

Estación de puerta de villa

Manual de usuario



Prefacio

General

Este manual presenta la instalación, funciones y operaciones del dispositivo de estación de puerta de villa (en adelante, "el VTO"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para consultarlo en el futuro.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

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

Revisión histórica

Versión	Contenido de revisión	Fecha de lanzamiento
V1.0.4	Estructura añadida.	mayo 2024
V1.0.3	Descripción del puerto agregada.	febrero 2024
V1.0.2	Estructura añadida.	febrero 2024
V1.0.1	Estructura añadida.	diciembre 2023
V1.0.0	Primer lanzamiento.	agosto 2023

Aviso de protección de privacidad

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

Acerca del Manual

- El manual es sólo para referencia. Pueden encontrarse ligeras diferencias entre el manual y el producto.

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

Salvaguardias y advertencias importantes

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

Requisitos de operación



- Compruebe si la fuente de alimentación es correcta antes de su uso.
- No desenchufe el cable de alimentación en el costado del dispositivo mientras el adaptador esté encendido.
- Opere el dispositivo dentro del rango nominal de entrada y salida de energía.
- Transporte, utilice y almacene el dispositivo en las condiciones permitidas de humedad y temperatura.
- Si el dispositivo permanece apagado durante más de un mes, debe colocarse en su paquete original y sellarse. Asegúrese de mantenerlo alejado de la humedad y guárdelo en las condiciones permitidas de humedad y temperatura.
- No deje caer ni salpique líquido sobre el dispositivo y asegúrese de que no haya ningún objeto lleno de líquido sobre el dispositivo para evitar que el líquido fluya hacia él.
- No desmonte el dispositivo sin instrucción profesional.

requerimientos de instalación



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



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

Tabla de contenido

Prefacio.....	I Medidas de seguridad 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 (botón único).....		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.....		12
1.3 Modelo de botón.....		23
1.3.1 Panel frontal.....		23
1.3.2 Panel trasero.....		24
2 Inicializando el VTO.....		26
2.1 Internet.....		26
2.2 APLICACIÓN DMSS.....		26
3 Iniciar sesión y restablecer la contraseña.....		30
3.1 Iniciar sesión.....		30
3.2 Restablecer la contraseña.....		30
4 Página de inicio.....		31
5 Asistente de configuración.....		32
5.1 Configuración como servidor SIP.....		32
5.2 No configurar como servidor SIP.....		33
6 Configuración del dispositivo local.....		34
6.1 Configuraciones básicas.....		34
6.1.1 Estación de puerta de villa.....		34
6.1.2 Segunda Estación de Confirmación.....		37
6.2 Control de acceso.....		39
6.2.1 Configuración.....		39
6.2.2 RS-485.....		40
6.2.3 Configurar la contraseña.....		41
6.3 Configuración de Wiegand.....		42
6.4 Diseño.....		43
6.4.1 Diseño (varios botones).....		43
6.4.2 Diseño (múltiples módulos).....		45

6.5 Agregar el IPC.....	46
6.5.1 Agregar el IPC uno por uno.....	46
6.5.2 Exportación de la información de IPC en lotes.....	48
6.5.3 Importación de la información de IPC en lotes.....	48
7 Sistema.....	49
7.1 Vídeo.....	49
7.2 Audio.....	51
7.3 Tiempo.....	52
7.4 Usuario ONVIF.....	54
7.5 Configuración.....	55
7.6 Mantenimiento.....	55
7.7 Actualización.....	56
7.8 Información Legal.....	56
7.9 Información del sistema.....	56
8 Configuración del dispositivo.....	58
8.1 Gestión del n° de VTO.....	58
8.2 Gestión de VTH.....	59
8.3 Gestión del VTS.....	61
9 Gestión de personas.....	63
10 Configuración de red.....	67
10.1 TCP/IP.....	67
10.2 Puerto.....	68
10.3 Servidor SIP.....	68
10.4 Segunda estación de confirmación en cascada.....	72
10.5 Servicio de almacenamiento en la nube.....	73
10.6 UPnP.....	73
10.6.1 Habilitación de servicios UPnP.....	74
10.6.2 Agregar servicios UPnP.....	74
10.7 Wifi.....	76
10.8 Servicios basicos.....	76
11 Gestión de registros.....	79
11.1 Historial de llamadas.....	79
11.2 Registros de alarmas.....	79
11.3 Desbloquear registros.....	80
11.4 Registro.....	80
12 Gestión de seguridad.....	82
12.1 Estado de seguridad.....	82
12.2 Servicio del sistema.....	82
12.3 Defensa de ataque.....	83
12.3.1 Cortafuegos.....	83

12.3.2 Bloqueo de cuenta.....	84
12.3.3 Ataque Anti-DoS.....	85
12.4 Certificado CA.....	85
12.5 Cifrado de vídeo.....	86
12.6 Advertencia de seguridad.....	86
Configuración del modelo de 13 botones.....	88
13.1 Conexión de cables.....	88
13.2 Configuración VTH.....	89
Apéndice 1 Recomendaciones de ciberseguridad.....	91

1 estructura

1.1 Estación de puerta de villa (varios botones)

1.1.1 Panel frontal

Figura 1-1 Panel frontal

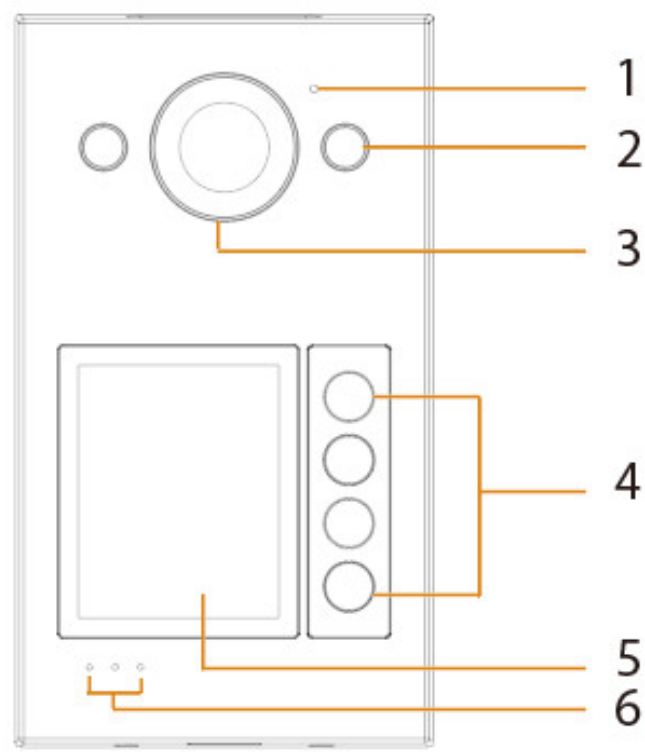


Tabla 1-1 Componentes

No.	Nombre	Función
1	micrófono	Entrada de audio.
2	Iluminador	Proporciona una luz constante para enfocar más fácilmente un sujeto en un entorno oscuro.
3	Cámara	Capture imágenes o grabe vídeos para el VTO.
4	Botones de llamada	Llame al VTH.
5	Área para pasar tarjetas	Pase las tarjetas registradas para desbloquear las puertas.
6	Indicadores	De izquierda a derecha: ● Timbre: VTO está llamando al VTH. ● Hablando: VTO está hablando con VTH. ● Desbloqueo: Desbloqueo de VTO exitoso.

1.1.2 Panel trasero



El puerto multifunción puede diferir según los modelos reales.

Figura 1-2 Panel trasero

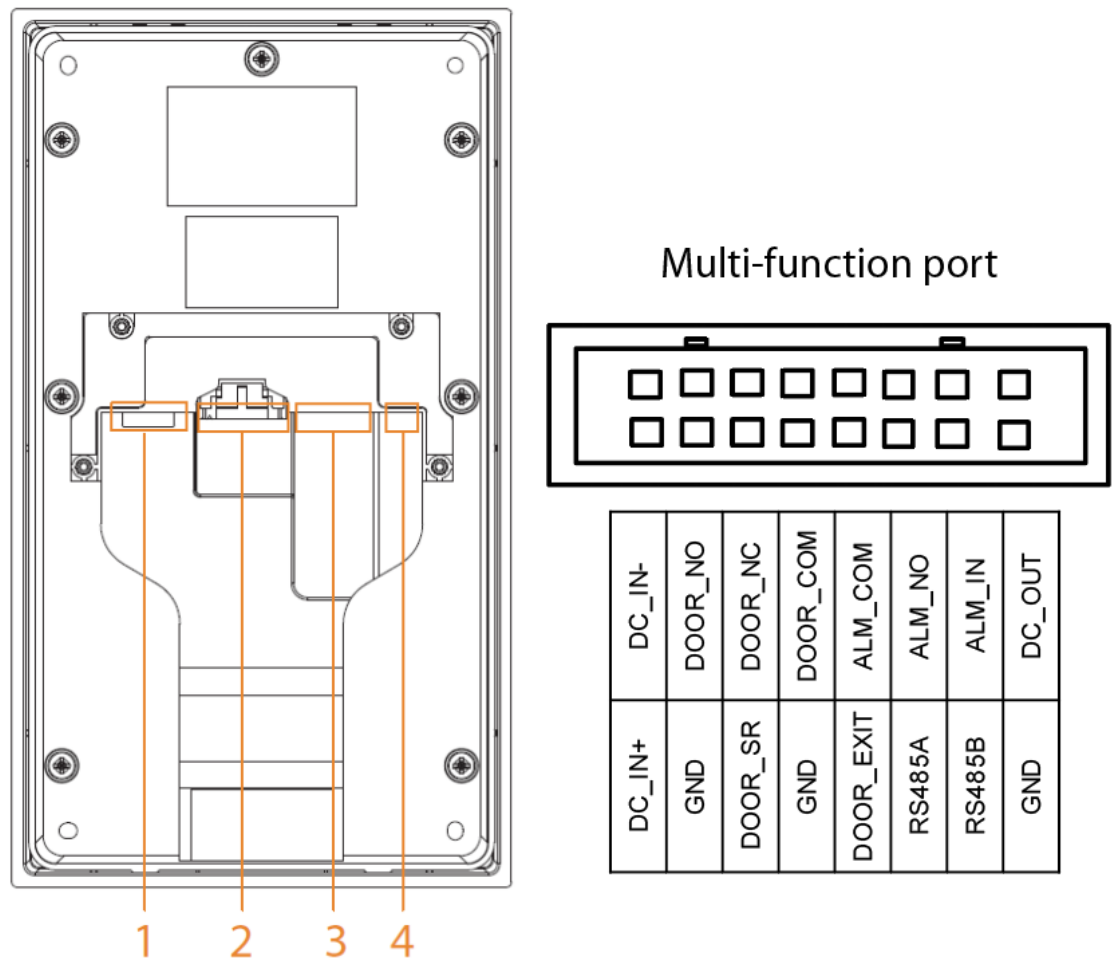


Tabla 1-2 Componentes

No.	Nombre	Función
1	ranura para tarjetas SD	Se utiliza para insertar una tarjeta SD para poder almacenar información de datos, 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 de producto.

Figura 1-3 Panel frontal

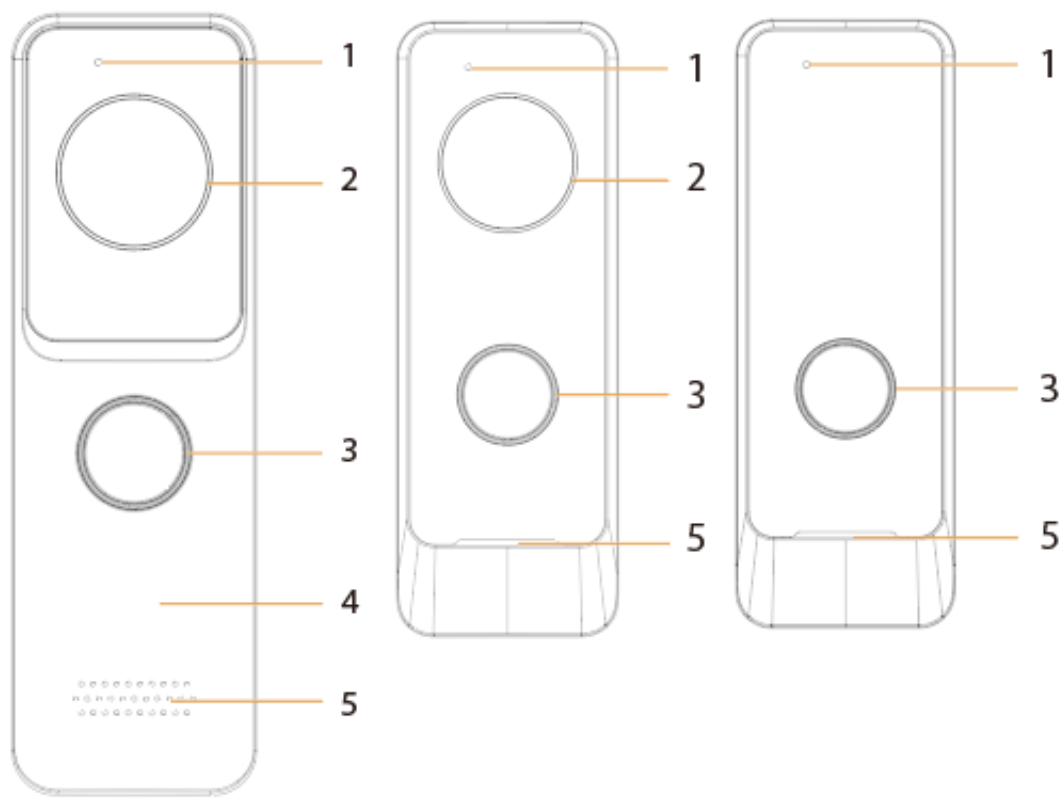


Tabla 1-3 Componentes

No.	Nombre	Función
1	micrófono	Entrada de audio.
2	Cámara	Capture imágenes o grabe vídeos para el VTO.
3	Botón de llamada	Llame al VTH.
4	Área para pasar tarjetas	Pase las tarjetas registradas para desbloquear las puertas. La función de deslizar la tarjeta solo está disponible en modelos selectos.
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 utilizados como ejemplos.

Figura 1-4 Panel trasero (1)

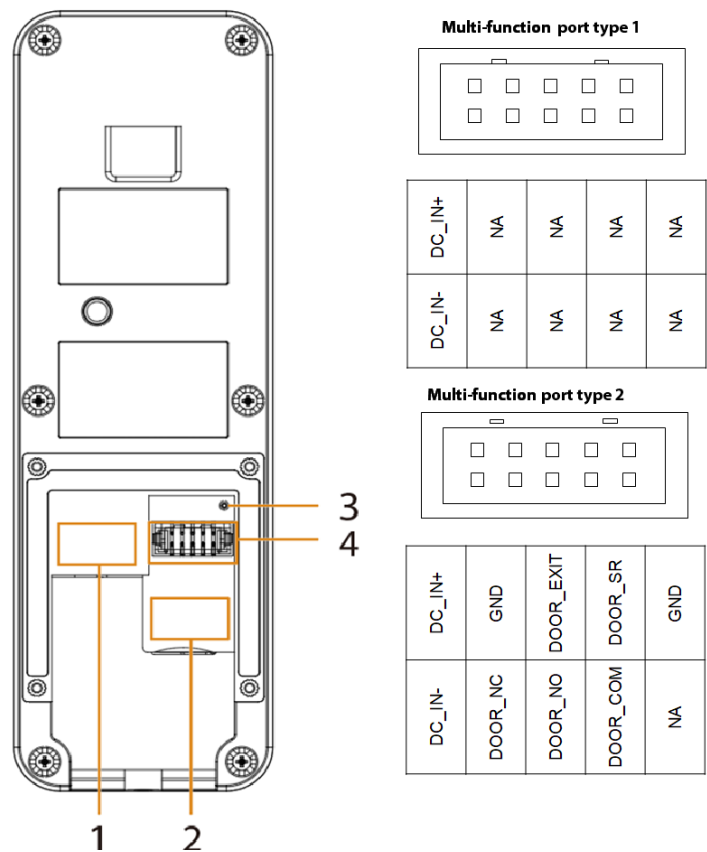


Tabla 1-4 Componentes

No.	Nombre	Función
1	Puerto de red	Se conecta a la red.
2	ranura para tarjetas SD	Inserte la tarjeta SD para poder almacenar información de datos, como imágenes y videos.
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 alimentación y un puerto detector de puerta.

