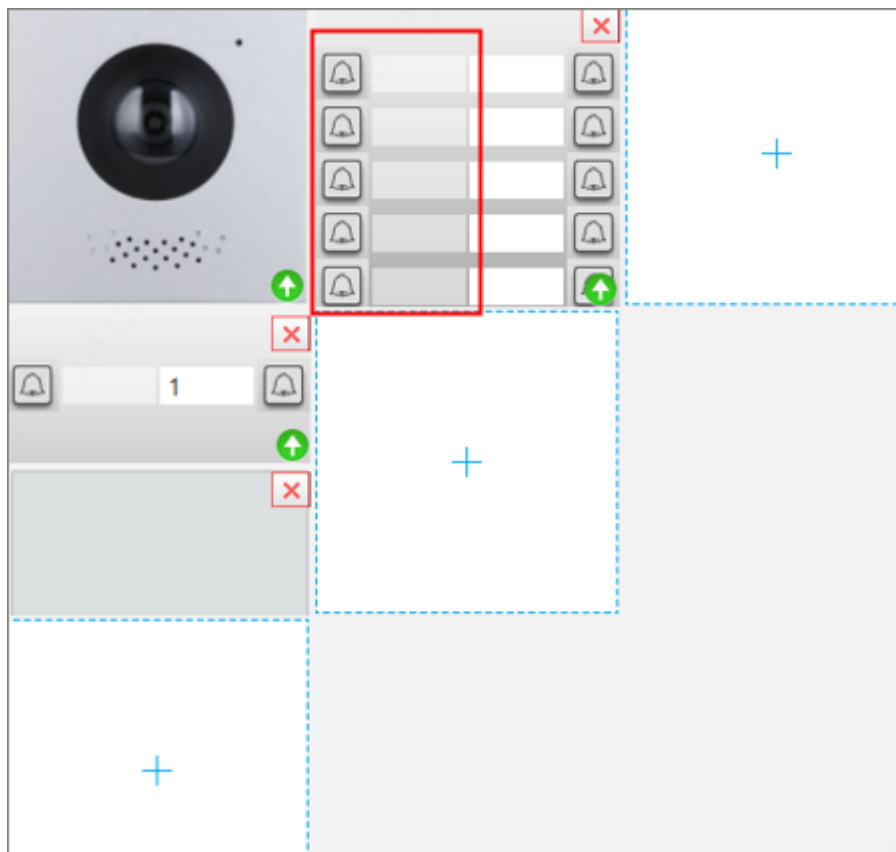
Parámetro	Descripción
Desbloqueo del trabajador postal	Configurar el desbloqueo del trabajador postal. - Haga clic  para habilitar la función. - Establezca el permiso de bloqueo desde Bloqueo local y Bloqueo externo. - Haga clic Configuración para configurar el cronograma de desbloqueo. - Haga clic DE ACUERDO.

Paso 5 Si desea vincular números de habitaciones al instalar otros módulos con placas de identificación para el VTO, repita los pasos 3 y 4 hasta que haya configurado todos los números de habitaciones.



Cuando el módulo de dos botones, el módulo de cuatro botones y el módulo de diez botones están configurados en modo de botón de una sola columna, el número de habitación en el botón izquierdo no se puede editar.

Figura 6-17 Botones no editables



Operaciones relacionadas



para ver la versión actual del módulo o cargar el archivo de actualización para actualizar el módulo.

6.7 Adición de IPC

Esta función solo está disponible cuando el servidor SIP está habilitado y el modo del dispositivo está configurado en apartamento pequeño.

Puede agregar los dispositivos IPC en la página web del VTO. Los VTH con el mismo servidor SIP en línea obtienen la información del IPC.



- Admite agregar el dispositivo con hasta 32 canales.
- Permite añadir directamente dispositivos IPC. Puede obtener el canal IPC añadiendo NVR/XVR/HCVR.

6.7.1 Agregar IPC uno por uno

Agregue la información del dispositivo de monitoreo de video uno por uno.



Sólo cuando el **Tipo de dispositivo** se establece como **Apartamento pequeño** y **Estación de vallas**, y la función SIP está habilitada, esta función puede estar disponible.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar **Configuración del dispositivo local** > **Información del IPC**.

Figura 6-18 Información del IPC

Refresh Import Export Default								
No.	Name	IP Address	Protocol Type	Stream Type	Port	Channel No.	Device Type	Operation
1			Local	Sub Stream	554	0	IPC	
2			Local	Sub Stream	554	0	IPC	
3			Local	Sub Stream	554	0	IPC	
4			Local	Sub Stream	554	0	IPC	
5			Local	Sub Stream	554	0	IPC	
6			Local	Sub Stream	554	0	IPC	
7			Local	Sub Stream	554	0	IPC	
8			Local	Sub Stream	554	0	IPC	

Paso 3 Hacer clic para configurar los parámetros.

Figura 6-19 Configurar los parámetros

Edit

X

Name

IP Address

0 . 0 . 0 . 0

Protocol Type

Local

▼

Stream Type

Sub Stream

▼

Device Type

IPC

▼

Channel No.

0

Encryption

☐

Username

admin

* Password

Port

554

OK

Cancel

Tabla 6-10 Descripción de parámetros del dispositivo de monitoreo de video

Parámetro	Descripción
Nombre	Introduzca el nombre del dispositivo IPC/VNR/XVR/HCVR.
Dirección IP	Introduzca la dirección IP del dispositivo IPC/VNR/XVR/HCVR.
Tipo de protocolo	Seleccione de Local y ONVIF según el dispositivo que agregues.
Tipo de flujo	Seleccione de Corriente principal y Subtransmisión .
Tipo de dispositivo	Seleccione el tipo según los dispositivos reales.
Canal Nro.	● Si agrega el IPC, es 1 por defecto. ● Si agrega el NVR/XVR/HCVR, es el canal de IPC que se configuró en el dispositivo VNR/XVR/HCVR.

Parámetro	Descripción
Cifrado	Mantener la coherencia con el estado de cifrado del dispositivo terminal.
Nombre de usuario	Ingrese el nombre de usuario y la contraseña que utilizó para iniciar sesión en la página web del dispositivo IPC/VNR/XVR/HCVR.
Contraseña	
Puerto	El valor es 554 por defecto.

Paso 4 Hacer clic **DE ACUERDO**.

6.7.2 Exportación de información de IPC en lotes

Exportar la información de IPC y guardarla en la computadora local.

Procedimiento

Paso 1 Hacer clic **Exportar**.

Paso 2 Ingrese la contraseña de inicio de sesión y luego haga clic en **DE ACUERDO**.

El archivo de configuración de IPC se guarda en la computadora local.

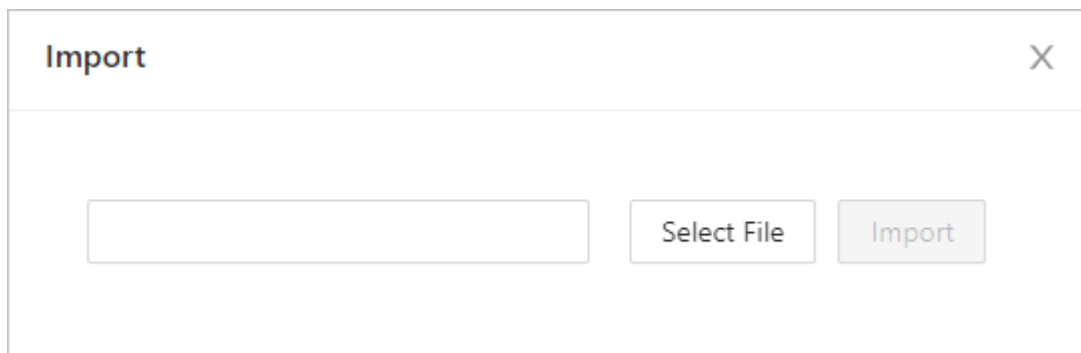
6.7.3 Importación de información de IPC en lotes

Importar la información de IPC al sistema.

Procedimiento

Paso 1 Hacer clic **Importar** luego ingrese la contraseña de inicio de sesión.

Figura 6-20 Importación



Paso 2 Seleccione el archivo y haga clic en **Importar**.

7 Configuración del dispositivo

Este capítulo explica cómo agregar, modificar y eliminar VTO, VTH, VTS e IPC, y cómo enviar mensajes desde el servidor SIP a VTO y VTH cuando el VTO funciona como servidor SIP. Si utiliza otros servidores como servidor SIP, consulte el manual correspondiente para obtener más información.

7.1 Gestión de VTO

Puede agregar VTO al servidor SIP y todos los VTO conectados al mismo servidor SIP pueden llamarse entre sí.

Procedimiento

- Paso 1** Inicie sesión en la página web del VTO que funciona como servidor SIP. Seleccione
- Paso 2** **Configuración del dispositivo**. Haga clic **Agregar**.
- Paso 3**
- Paso 4** Configurar los parámetros.

Figura 7-1 Agregar VTO

Add X

Device Type VTO

* No. 8001

* Registration Password *****

Building No.

Unit No.

* IP Address 127 .

* Username admin

* Password *****

OK Cancel

Tabla 7-1 Agregar configuración de VTO

Parámetro	Descripción
Tipo de dispositivo	Seleccionar VTO .
No.	El número de VTO que usted configuró.
Contraseña de registro	Déjalo como predeterminado.

Parámetro	Descripción
Edificio No.	Disponible solo cuando los servidores de la plataforma o VTS funcionan como servidor SIP.
Unidad N°	
Dirección IP	Dirección IP del VTO.
Nombre de usuario	Nombre de usuario y contraseña utilizados para iniciar sesión en la página web de la VTO.
Contraseña	

Paso 5

Hacer clic **DE ACUERDO**.



Hacer clic  para editar el VTO, o  para eliminar los VTO agregados, pero el que tienes Los datos registrados no se pueden modificar ni eliminar.

7.2 Gestión de VTH

Puede agregar números de sala al servidor SIP y luego configurar el número de sala en los VTH para conectarlos a la red.

Procedimiento

Paso 1 Inicie sesión en la página web del servidor SIP. Seleccione

Paso 2 **Configuración del dispositivo.** Haga clic **Agregar**.

Paso 3

Paso 4 Configurar los parámetros.

