Estación maestra

Manual de usuario

V1.0.0

Prefacio

General

Este manual presenta las operaciones básicas de la estación maestra.

Las instrucciones de seguridad

Las siguientes palabras de advertencia categorizadas con significado definido pueden aparecer en el manual.

Palabras de advertencia	Sentido
PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
Nota	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de la revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento	Abril de 2020

Acerca del manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No nos hacemos responsables de ninguna pérdida causada por las operaciones que no cumplan con el manual. El manual se
- actualizaría de acuerdo con las leyes y regulaciones más recientes de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.

- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más actualizado y la documentación complementaria. Todavía puede haber desviaciones en los datos técnicos, la
- descripción de funciones y operaciones, o errores en la impresión. Si hay alguna duda o disputa, nos reservamos el derecho a una explicación final. Actualice el software del lector o pruebe con otro software de lectura convencional si no puede abrir el manual (en
- formato PDF).

- Todas las marcas comerciales, marcas comerciales registradas y los nombres de empresas que aparecen en el manual son propiedad de sus respectivos propietarios.
- Visite nuestro sitio web, póngase en contacto con el proveedor o el servicio de atención al cliente si se produce algún problema al utilizar el dispositivo.
- Si existe alguna duda o controversia, nos reservamos el derecho a una explicación final.

Advertencias y medidas de seguridad importantes

La siguiente descripción es el método de aplicación correcto de la estación maestra. Lea atentamente el manual antes de usarlo para evitar peligros y pérdidas materiales. Cumpla estrictamente con el manual durante la aplicación y consérvelo correctamente después de leerlo.

Requisitos operativos

- No coloque ni instale el dispositivo en un área expuesta a la luz solar directa o cerca de un dispositivo generador de calor.
- No instale el dispositivo en un área húmeda, polvorienta o fuliginosa.
- Mantenga su instalación horizontal, o instálelo en lugares estables, y evite que se caiga.
- No gotee ni salpique líquidos sobre el dispositivo; No coloque sobre el dispositivo nada lleno de líquido para evitar que los líquidos fluyan hacia el dispositivo.
- Instale el dispositivo en lugares bien ventilados; no bloquee su abertura de ventilación. Utilice el dispositivo solo
- dentro del rango nominal de entrada y salida.
- No desmonte el dispositivo de forma arbitraria.
- El dispositivo se utilizará con cables de red apantallados.

requerimientos de energía

- El producto utilizará cables eléctricos (cables de alimentación) requeridos por la región donde se utilizará el dispositivo.
- Utilice una fuente de alimentación que cumpla con los requisitos de SELV (voltaje de seguridad muy bajo) y suministre energía con un voltaje nominal que cumpla con la Fuente de energía limitada en IEC60950-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas del dispositivo.
- El acoplador de electrodomésticos es un dispositivo de desconexión. Durante el uso normal, mantenga un ángulo que facilite la operación.
- No corte la fuente de alimentación durante la actualización del dispositivo.

- Riesgo de explosión si se reemplaza la batería por un tipo incorrecto.
- No arrojar ni sumergir en agua, calentar a más de 100 ℃ (212 ℉), reparar o desmontar, dejar en un ambiente de presión de aire extremadamente baja o ambiente de temperatura extremadamente alta, aplastar, perforar, cortar o incinerar.
- Deseche la batería según lo requieran las ordenanzas o regulaciones locales.

Tabla de contenido

1. Información general

1.1 Introducción

- Puede tener videollamadas bidireccionales con monitores interiores (VTH), estaciones de puerta (VTO) y estaciones de cerca.
- Puede ver videos capturados por cámaras IP, estaciones de puerta (VTO) y estaciones de cerca en la estación maestra.
- Desbloquee las puertas de forma remota.
- Puede enviar llamadas de emergencia a la estación maestra a través de monitores interiores (VTH) y estaciones de puerta (VTO).

1.2 Características

- Operación fácil; no es necesario instalarlo; soporte 0–45 ° ajustable. Admite múltiples
- dispositivos de monitoreo; como máximo 4 canales 1080P. Pantalla táctil capacitiva LCD de
- 10 pulgadas, interacción persona-computadora. Dos modos de llamada: manos libres y
- auricular.
- Expansión de tarjeta SD.
- 1 puerto de salida HDMI; resolución máxima 1024 × 600.

1.3 Apariencia

El VTS se puede colocar sobre el escritorio a través del soporte. El ángulo del soporte (0–45 °) es ajustable.

Panel frontal

Figura 1-1 Apariencia

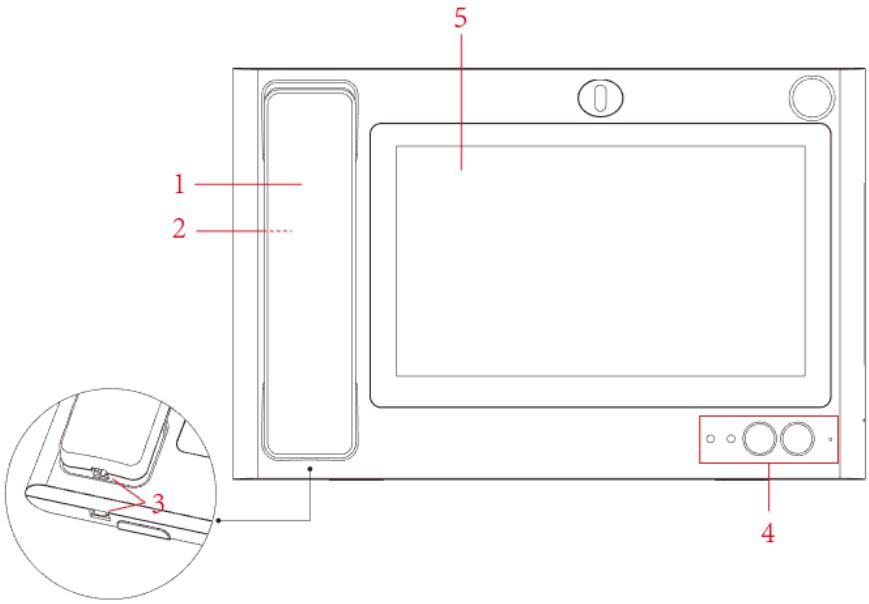


Tabla 1-1 Descripción del panel frontal

No.	Parámetro	Descripción
1	MIC	Convierte el sonido en una señal eléctrica.
2	Altavoz	Emite sonido.
3	Puerto telefónico	Conectado a la estación maestra y al micrófono. De izquierda a derecha:
4	Indicador	• Indicador de encendido Si el indicador está encendido, indica que el dispositivo está encendido. Si el indicador está apagado, el dispositivo no está conectado a la fuente de alimentación. • Indicador de información Si la luz indicadora está encendida, indica que el dispositivo tiene una llamada perdida. Si la luz indicadora está apagada, la llamada perdida se ha procesado o no hay llamadas perdidas. • Botón de desbloqueo Cuando esté haciendo llamadas, viendo videos o hablando con otras personas a través del VTS, presione el botón de desbloqueo y podrá abrir las puertas de forma remota. • Botón de manos libres Presione el botón y luego puede seleccionar el modo de manos libres o el modo de auricular. • MIC incorporado Entradas de sonido.
5	Pantalla y toque	Pantalla y área táctil.