Figura 1-5 Panel trasero (2)

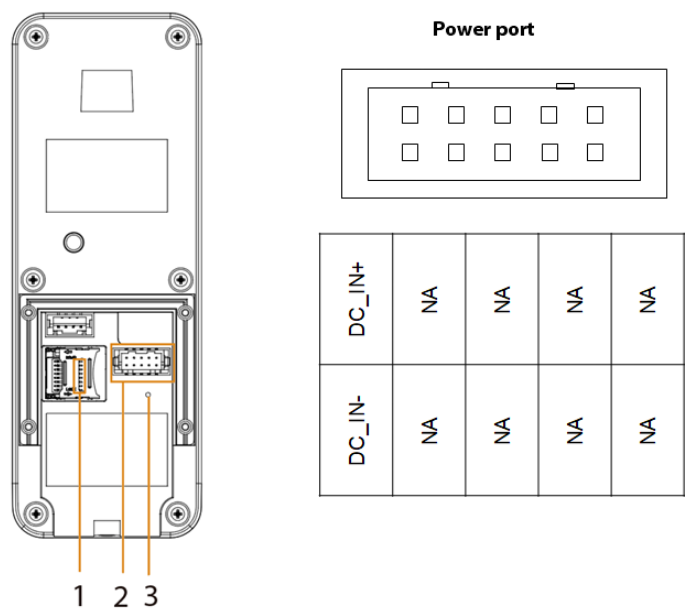


Tabla 1-5 Componentes

No.	Nombre	Función
1	ranura para tarjetas SD	Inserte la tarjeta SD para poder almacenar información de datos, como imágenes y videos.
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

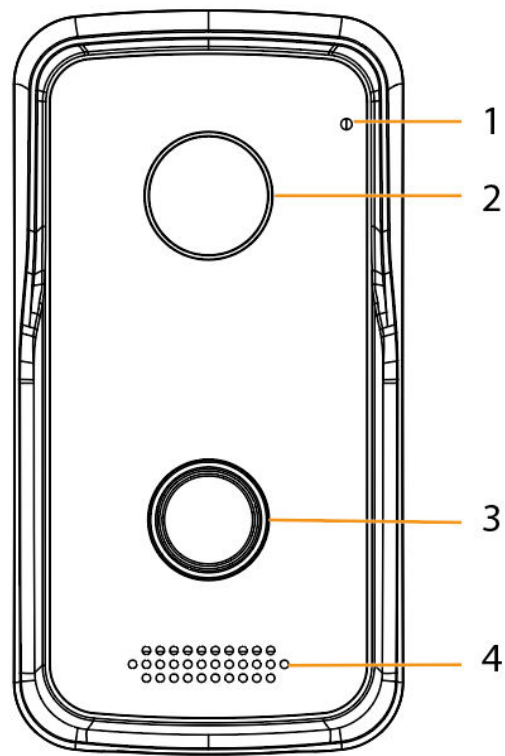


Tabla 1-6 Componentes

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

1.2.2.2 Panel trasero

Figura 1-7 Panel trasero

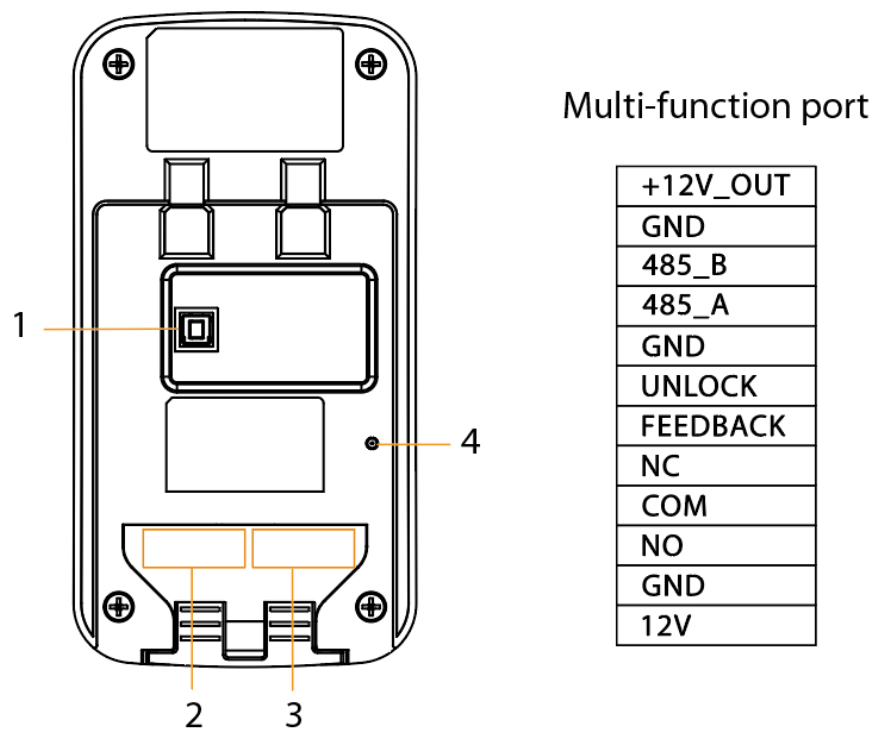


Tabla 1-7 Componentes

No.	Nombre	Función
1	Botón de manipulación	- Después de retirar el dispositivo instalado de la pared u otros lugares, el dispositivo emitirá un pitido y se generará el registro de alarma. - Dentro de los 5 minutos posteriores a que se enciende el dispositivo, si presiona el botón de manipulación 5 veces en 8 segundos, el dispositivo emite un pitido y elimina la información de la cuenta. Se generará el registro de alarma.
2	Puertos multifunción	Puerto de alarma, puerto 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.

1.2.3 Serie G

1.2.3.1 Panel frontal

Figura 1-8 Panel frontal

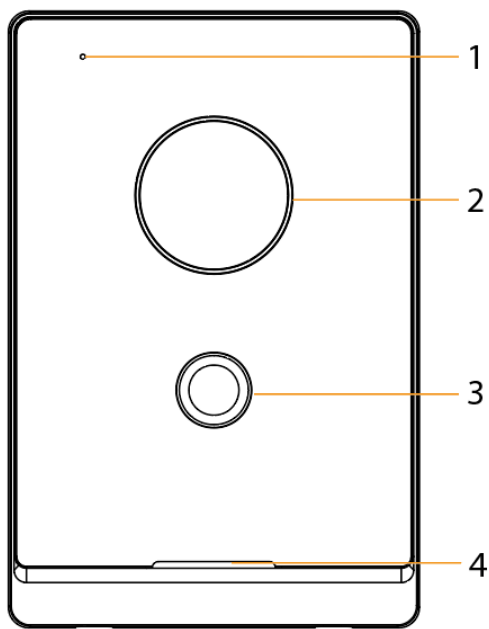


Tabla 1-8 Componentes

No.	Nombre	Función
1	micrófono	Entrada de audio.
2	Cámara	Capture imágenes o grabe vídeos para el VTO.
3	Botón de llamada	Llame al VTH. El botón muestra diferentes colores en diferentes estados. ● En espera: sin luz. ● Llamada no contestada: Verde fijo. ● Llamada respondida: 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 de respiración verde.
4	Vocero	Salida de audio.

1.2.3.2 Panel trasero

Figura 1-9 Panel trasero

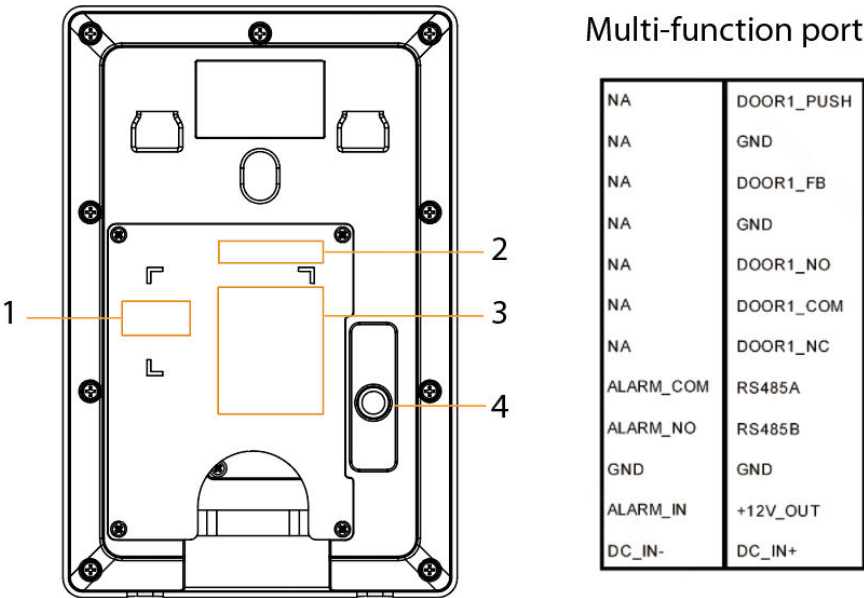


Tabla 1-9 Componentes

No.	Nombre	Función
1	Puerto de red	Se conecta a la red.
2	Puerto multifunción	Puerto de alarma, puerto detector de puerta, puerto 485, puerto de alimentación y más.
3	ranura para tarjetas SD	Inserte la tarjeta SD para poder almacenar información de datos, como imágenes y videos.
4	Botón de manipulación	- Después de retirar el dispositivo instalado de la pared u otros lugares, el dispositivo emitirá un pitido y se generará el registro de alarma. - Dentro de los 5 minutos posteriores a que se enciende el dispositivo, si presiona el botón de manipulación 5 veces en 8 segundos, el dispositivo emite un pitido y elimina la información de la cuenta. Se generará el registro de alarma.

1.2.4 Serie E

1.2.4.1 Panel frontal

Figura 1-10 Panel frontal

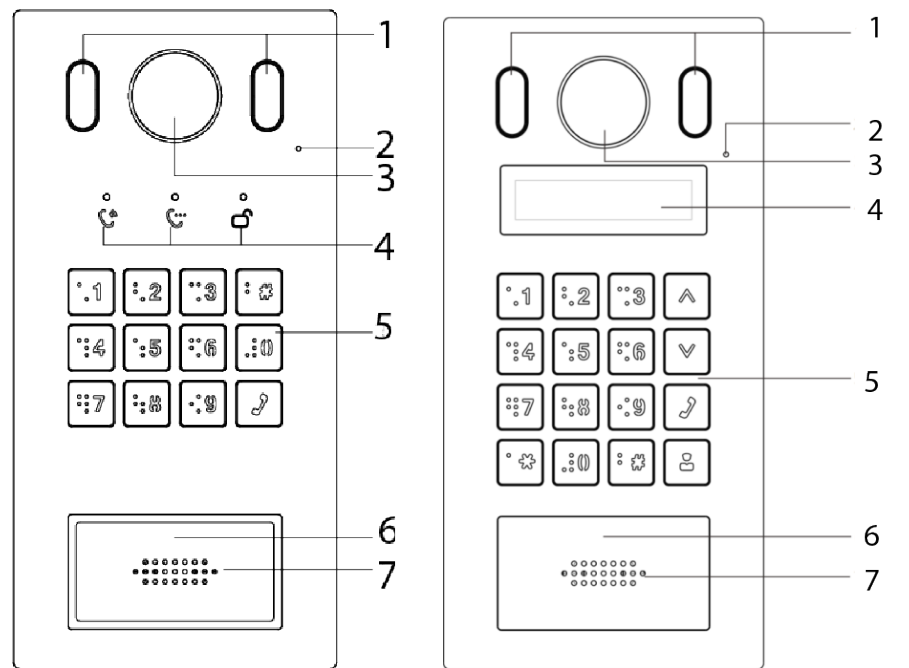


Tabla 1-10 Descripción del panel frontal

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

1.2.4.2 Panel trasero

Figura 1-11 Panel trasero

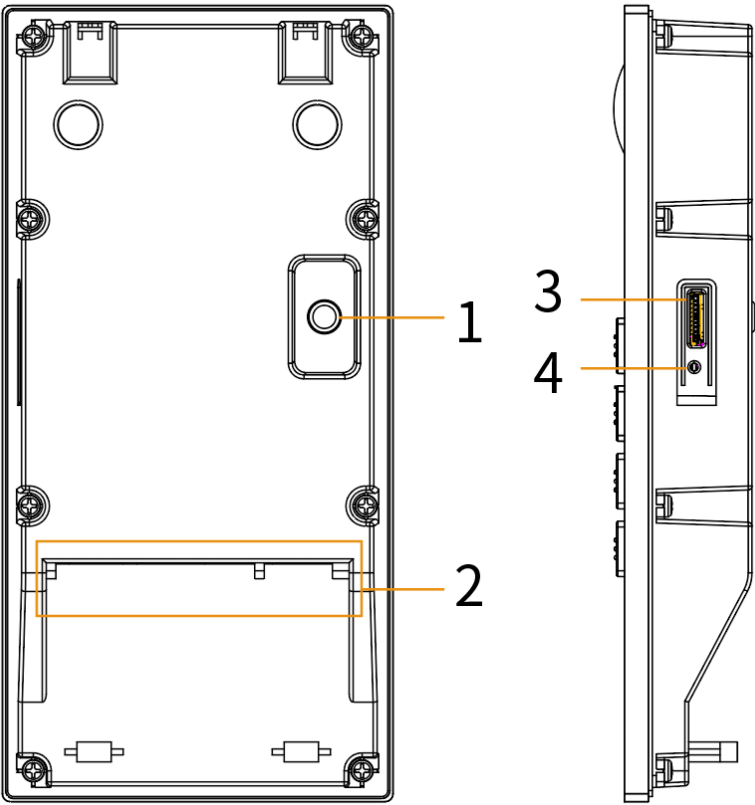
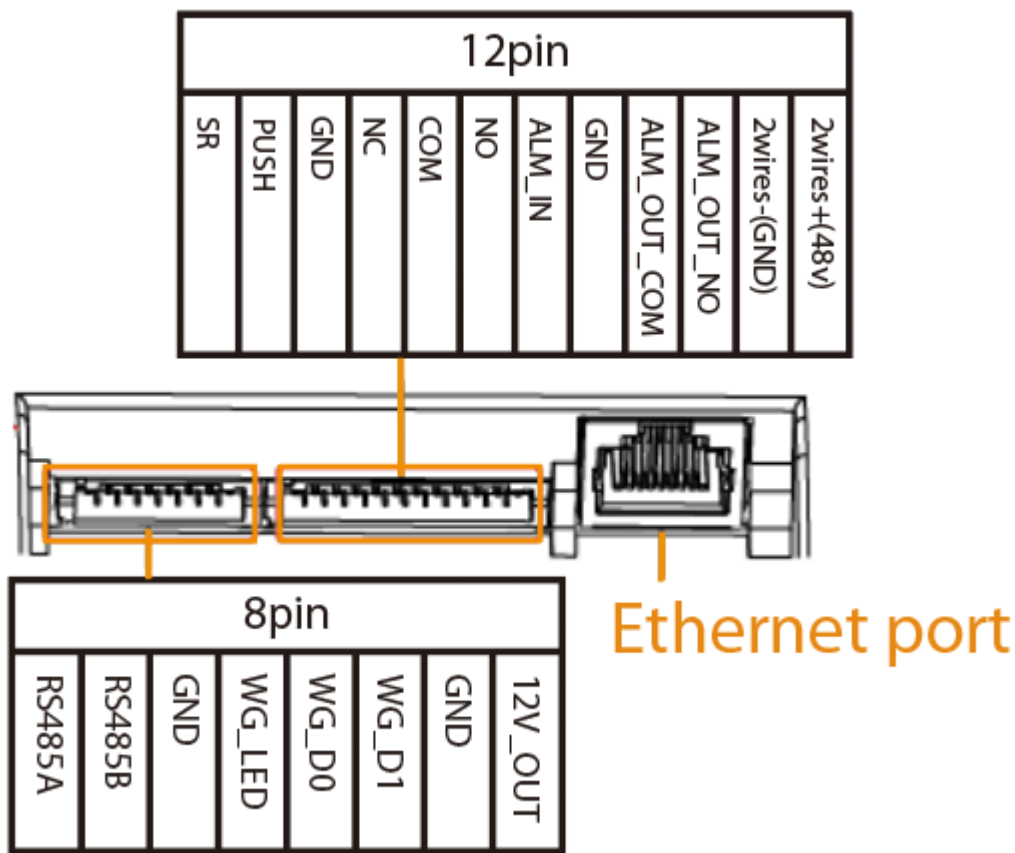


Tabla 1-11 Descripción del panel trasero

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

Figura 1-12 Puerto multifunción



1.2.5 Serie F

1.2.5.1 Panel frontal

Figura 1-13 Panel frontal

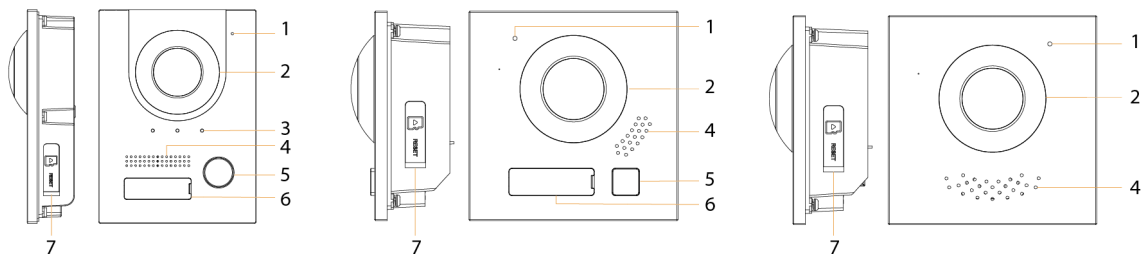


Tabla 1-12 Descripción del panel frontal

No.	Nombre	Descripción
1	Micrófono	Entrada de audio.
2	Cámara	Capture imágenes o grabe vídeos para el VTO.

No.	Nombre	Descripción
3	Indicadores	Muestra el estado al llamar, hablar y desbloquear.
4	Vocero	Salida de audio.
5	Botón de llamada	Llame al VTH y al centro de gestión.
6	Placa de nombre	Muestra la información personalizada.
7	Ranura para tarjeta y botón de reinicio	● Inserte la tarjeta SD para poder almacenar información de datos, como imágenes y videos. ● Mantenga presionado el botón durante varios segundos para restablecer la configuración de fábrica.

1.2.5.2 Panel trasero

Figura 1-14 Panel trasero

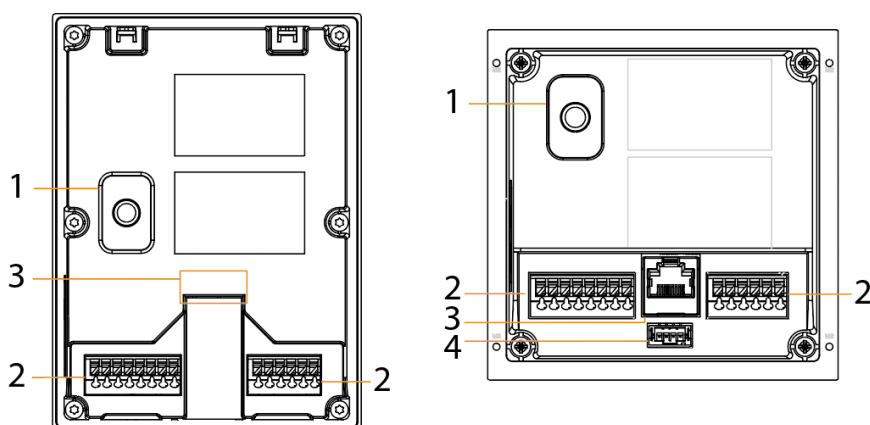


Tabla 1-13 Descripción del panel trasero

No.	Nombre	Función
1	Botón de manipulación	● Después de retirar el dispositivo instalado de la pared u otros lugares, el dispositivo emitirá un pitido y se generará el registro de alarma. ● Dentro de los 5 minutos posteriores a que se enciende el dispositivo, si presiona el botón de manipulación 5 veces en 8 segundos, el dispositivo emite un pitido y elimina la información de la cuenta. Se generará el registro de alarma.
2	Puertos multifunción	Puerto de alarma, puerto detector de puerta, puerto 485, puerto de alimentación y más.
3	Puerto de red	Conéctese a la red.
4	Puerto de conexión en cascada	Conéctese a otros módulos.