- Seleccione el tipo de dispositivo como **VTH**.

Figura 7-2 Agregue VTH uno por uno

Add
X

Device Type
VTH

Add Mode
Add One by One

First Name
Please enter

Last Name
Please enter

Alias
Please enter

* Room No.
Please enter

Registration Mode
Public

* Registration Password

Floor

OK
Cancel

Tabla 7-2 Descripción de parámetros

Parámetro	Descripción
Nombre de pila	Introduce la información que necesitas para diferenciar cada estancia.
Apellido	
Alias	
Habitación N°	Ingresa un número de habitación y luego configure el número en un VTH para conectarlo a la red.
Modo de registro	Seleccionar Público .
Contraseña de registro	Déjalo como predeterminado.
Piso	Seleccione el piso al cual se le puede dar el permiso.  Este parámetro solo está disponible cuando Modo de control de elevación se selecciona como Con controlador de ascensor.

- Seleccione el modo agregar como **Agregar en lotes**.



Agregar en lotes no está disponible cuando el modo del dispositivo está configurado en villa.

Figura 7-3 Agregar VTH en lotes

Tabla 7-3 Descripción de parámetros

Parámetro	Descripción
Pisos en la unidad	Configurar el número de pisos y habitaciones.
Habitaciones en cada piso	
Primera habitación n.º del 1.er piso	Configure el primer número de habitación en el primer y segundo piso, el número de habitación se generará automáticamente.
Primera habitación n.º del 2.º piso	

Paso 5

Hacer clic **DE ACUERDO**.



Hacer clic

para editar el VTH, o  para eliminar los VTH añadidos, pero el que tienes

Los datos registrados no se pueden modificar ni eliminar.

7.3 Gestión de VTS

Puede agregar un VTS al servidor SIP para que funcione como centro de administración. También puede administrar, llamar y recibir llamadas de todos los VTO y VTH de la red. Consulte el manual del usuario correspondiente para obtener más información.

Procedimiento

- Paso 1** Inicie sesión en la página web del VTO que funciona como servidor SIP. Seleccione
- Paso 2** **Configuración del dispositivo.** Haga clic **Agregar**.
- Paso 3**
- Paso 4** Configurar los parámetros.

Figura 7-4 Agregar VTS

Add

X

Device Type

VTSTS

* VTS No.

Please enter

* IP Address

* Registration Password

.....

OK

Cancel

Tabla 7-4 Agregar configuración de VTS

Parámetro	Descripción
Tipo de dispositivo	Seleccionar VTSTS .
N.º VTS	El número del VTS.
Contraseña de registro	Déjalo como predeterminado.
Dirección IP	Dirección IP de VTS.

Paso 5 Hacer clic**DE ACUERDO**.

Gestión de 8 personas



La información de la tarjeta y de la huella dactilar registrada en el VTO se cargará en la gestión de personas en tiempo real.

Procedimiento

- Paso 1
- Inicie sesión en la página web.
- Paso 2
- Seleccione**Gestión de personas**.

Figura 8-1 Gestión de personas

AddImport PersonExport PersonDeleteClearRefresh						Person ID/Room No./Username		Q
☐	No.	Person ID	Room No.	Username	Verification Mode	Operation		
☐	1	1	1	rh81f0c3n3d9xwi2a	3			
☐	2	2	2	e3tb2gy8q7qjm1d6	1			
☐	3	10000001	300	b4zgy57eomk6rh81f0c3n3d9xwi2a	2			
☐	4	10000002	301	z5shofvwnil0n4e3tb2gy8q7qjm1d6	2			
☐	5	10000003	302	ka4jugbqro215lpxzfyc6wt7dvm38s	2			
☐	6	10000004	303	l5k18r6dbwgtm7yfe92apcuvon34z	2			
☐	7	10000005	304	ukr2fh5iz4bsm8eaq6j0w3x1v7ycon	2			
☐	8	10000006	305	l6odr0vkic2wb1hiysjap57zftn94gq	2			
☐	9	10000007	306	teu7r6amdphkwsx12fb5yc8v0q4njz	2			
☐	10	10000008	307	8n5ytkaf9qzo0ecwvd1fhvimi62ulgb3	2			
5000 records						<1234...500> 10 / page Go to Page		

- Paso 3
- Hacer clic**Agregar**.
- Paso 4
- Configure los parámetros y luego haga clic en**DE ACUERDO**.

Figura 8-2 Agregar la persona

Add
X

* Person ID

* Room No.

xxxxxx

Username

* Validity Period

Forever

* Lock Permission

☒ Local Lock
☒ External Lock

Multi-Door Unlock ⓘ

☐

Verification Mode

> Password
Not Added

> Card
Not Added

OK

Cancel

Tabla 8-1 Descripción de los parámetros de la persona

Parámetro	Descripción
Identificación de persona	Personaliza el número.
Habitación N°	Introduzca el número de habitación correspondiente del VTH.
Nombre de usuario	Introduzca el nombre de usuario.
Periodo de validez	Configure el período de validez durante el cual las personas tienen permisos de acceso.
Permiso de bloqueo	Configurar el permiso de bloqueo. Puedes habilitar el permiso para el bloqueo local y el bloqueo externo simultáneamente.
Desbloqueo de múltiples puertas	Cuando la verificación sea exitosa, la cerradura local y la cerradura externa se abrirán al mismo tiempo.  La contraseña personal no admite esta función.
Contraseña	1. Seleccionar Contraseña>Agregar. 2. Ingrese la contraseña y luego confírmela nuevamente.  La contraseña debe constar de 4 a 6 dígitos. 3. Haga clic DE ACUERDO.

Parámetro	Descripción
Tarjeta	1. Seleccionar Tarjeta>Agregar. 2. Ingrese el número de tarjeta. O puede hacer clic en Tarjeta de emisión y luego pase la tarjeta por el VTO. 3. Haga clic DE ACUERDO. Puedes gestionar las tarjetas a través de los siguientes iconos. ●  :Configure la tarjeta como tarjeta principal o tarjeta general. ●  Si perdió su tarjeta, haga clic para reportar la pérdida. El ícono se vuelve... . ●  La tarjeta no se puede usar para abrir la puerta. Haz clic para que sea válida. ●  :Editar el nombre de la tarjeta. ●  :Eliminar la tarjeta.
Huella dactilar	Si se añade algún tipo de dispositivo modular Configuración del dispositivo local> Disposición Se admite huella dactilar. 1. Seleccionar Huella dactilar>Agregar. 2. Registre su huella digital según las indicaciones. 3. Haga clic DE ACUERDO.
Piso	Seleccione el piso al cual se le puede dar el permiso.  Este parámetro solo está disponible cuando Modo de control de elevación se selecciona como Sin controlador de ascensor.

Operaciones relacionadas

- Hacer clic **Persona de exportación** y luego ingrese la contraseña de cifrado para el archivo para exportar la información de la persona.
- Hacer clic **Importar persona** y luego seleccione el archivo para importar la información de la persona.

9 Configuración de red

Este capítulo presenta cómo configurar los parámetros de red.

9.1 TCP/IP

Debe configurar la información TCP/IP para conectar el VTO a la red.

Procedimiento

- Paso 1 Inicie sesión en la página web de la VTO.
- Paso 2 Seleccione **Configuración de red** > **TCP/IP**.
- Paso 3 Configure los parámetros TCP/IP.

Figura 9-1 TCP/IP

The image shows a web-based configuration interface for TCP/IP settings. At the top, there is a 'DHCP' toggle switch which is currently turned off. Below this are several input fields: 'MAC Address', 'IP Address', 'Subnet Mask', and 'Default Gateway', each with a multi-segmented input box. Below these are 'Preferred DNS' and 'Alternate DNS' fields, each with a four-segment IP address box. The 'Preferred DNS' field contains '8 . 8 . 8 . 8' and the 'Alternate DNS' field contains '8 . 8 . 4 . 4'. At the bottom, there is a 'Transmission Mode' section with two radio buttons: 'Multicast' (which is selected) and 'Unicast'. At the very bottom, there are three buttons: 'Apply' (in blue), 'Refresh', and 'Default'.

Tabla 9-1 Descripción de parámetros

Parámetro	Descripción
DHCP	Asigna automáticamente direcciones IP y otros parámetros de configuración de red.
Dirección IP	Su dirección IP planificada para el VTO.

Parámetro	Descripción
DNS preferido	Es 8.8.8.8 por defecto.
DNS alternativo	Es 8.8.4.4 por defecto.
Modo de transmisión	● Multidifusión: ideal para conversaciones por vídeo. ● Unicast: ideal para llamadas grupales.  No se recomienda la unidifusión cuando la plataforma se utiliza como servidor SIP.

Paso 4 Hacer clic **Aplicar**.

9.2 Puerto

Procedimiento

Paso 1 Seleccionar **Configuración de red**>

Paso 2 **Puerto**. Configure los parámetros.

Figura 9-2 Puerto

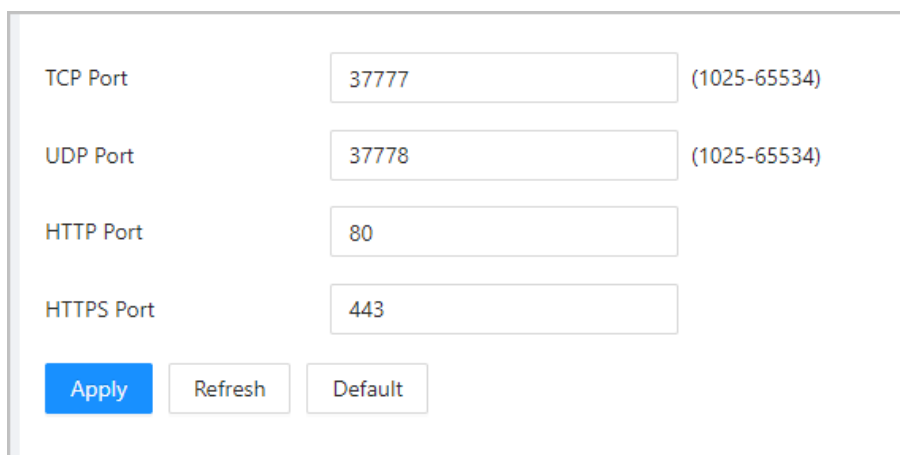


Tabla 9-2 Descripción de parámetros

Parámetro	Descripción
Puerto HTTP	Ahora puede ingresar la dirección IP http://VTO: Puerto HTTP para iniciar sesión en el VTO.
Puerto TCP/UDP	Se utiliza para acceder al VTO con dispositivos en otras redes.
Puerto HTTPS	Ahora puede ingresar la dirección IP https://VTO: Puerto HTTPS para iniciar sesión en el VTO.