Panel trasero

Figura 1-2 Panel trasero

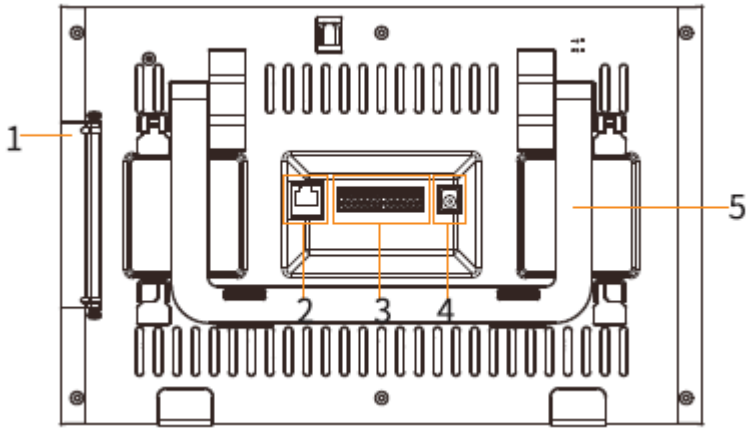


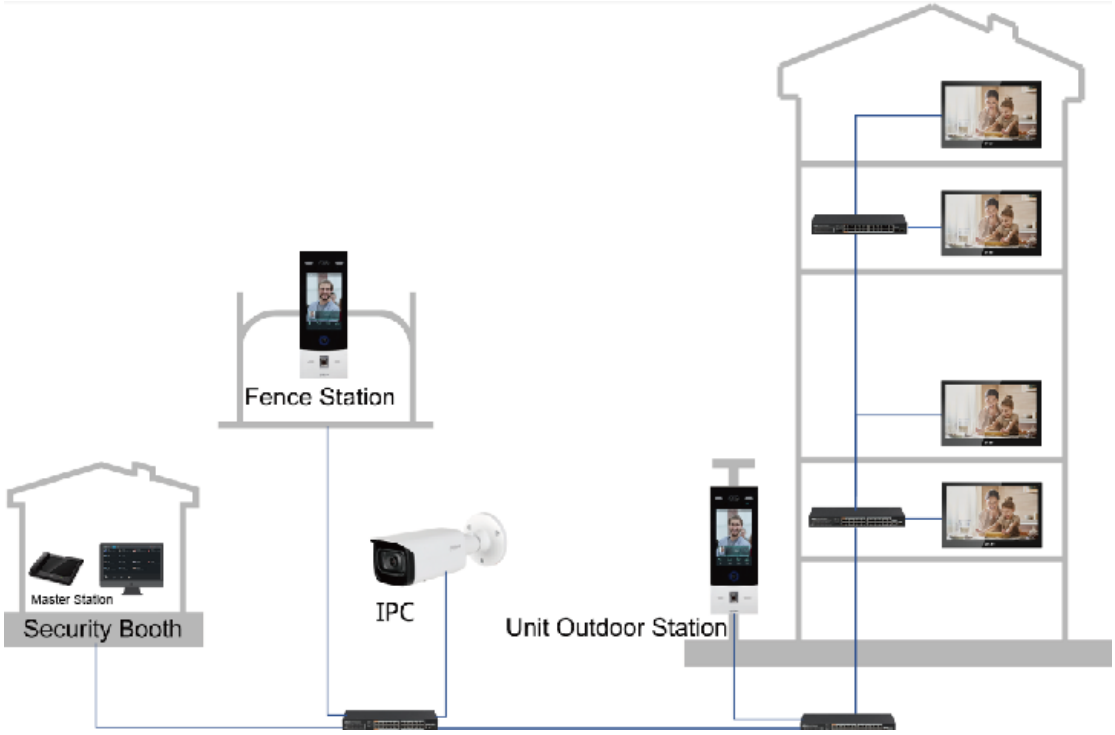
Tabla 1-2 Descripción del panel trasero

No.	Parámetro	Descripción
1	Puerto	• Puerto de transmisión de video HDMI, solo para video. Puerto USB. • • Puerto USB. • Ranura para tarjetas SD.
2	Puerto de red	Se utiliza para conectar el cable RJ-45. Los puertos
3	Puerto de 12 pines	de izquierda a derecha son: • Puerto de salida de energía. • GNS. • Puerto de entrada de alarma 1. • Puerto de entrada de alarma 2. • Puerto de entrada de alarma 3. • Puerto de entrada de alarma 4. • Puerto de entrada de energía. • GND. • Puerto RS-485A. • RS-485B por. • Puerto de salida de alarma NO. Puerto • de salida de alarma COM. Energía DC 12V
4	Puerto de alimentación	
5	Soporte	Coloque el maestro en el escritorio. Puede ajustar el ángulo del soporte a una posición adecuada.

2 Cableado

- Utilice el adaptador de corriente que viene en la caja con la estación maestra. No utilice otros adaptadores de corriente.
- Antes de encender el VTS, asegúrese de que todos los cables estén conectados correctamente. Si el VTS está funcionando normalmente, la luz indicadora estará en rojo.

Figura 2-1 Conexión de cables

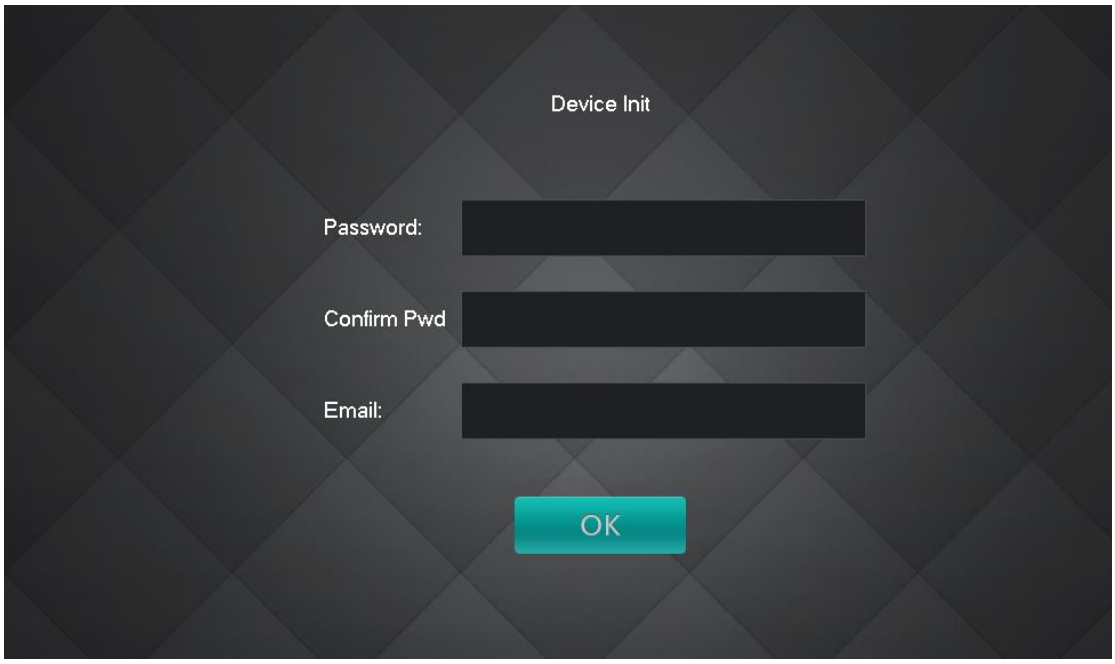


3 Configuración

3.1 Inicialización

Por primera vez, debe configurar la contraseña y el correo electrónico. La contraseña se utiliza para ingresar **Inicio de sesión avanzado** interfaz.

Figura 3-1 Inicialización

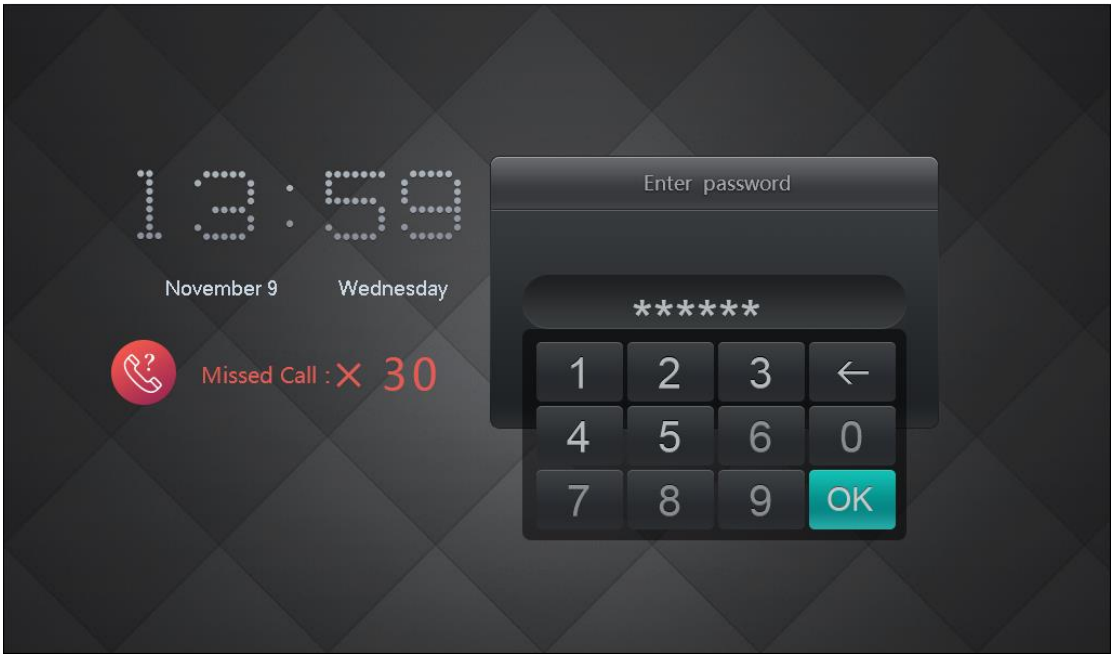


- Si olvidas el **Inicio de sesión avanzado** contraseña, puede restablecer la contraseña con la dirección de correo electrónico que ingresó aquí.
- La contraseña debe tener 6 números.