Figura 1-15 Puertos multifunción

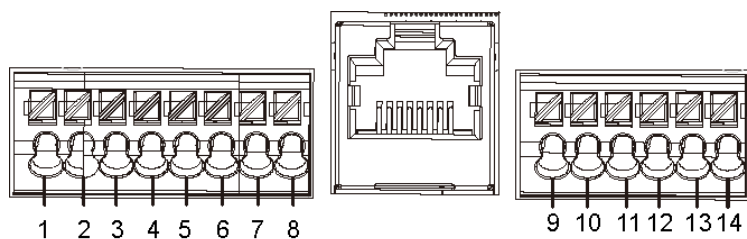


Tabla 1-14 Descripción del puerto

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	+ 12V_SALIDA	9	PUERTA_BOTÓN
3	RS-485_B	10	PUERTA_FEEDBACK
4	RS-485_A	11	Tierra
5	ALARMA_NO	12	PUERTA_NC
6	ALARMA_COM	13	PUERTA_COM
7	● 2 cables+(48V) para una cámara digital de 2 hilos módulo ● 12 V_IN para un completamente digital Módulo de cámara	14	PUERTA_NO

1.2.5.3 Módulo indicador

Figura 1-16 Panel frontal

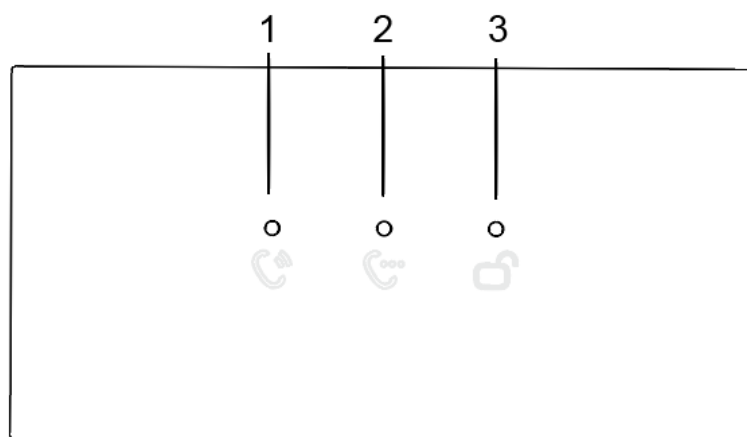


Tabla 1-15 Descripción del panel frontal

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

Figura 1-17 Panel trasero

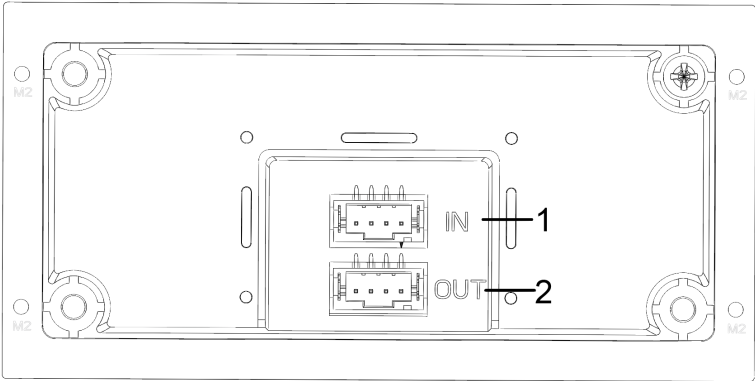


Tabla 1-16 Descripción del panel trasero

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

1.2.5.4 Módulo de botones

El módulo de un botón, el módulo de dos botones y el módulo de cinco botones están disponibles con la misma función. Aquí tomamos como ejemplo el módulo de cinco botones.

Figura 1-18 Panel frontal del módulo de cinco botones

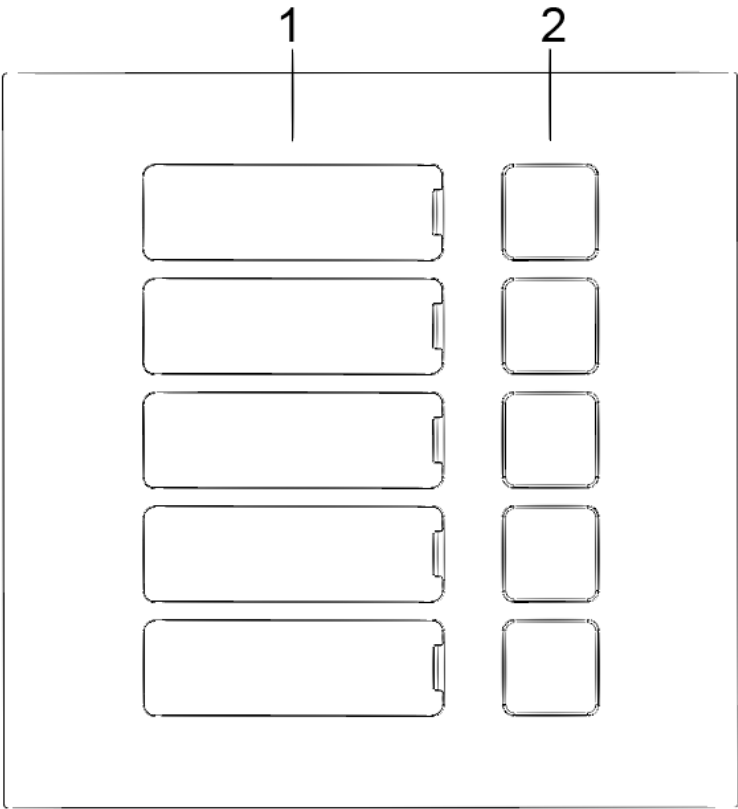


Tabla 1-17 Descripción del panel frontal

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

Figura 1-19 Panel trasero del módulo de cinco botones

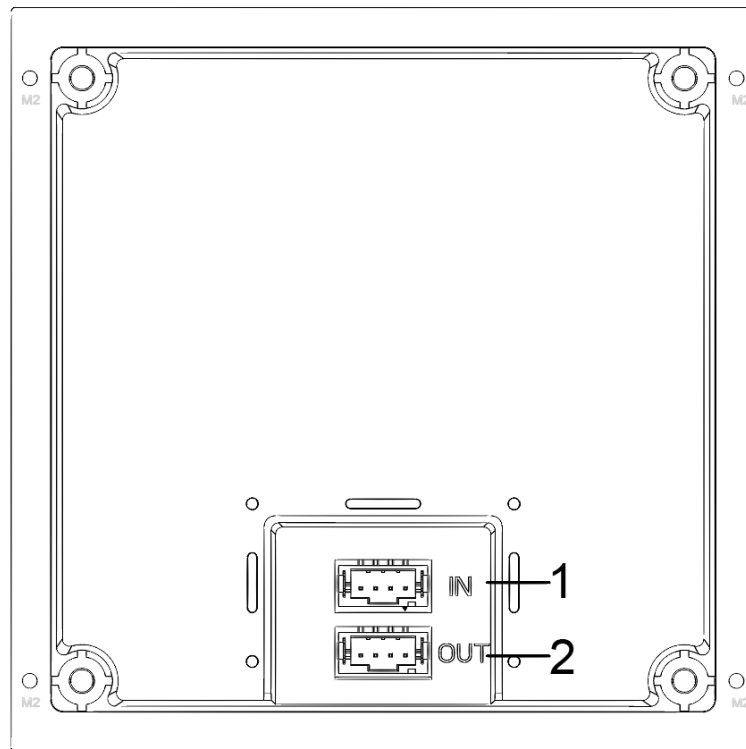


Tabla 1-18 Descripción del panel trasero

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

1.2.5.5 Módulo de teclado (con Braille)



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

Figura 1-20 Módulo de teclado

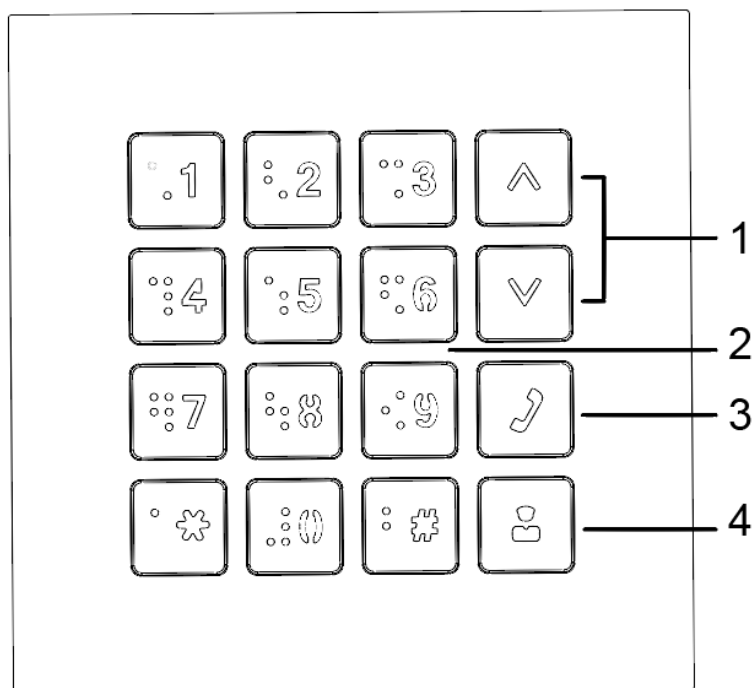


Tabla 1-19 Descripción del módulo de teclado

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

1.2.5.6 Módulo de tarjeta

Hay 2 tipos de módulo de tarjeta. Seleccione entre el módulo de tarjeta de identificación y el módulo de tarjeta IC según sea necesario.



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

Figura 1-21 Módulo de tarjeta



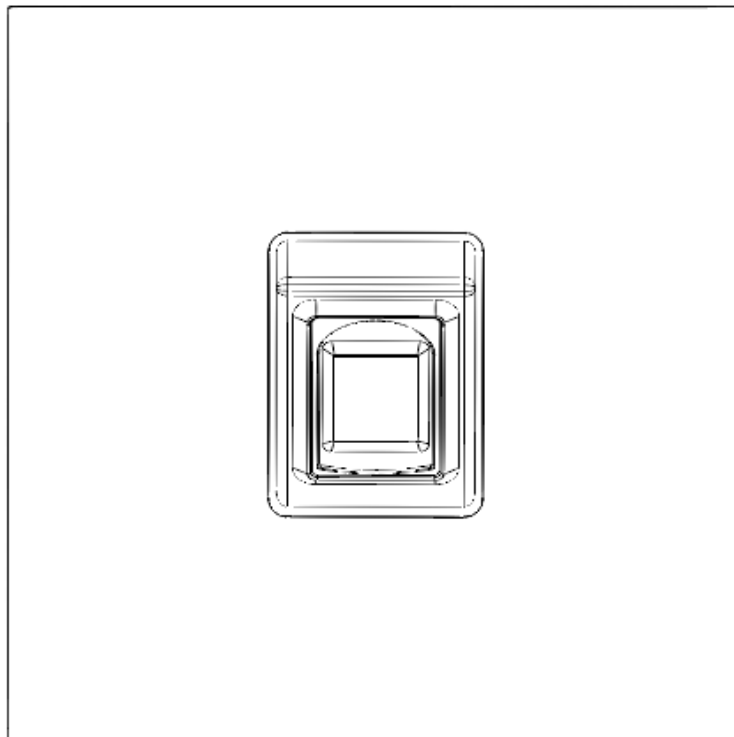
1.2.5.7 Módulo de huellas dactilares

Recoge y verifica huellas dactilares.



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

Figura 1-22 Módulo de huellas dactilares



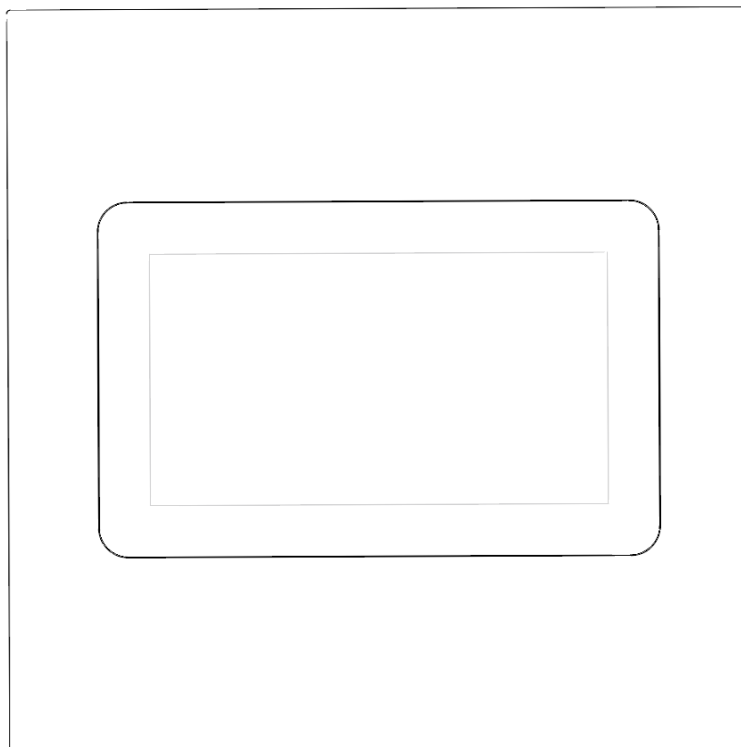
1.2.5.8 Módulo de visualización

Muestra información del usuario.



Los paneles posteriores del módulo de visualización y del módulo de botones tienen diferentes posiciones de puerto, pero las funciones de los puertos son las mismas.

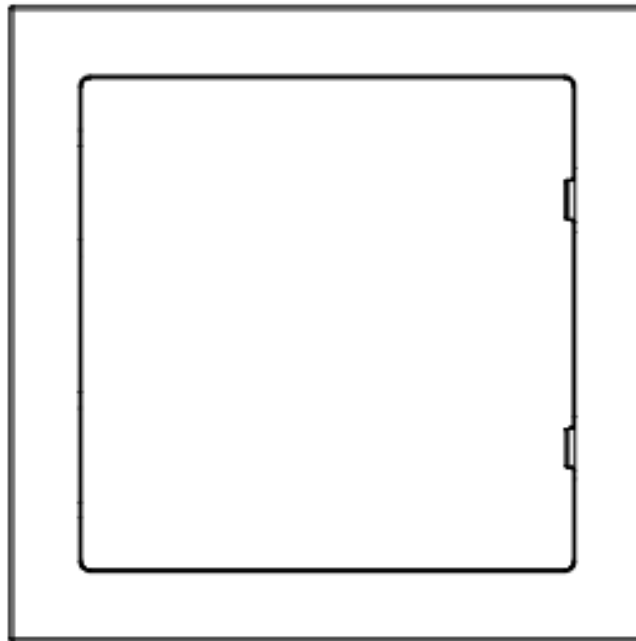
Figura 1-23 Módulo de visualización



1.2.5.9 Módulo de Información

Muestra el número de habitación y el mensaje del huésped.

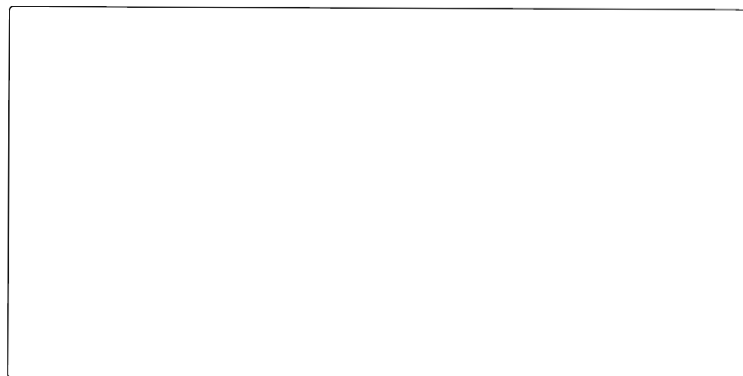
Figura 1-24 Módulo de información



1.2.5.10 Módulo en blanco

Para una mejor apariencia, use el módulo en blanco si hay espacio adicional al colocar los módulos.

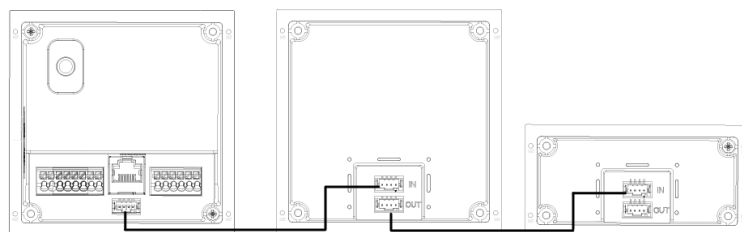
Figura 1-25 Módulo en blanco



1.2.5.11 Conexión en cascada

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

Figura 1-26 Ejemplo de conexión en cascada



1.3 Modelo de botón

1.3.1 Panel frontal

Figura 1-27 Panel frontal

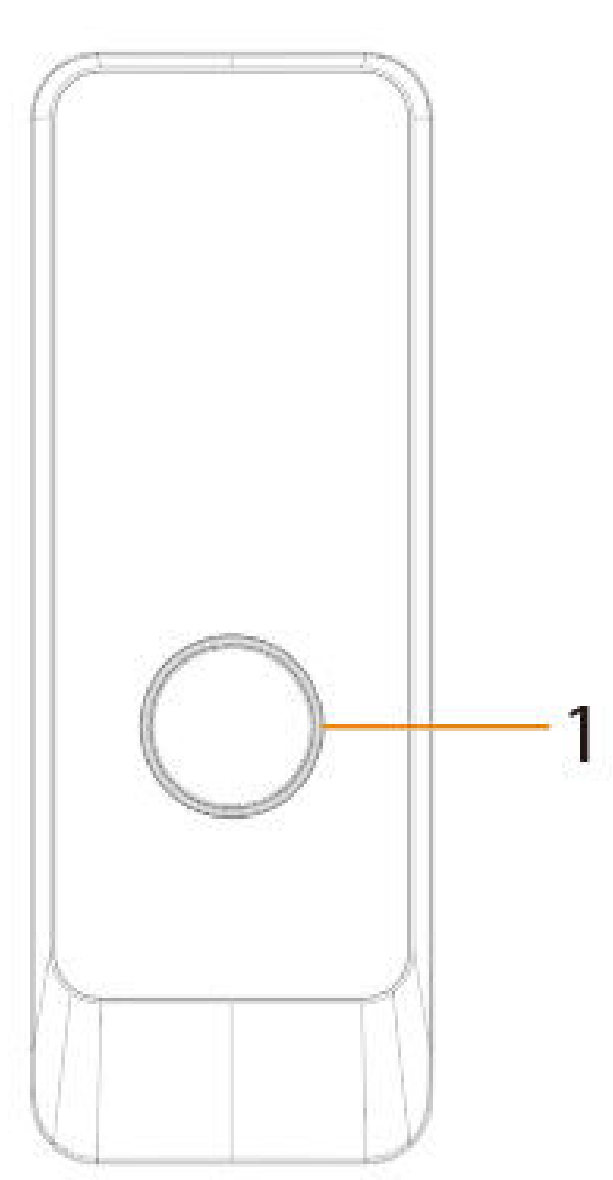


Tabla 1-20 Componentes

No.	Nombre	Función
1	presiona el botón	El modelo de botón se puede conectar al VTH. Presione el botón en el modelo y el VTH recibe una señal de alarma.