Paso 3 Hacer clic **Aplicar**.

9.3 Servidor SIP

Debe haber un servidor SIP en la red para que todos los VTO y VTH conectados puedan comunicarse entre sí. Puede usar un VTO u otros servidores como servidor SIP.

Procedimiento

Paso 1 Seleccionar **Configuración de red>Servidor SIP**

Paso 2 Seleccione un tipo de servidor.

- El VTO en el que ha iniciado sesión como servidor SIP: Habilitar **Servidor SIP local** y luego configure los parámetros para el VTO.



Algunos parámetros se volverían grises después de habilitar la **Servidor SIP local** función.

Figura 9-3 VTO actual como servidor SIP

Local SIP Server ☒

Port

SIP No.

Registration Password

SIP Domain

Cascade SIP Server ☐

Backup SIP Server ☐

- Si otro VTO funciona como servidor SIP: Seleccione el tipo de SIP como **Dispositivo** y luego configure los parámetros para que el VTO funcione como SIP.



Si el VTO en el que ha iniciado sesión no funciona como servidor SIP, no lo habilite **Servidor SIP local**. De lo contrario la conexión fallaría.

Figura 9-4 Otro VTO como servidor SIP

Local SIP Server

Server Type

Device

Server Address

Port

5060

SIP No.

8001

Registration Password

SIP Domain

VDP

SIP Server Username

admin

SIP Server Password

Apply

Refresh

Default

Tabla 9-3 Configuración del servidor SIP (VTO como servidor SIP)

Parámetro	Descripción
Dirección del servidor	Dirección IP planificada del VTO.
Puerto	5060 por defecto.
N.º SIP	VDP por defecto. Déjelo como predeterminado.
Contraseña de registro	
Dominio SIP	
Nombre de usuario del servidor SIP	Nombre de usuario y contraseña utilizados para iniciar sesión en la página web del servidor SIP.
Contraseña del servidor SIP	

- La plataforma DSS funciona como servidor SIP: Establecer **Servidor SIP privado** como **Tipo de servidor** y luego configure los parámetros.

Figura 9-5 Servidor SIP privado

Local SIP Server

Server Type

Private SIP Server

Server Address

Port

5080

SIP No.

8001

Registration Password

SIP Domain

VDP

Device as Alternate Server

Alternate IP

Alternate Server Username

admin

Alternate Server Password

Alternate VTS IP

0 . 0 . 0 . 0

Apply

Refresh

Default

Tabla 9-4 Descripción del servidor SIP (plataforma como servidor SIP)

Parámetro	Descripción
Dirección del servidor	Dirección IP del servidor SIP.
Puerto	5080 por defecto cuando la plataforma funciona como servidor SIP.
N.º SIP	Déjalo por defecto.
Contraseña de registro	
Dominio SIP	
Dispositivo como servidor alternativo	Habilítelo para que pueda configurar la IP alternativa de VTS.
IP alternativa	El servidor alternativo se usará como servidor SIP cuando Express o DSS dejen de responder. Le recomendamos configurar la dirección IP alternativa. ◇ Si lo habilitas Dispositivo como servidor alternativo El VTO actual en el que ha iniciado sesión sirve como servidor alternativo. ◇ Si desea que otro VTO sirva como servidor alternativo, debe ingresar la dirección IP de ese VTO en el campo IP alternativa cuadro de texto. No habilitar Dispositivo como servidor alternativo en este caso.
Nombre de usuario/contraseña del servidor alternativo	Se utiliza para iniciar sesión en el servidor alternativo.
IP alternativa de VTS	Dirección IP del VTS alternativo.

Paso 3 Hacer clic **Aplicar**.



- Para algunos servidores de terceros, si el intercomunicador selecciona dos métodos de desbloqueo del **RFC 2833** y **INFORMACIÓN SIP** al mismo tiempo, el código de desbloqueo no estará disponible para desbloquear el intercomunicador.
- Cuando se utiliza un servidor de terceros para brindar soporte a un intercomunicador de terceros, puede ocurrir una excepción de intercomunicador o SIP fuera de línea en algunos servidores.

- Si **Servidor de terceros: Asterisk** **Intercomunicador SIP** Seleccione dos métodos de desbloqueo del **RFC 2833** y **INFORMACIÓN SIP** Al mismo tiempo, el código de desbloqueo no estará disponible para desbloquear el intercomunicador.
- Si el intercomunicador IB se desconecta frecuentemente del servidor 3CX, es necesario eliminar la relación de mapeo.

9.4 Segunda estación de confirmación en cascada

Se aplicó a la situación en la que la segunda estación de confirmación se conecta al VTH.

Prerrequisitos

La versión del software del VTH debe ser V4.7 y posterior.

Procedimiento

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

Paso 2 Configurar la información de la segunda estación de confirmación en **Configuración del dispositivo local** > **Configuración básica**.



El tipo de dispositivo debe configurarse como **Segunda Estación de Confirmación**.

Paso 3 Colocar **Tipo de servidor** como **Dispositivo** y luego configure los parámetros. En esta situación en cascada, el VTH funciona como servidor SIP.

Figura 9-6 Configuración del servidor SIP (VTH como servidor SIP)

Tabla 9-5 Descripción de la configuración del servidor SIP (VTH como servidor SIP)

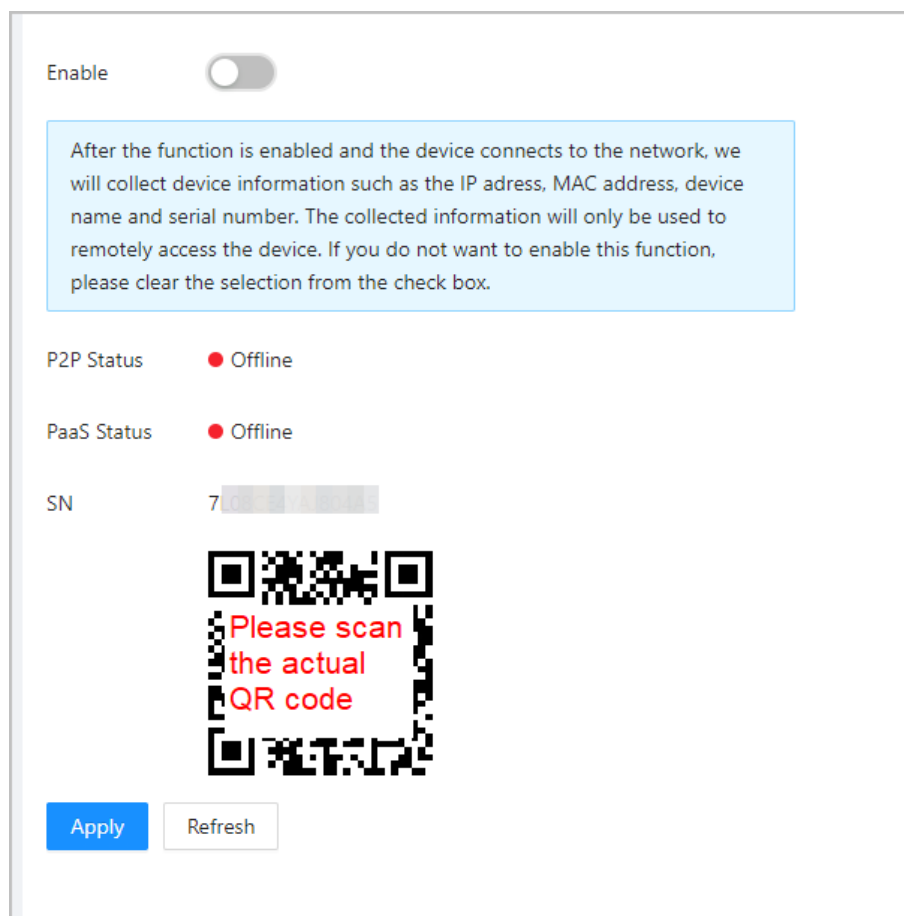
Parámetro	Descripción
Dirección del servidor	Su dirección IP planificada del VTH.
Puerto	5060 por defecto.
N.º SIP	Déjalo como predeterminado.
Contraseña de registro	
Dominio SIP	
Nombre de usuario del servidor SIP	Nombre de usuario y contraseña utilizados para iniciar sesión en el VTH que sirve como servidor SIP.
Contraseña del servidor SIP	

Paso 4 Hacer clic **Aplicar**.

9.5 Servicio en la nube

Habilitar el **Servicio en la nube** función y luego puede escanear el código QR con su teléfono para agregar el VTO a la aplicación en su teléfono.

Figura 9-7 Servicio en la nube



9.6 UPnP

Cuando el VTO funciona como servidor SIP, puede configurar la función UPnP para permitir que los dispositivos WAN inicien sesión en el VTO.

Figura 9-8 UPnP

Enable ☐

Apply

Refresh

Default

Add

Service Name	Service Type	Protocol	Internal Port	External Port	Status	Enable	Modify
HTTP	CustomService	TCP	80	8080	Mapping Failed	☒	
TCP	CustomService	TCP	37777	37777	Mapping Failed	☒	
UDP	CustomService	UDP	37778	37778	Mapping Failed	☒	
RTSP	CustomService	TCP	554	554	Mapping Failed	☒	
PrivService	CustomService	TCP	18877	18877	Mapping Failed	☒	
SIP	CustomService	UDP	5060	5060	Mapping Failed	☒	
Rtp	CustomService	UDP	15001	15001	Mapping Failed	☒	
Rtp	CustomService	UDP	15002	15002	Mapping Failed	☒	
Rtp	CustomService	UDP	15003	15003	Mapping Failed	☒	
Rtp	CustomService	UDP	15004	15004	Mapping Failed	☒	

22 records

<

1

2

3

>

10 / page

Go to

Page

Preparación

- Habilite la función UPnP en el enrutador y luego configure una dirección IP WAN para el enrutador.
- Conecte el VTO al puerto LAN del enrutador.