3.2 Iniciar sesión

Introduzca la contraseña de inicio de sesión del VTS (123456 de forma predeterminada y no se puede modificar) y luego toque **OKAY.**

Figura 3-2 Inicio de sesión



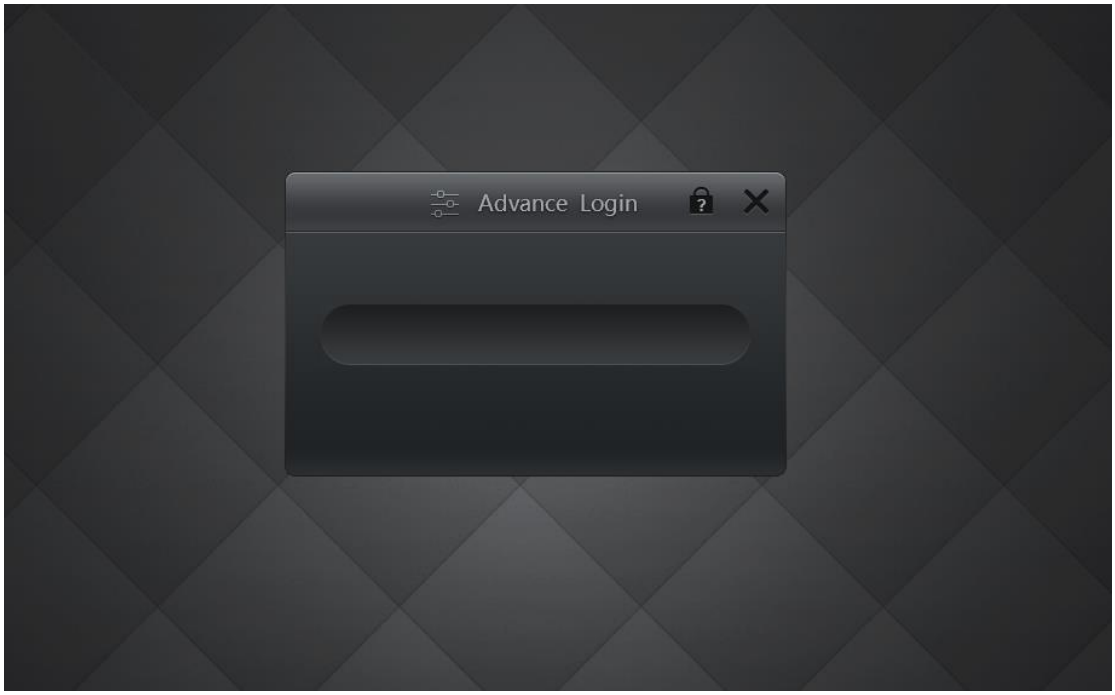
3.3 Restablecimiento de la contraseña

Si olvida la contraseña para iniciar sesión en **Inicio de sesión avanzado** interfaz, puede guardar la contraseña a través de la dirección de correo electrónico que ingresó en el **Inicialización** interfaz.

Debe habilitar la función de restablecimiento de contraseña. Consulte "3.8 Restablecimiento de mensajes".

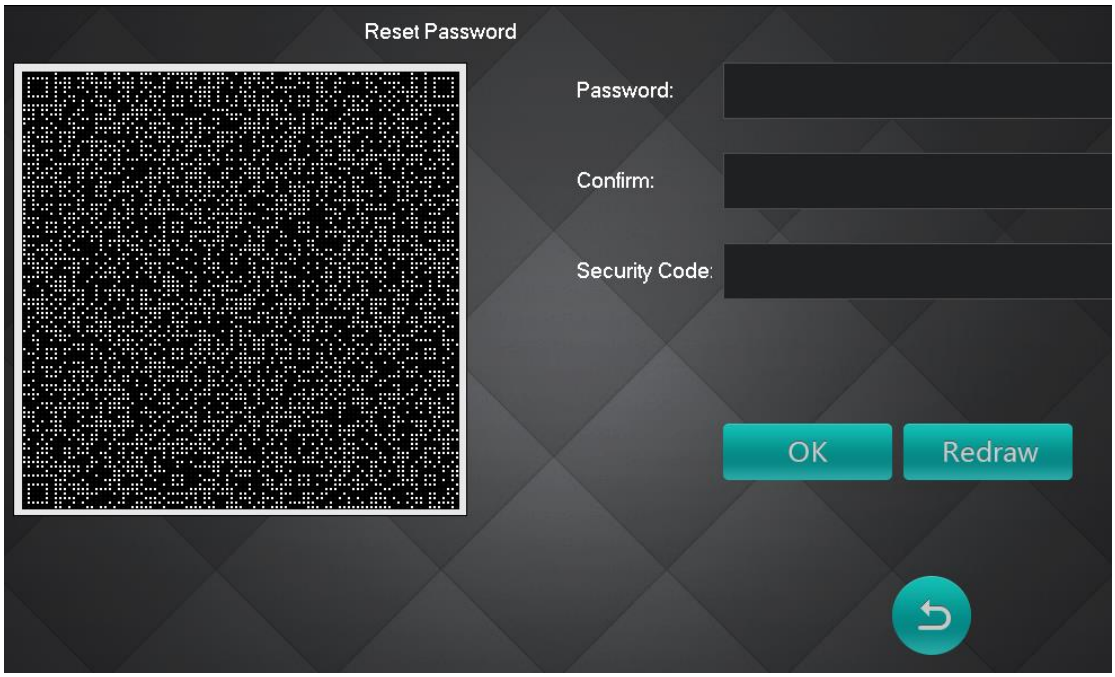
Paso 1 toque sobre el **Inicio de sesión avanzado** interfaz.

Figura 3-3 Inicio de sesión avanzado



Paso 2 Toque **OKAY.**

Figura 3-4 Restablecer contraseña



Paso 3 Escanee el código QR en la interfaz con cualquier aplicación que tenga función de escaneo.

Se mostrará una cadena. Envía la cadena a support_gpwd@htmicrochip.com con la dirección de correo

Paso 4 electrónico configurada en el **Inicialización** interfaz.

Se enviará un código de seguridad a su dirección de correo electrónico.

Paso 5 Ingrese la nueva contraseña, confirme la contraseña y el código de seguridad.

Paso 6 Toque **OKAY.**

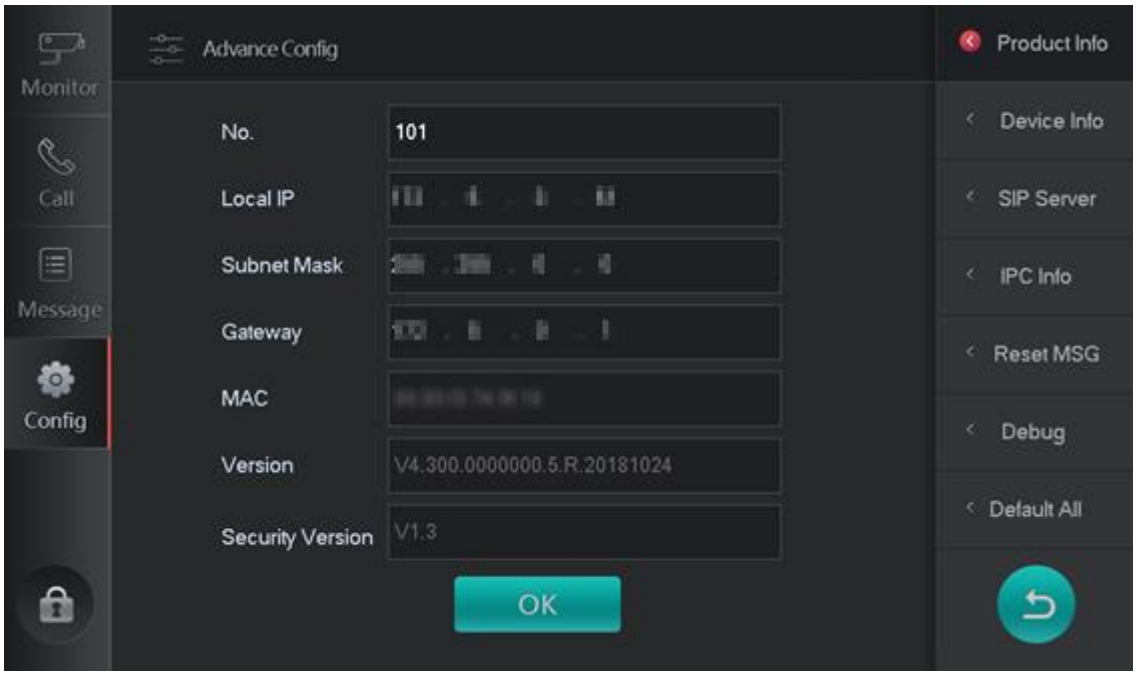
Se restablece la contraseña.

3.4 Configuración local

Puede configurar el número de dispositivo, la dirección IP, la máscara de subred y la puerta de enlace seleccionando **Configuración> Configuración avanzada> Información del producto.**

- los **Inicio de sesión avanzado** La contraseña se establece durante la inicialización o se puede modificar en el **Restablecer la contraseña** interfaz.
- Asegúrese de que la dirección IP que ingresó esté en el mismo segmento de red que las estaciones de puerta y los monitores interiores; de lo contrario, los dispositivos no se pueden comunicar entre sí.