1.3.2 Panel trasero

Figura 1-28 Panel trasero

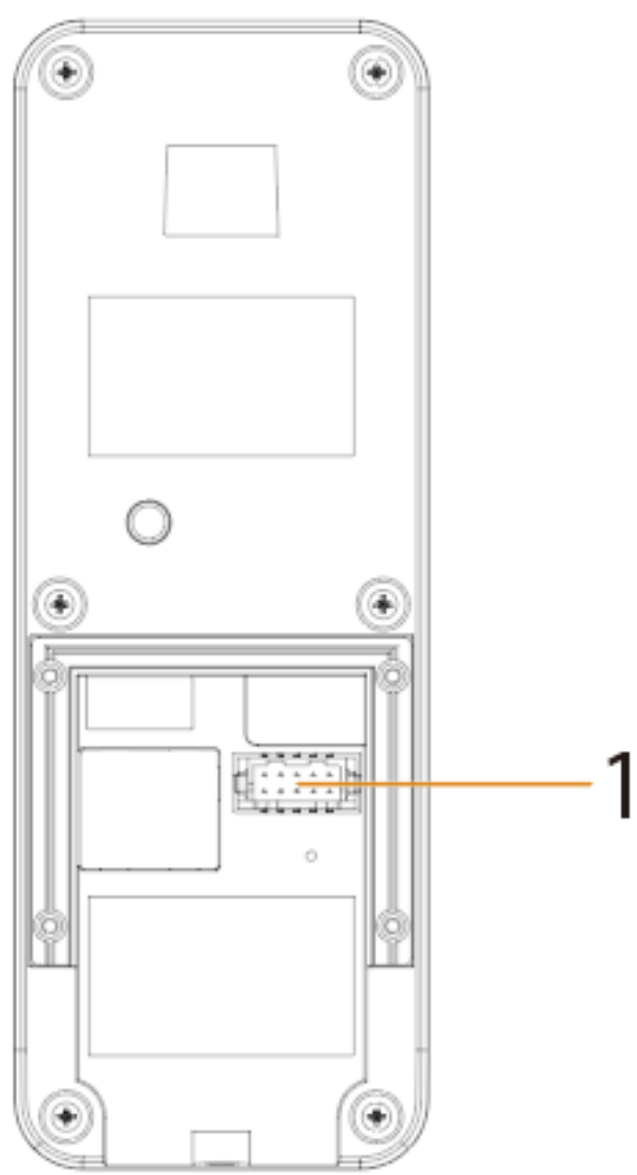
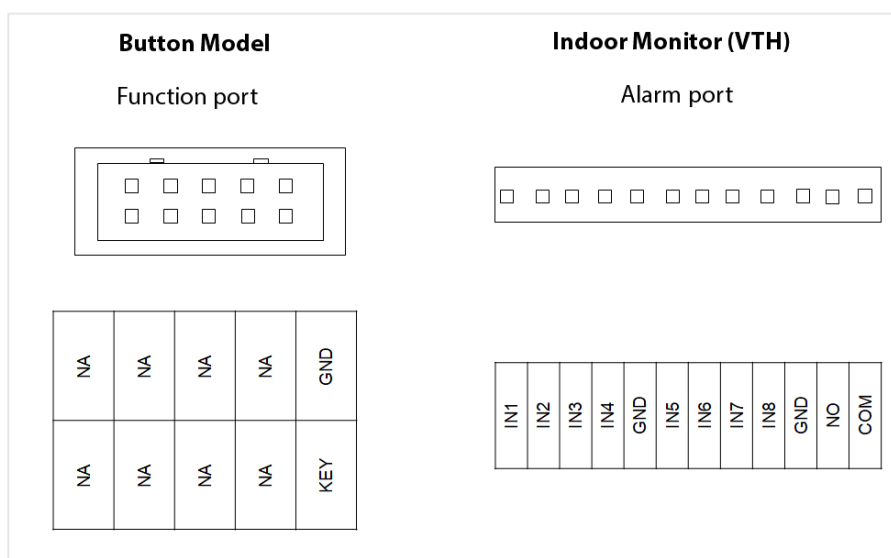


Tabla 1-21 Componentes

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

Figura 1-29 Conexión de cables



Conecte el puerto KEY del modelo de botón a cualquiera de los puertos de entrada de alarma del monitor interior (VTH) con un hilo de cable. Después de eso, 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 Inicializando el 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 Sobre el **Inicio del dispositivo** página, ingrese y confirme la contraseña y luego haga clic en **Próximo**.



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

Etapas 4 Seleccione el **Correo electrónico** casilla de verificación e ingrese una dirección de correo electrónico para restablecer la contraseña. Hacer clic

Paso 5 **Próximo**.

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

Paso 7 Ingrese 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 puede inicializar el VTO en la aplicación DMSS. Para conocer el funcionamiento detallado de la aplicación, consulte su manual de usuario.

Requisitos previos

Ha descargado el DMSS en APP Store (iOS) o Google Play (Android), ha creado una cuenta e 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 el mensaje de voz.



La función de punto de acceso es para permitirle conectar el VTO a la red a través de **configuración de punto de acceso** en la aplicación.

Paso 3 Agregue el VTO a la aplicación DMSS.

1. Sobre el **Hogar** pantalla, toque y luego seleccione **SN/escanear**.

2. Agregue un VTO.

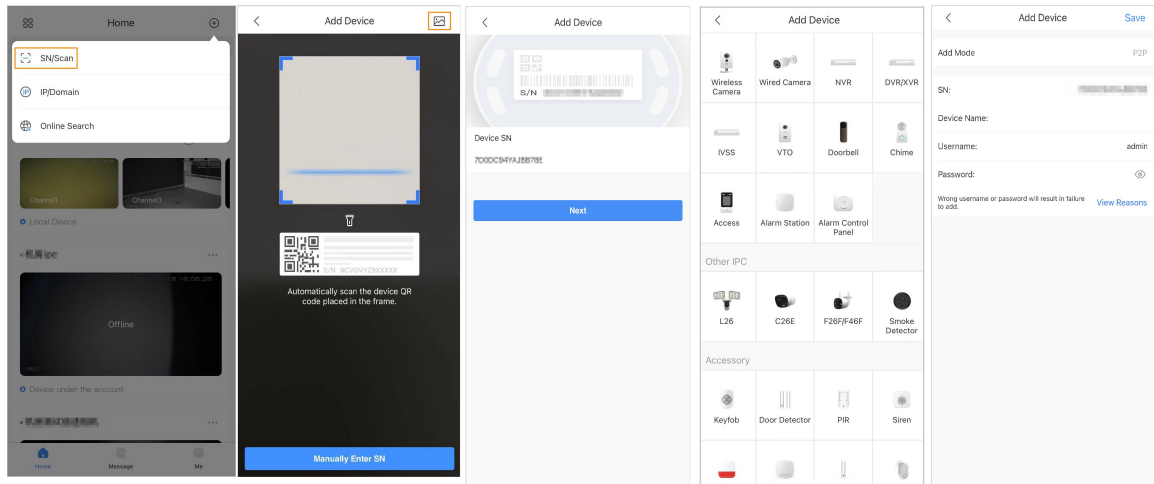
3. Puede agregar escaneando el código QR en el panel trasero del VTO.

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



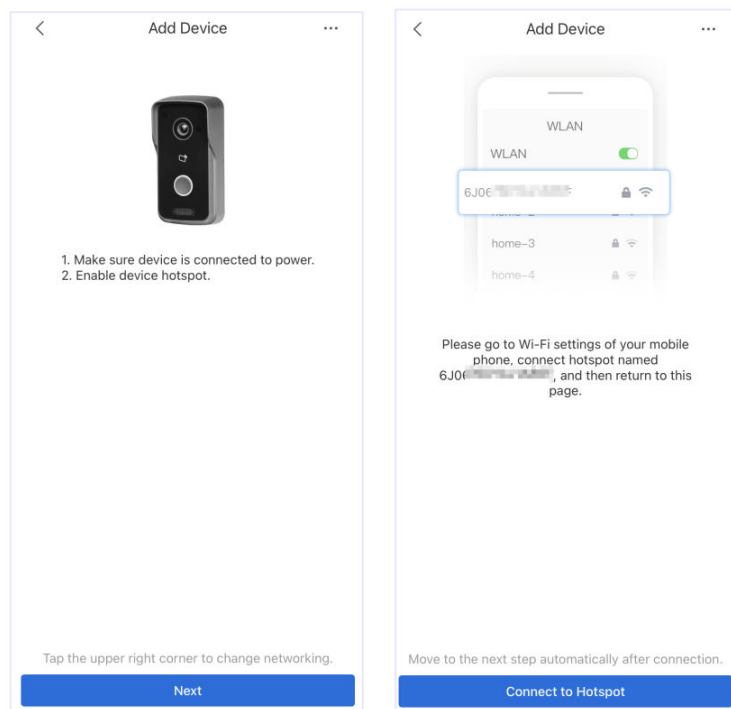
7. Configure la red cambiando la red a **Configuración de punto de acceso**, y luego toque **Próximo**.

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



Etapas 4 Complete la inicialización según las instrucciones de la aplicación.

1. Ingrese la contraseña que planeó para el VTO, confírmela y luego toque **Próximo**.

2. Seleccione **Acceso a la nube** y **Verificación automática** y luego toque **DE ACUERDO**.

El proceso de inicialización está completo.

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

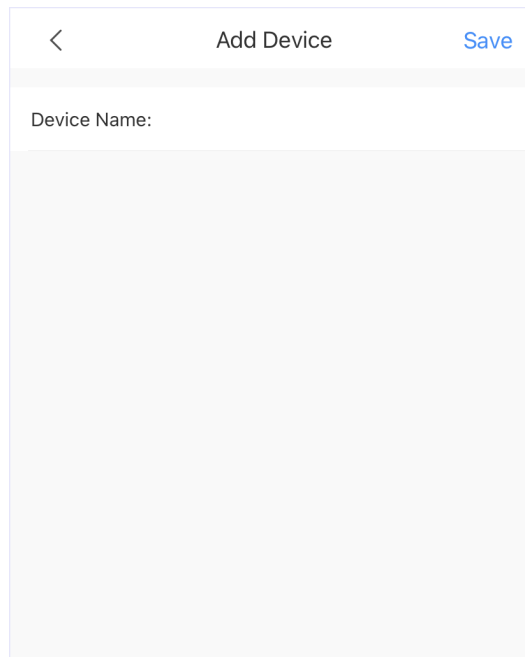
Add Device

Connecting to the router... 58

Cancel Config

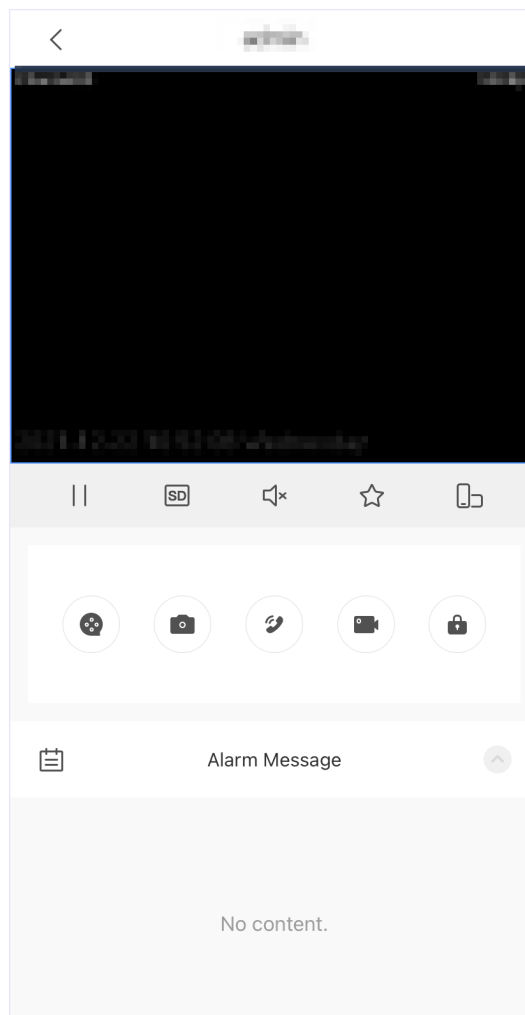
Paso 6 Configure el nombre del dispositivo y luego toque**Ahorrar**.

Figura 2-5 Configurar el nombre del dispositivo



Paso 7 Vea el vídeo de seguimiento desde la cámara del VTO.

Figura 2-6 Monitorear



3 Iniciar sesión y restablecer la contraseña

3.1 Iniciar sesión

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

Procedimiento

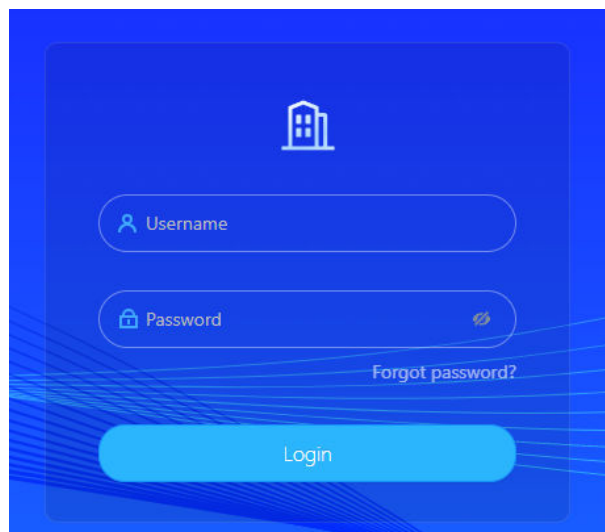
Paso 1 Vaya a la dirección IP del VTO en el navegador.



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

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

Figura 3-1 Iniciar sesión



3.2 Restablecer 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**. Escanee el código QR y obtendrá 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.

Etapa 4 Ingrese 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 al cliente para obtener ayuda.
- El código de seguridad será válido sólo durante 24 horas después 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

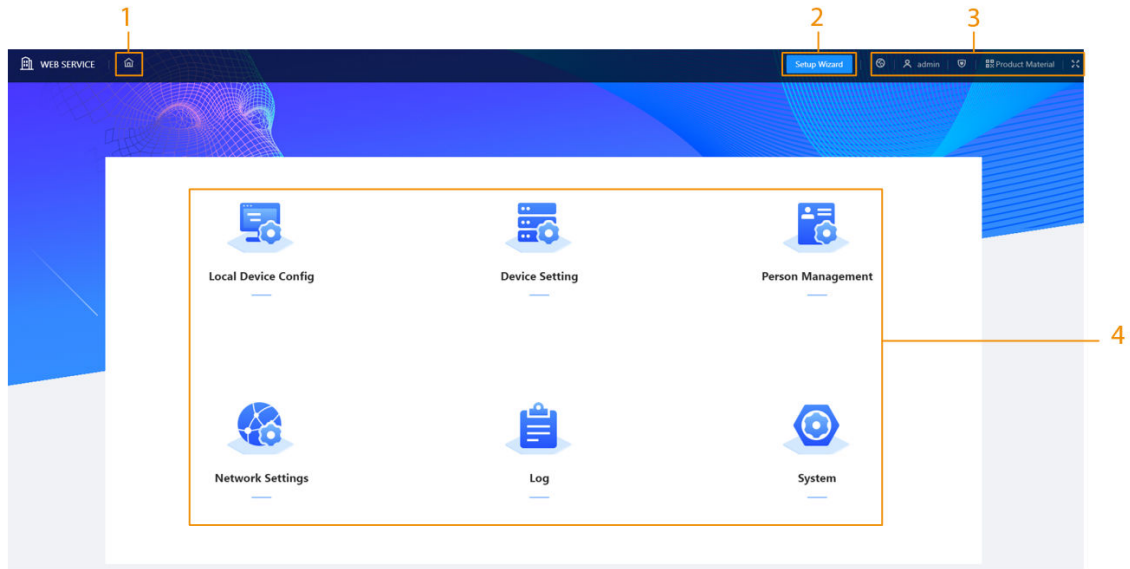


Tabla 4-1 Introducción a la página de inicio

No.	Función	Descripción
1	Botón de inicio	Vuelve a la página de inicio.
2	Asistente de configuración	Configure el servidor SIP de VTO.
3	Barra de navegación	: Cambiar idioma de la página web del VTO. : cambie la contraseña, cierre sesión en el dispositivo actual, reinicie el sistema y restaure el dispositivo a la configuración de fábrica. : vea y configure los ajustes de seguridad. : Escanee el código QR para obtener el materiales del producto. : vea la página web en modo de pantalla completa.
4	función VTO	Diferentes áreas funcionales de la VTO.

5 Asistente de configuración

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

5.1 Configuración como servidor SIP

Configure el VTO como servidor SIP.

Requisitos previos

Ha agregado VTO en la página web. Si no, puedes agregarlos **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** Seleccione **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 buttons: 'Set as SIP Server' (highlighted in blue) and 'Do not Set as SIP Server'. 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 ha tenido uno que funcione como servidor SIP.