9.6.1 Habilitación de servicios UPnP

Procedimiento

- Paso 1

Seleccionar**Configuración de red>UPnP**.
- Paso 2

Seleccione los servicios enumerados y luego haga clic en**Permitir**.
- Paso 3

Haga clic**Aplicar**.

9.6.2 Agregar servicios UPnP

Procedimiento

- Paso 1

Seleccionar**Configuración de red>UPnP**. Haga clic**Agregar**.
- Paso 2

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

Figura 9-9 Agregar un servicio UPnP

Add

Enable

* Service Name

VTO1

* Service Type

VTO

Protocol

TCP

* Internal Port

3

* External Port

3

OK

Cancel

Tabla 9-6 Descripción de parámetros

Parámetro	Descripción
Nombre del servicio	Introduzca el nombre y el tipo del servicio.
Tipo de servicio	
Protocolo	Seleccionar TCP o UDP .
Puerto interno	Puerto interno del servicio.  ● Si necesita configurar esta función para varios dispositivos, asegúrese de que los puertos no sean los mismos. ● El número de puerto que utilice no debe estar ocupado. ● El número de puerto interno y externo deben ser el mismo.
Puerto externo	Puerto externo del servicio.  ● Si necesita configurar esta función para varios dispositivos, asegúrese de que los puertos no sean los mismos. ● El número de puerto que utilice no debe estar ocupado. ● El número de puerto interno y externo deben ser el mismo.

9.7 Wi-Fi

Si el VTO admite la función Wi-Fi, configure los parámetros aquí.

Procedimiento

- Paso 1 Inicie sesión en la página web de la VTO.
- Paso 2 Seleccione**Configuración de red>Wi-Fi**.
- Paso 3 Establecer el**Wi-Fi**estado como**En**.
Se muestran todas las redes disponibles.

Figura 9-10 Wi-Fi

Wi-Fi 			
Name	Signal Strength	Status	Connect
XXXXXXXXXX			+
XXXXXXXXXX			+
XXXXXXXXXX			+
XXXXXXXXXX			+
XXXXXXXXXX			+
XXXXXXXXXX			+
XXXXXXXXXX			+
XXXXXXXXXX			+
XXXXXXXXXX			+

- Paso 4 Hacer clic+del Wi-Fi que elegiste, ingresa la contraseña de la misma y luego conéctate a la red.

9.8 Servicios básicos

Configurar funciones que involucran la seguridad del dispositivo.

Procedimiento

- Paso 1 Seleccionar**Configuración de red>Servicios básicos**Habilite
- Paso 2 las funciones de seguridad según sus necesidades.

Figura 9-11 Servicios básicos

SSH

There might be safety risk if this service is enabled.

CGI

Mobile Push Notifications

Password Reset

Outbound Protection of S...

There might be data leakage risk if this service is disabled.

Multicast/Broadcast Search

Authentication Mode

Security Mode (Recommended)

Emergency Maintenance

For easy access to our after-sales service, enable this function. If the device has any trouble performing functions, such as updating, the system will automatically enable this function.

Password Expires in

Never

Private Protocol

*Before enabling private protocol TLS, make sure that the corresponding device or software supports this function.

TLSv1.1

LLDP

Apply

Refresh

Default

Tabla 9-7 Descripción de los parámetros de seguridad

Parámetro	Descripción
SSH	Una alternativa segura a los protocolos remotos no seguros. Le recomendamos que lo desactive porque podría haber riesgos de seguridad si este servicio está habilitado.
CGI	El uso del comando CGI. Le recomendamos que lo desactive. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fugas de datos.
Push móvil Notificación	Envía información a la aplicación en el teléfono. Le recomendamos desactivarla si no necesita esta función. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fugas de datos.
Restablecer contraseña	Si está desactivado, no podrá restablecer la contraseña.
Servicio de salida Protección de la información	Proteja sus contraseñas. Le recomendamos activarlo. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fugas de datos.

Parámetro	Descripción
Multidifusión/Difusión Buscar	Habilítelo para que otros dispositivos puedan encontrar el VTO.  Le recomendamos que lo desactive. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fugas de datos.
Modo de autenticación	● Modo de seguridad(recomendado): Admite inicio de sesión con autenticación Digest. ● Modo de compatibilidad: Utilice el antiguo método de inicio de sesión.  Le recomendamos usar el modo de seguridad. El modo compatible podría exponer el VTO a riesgos de seguridad y fugas de datos.
Emergencia Mantenimiento	Para acceder fácilmente a nuestro servicio posventa, active esta función. Si el dispositivo presenta algún problema al realizar funciones, como la actualización, el sistema la activará automáticamente.
La contraseña caduca en	● Seleccione un período de vencimiento de 30 días, 60 días, 90 días, 180 días, Costumbre y Nunca. ● Si selecciona Costumbre, debe configurar un día de vencimiento entre 0 y 180.
Protocolo privado	Antes de habilitar el protocolo privado TLS, asegúrese de que el dispositivo o software correspondiente admita esta función.
TLSv1.1	 Le recomendamos que lo desactive porque podría haber riesgos de seguridad si este servicio está habilitado.
LLDP	Mejora la eficiencia del intercambio de información entre dispositivos de red.

Paso 3 Hacer clic **Aplicar**.

9.9 Registro automático

VTO se registra automáticamente en el servidor e informa su dirección IP al servidor designado.

Procedimiento

Paso 1 Inicie sesión en la página web de VTO.

Paso 2 Seleccionar **Configuración de red > Registro automático**.

Paso 3 Habilite la función. Introduzca la dirección del servidor, el número de puerto y el ID de registro.

Figura 9-12 Registro automático

Enable

☒

Server Address

Port

(1-65535)

Registration ID

Apply

Refresh

Default

Tabla 9-8 Descripción de parámetros

Parámetro	Descripción
Dirección del servidor	Dirección IP o nombre de dominio del servidor que se necesita en el registro.
Puerto	Número de puerto que el servidor registra automáticamente.
ID de registro	El servidor distribuye un ID para el dispositivo. Debe ser coherente con el ID registrado en el servidor.

Paso 4 Hacer clic **Aplicar**.

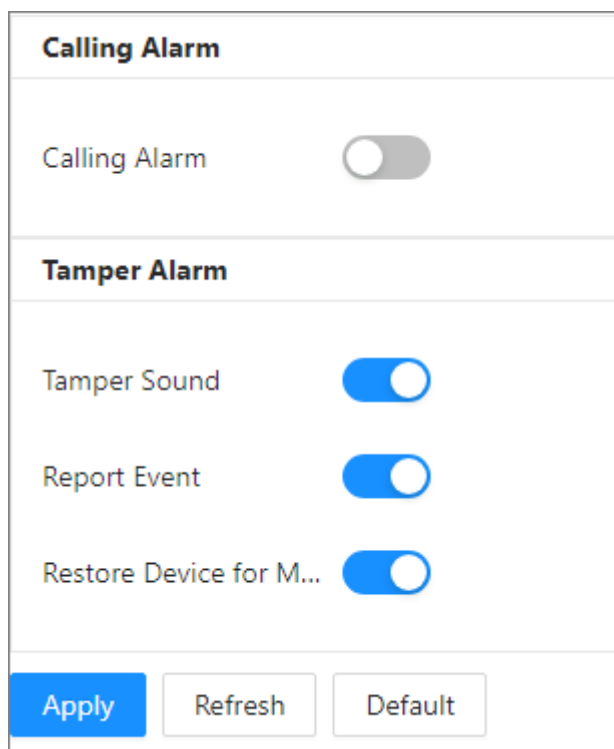
Sistema 10

10.1 Alarm

Procedimiento

Paso 1 Seleccionar **Sistema>Alarma**.

Figura 10-1 Alarma



Paso 2 Configure los parámetros que tendrán efecto al realizar el cambio.

Tabla 10-1 Descripción de los parámetros de alarma

Parámetro	Descripción
Alarma de llamada	Al iniciarse la llamada, se conectará la salida de alarma. Si la interfaz de salida de alarma está conectada a un zumbador, este emitirá un pitido.
Sonido de manipulación	Configura si el dispositivo silba localmente o no. Está habilitado por defecto.
Reportar evento	Configure si el dispositivo debe informar la alarma de manipulación a la aplicación, la unidad interior y el backend de la plataforma. Está habilitado por defecto.
Restaurar dispositivo para múltiples alarmas de manipulación	Dentro de los 10 minutos posteriores a que se enciende el dispositivo, si presiona continuamente el botón de manipulación 5 veces en 8 segundos, el dispositivo emite un pitido y elimina la información de la cuenta.

Paso 3 Hacer clic **Aplicar**.

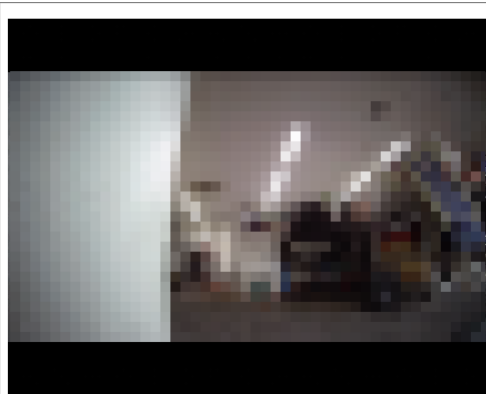
10.2 Vídeo

Configure el formato y la calidad de vídeo y audio del VTO.

Procedimiento

Paso 1 Seleccionar **Sistema>Vídeo**.

Figura 10-2 Vídeo



Bit Rate

Status

Exposure

Image

Main Stream

Resolution720P

Frame Rate (FPS)25

Bit Rate1024Kbps

CompressionH.264

Sub Stream

ResolutionCIF

Frame Rate (FPS)25

Bit Rate256Kbps

CompressionH.264

Paso 2 Configure los parámetros que tendrán efecto al realizar el cambio.