Figura 3-5 Configuración local



3.5 Adición de estaciones de puerta (VTO) / estación de valla

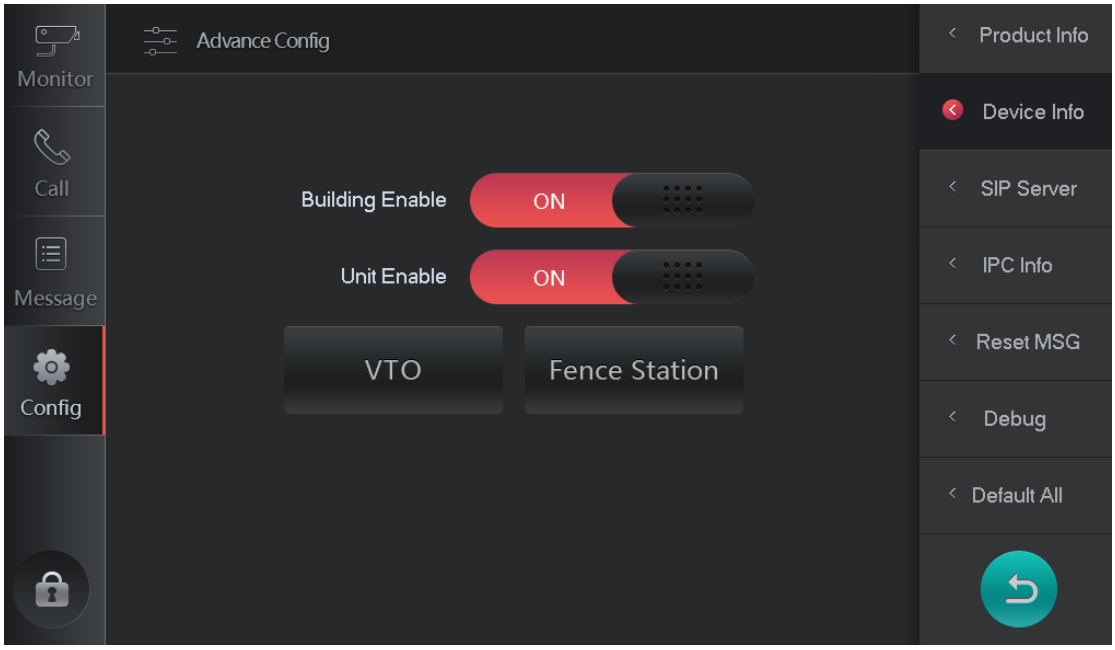
Puede agregar estaciones de puerta (VTO) y estaciones de cerca una por una o en lotes seleccionando **Configuración> Configuración avanzada> Información del dispositivo.**

Antes de agregar estaciones de puerta y estaciones de cerca, asegúrese de que estén conectadas a la fuente de alimentación y que estén en el mismo segmento de red.

- Agregar una estación de puerta (VTO)

Paso 1 Seleccione **Configuración> Configuración avanzada> Información del dispositivo.**

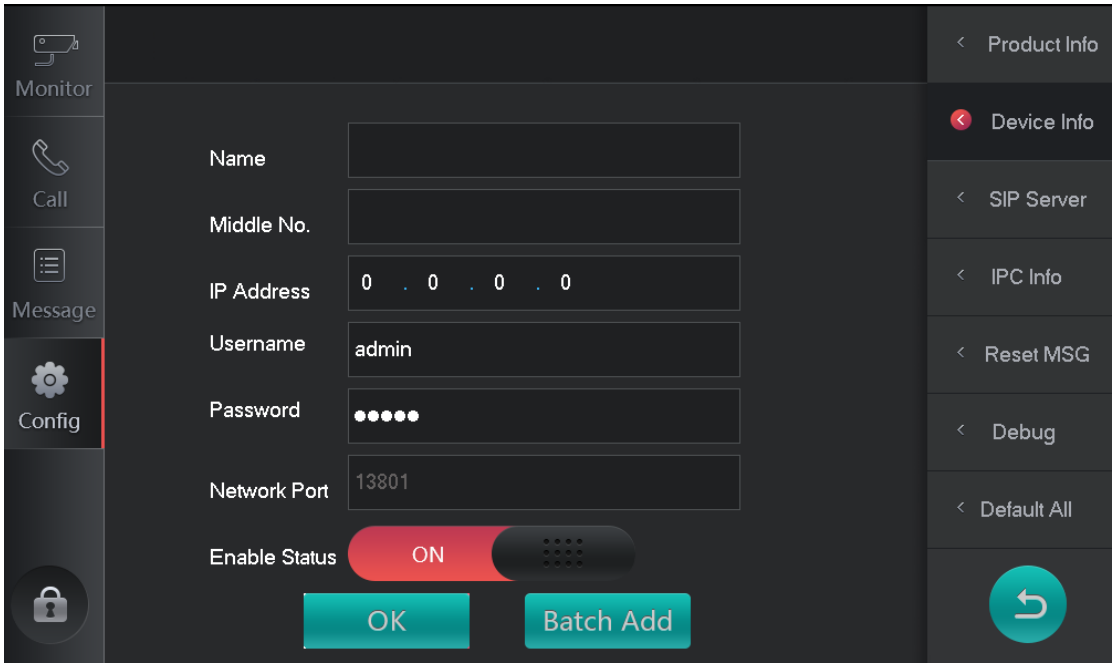
Figura 3-6 Información del dispositivo



Paso 2 Toque **VTO.**

Paso 3 Toque **Añadir.**

Figura 3-7 Agregar un dispositivo



Paso 4 Ingrese el nombre, el número intermedio, la dirección IP, el nombre de usuario y la contraseña, y luego encienda el **Habilitar estado.**

Paso 5 Grifo **OKAY.**

" Por favor espera" se visualiza. Grifo **Okay** para continuar agregando estaciones de puerta (VTO). Las estaciones de puerta agregadas (VTO) se pueden ver seleccionando **Monitor> Estación de puerta / Estación de valla.**

- Agregar estaciones de puerta (VTO) en lotes

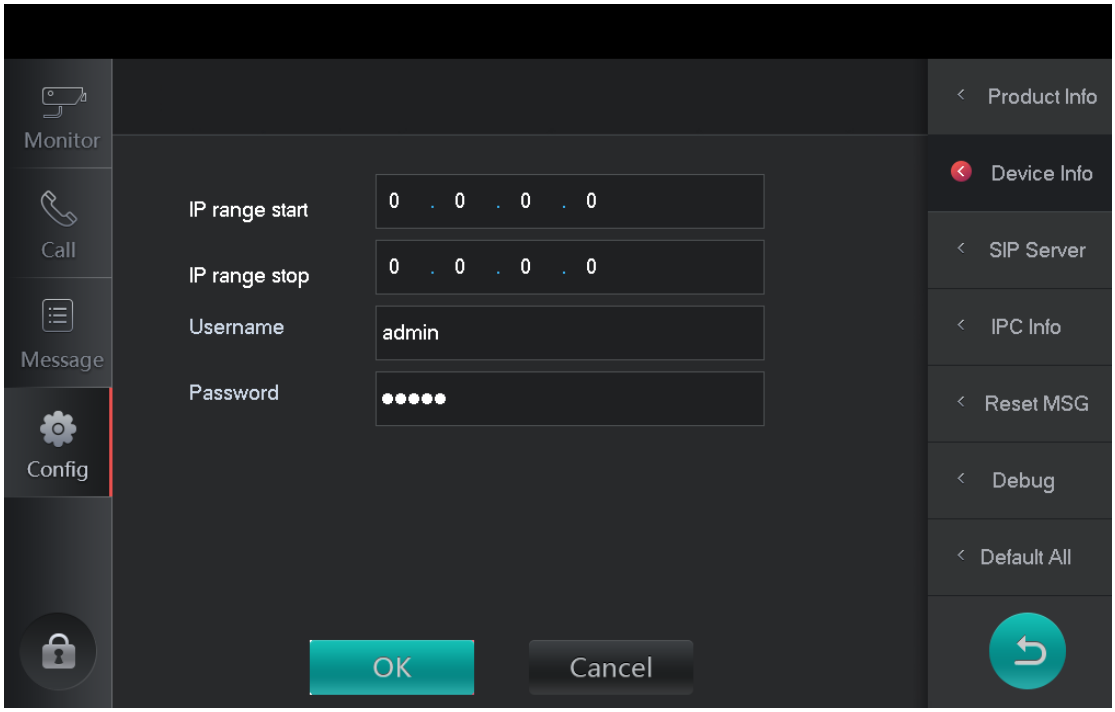
Paso 1 Seleccione **Config> Advance Condig> Información del dispositivo.**

Paso 2 Toque **VTO.**

Paso 3 Toque **Añadir.**

Paso 4 Toque **Agregar lote.**

Figura 3-8 Agregar estaciones de puerta (VTO) en lotes



Paso 5 Introduzca la IP inicial, la IP final, el nombre de usuario y la contraseña.

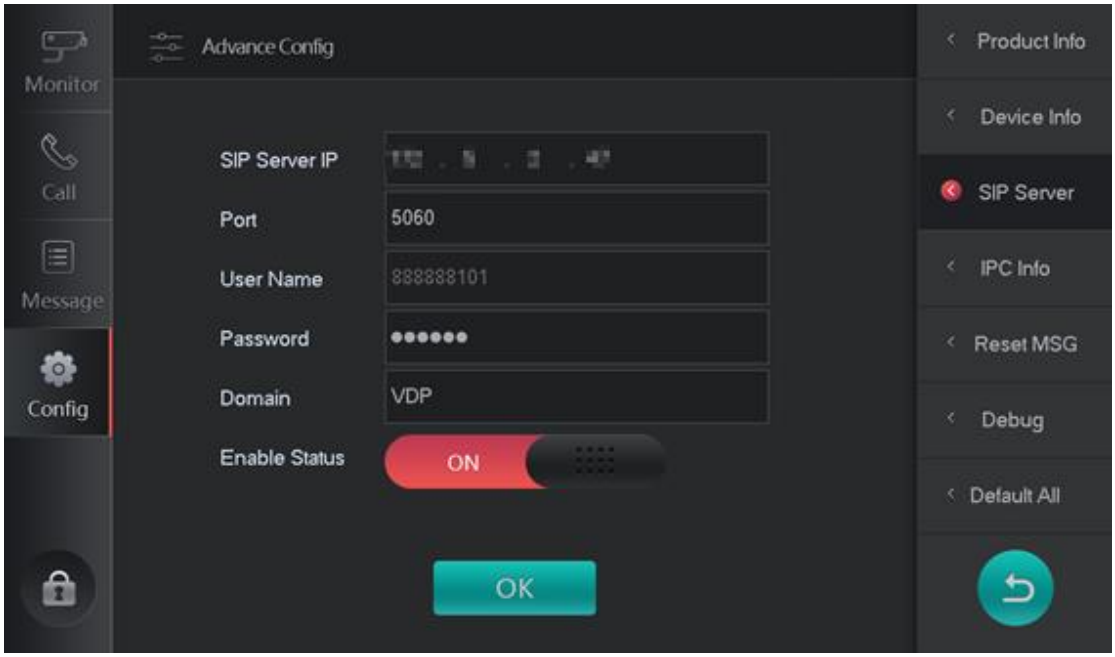
Paso 6 Toque **OKAY.**

" **Por favor espera"** se visualiza. Grifo **Okay** para continuar agregando estaciones de puerta (VTO). Las estaciones de puerta agregadas (VTO) se pueden ver seleccionando **Monitor> Estación de puerta / Estación de valla.**

3.6 Configuración del servidor SIP

Paso 1 Seleccione **Configuración> Configuración avanzada> Servidor SIP.**

Figura 3-9 Configuración del servidor SIP



Paso 2 Configure los parámetros.