Figura 5-2 Seleccione el servidor SIP

The screenshot shows a table with columns: Device Type, SIP No., IP Address, Online Status, and Operation. The table lists 11 records. The first record is a VTO (8001, 127.0.0.1, Online) and the rest are VTHs (990140 to 990148, all Offline). The 'Operation' column contains edit and delete icons. At the bottom, there are navigation buttons (Exit, Back, OK) and pagination controls (1/11 records, 10/page, Go to, 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	

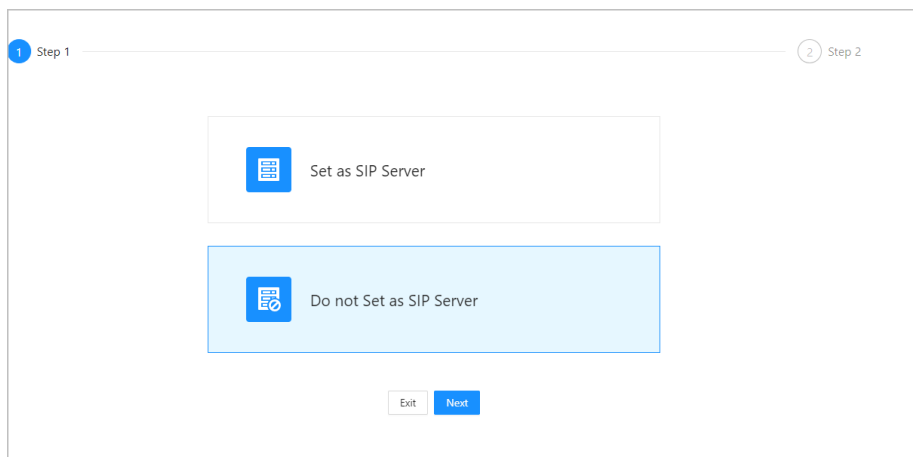
5.2 No configurar como servidor SIP

Si desea cambiar el servidor SIP, debe 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 configurar como servidor SIP** y luego haga clic en **Próximo**.

Figura 5-3 No configurar como servidor SIP



- 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

A screenshot of a web-based configuration interface for Step 1. At the top, there is a progress bar with two steps: 'Step 1' (active, marked with a blue circle and number 1) and 'Step 2' (inactive, marked with a grey circle and number 2). The main area contains a form with the following fields: 'VTO ID' (text input with value '8002'), 'Server Type' (dropdown menu with value 'Device'), 'IP Address' (text input with value '172.16.1.1'), 'Port' (text input with value '5060'), 'Username' (text input with value '8002'), 'Password' (password input with masked characters), 'SIP Domain' (text input with value 'VDP'), 'SIP Server Username' (text input with value 'admin'), and 'SIP Server Password' (empty text input). At the bottom center, there are three buttons: 'Exit' (grey), 'Back' (grey), and 'OK' (blue).

6 Configuración del dispositivo local

Este capítulo presenta la configuración detallada del VTO.



Se pueden encontrar ligeras diferencias en diferentes modelos.

6.1 Configuraciones básicas

Configure los ajustes básicos del dispositivo.

6.1.1 Estación de puerta de villa

Procedimiento

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

Paso 2 **básicos**. Configure los parámetros.

Figura 6-1 Configuración básica (estación villa)

Local Device Config

Device Type

Villa Station

Device Name

Villa Room No.

9901

VTO ID

8001

Group Call

☒

Management Center

888888

Management Center Call Peri...

00:00:00

-

23:59:59

☐

Call Period

Setting

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	Seleccionar de Estación Villay Apartamento pequeño.  El pequeño apartamento está disponible en modelos selectos.
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 VTH.
ID de VTO	Se utiliza para diferenciar cada VTO y le recomendamos configurarlo según la unidad o el número de edificio, y luego puede agregar VTO al servidor SIP utilizando sus números.  El número no se puede cambiar cuando el VTO actúa como servidor SIP.
Centro de Gestión	888888 de forma predeterminada.
Período de llamada del centro de gestión	Configure el período de tiempo en el que el VTO puede llamar al centro de gestión y luego habilite la función.
Llamada grupal	Habilítelo en el VTO que funciona como servidor SIP, y cuando un VTH principal reciba una llamada, todos los VTH de extensión también recibirán la llamada.
Período de llamada	El período de tiempo en el que el VTO llama a otros dispositivos no está limitado. Hacer clic Configuración para configurar el periodo de llamada en un día/ semana.
Método de almacenamiento	Tarjeta SD por defecto.

Parámetro	Descripción
Uso de la tarjeta SD	Muestra la capacidad total y utilizada de la tarjeta SD. Puedes hacer clic Formatear tarjeta SD para eliminar todos los datos de la tarjeta SD.
Captura automática mientras se desbloquea	Tome una instantánea y guárdela en la tarjeta SD del VTO cuando el VTO se esté desbloqueando.
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 video 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 una llamada	Realice una grabación cuando el VTO esté en una llamada y guárdela en la tarjeta SD del VTO.

Paso 3 Hacer clic **Aplicar**.

6.1.2 Segunda Estación de Confirmación



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

Procedimiento

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

Paso 2 **básicos**. Configure 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 VTH.
ID de VTO	Se utiliza para diferenciar cada VTO y le recomendamos configurarlo según la unidad o el número de edificio, y luego puede agregar VTO al servidor SIP utilizando sus números.  El número no se puede cambiar cuando el VTO actúa como servidor SIP.
Centro de Gestión	888888 de forma predeterminada.
Período de llamada del centro de gestión	Configura la hora si solo deseas recibir llamadas de VTH durante un período específico y luego habilita la función.
Período 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 diferentes series de modelos tienen variadas funciones de control de acceso. A continuación se muestra el ejemplo de configuración del modelo serie Q.

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... 15 s (1-20)

Door Unlocked Duration 2 s (1-20)

Check Door Detector Signal ... ☐

Door Detector Alarm Thresh... 30 s (1-9999)

Door Detector Status ☒ NC ☐ NO

Report Status of Door Detector ☒

Unlock Code 123

Lock ☒ Door 1 Local Lock ☐ Door 2 Lock

IC Card ☒

IC Card Encryption & Verifica... ☐

Apply Refresh Default

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

Parámetro	Descripción
Intervalo entre desbloques consecutivos	La puerta sólo se podrá volver a desbloquear después de ese intervalo.
Duración de la puerta desbloqueada	El tiempo durante el cual la cerradura permanece abierta.
Verifique la señal del detector de puerta antes de cerrar	Habilite la función según sus necesidades.
Umbral de alarma del detector de puerta	El umbral de tiempo en el que se activa la alarma del detector de puerta.

Parámetro	Descripción
Estado del detector de puerta	● CAROLINA DEL NORTE: Normalmente cerrado. ● NO: Normalmente abierto.
Informe del estado del detector de puerta	Sincronice el estado del sensor de puerta con los monitores interiores (VTH).
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.
Cerrar	● Cerradura local de la puerta 1: Bloqueo local. ● Cerradura de la puerta 2: Cerradura RS-485. Seleccione el tipo de bloqueo para desbloquear el bloqueo que seleccione.
Tarjeta IC	Habilite la función para que los usuarios puedan deslizar tarjetas para desbloquear la puerta.
Cifrado y verificación de tarjetas IC	Habilite la función para que el cifrado y la verificación de la tarjeta IC surtan efecto.

Paso 3 Hacer clic **Aplicar**.

6.2.2 RS-485

Procedimiento

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

Paso 2 Configura 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

☒ Door 1 Local Lock
☐ Door 2 Lock

Apply

Refresh

Default

Tabla 6-4 Descripción de RS-485

Parámetro	Descripción
Tipo de puerto	Cerrar por defecto.

Parámetro	Descripción
Intervalo entre desbloques consecutivos	La puerta sólo se podrá volver a desbloquear después de ese intervalo.
Duración del desbloqueo	El tiempo durante el cual la cerradura permanece abierta.
Código de desbloqueo	Puede conectar un teléfono de terceros, como un teléfono SIP, al VTO y usar el comando para abrir la puerta de forma remota. El comando predeterminado es 456.
Cerrar	Selecciona el Cerrar escriba para desbloquear el bloqueo que seleccione. ● Cerradura local de la puerta 1: Bloqueo local. ● Cerradura de la puerta 2: 485 cerradura.

Paso 3 Hacer clic **Aplicar**.

6.2.3 Configurar la contraseña

Configurar la contraseña de apertura de puerta.

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar **Configuración del dispositivo local** > **Control de acceso** > **Configuración de contraseña**.

Figura 6-6 Configuración de contraseña

Add

Export

Import

Clear

Refresh

No.	Username	Password	Operation
1	nvu19	*****	
2	z4qef	*****	
3	6d39f	*****	

Paso 3 Hacer clic **Agregar**.

Figura 6-7 Agregar la contraseña

Add

* Username

2

* Password

OK

Cancel

Etapas 4 Configure el nombre de usuario y la contraseña y luego haga clic en **DE ACUERDO**.

Operaciones relacionadas

- Editar: haga clic  para editar la contraseña.
- Eliminar: haga clic  para eliminar la contraseña.
- Borrar: haga clic **Clarop** para eliminar todas las contraseñas.
- Actualizar: haga clic **Actualizar** para actualizar la página.
- Hacer clic **Exportar** o **Importar** para exportar o importar la contraseña.

6.3 Configuración de Wiegand

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

Procedimiento

- Paso 1 Inicie sesión en la página web.
- Paso 2 Seleccionar **Configuración del dispositivo local** > **Configuración**
- Paso 3 **Wiegand**. Configure los parámetros de Wiegand.

Figura 6-8 Entrada Wiegand

Wiegand Settings

☒ Wiegand Input ☐ Wiegand Output

Apply

Refresh

Default

Figura 6-9 Salida Wiegand

Wiegand Settings

☐ Wiegand Input ☒ Wiegand Output

Transmission Mode

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.

Apply

Refresh

Default

Tabla 6-5 Descripción de los parámetros Wiegand

Parámetro		Descripción
Configuración Wiegand		● Seleccionar Entrada Wiegand cuando hay otros dispositivos de reconocimiento conectados. ● Seleccionar Salida Wiegand cuando el VTO funciona como dispositivo de reconocimiento. Puede conectar el controlador de acceso u otros dispositivos al VTO.
Salida Wiegand	Tipo de salida Wiegand	Seleccione un formato Wiegand para leer números de tarjetas o números de identificación. ● Wiegand26: Lee tres bytes o seis dígitos. ● Wiegand34: Lee cuatro bytes u ocho dígitos. ● Wiegand66: Lee ocho bytes o dieciséis dígitos.
	Ancho de pulso	Ingrese el ancho del pulso y el intervalo de pulso de la salida Wiegand.
	Intervalo de pulso	

Etapas 4 Hacer clic **Aplicar**.

6.4 Diseño

6.4.1 Diseño (varios botones)

Esta función solo está disponible para modelos selectos con múltiples botones (1 botón, 2 botones y 4 botones). A continuación se muestra un ejemplo de configuración para el VTO que tiene un botón instalado en su dispositivo.

Procedimiento

- Paso 1** Inicie sesión en la página web de la VTO. Seleccionar
- Paso 2** **Configuración del dispositivo local** > **Disposición**.
- Paso 3** Haga clic en las placas de identificación al lado de donde instaló los botones y luego seleccione el número de habitación en la lista. **Módulo** quiere unir. 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 están configurados en **Configuración del dispositivo**. Para obtener más información, consulte "8.2 Gestión de VTH".
- Debe configurar el número de habitación según la posición de instalación de los botones. Por ejemplo, si solo ha instalado un botón al lado de la primera placa de identificación, deberá hacer clic en el módulo de la primera placa de identificación para configurar el número de habitación en la página web. Si ha instalado un botón al lado de la cuarta placa de identificación, deberá hacer clic en el módulo de la cuarta placa de identificación para configurar el número de habitación en la página web. Mantenga la regla de configuración anterior cuando instale 2 botones o 4 botones en el VTO y configure los números de habitación correspondientes en la página web.

Figura 6-10 Instalación del cuarto botón

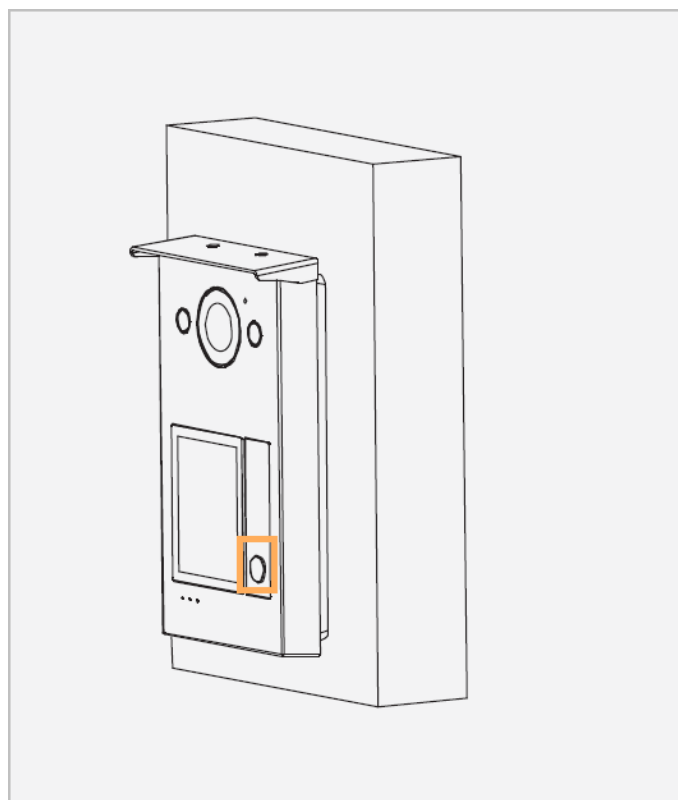


Figura 6-11 Configure la cuarta placa de identificación (1)

Una captura de pantalla de una interfaz de configuración. A la izquierda, hay una representación visual del dispositivo con un recuadro naranja y el número '1' que indica la posición de la cuarta placa de identificación. A la derecha, se encuentra un formulario con el título 'Module' y un botón 'Clear'. Debajo del título, hay cuatro opciones de selección por radio: 9901, 9902, 9903 y 9904. La opción 9904 está seleccionada y resaltada con un recuadro naranja, con el número '2' indicando esta selección. En la parte inferior del formulario, hay dos botones: 'Apply' (en azul) y 'Refresh'.

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

Figura 6-12 Configure la cuarta placa de identificación (2)

The screenshot shows a configuration interface for a VTO device. On the left is a visual representation of the device with a camera and a display showing the number '9904'. On the right is a 'Module' configuration panel with a 'Clear' button and four radio button options: 9901, 9902, 9903, and 9904. The 9904 option is selected. At the bottom of the interface are 'Apply' and 'Refresh' buttons.

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

6.4.2 Diseño (múltiples módulos)

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

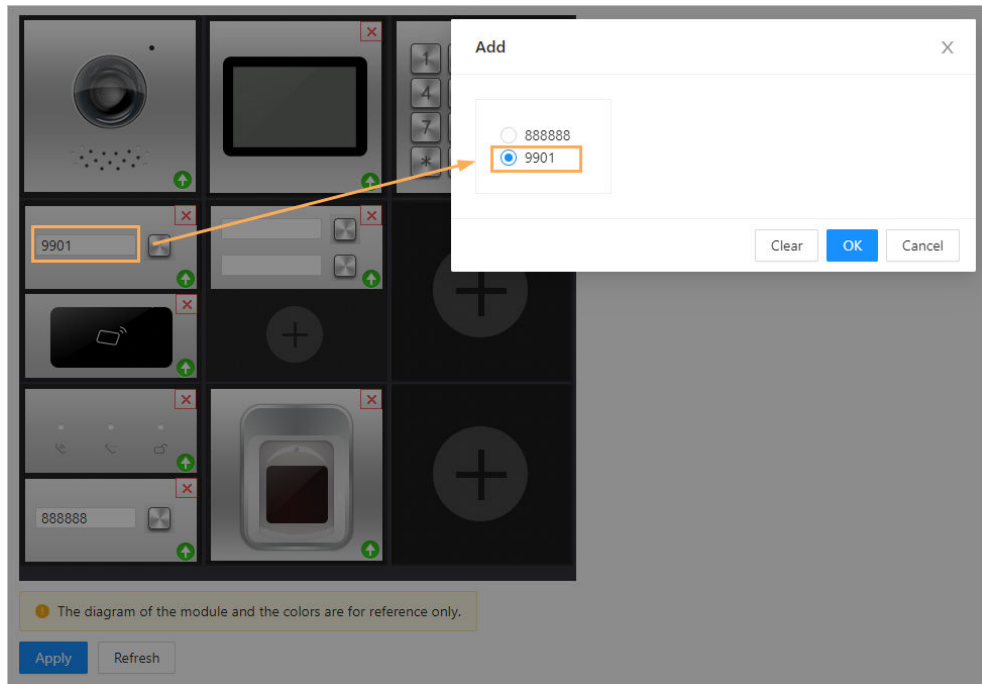
Procedimiento

- Paso 1** Inicie sesión en la página web de la VTO. Seleccionar
- Paso 2** **Configuración del dispositivo local>Disposición.**
- Paso 3** Haga clic en las placas de identificación del módulo correspondiente y luego seleccione el número de habitación que desea vincular.



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 están configurados en **Configuración del dispositivo**. Para obtener más información, consulte "8.2 Gestión de VTH".

Figura 6-13 Configurar la placa de identificación



Etapas Hacer clic **DE ACUERDO** para guardar el número de habitación seleccionado.

Paso 5 Si desea vincular los números de habitación cuando instala otros módulos con placas de identificación para el VTO, repita del Paso 3 al Paso 4 hasta que haya configurado todos los números de habitación.

Operaciones relacionadas

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

6.5 Agregar el IPC

Si el VTO actual funciona como servidor SIP, puede agregar los dispositivos IPC en la página web del VTO. Los VTH con el mismo servidor SIP en línea obtienen la información de IPC.



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

6.5.1 Agregar el IPC uno por uno

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

Procedimiento

Paso 1 Inicie sesión en la página web.

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

Figura 6-14 Información de IPC

RefreshImportExportDefault

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 6-15 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 6-6 Descripción de los parámetros del dispositivo de monitoreo de video

Parámetro	Descripción
Nombre del consultor	Ingrese el nombre del dispositivo IPC/VNR/XVR/HCVR.
Dirección IP	Ingrese la dirección IP del dispositivo IPC/VNR/XVR/HCVR.
Tipo de protocolo	Seleccionar de LocalyONVIF según el dispositivo que agregues.
Tipo de transmisión	Seleccionar de ConvencionalySub corriente .
Tipo de dispositivo	Seleccione el tipo según los dispositivos reales.
Canal No.	● 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.
Cifrado	Mantenga 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.