Tabla 10-2 Descripción de los parámetros de vídeo

Parámetro			Descripción
Tasa de bits	Corriente principal	Resolución	● 720P:1280 × 720. ● WVGA:800 × 480. ● D1:704 × 576. ● CIF:352 × 288.
		Velocidad de cuadros (FPS)	● Si selecciona elEstándar de vídeocomoCAMARADA:El rango es de 1 a 25. ● Si selecciona elEstándar de vídeocomoNTSC:El rango es de 1 a 30). Cuanto mayor sea el valor, más fluido será el vídeo, pero requerirá más ancho de banda.
		Tasa de bits	Cuanto mayor sea el valor, mejor será la calidad del vídeo, pero requerirá más ancho de banda.
		Compresión	En comparación con H.264, H.265 requiere un ancho de banda menor.

Parámetro			Descripción
	Subtransmisión	Resolución	● 1080P:1920 × 1080. ● WVGA:800 × 480. ● QVGA:320 × 240. ● D1:704 × 576. ● CIF:352 × 288.
		Velocidad de cuadros (FPS)	El rango es de 1 a 25. Cuanto mayor sea el valor, más fluido será el vídeo, pero requerirá más ancho de banda.
		Tasa de bits	Incluye 224 Kbps, 256 Kbps, 320 Kbps, 384 Kbps, 448 Kbps, 512 Kbps, 640 Kbps y 768 Kbps. Cuanto mayor sea el valor, mejor será la calidad del video, pero requiere mayor ancho de banda.
		Compresión	H.264. H.265.
Estado	Modo de escena		Selecione de Auto , Desactivar , Soleado y Noche . Auto Está seleccionado de forma predeterminada.
	Modo de compensación		● BLC:Compensación de contraluz. Mejora la claridad del objetivo en la imagen. ● Amplio rango dinámico (WDR):Amplio rango dinámico. Mejora el brillo de las zonas oscuras y reduce el brillo de las zonas brillantes para mejorar la imagen. ● Centro de salud de alto nivel:Alta compensación de luz. Reduce el brillo de los puntos fuertes para mejorar la imagen general. ● Desactivar:No utilice ningún modo de compensación.
	Día/Noche		Selecione de Color , Auto y Blanco y negro .
	Estándar de vídeo		Seleccionar CAMARADA o NTSC según tu zona.
	Sensibilidad del iluminador		Configurar el valor de sensibilidad. ● Si la intensidad de la iluminación es inferior al valor configurado, se encenderá el iluminador. ● Si la intensidad de la iluminación es mayor que el valor configurado, el iluminador se apagará.

Parámetro		Descripción
Exposición	Antiparpadeo	● 50 Hz:El sistema ajusta automáticamente la exposición según la luz ambiental para garantizar que no aparezcan rayas. ● 60 Hz:El sistema ajusta automáticamente la exposición según la luz ambiental para garantizar que no aparezcan rayas. ● Exterior:Si seleccionas Exterior, el modo de exposición se puede configurar en Ganar prioridad, Prioridad de obturador y Prioridad del iris. Diferentes dispositivos admiten distintos modos de exposición.
	Modo de exposición	● Auto:La exposición se ajusta automáticamente según el brillo de la escena si el brillo general de las imágenes está dentro del rango de exposición normal. ● Manual:Puedes ajustar el Ganar y Obturador valor manualmente. ● Prioridad de obturador:La cámara ajusta automáticamente el tamaño de la apertura según la velocidad de obturación seleccionada para garantizar una exposición adecuada.
	Compensación de exposición	Puede configurar el valor de compensación de exposición. El valor varía de 0 a 100. Cuanto mayor sea el valor, más brillante será la imagen.
	Reducción de ruido 3D	Reduzca el ruido de imágenes de varios fotogramas (al menos dos) utilizando la información interfotograma entre dos fotogramas adyacentes en un vídeo. Cuanto mayor sea el nivel, menor será el ruido y mayor la mancha de arrastre.
	Nivel NR	Grado de reducción de ruido. El valor varía de 0 a 100. Cuanto mayor sea el valor, menor será el ruido.
Imagen	Brillo	Cuanto mayor sea el valor, más brillante será la imagen.
	Contraste	Valor mayor para mayor contraste entre áreas brillantes y oscuras.
	Matiz	Aclara u oscurece el color. El valor predeterminado lo establece el sensor de luz, por lo que recomendamos mantenerlo.
	Saturación	Cuanto mayor sea el valor, más espeso será el color.
	Espejo	Muestra la imagen con el lado izquierdo y derecho invertidos.
	Voltear	Muestra la imagen al revés.
	Tiempo de visualización	Muestra la hora y fecha actuales en la imagen de vídeo.

Paso 3 (Opcional) Configure el videoclip.

Hacer clic **Izquierdo** **Bien** Para girar la pantalla hacia la izquierda o la derecha. Haga clic **Reiniciar** **Por**

defecto para restablecer o restablecer el dispositivo a sus valores predeterminados.



La función sólo está disponible para el modo F.

Operaciones relacionadas

Hacer clic **Por defecto** para restaurar las configuraciones predeterminadas.

10.3 Audio

Procedimiento

Paso 1 Seleccionar **Sistema** > **Audio**.

Paso 2 Configure los parámetros que tendrán efecto al realizar el cambio.

Figura 10-3 Audio

Audio Control

Voice Prompt while Ringing

Ringtone

Unlock

Alarm

Voice Messages

Audio Collection

Volume Control

Intercom Volume

+ 0

Microphone Volume

+ 0

Device Volume

+ 0

Apply

Refresh

Default

Audio File(Please upload a WAV or MP3 file. The file size must not exceed 100K.)

Audio Type	Audio File	Modify
Calling	-	
Busy	-	
Successfully Unlocked	-	
Nobody Answered	-	
Call Ended	-	
Nonexistent Number	-	

Tabla 10-3 Descripción de los parámetros de audio

Parámetro		Descripción
Control de audio	Aviso de voz mientras suena	Activa o desactiva cada tipo de sonido.
	Tono de llamada	
	Alarma	
	Mensajes de voz	
	Descubrir	
	Colección de audio	

Parámetro		Descripción
Control de volumen	Volumen del micrófono	Ajuste el volumen del micrófono del VTO. Cuanto mayor sea el valor, mayor será el volumen.
	Volumen del altavoz	Ajuste el volumen del altavoz. Cuanto más alto sea el valor, más alto será el volumen.
	Volumen del dispositivo	Ajuste el volumen del dispositivo. Cuanto mayor sea el valor, más alto será el volumen.

Paso 3 Hacer clic **Aplicar**.

Paso 4 (Opcional) Sube el archivo de audio haciendo clic en  junto al tipo de audio correspondiente (incluyendo llamadas, ocupado, desbloqueo exitoso, nadie respondió, llamada finalizada y número inexistente).



Sube un archivo WAV o MP3. El tamaño del archivo no debe superar los 100 KB.

10.4 Tiempo

Configure la zona horaria y los parámetros de horario de verano.

Procedimiento

Paso 1 Seleccionar **Sistema>Tiempo**.

Paso 2 Configurar la hora, la zona horaria y el horario de verano.

Figura 10-4 Tiempo

Time and Time Zone



Date :

2023-07-10 Monday

Time :

13:46:16

Time

☒ Manually Set

☐ NTP

System Time

2023-07-10 13:46:16



Sync PC

Time Format

YYYY-MM-DD

24-Hour

Time Zone

(UTC) Coordinated Universal Time

DST

Enable

☐

Type

☐ Date

☒ Week

Start Time

May

Final Week

Mon

00:00



End Time

Oct

Final Week

Mon

00:00



Apply

Refresh

Default

Tabla 10-4 Descripción de parámetros

Módulo	Parámetro	Descripción
Tiempo y tiempo Zona	Tiempo	● Configurado manualmente ● Protocolo de transferencia de calor (NTP)
	Hora del sistema	La hora del sistema VTO.  Cambiar la hora del sistema podría causar problemas en la búsqueda de videos y la publicación de información. Desactive la grabación de video y la captura automática de instantáneas antes de cambiarla.  Sólo aplicable bajo laConfigurado manualmentemodo.
	Sincronizar PC	Sincronice la hora del sistema VTO con su PC.  Sólo aplicable bajo laConfigurado manualmentemodo.

Módulo	Parámetro	Descripción
	Servidor	La dirección del servidor NTP.  Sólo aplicable bajo la Protocolo de transferencia de calor (NTP) modo.
	Actualización manual	Haga clic en el icono y la hora del dispositivo VTO se sincronizará automáticamente con el servidor.  Sólo aplicable bajo la Protocolo de transferencia de calor (NTP) modo.
	Puerto	Número de puerto del servidor NTP.  Sólo aplicable bajo la Protocolo de transferencia de calor (NTP) modo.
	Intervalo	Ciclo de actualización de tiempo VTO. 30 minutos como máximo.  Sólo aplicable bajo la Protocolo de transferencia de calor (NTP) modo.
	Formato de hora	Para el formato de fecha, seleccione una de las siguientes opciones: ● AAAA-MM-DD ● MM-DD-AAAA ● DD-MM-AAAA Para el formato de hora, seleccione uno de los siguientes: ● 24 horas ● 12 horas
	Huso horario	Seleccione la zona horaria para el sistema VTO.
Horario de verano	Permitir	Haga clic para habilitar el Horario de verano función.
	Tipo	Seleccionar Fecha o Semana según sea necesario y luego configure el período específico.
	Hora de inicio	Configure la hora de inicio y la hora de finalización del horario de verano.
	Fin de los tiempos	

Paso 3 Hacer clic **Aplicar**.

10.5 Usuario de ONVIF

Agregar cuentas para dispositivos para monitorear el VTO a través del protocolo ONVIF.



Solo se admiten los perfiles C y S, mientras que el formato de codificación y los parámetros de imagen no son compatibles.

Procedimiento

- Paso 1** Seleccionar **Sistema** > **Usuario de ONVIF**. Haga
- Paso 2** clic **Agregar**.
- Paso 3** Ingrese la información y luego haga clic **DE ACUERDO**.

Los dispositivos ONVIF pueden monitorear el VTO mediante la cuenta.

Figura 10-5 Usuario de ONVIF

The image shows a software dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains three labeled input fields, each preceded by a red asterisk indicating it is required:

- * Username:** The input field contains the text "Jack".
- * Password:** The input field contains masked characters ".....". Below the field is a password strength indicator consisting of a horizontal bar that is approximately two-thirds filled with orange and one-third with light blue.
- * Confirm Password:** The input field contains masked characters ".....".