Tabla 3-1 Configuración del servidor SIP

Parámetro	Descripción
IP del servidor SIP	Ingrese la dirección IP del servidor SIP.
Puerto	• Cuando la plataforma funciona como servidor SIP, el puerto de red es 5080. Cuando VTO funciona • como servidor SIP, el puerto de red es 5060. No es necesario modificarlo. Mantenga el valor
Nombre de usuario	predeterminado.
Contraseña	123456 por defecto.
Dominio	Mantenga el valor predeterminado.

Paso 3 Seleccione **EN** Para el **Habilitar estado.**

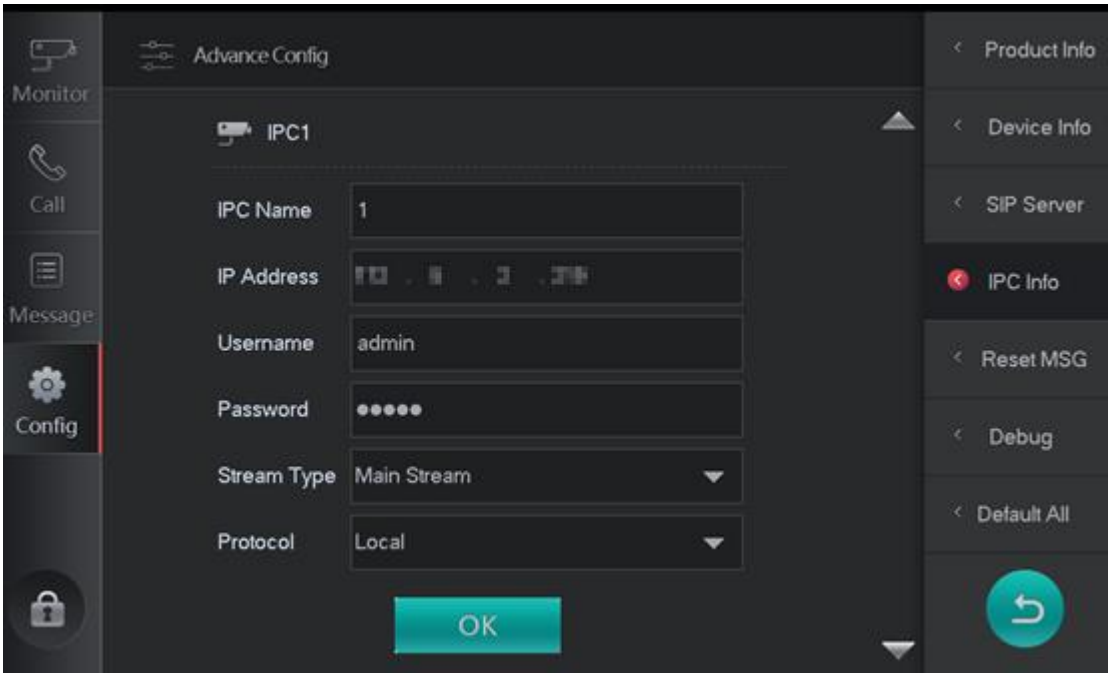
Paso 4 Toque **OKAY.**

3.7 Agregar cámaras IP

Puede agregar hasta 32 cámaras IP. Puede ver videos de monitoreo capturados por las cámaras IP.

Paso 1 Seleccione **Configuración> Configuración avanzada> Información de IPC.**

Figura 3-10 Agregar cámaras IP



Paso 2 Configure los parámetros.

Tabla 3-2 Agregar cámaras IP

Parámetro	Descripción
Nombre del IPC	Ingrese el nombre de la cámara IP. Ingrese la
Dirección IP	dirección IP de la cámara IP.
Nombre de usuario	Nombre de usuario y contraseña utilizados para iniciar sesión en la interfaz web de IPC.
Contraseña	
Tipo de flujo	• Flujo principal: flujo grande, alta definición, ocupa un gran ancho de banda, adecuado para almacenamiento local. • Sub Stream: videos fluidos, ocupa poco ancho de banda, adecuado para transmisión de red de bajo ancho de banda.
Protocolo	Dos opciones: protocolo local y protocolo Onvif. Seleccione según sea necesario.

Paso 3 Toque **OKAY.**

Las cámaras IP agregadas se pueden ver seleccionando **Monitor> Cámara IP.**

Puede tocar para continuar agregando cámaras IP.

3.8 Restablecimiento de mensajes

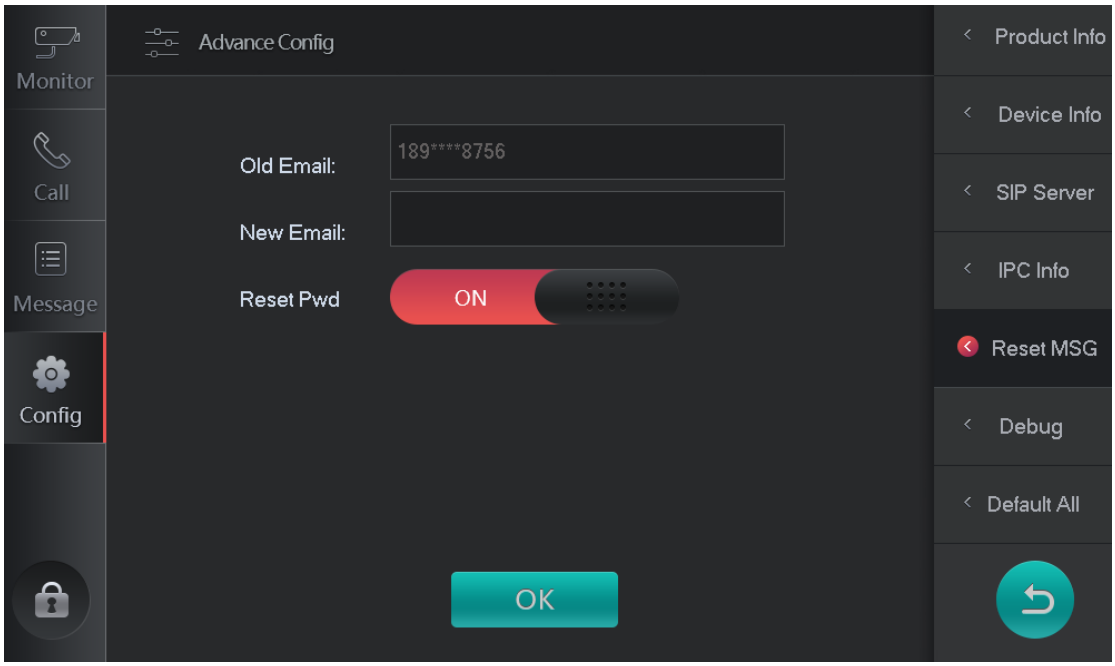
Puede modificar la dirección de correo electrónico que ingresó durante la inicialización para restablecer la contraseña.

Paso 1 Seleccione **Configuración> Configuración avanzada> Restablecer MSG.**

Paso 2 Ingrese un nuevo correo electrónico.

Paso 3 Toque el **APAGADO** para habilitar la función de restablecimiento de contraseña.

Figura 3-11 Restablecimiento de contraseña



Paso 4 Toque **OKAY.**

3.9 Depurar

La función de depuración es solo para ingenieros.