Etapas 4

Hacer clic **DE ACUERDO**.

6.5.2 Exportación de la información IPC en lotes

Exporte la información de IPC y guarde la información 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.

6.5.3 Importación de la información de IPC en lotes

Importe la información del IPC al sistema.

Procedimiento

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

Figura 6-16 Importar

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

7 sistema

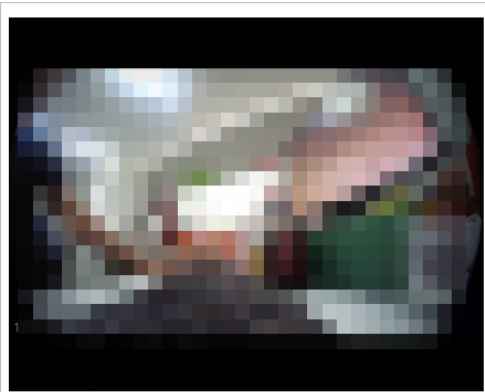
Vídeo 7.1

Configurar el formato y calidad de vídeo y audio del VTO.

Procedimiento

Paso 1 Seleccionar **Sistema>Vídeo**.

Figura 7-1 Vídeo



Video Clip

LeftRightReset

Default

Bit Rate

StatusImage

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 entrarán en vigor tras el cambio.

Tabla 7-1 Descripción del parámetro de vídeo

Parámetro		Descripción
Tasa de bits	Resolución (principal Arroyo)	● 720P:1280 × 720. ● WVGA:800 × 480. ● D1:704 × 576. ● CIF:352 × 288.
	Velocidad de fotogramas (FPS) (transmisión principal)	● 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 (transmisión principal)	Incluye 768 Kbps, 896 Kbps, 1024 Kbps, 1,25 Mbps, 1,5 Mbps, 1,75 Mbps, 2 Mbps y 4 Mbps y más. Cuanto mayor sea el valor, mejor será la calidad del vídeo, pero requiere más ancho de banda.

Parámetro		Descripción
	Compresión (principal Arroyo)	H.264. H.265.  En comparación con H.264, H.265 requiere un ancho de banda menor.
	Resolución (subtransmisión)	● 1080P:1920 × 1080. ● WVGA:800 × 480. ● QVGA:320 × 240. ● D1:704 × 576. ● CIF:352 × 288.
	Velocidad de fotogramas (FPS) (subtransmisión)	El rango es de 1 a 25. Cuanto mayor sea el valor, más fluido será el vídeo, pero requiere más ancho de banda.
	Velocidad de bits (subtransmisión)	Incluye 224 Kbps, 256 Kbps, 320 Kbps, 384 Kbps, 448 Kbps, 512 Kbps, 640 Kbps, 768 Kbps. Cuanto mayor sea el valor, mejor será la calidad del vídeo, pero requiere más ancho de banda.
	Compresión (Sub Arroyo)	H.264. H.265.
Estado	Modo escena	Seleccionar de Auto , Desactivar , Soleado y Noche . Auto está seleccionado de forma predeterminada.
	Modo de compensación	● BLC:Compensación de luz de fondo. Mejora la claridad del objetivo en la imagen. ● WDR:Amplio rango dinámico. Mejore el brillo de las áreas oscuras y reduzca el brillo de las áreas brillantes para mejorar la imagen. ● CHL:Alta compensación de luz. Reduzca el brillo de los puntos fuertes para mejorar la imagen general. ● Desactivar: No utilice ningún modo de compensación.
	Día/Noche	Seleccionar de Color , Auto y B/N .
	Estándar de vídeo	Seleccionar CAMARADA o NTSC según tu zona.
	Sensibilidad del iluminador	Configure el valor de sensibilidad. ● Si la intensidad de la iluminación es inferior al valor configurado, el iluminador se encenderá. ● Si la intensidad de la iluminación es mayor que el valor de configuración, el iluminador se apagará.
Imagen	Brillo	Cuanto mayor sea el valor, más brillante será la imagen.
	Contraste	Valor mayor para mayor contraste entre áreas brillantes y oscuras.

Parámetro		Descripción
	Matiz	Haz que el color sea más brillante o más oscuro. El valor predeterminado lo establece el sensor de luz y recomendamos mantenerlo predeterminado.
	Saturación	Cuanto mayor sea el valor, más denso será el color.
	Gama	Cambia el brillo de la imagen y mejora el rango dinámico de la imagen de forma no lineal. Cuanto mayor sea el valor, más brillante será la imagen.  Esta función está disponible en modelos selectos.
	Espejo	Muestre la imagen con los lados izquierdo y derecho invertidos.
	Voltear	Muestre la imagen al revés.
	Tiempo de visualización	Muestra la hora y fecha actuales en la imagen de vídeo.

Operaciones relacionadas

Hacer clic **Izquierdo** o **Bien** para ajustar la imagen de vídeo.

Hacer clic **Reiniciar** o **Por defecto** para restablecer las configuraciones de video o restaurar las configuraciones predeterminadas.

7.2 Audio

Procedimiento

Paso 1 Seleccionar **Sistema > Video**.

Paso 2 Configure los parámetros, que entrarán en vigor tras el cambio.

Figura 7-2 Audio

Audio Control

Voice Prompt while Ringing ☒
Ringtone ☒
Unlock ☒
Alarm ☒
Voice Messages ☒
Audio Collection ☒

Volume Control

Microphone Volume + 90
Speaker Volume + 80

Apply Refresh Default

Audio File(Only MP3 files that are up to 20 KB can be uploaded.)

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

Tabla 7-2 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	
	desbloquear	
	Colección de audios	
Control del volumen	Volumen del micrófono	Ajusta el volumen.
	Volumen del altavoz	

Paso 3 Hacer clic **Aplicar**.

Etapa 4 (Opcional) Cargue el archivo de audio haciendo clic  junto al tipo de audio correspondiente (incluyendo llamadas, ocupado, desbloqueado exitosamente, nadie respondió, llamada finalizada y número inexistente).



Sólo se pueden cargar archivos MP3 de hasta 20 KB.

7.3 Tiempo

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

Procedimiento

Paso 1 Seleccionar **Sistema>Tiempo**.

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

Figura 7-3 Hora

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 7-3 Descripción de parámetros

Módulo	Parámetro	Descripción
Tiempo y tiempo Zona	Tiempo	Establecer manualmente NTP
	Hora del sistema	La hora del sistema VTO.  Cambiar la hora del sistema puede causar problemas en la búsqueda de videos y publicación de información. Desactive la grabación de video y la instantánea automática antes de cambiarlas.  Sólo aplicable bajo elEstablecer manualmentemodo.
	Sincronizar PC	Sincronice la hora del sistema VTO con su PC.  Sólo aplicable bajo elEstablecer manualmentemodo.

Módulo	Parámetro	Descripción
	Servidor	La dirección del servidor NTP.  Sólo aplicable bajo el INTP modo.
	Actualización manual	Haga clic en el icono y la hora del dispositivo VTO se sincronizará automáticamente con el servidor.  Sólo aplicable bajo el INTP modo.
	Puerto	Número de puerto del servidor NTP.  Sólo aplicable bajo el INTP modo.
	Intervalo	Ciclo de actualización de hora VTO. 30 minutos como máximo.  Sólo aplicable bajo el INTP modo.
	Formato de tiempo	Para el formato de fecha, seleccione uno de los siguientes: ● AAAA-MM-DD ● MM-DD-AAAA ● DD-MM-AAAA Para el formato de hora, seleccione uno de los siguientes: ● 24 horas ● 12 horas
	Zona horaria	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 finalización del horario de verano.
	Hora de finalización	

Paso 3 Hacer clic **Aplicar**.

7.4 Usuario ONVIF

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

Procedimiento

Paso 1 Seleccionar **Sistema > Usuario ONVIF**.

Paso 2 Hacer clic **Agregar**.

Paso 3 Ingrese la información y luego haga clic **DE ACUERDO**.

Los dispositivos ONVIF pueden monitorear el VTO usando la cuenta.

Figura 7-4 Usuario ONVIF

Add X

* Username

* Password

* Confirm Password

OK Cancel

7.5 Configuración

Puede exportar e importar el archivo de configuración.

Procedimiento

Paso 1 Seleccionar **Sistema>configuración**.

Paso 2 Hacer clic **Exportar archivo de configuración**, o haga clic **Navegar** para seleccionar el archivo desde la computadora local y luego haga clic en **Importar archivo**.

Figura 7-5 Configuración

Config

Export Configuration File

File Browse Import File

Imported configuration will overwrite previous configuration.

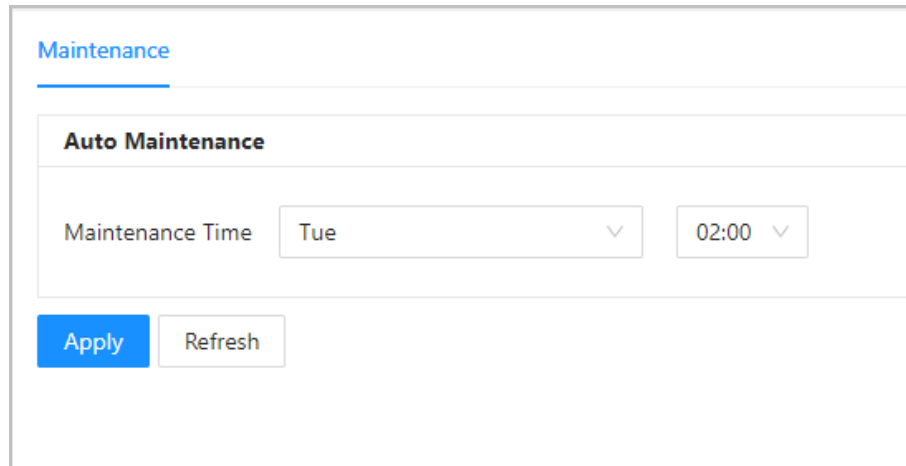
7.6 Mantenimiento

Procedimiento

Paso 1 Seleccionar **Sistema>Mantenimiento**. Configure el

Paso 2 tiempo de mantenimiento automático.

Figura 7-6 Mantenimiento automático



Paso 3 Hacer clic **Aplicar**.

7.7 Actualización

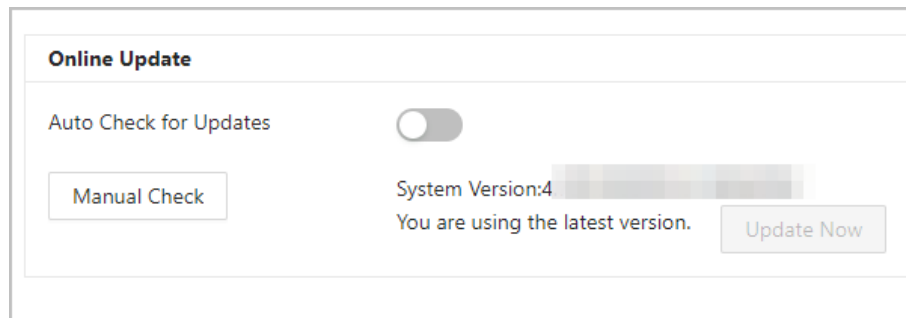
Procedimiento

Paso 1 Seleccionar **Sistema** > **Actualizar**. Seleccione

Paso 2 formas de verificar la actualización.

- **Verificación automática:** Seleccione la función para comprobar automáticamente si hay una nueva versión del sistema.
- **Verificación manual:** Seleccione la función para comprobar si hay una nueva versión del sistema.

Figura 7-7 Actualización



7.8 Información legal

Seleccionar **Sistema** > **Información legal**. Puede consultar avisos de información legal relacionados en esta sección.

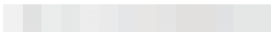
7.9 Información del sistema

Procedimiento

Paso 1 Seleccionar **Sistema** > **Información del sistema**.

Paso 2 Vea la versión del software, la versión de SCM y la versión básica de seguridad.

Figura 7-8 Información del sistema

Software Version	
SCM Version	2021-01-22
Security Baseline Version	

8 Configuración del dispositivo

Este capítulo presenta 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 está utilizando otros servidores como servidor SIP, consulte el manual correspondiente para obtener más detalles.

8.1 Gestión del nº 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. Seleccionar
- Paso 2** **Configuración del dispositivo**. Hacer clic **Agregar**.
- Paso 3**
- Etapas 4** Configure los parámetros.

Figura 8-1 Agregar VTO

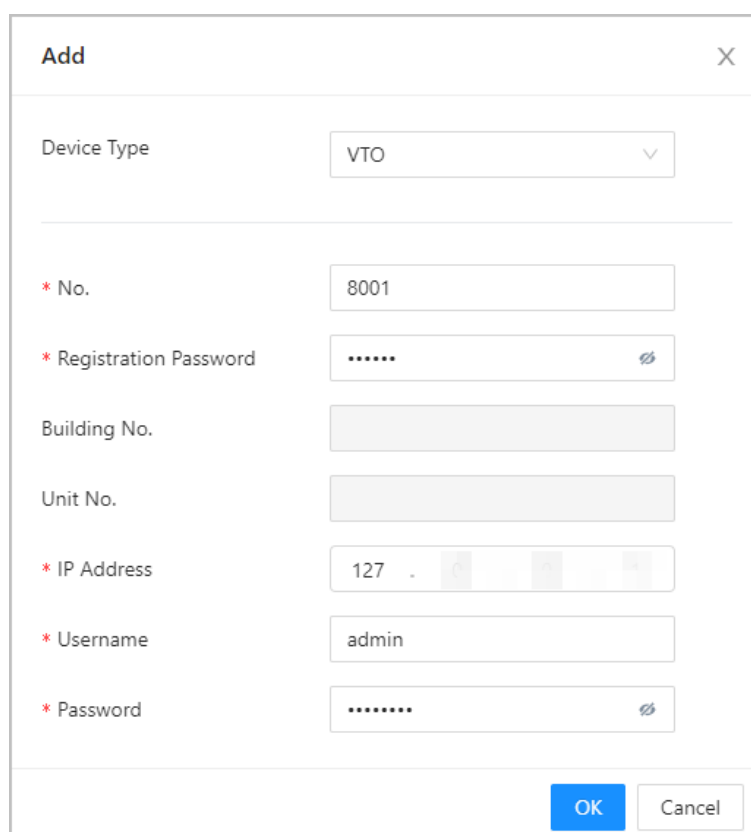


Tabla 8-1 Agregar configuración de VTO

Parámetro	Descripción
Tipo de dispositivo	Seleccionar VTO .
No.	El número VTO que configuró.
Contraseña de registro	Déjalo por defecto.

Parámetro	Descripción
Edificio número.	Disponible solo cuando los servidores de la plataforma funcionan como servidor SIP.
Numero de unidad.	
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 VTO añadidos, pero el que tienes iniciado sesión no se puede modificar ni eliminar.

8.2 Gestión de VTH

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

Procedimiento

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

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

Paso 3

Etapa 4 Configure los parámetros.

- Seleccione el modo de agregar como **Agregar uno por uno**.

Figura 8-2 Agregar VTH uno por uno

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields:

- Device Type:** A dropdown menu with "VTH" selected.
- Add Mode:** A dropdown menu with "Add One by One" selected.
- First Name:** A text input field with the placeholder "Please enter".
- Last Name:** A text input field with the placeholder "Please enter".
- Alias:** A text input field with the placeholder "Please enter".
- * Room No.:** A text input field with the placeholder "Please enter".
- Registration Mode:** A dropdown menu with "Public" selected.
- * Registration Password:** A password input field with masked characters "*****" and a toggle icon.

At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (white).

Tabla 8-2 Descripción de los parámetros

Parámetro	Descripción
Nombre de pila	Introduce la información que necesitas para diferenciar cada habitación.
Apellido	
Alias	
Habitación no.	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 por defecto.

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

Figura 8-3 Agregar VTH en lotes

Tabla 8-3 Descripción de los parámetros

Parámetro	Descripción
Pisos en la unidad	Configure el número de pisos, habitaciones.
Habitaciones en cada piso	
Primera Habitación No. en 1er Piso	Configure el primer número de habitación en el primer y segundo piso, el número de habitación se generará automáticamente.
Primera Habitación No. en 2do Piso	

Paso 5

Hacer clic **DE ACUERDO**.



Hacer clic

para editar el VTH, o  para eliminar VTH agregados, pero el que tienes iniciado sesión no se puede modificar ni eliminar.

8.3 Gestión del VTS

Puede agregar un VTS al servidor SIP y luego podrá usarlo como centro de administración. También puede gestionar, llamar o recibir llamadas de todos los VTO y VTH de la red. Consulte el manual del usuario correspondiente para obtener más detalles.

Procedimiento

- Paso 1** Inicie sesión en la página web del VTO que funciona como servidor SIP. Seleccionar
- Paso 2** **Configuración del dispositivo.** Hacer clic **Agregar**.
- Paso 3**
- Etapas 4** Configure los parámetros.

Figura 8-4 Agregar VTS

Add

X

Device Type

VTSTS

* VTS No.

Please enter

* IP Address

* Registration Password

.....

OK

Cancel

Tabla 8-4 Agregar configuración de VTS

Parámetro	Descripción
Tipo de dispositivo	SeleccionarVTS.
VTS No.	El número del VTS.
Contraseña de registro	Déjalo por defecto.
Dirección IP	Dirección IP del VTS.

Paso 5 Hacer clicDE ACUERDO.

Gestión de 9 personas

Agregar información del personal.



Las funciones de tarjeta y huella digital están disponibles en modelos selectos o cuando el dispositivo está conectado a los módulos correspondientes.

Procedimiento

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

Paso 2 Seleccionar **Gestión de personas**. Hacer clic

Paso 3 **Agregar**.

- VTO que no tienen otras funciones o módulos: ingrese la ID de la habitación, el número de la habitación, el nombre de usuario y luego haga clic en **DE ACUERDO**.

Figura 9-1 Agregar persona

The screenshot shows a modal dialog box titled 'Add' with a close button (X) in the top right corner. Inside the dialog, there are three labeled input fields: 'Person ID' containing '0123', 'Room No.' containing '8801', and 'Username' containing 'Li'. The 'Person ID' and 'Room No.' fields have a red asterisk icon to their left. At the bottom right of the dialog, there are two buttons: a blue 'OK' button and a white 'Cancel' button with a grey border.