At the bottom right of the dialog are two buttons: a blue "OK" button and a white "Cancel" button with a gray border.

11 Gestión de registros

Seleccionar **Centro de mantenimiento** > **Registro** Puede buscar diferentes registros y exportarlos a su computadora local.



Si el almacenamiento está lleno, se sobrescribirán los registros más antiguos. Realice copias de seguridad de los registros a tiempo.

11.1 Diagnóstico con un solo clic

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

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar **Centro de mantenimiento** > **Diagnóstico con un solo clic**.

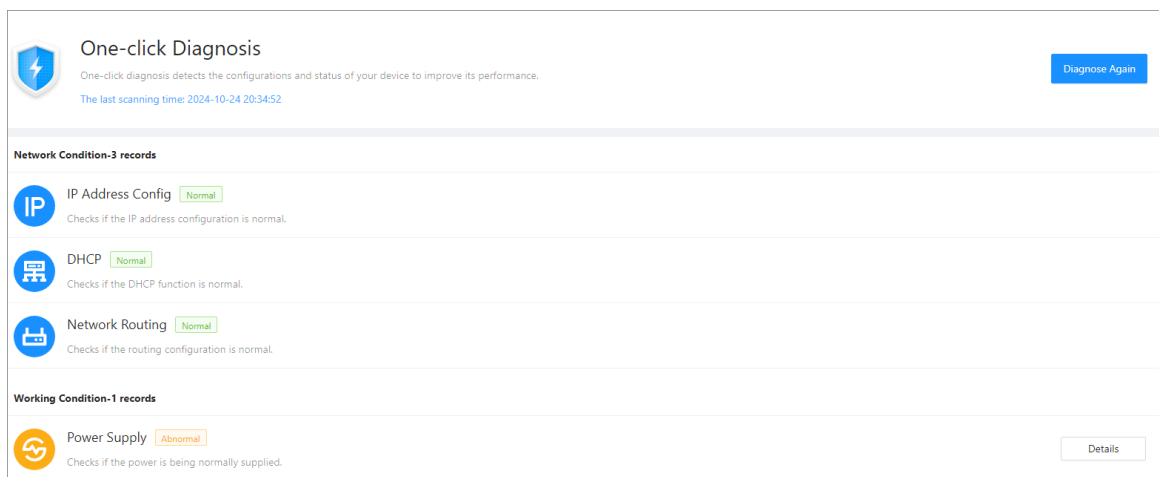
Paso 3 Haga clic **Diagnosticar**.

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

Paso 4 (Opcional) Haga clic en **Detalles** para ver detalles de artículos anormales.

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

Figura 11-1 Diagnóstico con un solo clic



11.2 Información del sistema

11.2.1 Información de la versión

Procedimiento

Paso 1 Seleccionar **Centro de mantenimiento** > **Información del sistema** > **Versión**.

Paso 2 Ver la versión del software, la versión de SCM y la versión base de seguridad.

Figura 11-2 Información del sistema

Device Model	
Device SN	
Hardware Version	
Software Version	
SCM Version	
Web Version	
Security Baseline Version	

11.2.2 Información legal

Seleccionar **Centro de mantenimiento>Información del sistema>Información legal**. Puede consultar los avisos de información legal relacionados en esta sección.

11.3 Capacidad de datos

Puedes ver cuántos usuarios, tarjetas e imágenes faciales puede almacenar el VTO. Inicia sesión en la página web y selecciona **Centro de mantenimiento>Capacidad de datos**.

11.4 Gestión del mantenimiento

11.4.1 Configuración

Puede exportar e importar el archivo de configuración.

Procedimiento

- Paso 1** Seleccionar **Centro de mantenimiento>Gestión de mantenimiento>Configuración**.
- Paso 2** Hacer clic **Exportar archivo de configuración**, o haga clic en **Navegar** para seleccionar el archivo de la computadora local y luego hacer clic **Importar archivo**.

Figura 11-3 Configuración

The screenshot shows a web interface titled "Config". It contains a button labeled "Export Configuration File". Below this, there is a "File" label next to a text input field, followed by a "Browse" button and an "Import File" button. At the bottom, a yellow message box states: "Imported configuration will overwrite previous configuration."

11.4.2 Mantenimiento

Procedimiento

- Paso 1 Seleccionar **Centro de mantenimiento>Gestión de mantenimiento>Mantenimiento**.
- Paso 2 Configure el tiempo de mantenimiento automático.

Figura 11-4 Mantenimiento automático

The screenshot shows a web interface titled "Maintenance". Under the "Auto Maintenance" section, there is a "Maintenance Time" label. To its right are two dropdown menus: the first is set to "Tue" and the second is set to "02:00". At the bottom of the section are two buttons: "Apply" (in blue) and "Refresh" (in white).

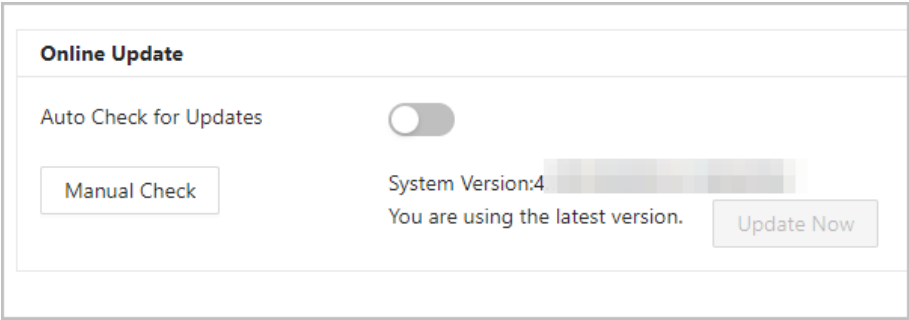
- Paso 3 Hacer clic **Aplicar**.

Actualización 11.5

Procedimiento

- Paso 1 Seleccionar **Centro de mantenimiento>Actualizar**
- Paso 2 Seleccione formas de comprobar la actualización.
- **Actualización de archivos:** Hacer clic **Navegar** para agregar el archivo de actualización y luego haga clic en **Actualizar**.
 - **Actualización en línea**
 - ◇ **Búsqueda automática de actualizaciones:** Habilite la función para verificar automáticamente si hay una nueva versión del sistema.
 - ◇ **Comprobación manual:** Seleccione la función para comprobar si hay una nueva versión del sistema.

Figura 11-5 Actualización en línea



11.6 Mantenimiento avanzado

Exportar

Seleccionar**Centro de mantenimiento>Mantenimiento avanzado>Exportar**para exportar el número de serie, la versión del firmware, los registros de funcionamiento del dispositivo y la información de configuración.

Captura de paquetes

1. Seleccionar**Centro de mantenimiento>Mantenimiento avanzado>Captura de paquetes**.
2. Ingrese el puerto del dispositivo.
3. Haga clic para iniciar la copia de seguridad del analizador de paquetes.

Figura 11-6 Captura de paquetes

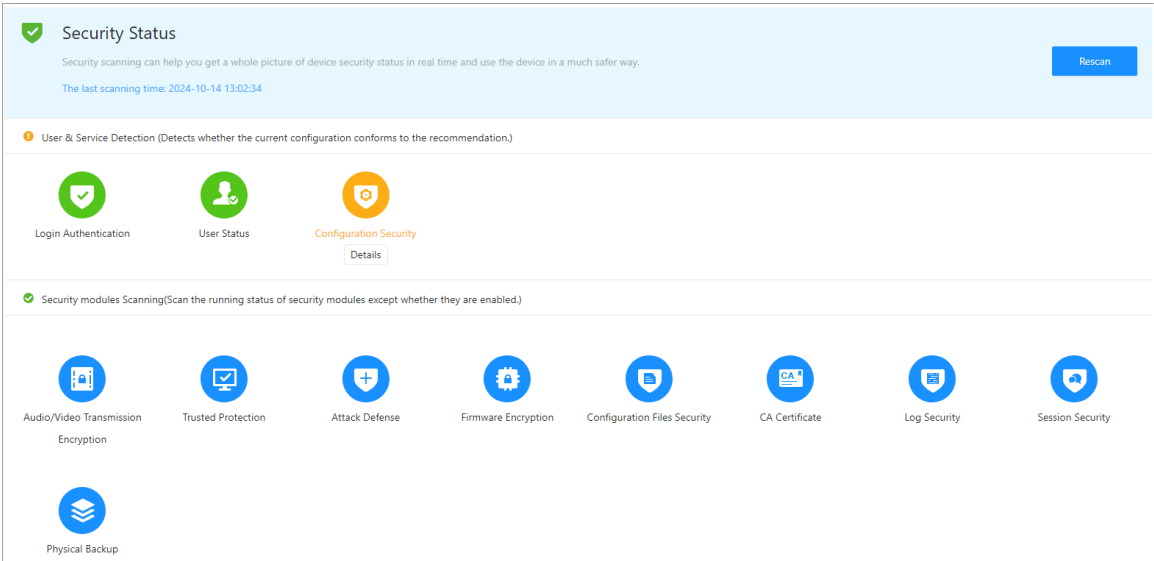
Packet Capture							
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Back...
eth0	[blurred]	Optional	Optional	Optional	Optional	0.00MB	▶
lo	[blurred]	127.0.0.1	Optional	Optional	Optional	0.00MB	▶

12 Gestión de la seguridad

12.1 Estado de seguridad

En la página de inicio, haga clic en , y luego seleccione **Estado de seguridad**.