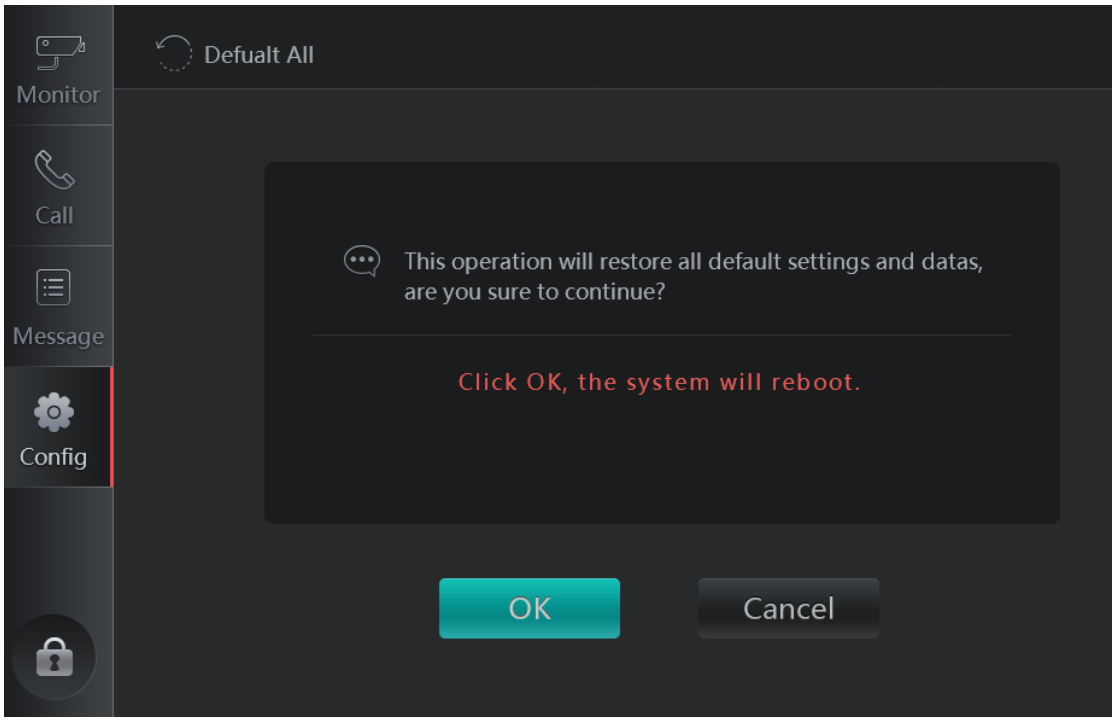
Paso 1 Seleccione **Configuración> Configuración avanzada> Depurar.**

Paso 2 Toque **APAGADO** para habilitar la función SSH.

3.10 DefaultAll

Puede restaurar el VTS a la configuración de fábrica seleccionando **Configuración> Configuración avanzada> Todo predeterminado.** Después de la restauración, el VTS se reiniciará.

Figura 3-12 Predeterminado



4 Operación básica

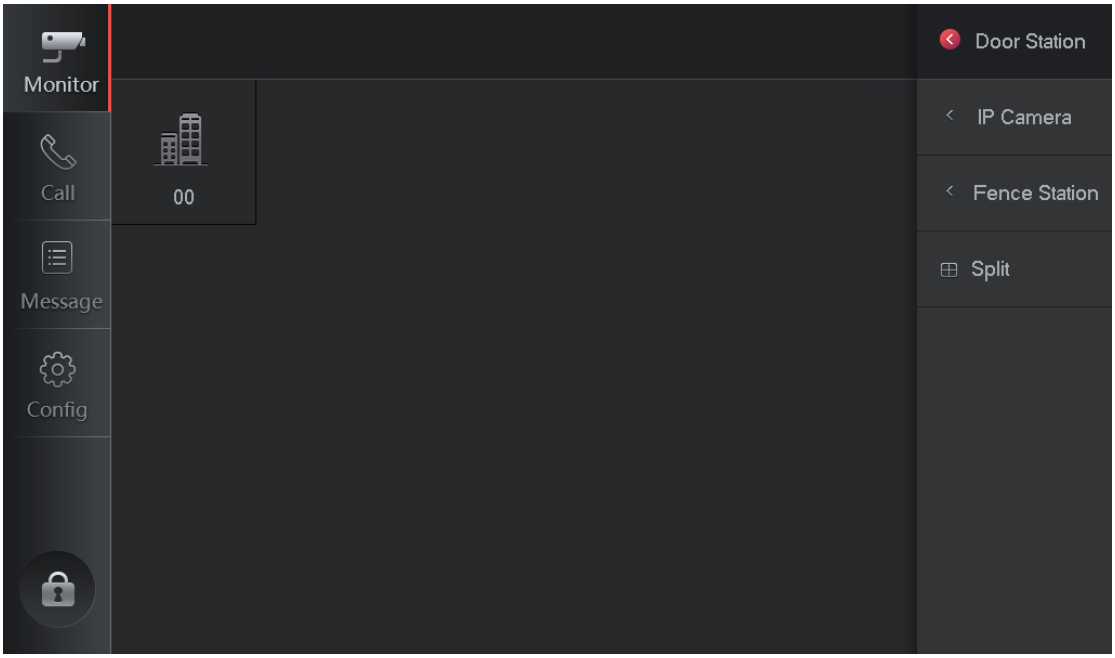
4.1 Ver videos de monitoreo

Puede ver videos capturados por cámaras IP, estaciones de puerta y estaciones de cerca que están conectadas al VTS.

Al ver videos capturados por cámaras IP, estaciones de puerta y estaciones de cerca, las operaciones son las mismas.

Paso 1 Seleccione **Monitor> Videoportero.**

Figura 4-1 Monitor



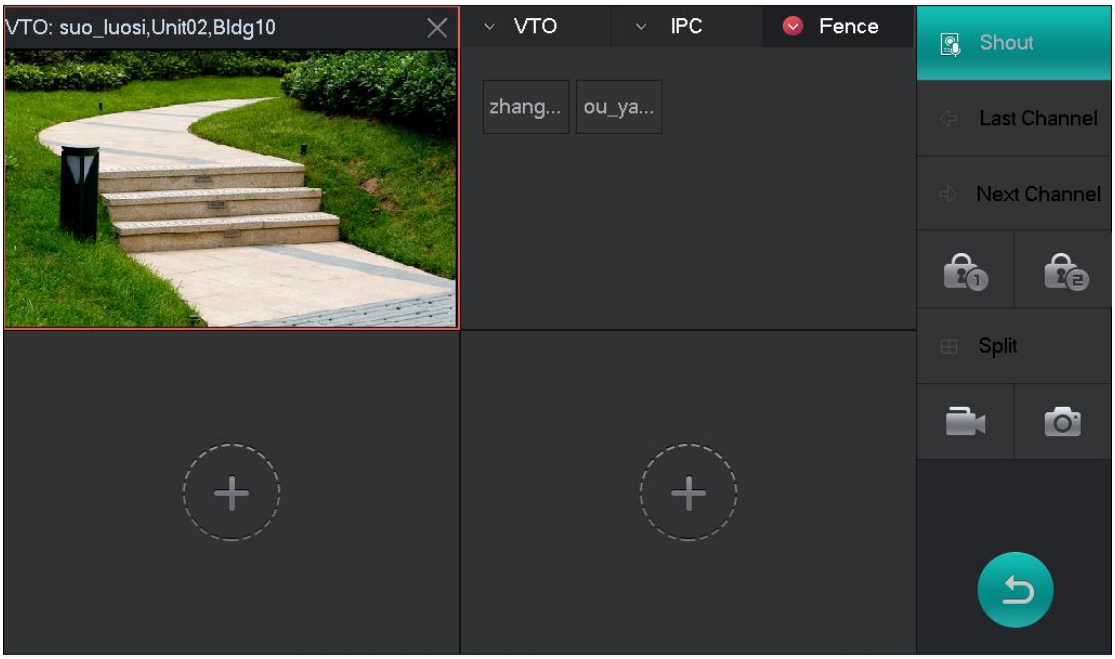
Paso 2 Seleccione una estación de puerta (VTO).

Figura 4-2 Ver videos de monitoreo

Tabla 4-1 Descripciones de cómo ver videos de monitoreo

Parámetro	Descripción	
Llamada	presione el **Gritar** para iniciar una llamada con la estación de puerta (VTO).	
Último canal Siguiente canal	Si hay más de una estación de puerta conectada a la estación maestra, toque **Último canal** y **Siguiente canal** para seleccionar diferentes estaciones de puerta (VTO). Si desea ver	
División	varios videos de monitoreo al mismo tiempo, toque **División** para agregar estaciones de puerta y cámaras IP. Vea la Figura 4-3.	
desbloquear	Grifo  para desbloquear puertas conectadas a estaciones de puerta (VTO).	
Grabar	Grifo  para grabar videos o tocar  para dejar de grabar videos.	• Si la tarjeta SD no está insertada, el icono será gris. • Las instantáneas y los videos se almacenan en la tarjeta SD.
Instantánea	Grifo  para tomar instantáneas.	