- VTO que tenga función o módulo de emisión de tarjetas:
 1. Ingrese la ID de la habitación, el número de la habitación, el nombre de usuario y seleccione el permiso de bloqueo.
 - ◇ Bloqueo1: bloqueo local.
 - ◇ Bloqueo 2: bloqueo 485.



Sólo los modelos que tienen 485 puertos admiten 2 tipos de cerraduras.

Figura 9-2 Agregar una persona

The 'Add' dialog box contains the following fields and controls:

- * Person ID:** Text input field with the value '0123'.
- * Room No.:** Text input field with the value '8801'.
- Username:** Text input field with the value 'Li'.
- * Lock Permission:** Two checked checkboxes labeled 'Lock 1' and 'Lock 2'.
- Card:** A button labeled 'Add'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

2. Haga clic **Agregar** junto a **Tarjeta** y luego ingrese el número de tarjeta y el nombre.

Figura 9-3 Tarjeta de problema

The 'Add Card' dialog box contains the following fields and controls:

- * Card Number:** Text input field with the value '0123456' and an 'Issue Card' button to its right.
- Name:** Text input field with the value 'Li'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

3. Haga clic **Tarjeta de emisión**.

La página web muestra el mensaje de cuenta regresiva (120 segundos). Una vez que comience la cuenta regresiva, deberá deslizar la tarjeta en el lector de tarjetas del VTO dentro de este período de tiempo. Después de pasarla, el VTO reconocerá automáticamente el número de la tarjeta.

Figura 9-4 Cuenta regresiva

The 'Add Card' dialog box shows a countdown state:

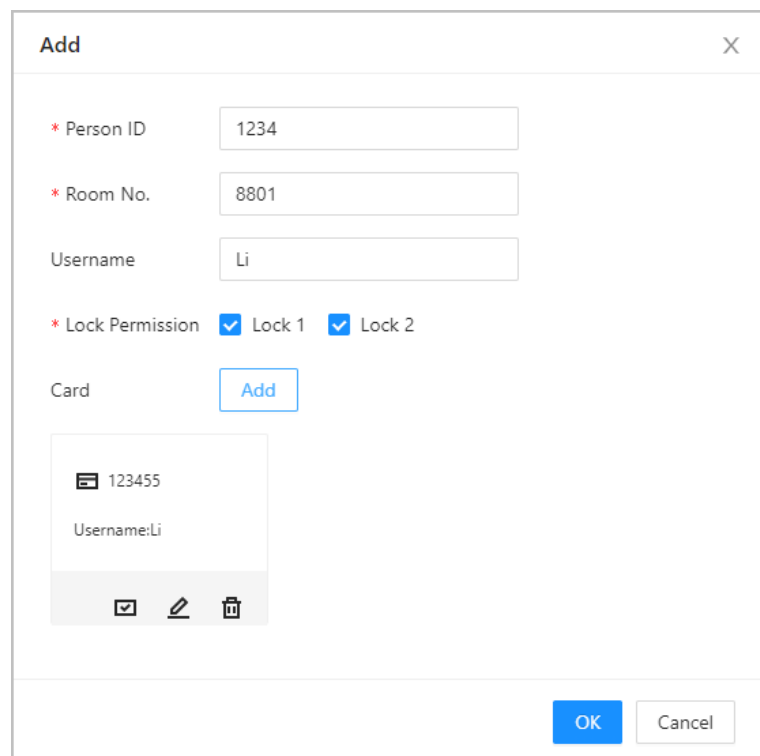
- * Card Number:** The input field is disabled (grayed out), and a 'Cancel(119)' button is visible to its right.
- Name:** Text input field with the value 'Li'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

4. Haga clic **DE ACUERDO** después de deslizar para completar el proceso de emisión.

Luego la ventana vuelve a **laAgregar**, añadiendo una tarjeta.

- ◇  : Reportar tarjeta perdida. Después de hacer clic en el icono, se convierte en .
- ◇  : edita la información de la tarjeta.
- ◇  : elimina la tarjeta agregada.

Figura 9-5 Tarjeta emitida



Add [X]

* Person ID

* Room No.

Username

* Lock Permission ☒ Lock 1 ☒ Lock 2

Card

 123455

Username:Li





5. Haga clic **DE ACUERDO**.

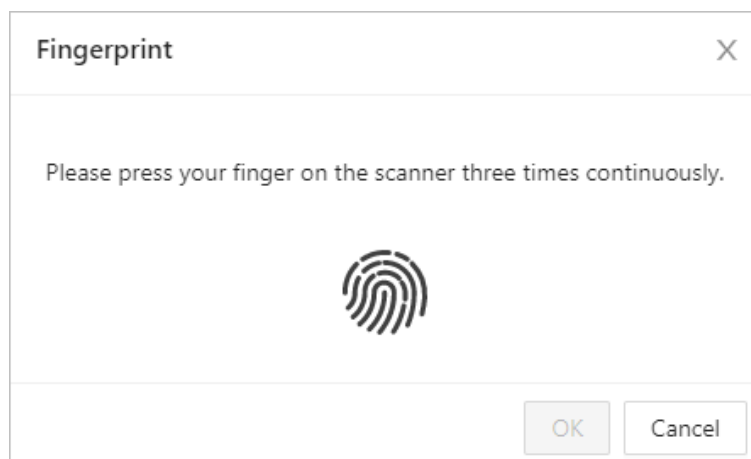
Figura 9-6 Tarjeta agregada exitosamente

Add	Import Person	Export Person	Delete	Clear	Refresh	Person ID/Room No./Username		Q
☐	No.	Person ID	Room No.	Username	Card	Operation		
☐	1	1234	8801	Li		 		
1 records							1	10 / page

- VTO que tiene función o módulo de huella dactilar:

1. Ingrese la ID de la habitación, el número de la habitación, el nombre de usuario y seleccione el permiso de bloqueo.
2. Haga clic **Agregar** junto a **Huella dactilar** luego presione con el dedo según se le indique.

Figura 9-7 Tarjeta de problema



3. Haga clic **DE ACUERDO**.

Luego la ventana vuelve a la **Agregar**, al que se le añade una huella digital. Puede editar el nombre de la huella digital.

4. Haga clic **DE ACUERDO**.

Operaciones relacionadas

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

10 configuraciones de red

Este capítulo presenta cómo configurar los parámetros de red.

10.1 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 Seleccionar **Configuración de la red** > **TCP/IP**
- Paso 3 . Configure los parámetros TCP/IP.

Figura 10-1 TCP/IP

MAC Address	c0
IP Address	172
Subnet Mask	255 . 255
Default Gateway	
Preferred DNS	8 . 8 . 8 . 8
Alternate DNS	8 . 8 . 4 . 4
Transmission Mode ☒ Multicast ☐ Unicast	
Apply Refresh Default	

Tabla 10-1 Descripción del parámetro

Parámetro	Descripción
Dirección IP	Su dirección IP planificada para el VTO.
DNS preferido	Es 8.8.8.8 por defecto.
DNS alternativo	Es 8.8.4.4 por defecto.
Modo de transmisión	● Multidifusión. ● Unidifusión.  Se prefiere la unidifusión cuando el conmutador no admite la función de multidifusión o cuando la conexión de red no es buena.

10.2 Puerto

Figura 10-2 Puerto

TCP Port

37777

(1025-65534)

UDP Port

37778

(1025-65534)

HTTP Port

80

HTTPS Port

443

Apply

Refresh

Default

Tabla 10-2 Descripción del parámetro

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

10.3 Servidor SIP

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

Procedimiento

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

Paso 2 Seleccione un tipo de servidor.

- El VTO en el que ha iniciado sesión como servidor SIP: seleccione el tipo SIP como **Dispositivo**y configure los parámetros para el VTO, y luego haga clic en junto a**Servidor SIP**.



Los parámetros se volverán grises después de habilitar el**Servidor SIP**función.

Figura 10-3 VTO actual como servidor SIP

SIP Server	☒
Server Type	Device
IP Address	192.168.1.1
Port	5060
Username	8001
Password	
SIP Domain	VDP
SIP Server Username	admin
SIP Server Password	
<button>Apply</button> <button>Refresh</button> <button>Default</button>	

- Si otro VTO funciona como servidor SIP: seleccione el tipo SIP como **Dispositivo** y 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 habilite **Servidor SIP**. De lo contrario, la conexión fallaría.

Figura 10-4 Otro VTO como servidor SIP

The image shows a configuration window for a SIP Server. At the top, there is a toggle switch labeled 'SIP Server'. Below it, the 'Server Type' is set to 'Device' in a dropdown menu. The 'IP Address' field contains '192...', 'Port' is '5060', 'Username' is '8001', 'Password' is masked with dots, 'SIP Domain' is 'VDP', 'SIP Server Username' is 'admin', and 'SIP Server Password' is also masked. At the bottom, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Tabla 10-3 Configuración del servidor SIP (VTO como servidor SIP)

Parámetro	Descripción
Dirección IP	Dirección IP planificada del VTO.
Puerto	5060 por defecto.
Nombre de usuario	Déjalo por defecto.
Contraseña	
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 **Tipo de servidor** como **Servidor SIP privado** y luego configure los parámetros.

Figura 10-5 Servidor SIP privado

The screenshot shows a configuration window for a Private SIP Server. At the top, there is a 'SIP Server' toggle switch that is currently turned on. Below it, the 'Server Type' is set to 'Private SIP Server' in a dropdown menu. The main configuration area consists of several input fields: 'IP Address' (192.), 'Port' (5080), 'Username' (8001), 'Password' (masked with dots), 'SIP Domain' (VDP), 'SIP Server Username' (admin), and 'SIP Server Password' (masked with dots). To the right of these fields is an 'Alternate' section with its own set of fields: 'Alternate IP' (192.), 'Alternate Server User...' (admin), 'Alternate Server Passw...' (masked with dots), 'Alternate VTS IP' (0 . 0 . 0 . 0), and an 'Alternate Server' toggle switch that is currently turned off. At the bottom left of the window are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Tabla 10-4 Descripción del servidor SIP (plataforma como servidor SIP)

Parámetro	Descripción
Dirección IP	Dirección IP del servidor SIP.
Puerto	5080 de forma predeterminada cuando la plataforma funciona como servidor SIP.
Usuario Contraseña	Déjalo por defecto.
Dominio SIP	
Nombre de usuario/contraseña del servidor SIP	Se utiliza para iniciar sesión en el servidor SIP.
IP alternativa	El servidor alternativo se utilizará como servidor SIP cuando Express/DSS deje de responder. Le recomendamos configurar la dirección IP alternativa.  ◇ Si habilitas 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 alternativacaja de texto. No actives Servidor alternativo en este caso.
Nombre de usuario/contraseña del servidor alternativo	Se utiliza para iniciar sesión en el servidor alternativo.
IP VTS alternativa	Dirección IP del VTS alternativo.
Servidor alternativo	Habilítelo para que pueda configurar la IP VTS alternativa.

Paso 3 Hacer clic **Aplicar**.

10.4 Segunda estación de confirmación en cascada

Se aplicó a la situación en la que la segunda estación de confirmación cae en cascada al VTH.

Requisitos previos

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

Procedimiento

- Paso 1** Seleccionar**Configuración de la red>Servidor SIP**.
- Paso 2** Configure la información de la segunda estación de confirmación en**Configuración del dispositivo local>Ajustes básicos**.



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 10-6 Configuración del servidor SIP (VTH como servidor SIP)

Tabla 10-5 Descripción de la configuración del servidor SIP (VTH como servidor SIP)

Parámetro	Descripción
Dirección IP	Su dirección IP planificada del VTH.
Puerto	5060 por defecto.
Nombre de usuario	Déjalo por defecto.
Contraseña	
Dominio SIP	

Parámetro	Descripción
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	

Etapas 4 Hacer clic **Aplicar**.

10.5 Servicio en la nube

Habilitar el **Servicio de almacenamiento 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 10-7 Servicio en la nube

Enable
☐

After the function is enabled and the device connects to the network, we will collect device information such as the IP address, MAC address, device name and serial number. The collected information will only be used to remotely access the device. If you do not want to enable this function, please clear the selection from the check box.

P2P Status

● Offline

PaaS Status

● Offline

SN

7



Please scan the actual QR code

Apply

Refresh

10.6 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 10-8 UPnP

Enable

Apply

Refresh

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		
Rtp	CustomService	UDP	15001	15001	Mapping Failed		
Rtp	CustomService	UDP	15003	15003	Mapping Failed		
Rtp	CustomService	UDP	15005	15005	Mapping Failed		
Rtp	CustomService	UDP	15006	15006	Mapping Failed		
Rtp	CustomService	UDP	15007	15007	Mapping Failed		
Rtp	CustomService	UDP	15008	15008	Mapping Failed		
Rtp	CustomService	UDP	15009	15009	Mapping Failed		

17 records

<

1

2

>

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.

10.6.1 Habilitación de servicios UPnP

Procedimiento

- Paso 1** Seleccionar **Configuración de la red>UPnP**.
- Paso 2** Habilite los servicios enumerados.
- Paso 3** Seleccionar **Permitir**.
- Etapas 4** Hacer clic **Ahorrar**.

10.6.2 Agregar servicios UPnP

Procedimiento

- Paso 1** Seleccionar **Configuración de la red>UPnP**.
- Paso 2** Hacer clic **Agregar**.
- Paso 3** Configure los parámetros y luego haga clic en **DE ACUERDO**.

Figura 10-9 Agregar un servicio UPnP

Add

Enable

* Service Name

VTO1

* Service Type

VTO

Protocol

TCP

* Internal Port

3

* External Port

5

OK

Cancel

Tabla 10-6 Descripción del parámetro

Parámetro	Descripción
Nombre del Servicio	Ingrese el nombre y tipo del servicio.
Tipo de servicio	
Protocolo	Seleccionar tcpoUDP .
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 debe 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 debe ser el mismo.

10.7 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 la red>Wifi**.
- Paso 3 Seleccione el**Wifi**status como**En**.

Se muestran todas las redes disponibles.

Figura 10-10 Wi-Fi

Wi-Fi 			
Name	Signal Strength	Status	Connect
[Redacted]			+
[Redacted]			+
[Redacted]			+
[Redacted]			+
[Redacted]			+
[Redacted]			+
[Redacted]			+
[Redacted]			+
[Redacted]			+

- Etapa 4 Hacer clic+del Wi-Fi que eligió, ingrese la contraseña del mismo y luego conéctese a la red.

10.8 Servicios Básicos

Configurar funciones que involucran la seguridad del dispositivo.

Procedimiento

- Paso 1 Seleccione**Configuración de la red>Servicios basicos**. Habilite las
- Paso 2 funciones de seguridad según sus necesidades.

Figura 10-11 Servicios básicos

SSH
☒

There might be safety risk if this service is enabled.

CGI
☒

There might be safety risk if this service is enabled.

Mobile Push Notifications
☒

There might be safety risk if this service is enabled.

Password Reset
☒

ONVIF
☒

There might be safety risk if this service is enabled.

Outbound Protection of S...
☐

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

Multicast/Broadcast Search
☒

There might be safety risk if this service is enabled.

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
☐

Tabla 10-7 Descripción del parámetro de seguridad

Parámetro	Descripción
SSH	Una alternativa segura a los protocolos remotos no seguros. Le recomendamos que lo desactive porque podría haber riesgos para la seguridad si este servicio está habilitado.
CGI	El uso del comando CGI. Le recomendamos que lo apague. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
Empuje móvil Notificación	Envía información a la aplicación del teléfono. Le recomendamos que lo apague si no necesita esta función. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
Restablecimiento de contraseña	Si está desactivado, no podrá restablecer la contraseña.

Parámetro	Descripción
ONVIF	Permita que terceros extraigan la transmisión de video del VTO a través del protocolo ONVIF.  Recomendamos apagarlo. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
Servicio saliente Protección de la información	Proteja sus contraseñas.  Le recomendamos que lo encienda. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
Multidifusión/difusión Buscar	Habilítelo para que otros dispositivos encuentren el VTO.  Le recomendamos que lo apague. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
modo de autenticación	● modo de seguridad(recomendado): Admite el inicio de sesión con autenticación implícita. ● Modo de compatibilidad: Utilice el antiguo método de inicio de sesión.  Le recomendamos utilizar el modo de seguridad. El modo compatible puede exponer al VTO a riesgos de seguridad y fuga de datos.
Emergencia Mantenimiento	Para acceder fácilmente a nuestro servicio postventa, habilite esta función. Si el dispositivo tiene problemas para realizar funciones, como la actualización, el sistema habilitará automáticamente esta función.
La contraseña caduca en	● Seleccione un período de vencimiento de 30 días, 60 días, 90 días, 180 días, CostumbreyNunca. ● Si seleccionas 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 para la seguridad si este servicio está habilitado.

Paso 3 Hacer clic **Aplicar**.

11 Gestión de registros

Seleccionar **Registro**. Puede buscar diferentes registros y exportarlos a su computadora local.



Si el almacenamiento está lleno, se sobrescribirán los registros más antiguos. Haga una copia de seguridad de los registros a tiempo.

11.1 Historial de llamadas

Seleccionar **Registro** > **Historial de llamadas**.

Figura 11-1 Historial de llamadas

Please keep unencrypted files well to avoid data leakage.

Export

No.	Call Type	Room No.	Start Time	Call Duration (min)	End Status
1	Incoming	9902	2000-03-18 00:40:45	00:30	Answered
2	Outgoing	9903	2000-03-17 08:51:39	00:00	Missed
3	Incoming	9904	2000-03-14 04:08:05	00:39	Answered
4	Incoming	9904	2000-03-14 04:05:57	00:19	Answered
5	Incoming	9905	2000-03-11 00:34:46	00:12	Answered
6	Incoming	9904	2000-03-10 08:11:20	00:12	Answered
7	Incoming	9904	2000-03-10 02:26:20	00:06	Answered
8	Incoming	9904	2000-03-10 02:25:54	00:21	Answered
9	Incoming	9904	2000-03-10 02:25:09	00:44	Answered
10	Incoming	9904	2000-03-10 00:53:06	00:06	Answered

681 records

<12345...69>10 / pageGo toPage

11.2 Registros de alarmas

Seleccionar **Registro** > **Registros de alarma**.

Figura 11-2 Alarma

Please keep unencrypted files well to avoid data leakage.