Figura 12-1 Estado de seguridad

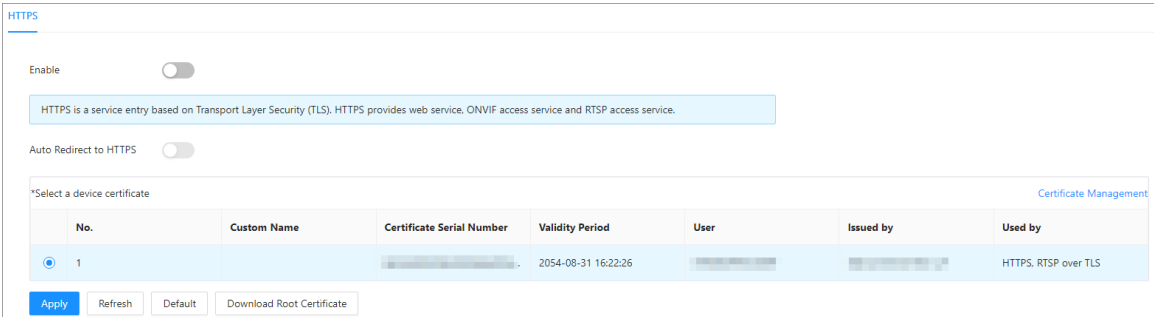


12.2 Servicio del sistema

Procedimiento

- Paso 1** En la página de inicio, haga clic en , y luego seleccione **Servicio del sistema**.
- Paso 2** Seleccione un certificado de dispositivo y luego habilite la función HTTPS.

Figura 12-2 Servicio del sistema



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

12.3 Defensa de ataque

12.3.1 Cortafuegos

Puede habilitar diferentes tipos de firewall para controlar el acceso de la red al VTO.

Procedimiento

Paso 1 En la página de inicio, haga clic en , y luego seleccione **Ataque Defensa** > **Cortafuegos**.

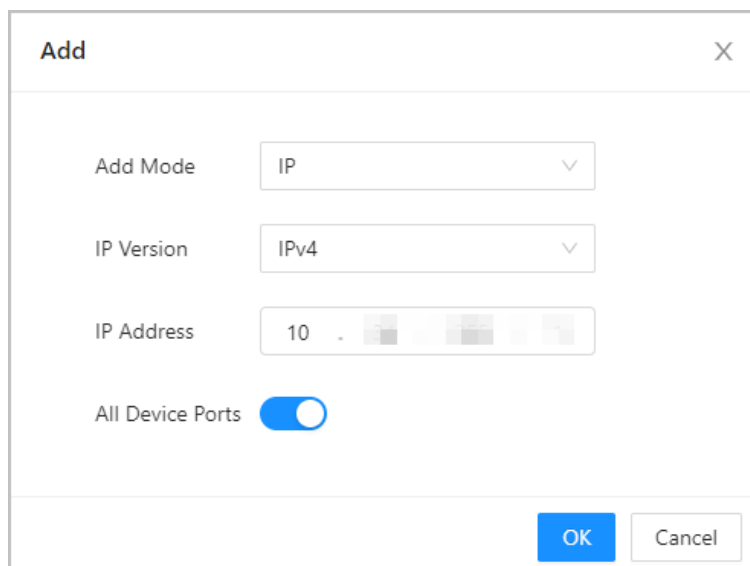
Paso 2 Haga clic en  junto a **Permitir**.

Paso 3 Seleccione el **Modo** como cualquiera **Lista de permitidos** o **Lista de bloqueo**.

- Lista de permitidos: dispositivos a los que se les ha concedido acceso.
- Lista de bloqueo: Dispositivos a los que se les ha prohibido el acceso.

Paso 4 Hacer clic **Agregar** para agregar la dirección IP a la lista blanca o negra.

Figura 12-3 Agregar



El formulario 'Add' tiene un título 'Add' y un botón de cerrar 'X' en la esquina superior derecha. Contiene los siguientes campos:

- Add Mode:** Un menú desplegable con 'IP' seleccionado.
- IP Version:** Un menú desplegable con 'IPv4' seleccionado.
- IP Address:** Un campo de entrada con el valor '10' y un icono de selección de color.
- All Device Ports:** Un interruptor de encendido/apagado que está activado (azul).

En la parte inferior derecha hay dos botones: 'OK' (azul) y 'Cancel' (gris).

Paso 5 Hacer clic **DE ACUERDO**.

Paso 6 Seleccione una dirección IP agregada para la lista blanca o la lista negra y luego haga clic en **Aplicar**.

Figura 12-4 Aplicar

The screenshot shows the Firewall configuration interface. At the top, there are tabs for 'Firewall', 'Account Lockout', and 'Anti-DoS Attack'. The 'Firewall' tab is active. Below the tabs, there is an 'Enable' toggle switch which is turned on. Under 'Mode', the 'Allowlist' radio button is selected, and the 'Blocklist' radio button is unselected. A light blue box contains the text: 'Only source hosts whose IP/MAC are in the following list are allowed to access corresponding ports of the device.' Below this box are 'Add' and 'Delete' buttons. A table with the following columns is shown: 'No.', 'Host IP/MAC', 'Port', and 'Operation'. The table contains one record with 'No.' 1, 'Host IP/MAC' 12, and 'Port' All Device Ports. Below the table, it says 'Total 1 records'. At the bottom, there are 'Apply', 'Refresh', and 'Default' buttons. A pagination control shows '1' of 1 records.

No.	Host IP/MAC	Port	Operation
1	12	All Device Ports	

12.3.2 Bloqueo de cuenta

Procedimiento

Paso 1 En la página de inicio, haga clic en , y luego seleccione **Ataque Defensa>Bloqueo de cuenta**.

Paso 2 Configure los intentos de inicio de sesión y el tiempo de bloqueo para la cuenta del dispositivo y el usuario ONVIF.

Figura 12-5 Bloqueo de cuenta

The screenshot shows the Account Lockout configuration interface. At the top, there are tabs for 'Firewall', 'Account Lockout', and 'Anti-DoS Attack'. The 'Account Lockout' tab is active. Below the tabs, there are two sections: 'Device Account' and 'ONVIF User'. Each section has a 'Login Attempt' dropdown menu and a 'Lock Time' input field with a 'min' label. For 'Device Account', 'Login Attempt' is set to '5time(s)' and 'Lock Time' is set to '5'. For 'ONVIF User', 'Login Attempt' is set to '30time(s)' and 'Lock Time' is set to '5'. At the bottom, there are 'Apply', 'Refresh', and 'Default' buttons.

Paso 3 Hacer clic **Aplicar**.

12.3.3 Ataque anti-DoS

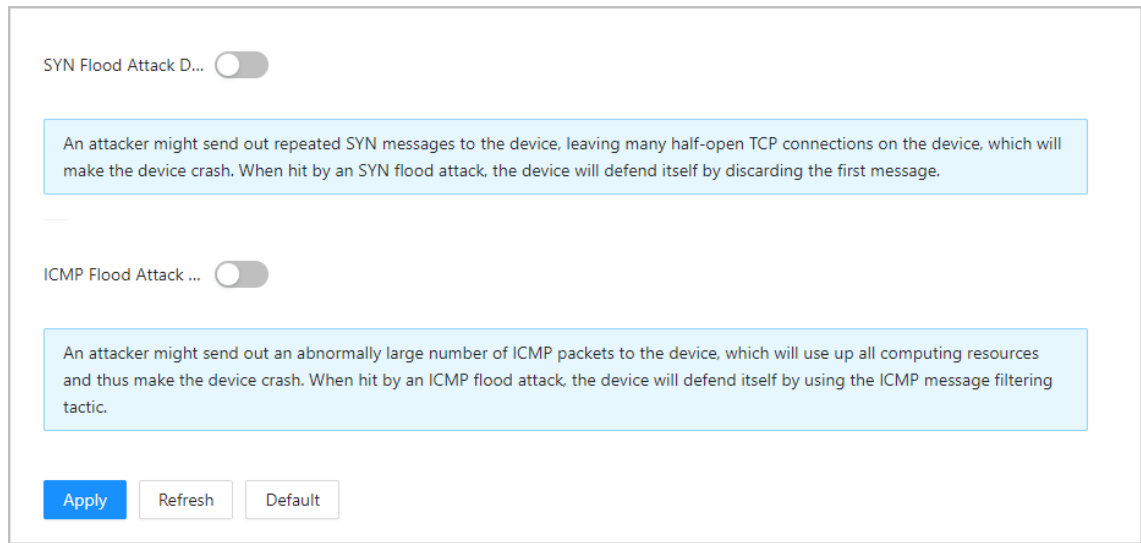
Procedimiento

- 

Paso 1 En la página de inicio, haga clic en **Ataque Defensa**, y luego seleccione **Ataque anti-DoS**.

Paso 2 Habilitar o deshabilitar la **Defensa contra ataques de inundación SYN** o **Defensa contra ataques de inundación ICMP** función.

Figura 12-6 Ataque anti-DoS



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

12.4 Certificado CA

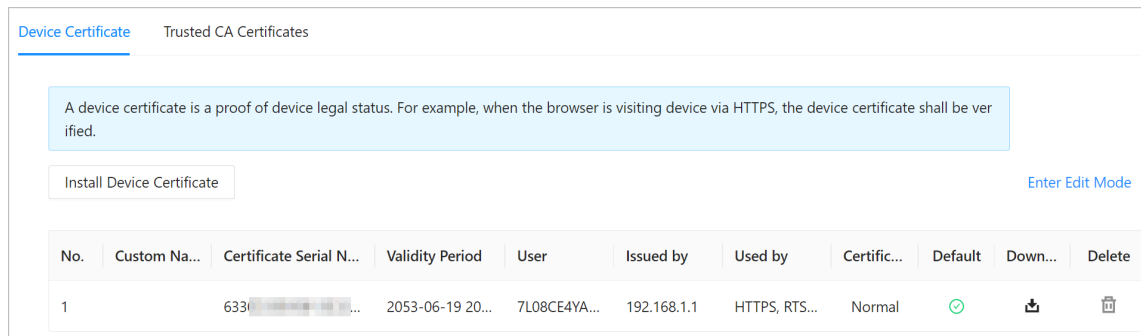
Procedimiento

- 

Paso 1 En la página de inicio, haga clic en **Certificado CA**.

 - Certificado del dispositivo

Figura 12-7 Certificado del dispositivo



- Certificados de CA de confianza

Figura 12-8 Certificados de CA de confianza

Device Certificate [Trusted CA Certificates](#)

A trusted CA certificate is used to verify the legal status of a host. For example, a switch CA certificate shall be installed for 802.1x authentication.