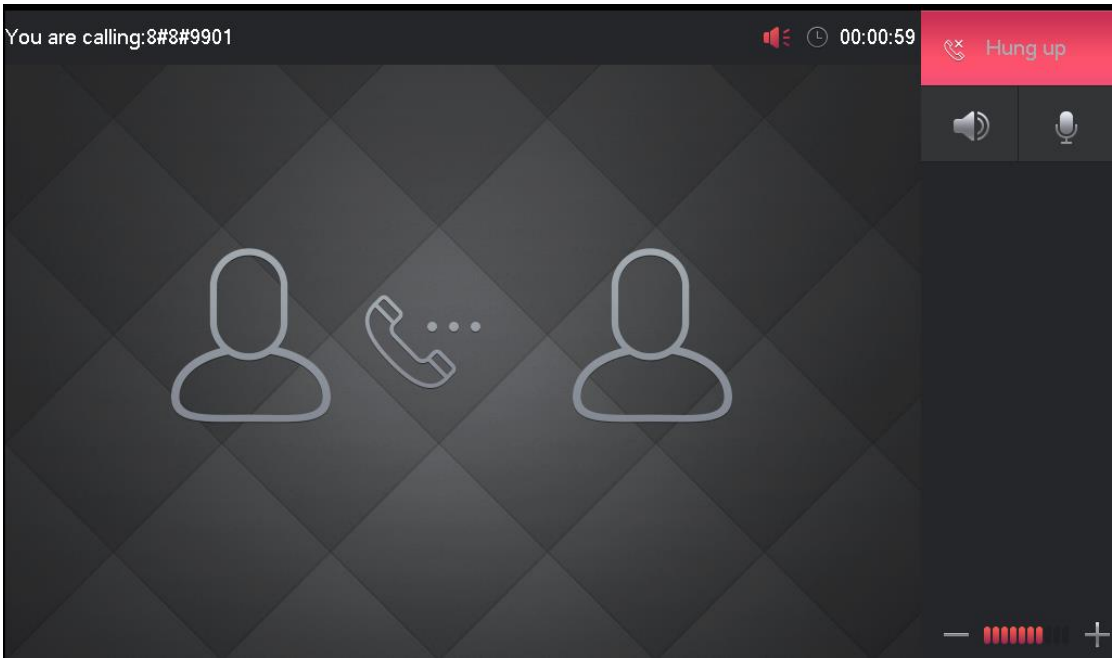
Figura 4-3 Ver varios videos de monitoreo



4.2 Realizar llamadas a monitores interiores

Puede llamar a las estaciones de puerta (VTO) a través de la estación maestra.

Figura 4-4 Llamar a monitores interiores



4.2.1 Llamar a monitores interiores (VTH)

Ingrese el número del edificio, el número del apartamento y el número de la habitación, y luego puede llamar a los monitores interiores (VTH).

Figura 4-5 Llamar a monitores interiores

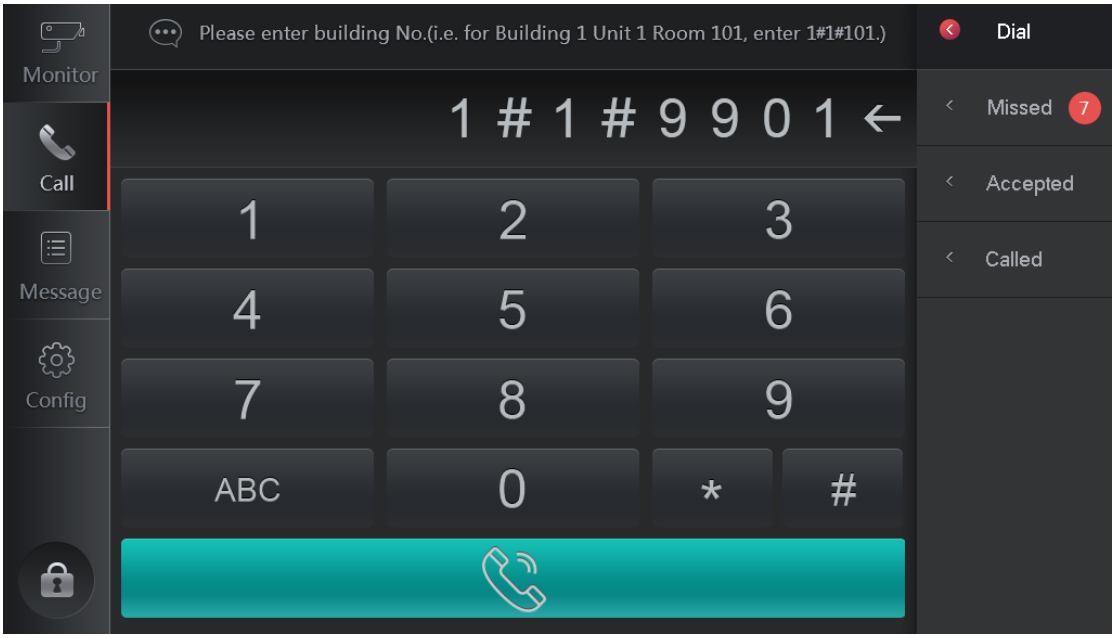


Figura 4-6 Durante la llamada con el monitor interior

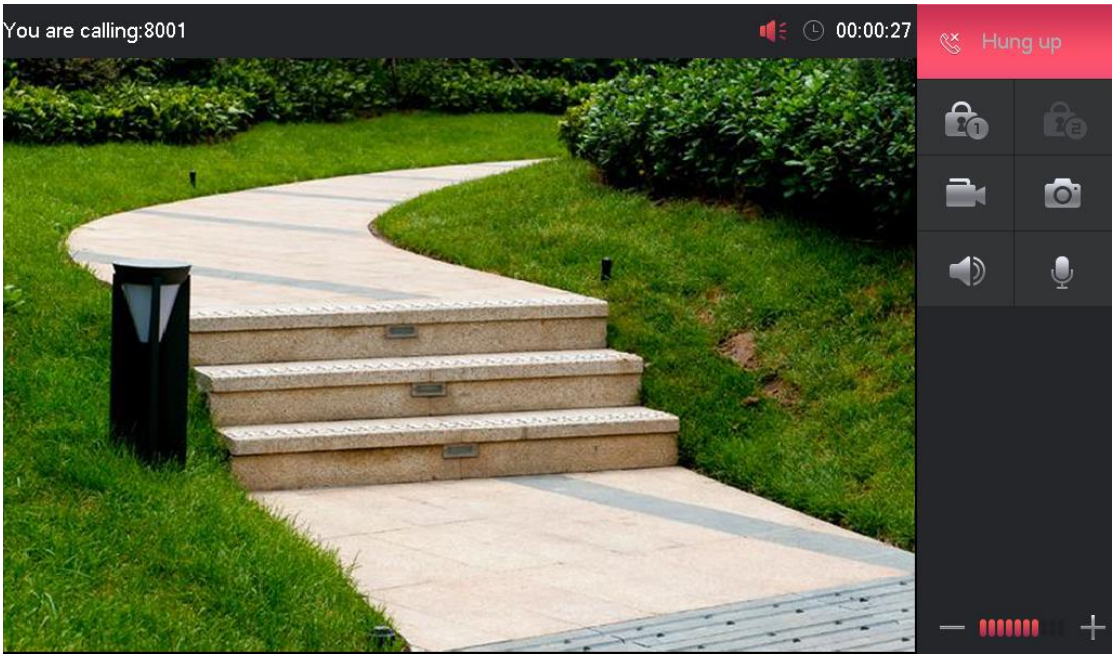


Tabla 4-2 Detalles de la realización de llamadas a monitores interiores

Icono	Nombre	Descripción	
Hung up	Colgar	Durante una llamada, toque Hung up para colgar la llamada.	
	Altavoz	Se utiliza para encender / apagar la salida de audio de la estación maestra.	
	MIC	Se usa para encender / apagar la entrada de audio VTS.	
	Grabar	Grifo para grabar videos o tocar • dejar de grabar videos.	• Si la tarjeta SD no está insertada, el icono será gris.
	Instantánea	Grifo para tomar instantáneas.	• Instantáneas y videos se almacenan en la tarjeta SD.
	Volumen	Ajusta el volúmen.	

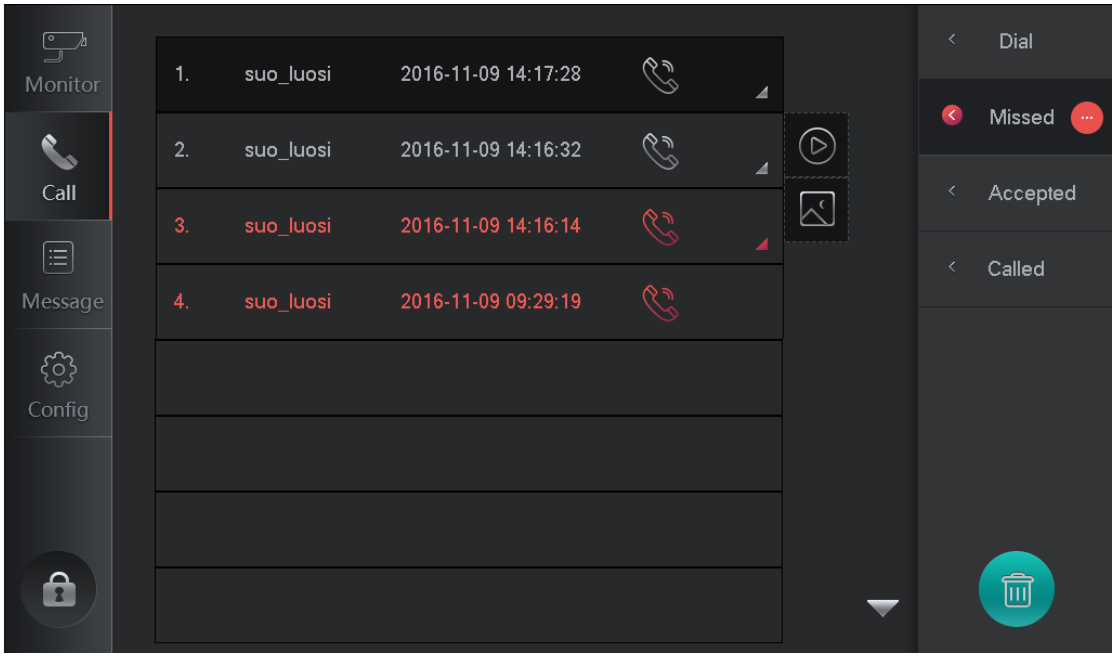
4.2.2 Registros de llamadas

Puede ver y borrar todos los registros de llamadas.