Export

No.	Room No.	Event	Channel	Start Time
1	8001	Tamper	1	2023-07-11 02:00:53
2	8001	Tamper	1	2023-07-07 10:07:18
3	8001	Tamper	1	2023-07-06 22:16:19
4	8001	Tamper	1	2023-07-06 22:09:52
5	8001	Tamper	1	2023-07-04 02:00:49
6	8001	Tamper	1	2023-06-29 16:29:49
7	8001	Tamper	1	2023-06-29 16:26:59
8	8001	Tamper	1	2023-06-29 15:22:09
9	8001	Tamper	1	2023-06-29 15:22:08
10	8001	Tamper	1	2023-06-27 14:07:57

12 records

<12>

10 / pageGo toPage

11.3 Desbloquear registros

Seleccionar**Registro>Desbloquear registros.**

Figura 11-3 Desbloquear

Please keep unencrypted files well to avoid data leakage.

Export

No.	Unlock Method	VTO ID	Person ID	Room No.	Username	Card	Unlock Results	Unlock Time
1	Remote Unlock	8001		9901			Succeed	2023-07-06 20:59:...
2	Remote Unlock	8001		9901			Succeed	2023-06-29 15:17:...

2 records

<12>

10 / page

11.4 Registro

Seleccionar**Registro>Registro.**

Seleccione el rango de tiempo y el tipo, y luego podrá ver toda la información del registro.

Figura 11-4 Registro

Please keep unencrypted files well to avoid data leakage.

Time Range

2023-07-10 00:00:00 → 2023-07-11 00:00:00

Type

All

Search

Reset

☐ Encrypt Log Backup

Export

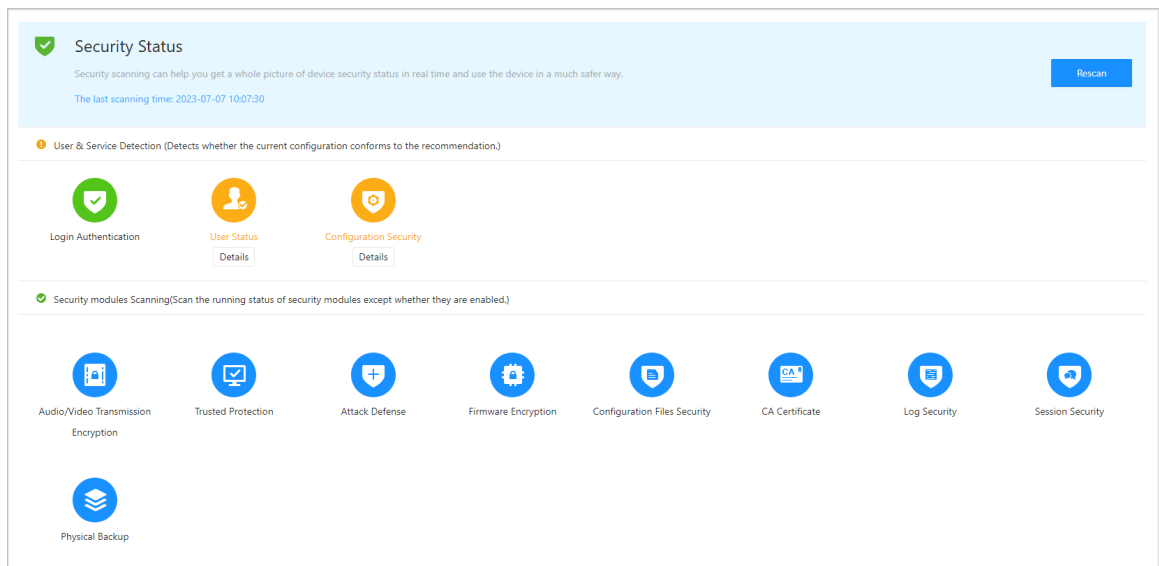
No.	Time	Type	Log Content
No Data			

12 Gestión de 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



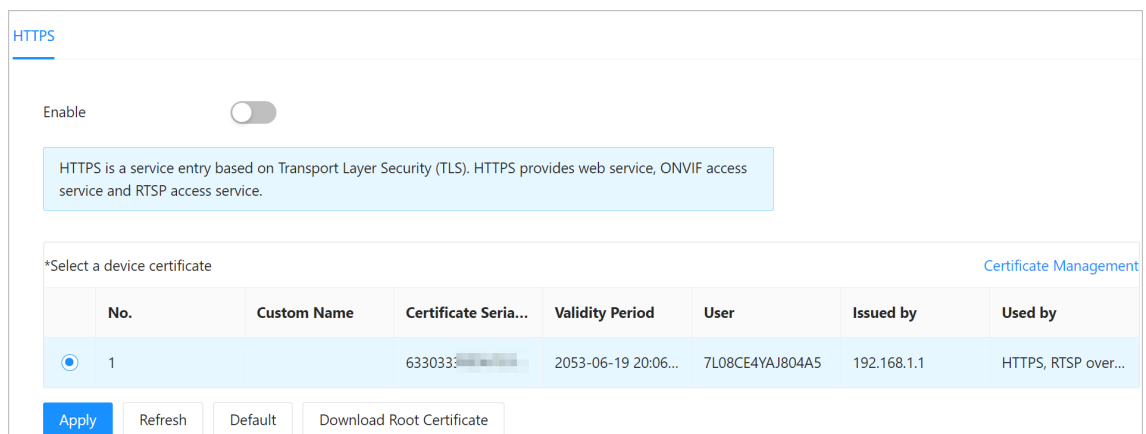
12.2 Servicio del sistema

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 red al VTO.

Procedimiento

- 

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

Paso 2 Seleccione el **Modo** cómo sea **Lista de permitidos** o **Lista de bloqueos**.

 - 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 3 Hacer clic **Agregar** para agregar la dirección IP a la lista de permitidos o de bloqueo.
- Figura 12-3 Agregar
- Add

Add Mode

IP

IP Version

IPv4

IP Address

10

All Device Ports

☒

OK

Cancel
- Etapas**

Paso 4 Hacer clic **DE ACUERDO**.

Paso 5 Hacer clic ☐ junto a **Permitir**.

Paso 6 Seleccione una dirección IP agregada para la lista de permitidos o de bloqueo y luego haga clic en **Aplicar**.
- 83

Figura 12-4 Aplicar

Firewall Account Lockout Anti-DoS Attack

Enable ☒

Mode ☒ Allowlist ☐ Blocklist

Only source hosts whose IP/MAC are in the following list are allowed to access corresponding ports of the device.

Add Delete

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

Total 1 records

Apply Refresh Default

12.3.2 Bloqueo de cuenta

Procedimiento

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

Paso 2 Configure los intentos de inicio de sesión y el tiempo de bloqueo.

Figura 12-5 Bloqueo de cuenta

Firewall Account Lockout Anti-DoS Attack

Device Account

Login Attempt 5time(s)

Lock Time 5 min

ONVIF User

Login Attempt 30time(s)

Lock Time 5 min

Apply Refresh Default

Paso 3 Hacer clic **Aplicar**.

12.3.3 Ataque anti-DoS

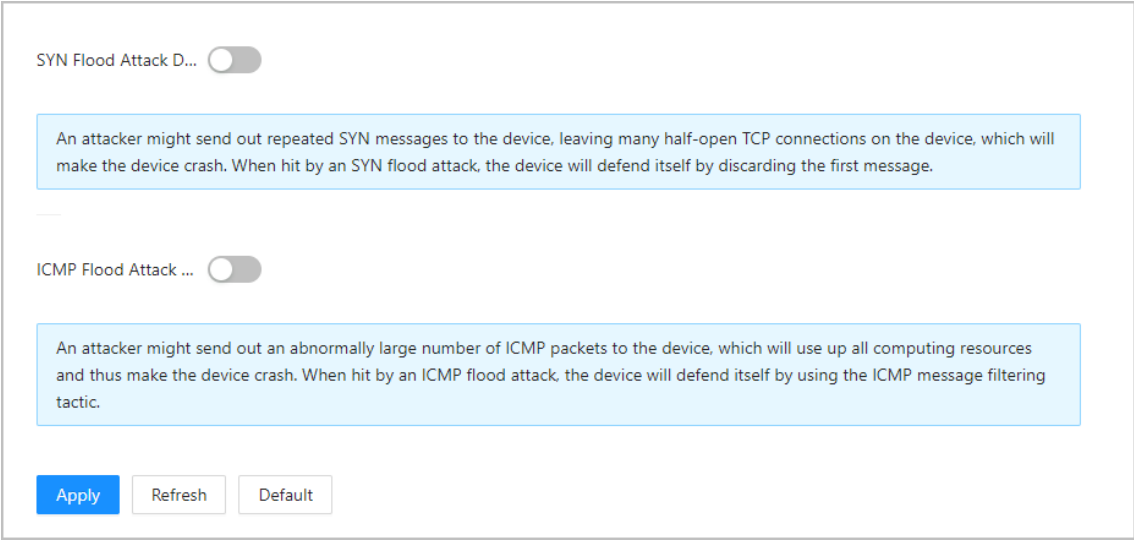
Procedimiento

- Paso 1**

En la página de inicio, haga clic en  y luego seleccione **Defensa de ataque>Ataque anti-DoS**.
- Paso 2**

Activar o desactivar la **Defensa contra ataques de inundación SYN** o **Defensa contra ataques de inundaciones ICMP** función.

Figura 12-6 Ataque Anti-DoS



- Paso 3**

Hacer clic **Aplicar**.

12.4 Certificado de CA

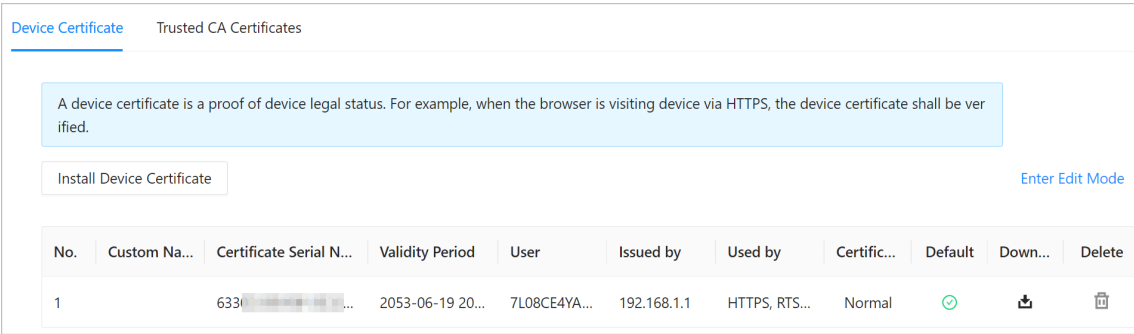
Procedimiento

- Paso 1**

En la página de inicio, haga clic en  y luego seleccione **Certificado de CA**.

 - Certificado de dispositivo

Figura 12-7 Certificado de dispositivo



- Certificados de CA confiables

Figura 12-8 Certificados de CA confiables

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 AES256-OFB

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

RTSP over TLS

Enable ☒

RTSP stream is encrypted by using TLS tunnel before transmission.

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

*Select a device certificate
Certificate Management

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1		63303339356133326136313...	2053-06-19 20:06:37	7L08CE4YAJ804A5	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. Presione el botón en el panel frontal del modelo y luego el VTH recibe una señal de alarma.

13.1 Conexión de cables

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

Figura 13-1 Modelo de botón

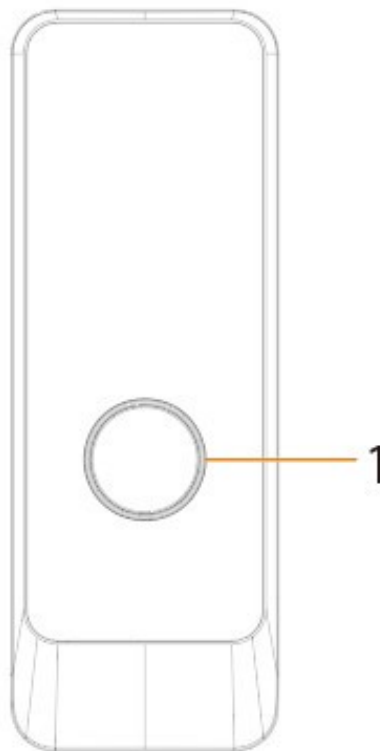
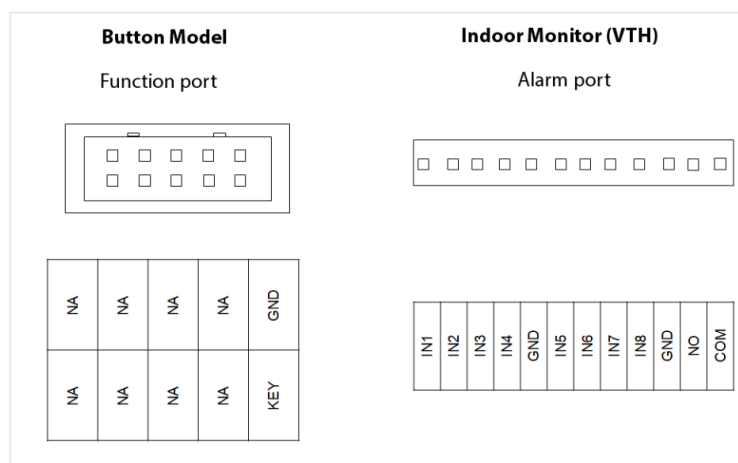


Tabla 13-1 Componente

No.	Nombre	Función
1	presiona el botón	El modelo de botón se puede conectar al VTH. Presione el botón en el modelo y el VTH recibe una señal de alarma.

Figura 13-2 Conexión de cables



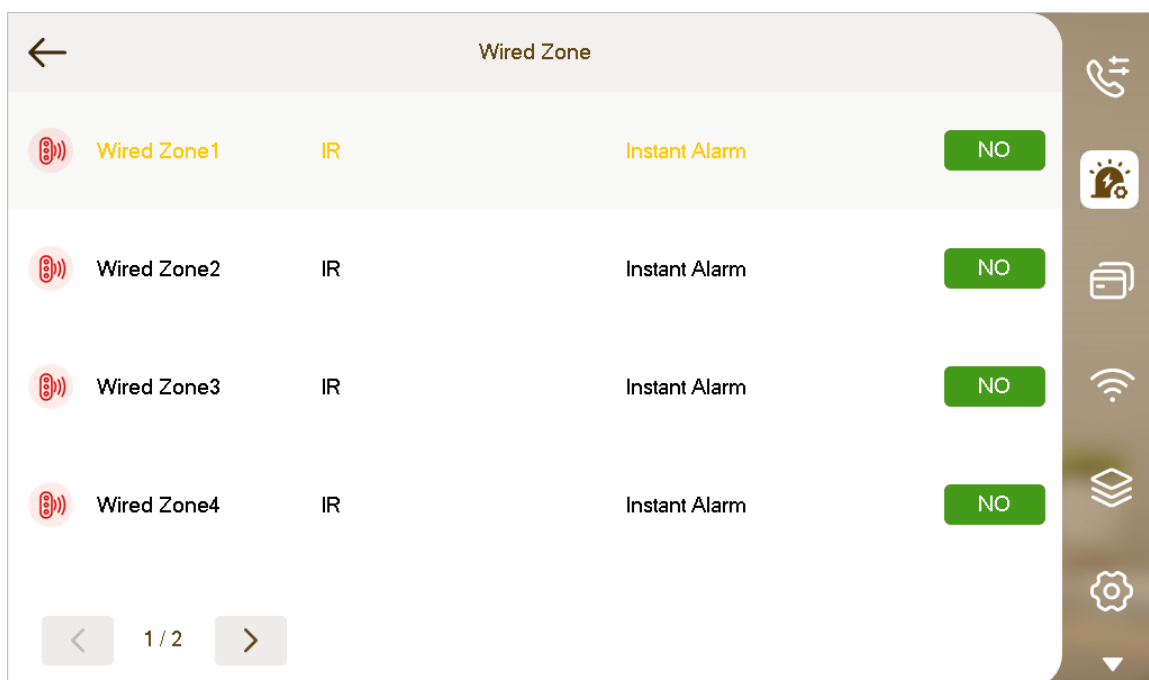
13.2 Configuración VTH

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** Seleccionar **Configuración > Alarma > Zona cableada** en el VTH.

Figura 13-3 Configuración de zona cableada



- Paso 3** Selecciona el **Tip** como **Timbre de la puerta** y configurar el resto de parámetros.

Tabla 13-2 Descripción del parámetro

Parámetro	Descripción	
Área	El número no se puede modificar.	
NO C	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 de armado, si se activa una alarma, el dispositivo emite una sirena de inmediato y entra en estado de alarma. ● Alarma de retraso: Después de armado, si se activa una alarma, el dispositivo ingresa al estado de alarma después de un tiempo específico, durante el cual puede desarmar y cancelar la alarma. ● Derivación: La alarma no se activará en el área. Después de desarmar, esta área volverá a su estado de funcionamiento normal. ● 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 se arma o desarma.  una zona en Eliminar El estado no se puede pasar por alto.	
Introducir retraso	Después de ingresar al retraso, cuando el área armada activa una alarma, ingresar al área armada desde el área no armada dentro del período de tiempo de retraso no generará una alarma de vinculación. Se producirá una alarma de enlace si finaliza el tiempo de retardo y no se desarma.	
Retardo de salida	Después del brazo, Alarma de retraso El área entrará en estado armado al final del Retardo de salida.  Si varias áreas configuran el retraso de salida, el mensaje en pantalla se ajustará al tiempo de retraso máximo.	El retraso sólo es válido para las áreas de Alarma de retraso.

Apéndice 1 Recomendaciones de ciberseguridad

Acciones obligatorias que se deben tomar para la seguridad básica de la red de dispositivos:

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

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

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

1. Protección física

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

2. Cambie las contraseñas con regularidad

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de que las adivinen o las descifren.

3. Establecer y actualizar contraseñas Restablecer información oportunamente

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

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilitar HTTPS

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

7. Enlace de dirección MAC

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

8. Asignar cuentas y privilegios de forma razonable

De acuerdo con los requisitos comerciales y de administración, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

9. Deshabilite los servicios innecesarios y elija modos seguros

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

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

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

10. Transmisión cifrada de audio y vídeo

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

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

11. Auditoría segura

- Verifique los usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo inició sesión sin autorización.
- Verifique el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se utilizaron para iniciar sesión en sus dispositivos y sus operaciones clave.

12. Registro de red

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

13. Construya un entorno de red seguro

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

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