[Install Trusted Certificate](#) [Enter Edit Mode](#)

No.	Custom Na...	Certificate Serial Nu...	Validity Period	User	Issued by	Used by	Certificate ...	Downlo...	Delete
1		3231...	2027-10-16 23:...	192.168.1.1	192.168.1.1		Normal		

12.5 Cifrado de vídeo

Procedimiento

- Paso 1** En la página de inicio, haga clic en , y luego seleccione **Cifrado de vídeo**.
- Paso 2** Configurar **Protocolo privado** y **RTSP sobre TLS** parámetros.

Figura 12-9 Cifrado de vídeo

[Encrypted Transmission](#)

Private Protocol

Enable ☐

Stream transmission is encrypted by using private protocol.

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

Encryption Type

Update Period... hr (0-720)

RTSP over TLS

Enable ☒

RTSP stream is encrypted by using TLS tunnel before transmission.

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

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

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
☒ 1		63303339356133326136313...	2053-06-19 20:06:37	7L08CE4YA0804A5	192.168.1.1	HTTPS, RTSP over TLS

[Apply](#) [Refresh](#) [Default](#)

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

12.6 Advertencia de seguridad

Procedimiento

- Paso 1** En la página de inicio, haga clic en , y luego seleccione **Advertencia de seguridad**.
- Paso 2** Habilite la función de monitoreo de eventos y luego haga clic en **Aplicar**.

Figura 12-10 Advertencia de seguridad

Enable ☐

Event Monitoring

 Invalid executable programs attempting to run

 Session ID bruteforcing

 Web directory bruteforcing

 Number of session connections exceeds limit

Security warning can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.

Apply

Refresh

Default

Configuración del modelo de 13 botones

El modelo de botón se puede conectar al VTH para que funcione como botón de entrada de alarma. Al presionar el botón en el panel frontal del modelo, el VTH recibirá una señal de alarma.

13.1 Conexión del cable

Conecte el puerto KEY del modelo de botón a cualquiera de los puertos de entrada de alarma del monitor interior (VTH) con un cable roscado.

Figura 13-1 Modelo de botón

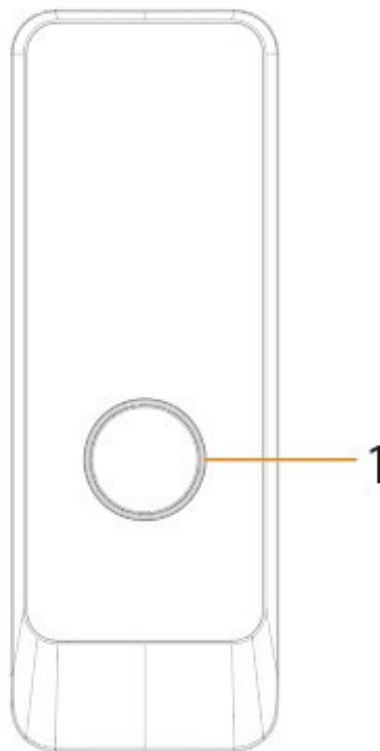
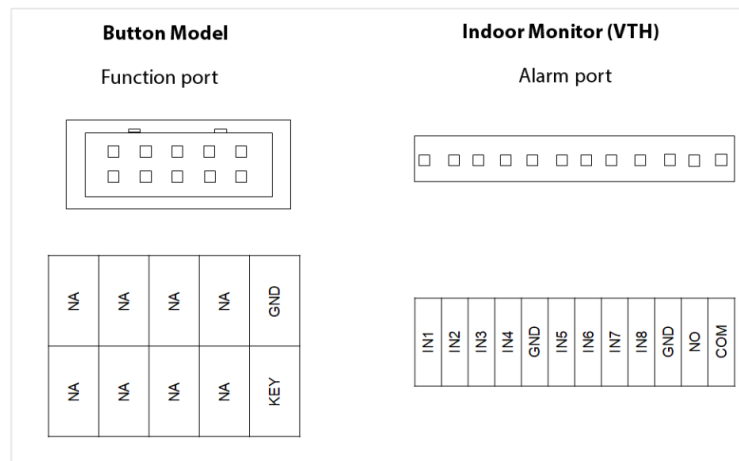


Tabla 13-1 Componente

No.	Nombre	Función
1	Presione el botón	El modelo de botón se puede conectar al VTH. Al presionarlo, el VTH recibe una señal de alarma.

Figura 13-2 Conexión del cable



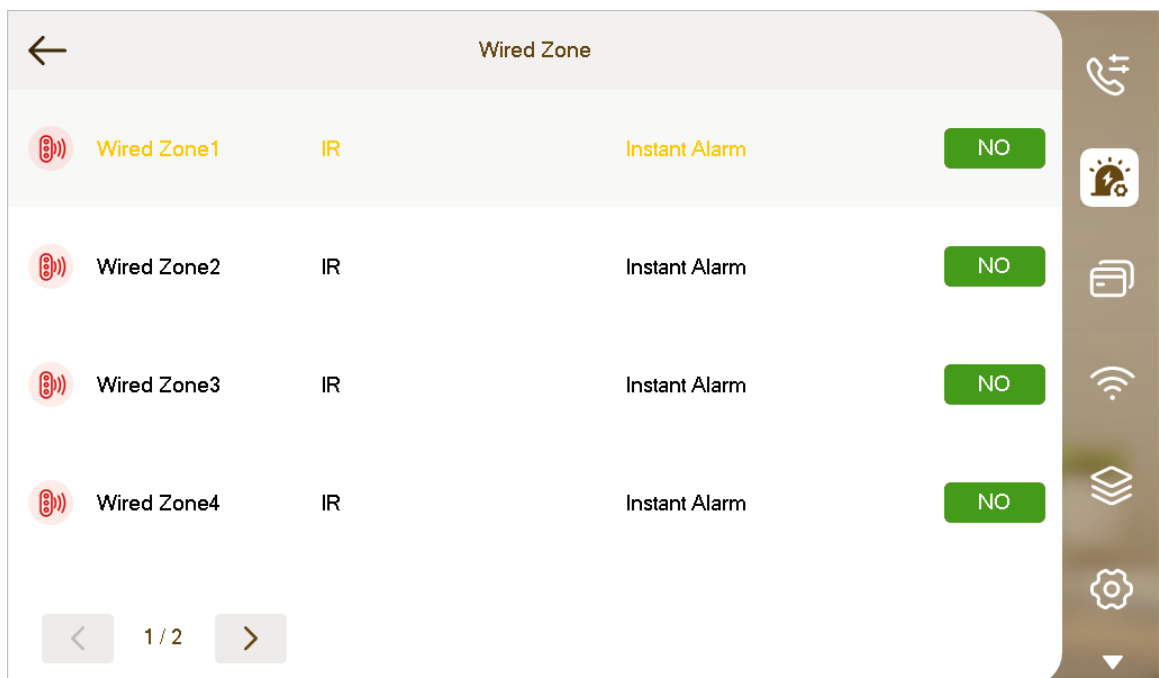
13.2 Configuración de VTH

Después de completar la conexión del cable, debe configurar el **tipo de zona cableada** como **Timbre de la puerta** en el VTH para recibir señales de alarma una vez que presione el botón modelo.

Procedimiento

- Paso 1** Encienda el VTH.
- Paso 2** Seleccione **Configuración > Alarma > Zona cableada** en el VTH.

Figura 13-3 Configuración de zona cableada



- Paso 3** Establezca el **Tipo** como **Timbre de la puerta**, y configure el resto de los parámetros.

Tabla 13-2 Descripción de parámetros

Parámetro	Descripción	
Área	El número no se puede modificar.	
NO/NC	Seleccione NO (normalmente abierto) o NC (normalmente cerrado) según el tipo de detector. Debe ser el mismo que el tipo de detector.	
Tipo	Seleccione el tipo correspondiente según el tipo de detector.	
Estado	● Alarma instantánea: Después del armado, si se activa una alarma, el dispositivo produce una sirena de inmediato y entra en estado de alarma. ● Alarma de retardo: Después del armado, si se activa una alarma, el dispositivo entra en estado de alarma después de un tiempo específico, durante el cual puede desarmar y cancelar la alarma. ● Derivación: La alarma no se activará en esta zona. Tras desactivarse, esta zona volverá a funcionar con normalidad. ● Eliminar: El área no es válida durante el armado/desarmado. ● 24 horas: La alarma se activará todo el tiempo en el área, independientemente de si está armada o desarmada.  Una zona en Eliminar El estado no se puede omitir.	
Retraso de entrada	Tras el retardo, si el área armada activa una alarma, entrar al área armada desde un área no armada dentro del retardo no activará la alarma de enlace. Esta se activará si el retardo finaliza y no se desarma.	
Retraso de salida	Después del brazo, Alarma de retardo El área entrará en estado de armado al final de Retraso de salida.  Si varias áreas establecen el retraso de salida, la solicitud en pantalla se ajustará al tiempo de retraso máximo.	El retraso sólo es válido para las zonas de Alarma de retardo.

Apéndice 1 Recomendación de seguridad

Gestión de cuentas

1. Utilice contraseñas complejas

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Cambie las contraseñas periódicamente

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

3. Asignar cuentas y permisos de forma adecuada

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

4. Habilitar la función de bloqueo de cuenta

La función de bloqueo de cuenta está habilitada por defecto. Se recomienda mantenerla habilitada para proteger la seguridad de la cuenta. Tras varios intentos fallidos de contraseña, la cuenta y la dirección IP de origen correspondientes se bloquearán.

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

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

Configuración del servicio

1. Habilitar HTTPS

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

2. Transmisión cifrada de audio y vídeo

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

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

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

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

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

4. Cambiar HTTP y otros puertos de servicio predeterminados

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

Configuración de red

1. Habilitar lista de permitidos

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

2. Vinculación de direcciones MAC

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

3. Construir un entorno de red seguro

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

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

Auditoría de seguridad

1. Comprobar usuarios en línea

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

2. Comprobar el registro del dispositivo

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

3. Configurar el registro de red

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

Seguridad del software

1. Actualizar el firmware a tiempo

Según las especificaciones operativas estándar de la industria, el firmware de los dispositivos debe actualizarse a la última versión oportunamente para garantizar que cuenten con las funciones y la seguridad más recientes. Si el dispositivo está conectado a la red pública, se recomienda activar la función de detección automática de actualizaciones en línea para obtener la información de actualización de firmware publicada por el fabricante de manera oportuna.

2. Actualice el software del cliente a tiempo

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

Protección física

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

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