Paso 1 Seleccione **Llamar> Perdido.**

- Textos en blanco: Se han visualizado registros. Textos
- naranjas: registros no visualizados.
- Graba con: Hay videos o instantáneas durante la llamada.

Figura 4-7 Registros de llamadas



Paso 2 Toque el registro de una llamada para ver los detalles.

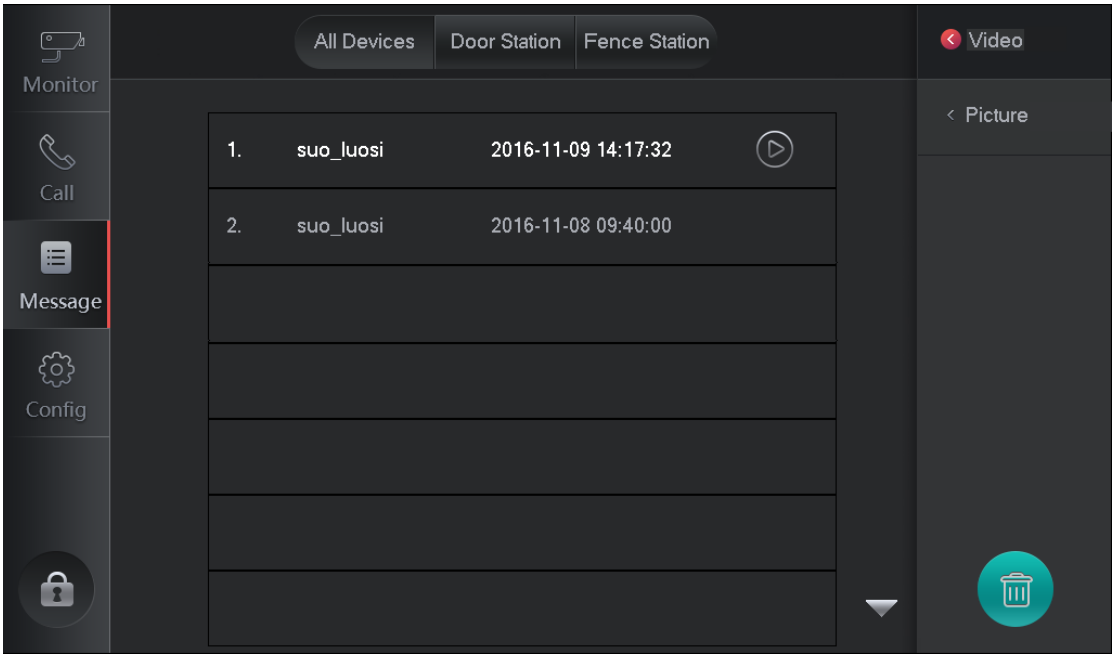
- Puede tocar para borrar todos los registros.
- Grifo o para ver los detalles del registro o de la instantánea

4.3 Mensaje

Puede ver o borrar videos e instantáneas de estaciones de vallas / VTO en el **Mensaje** interfaz.

Paso 1 toque **Mensaje> Todos los dispositivos.**

Figura 4-8 Mensaje



Paso 2 Puede ver videos grabados o instantáneas.

- Seleccione **Vídeo,** y luego toque  para ver videos grabados.
- Seleccione **Imagen,** y luego toque  para ver instantáneas.

Tabla 4-3 Detalles de la interfaz de mensajes

Icono	Descripción	Icono	Descripción
	Pausa		Canal anterior
	Detener		Siguiente canal
	Juego lento		Volumen encendido / apagado
	Avance rápido		Salida
	Ajusta el volúmen	-	-

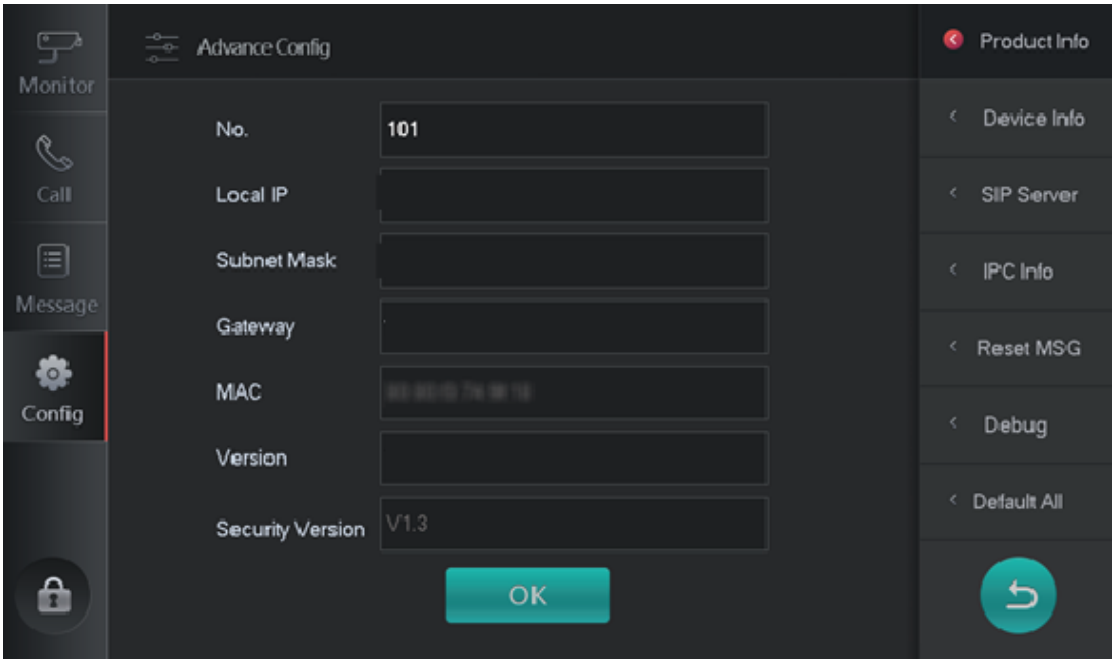
4.4 Desbloquear

Cuando haya llamadas entrantes, durante las llamadas o cuando vea videos capturados por estaciones de puerta o cámaras IP en el monitor interior (VTH), toque esta tecla para desbloquear las cerraduras conectadas a las estaciones de puerta correspondientes (VTO).

4.5 Versión

Puede ver información detallada de la estación maestra en **Configuración> Configuración avanzada> Información del producto.**

Figura 4-9 Versión



4.6 Configuración básica

Puede configurar la pantalla VTS, el timbre, la tarjeta SD y la duración de la llamada en el **Config** interfaz.

4.6.1 Pantalla

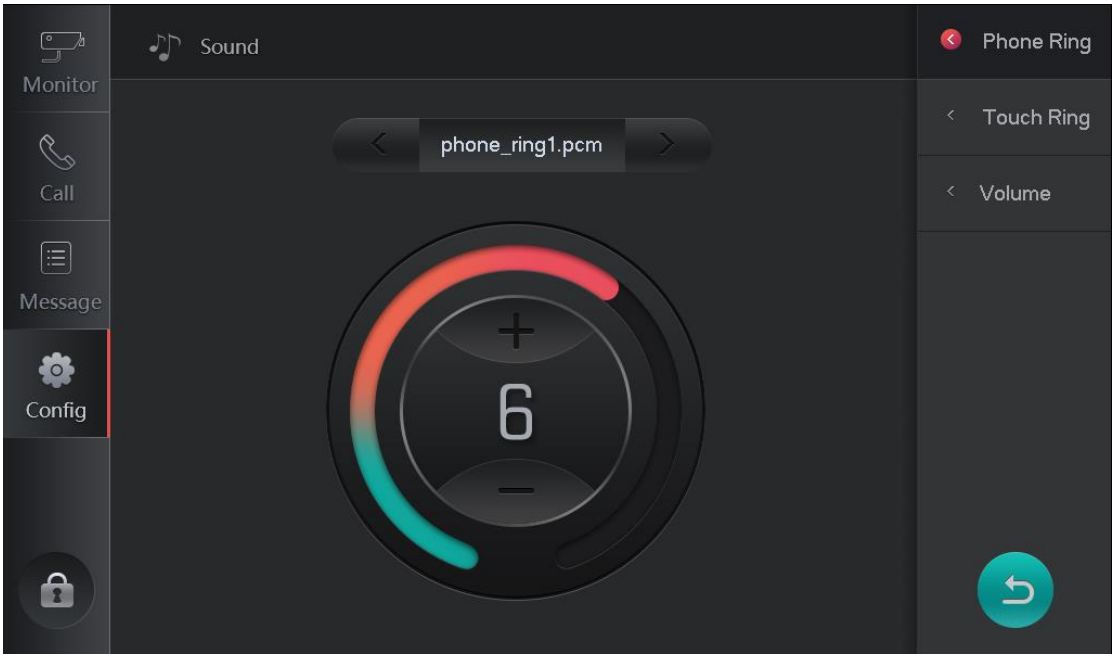
Puede ajustar el brillo de la pantalla y el tiempo de apagado de la pantalla en **Config> Pantalla.**

4.6.2 Tonos

4.6.2.1 Tono de llamada

Puede seleccionar tonos de llamada y ajustar el volumen en **Config> Sonido> Timbre de teléfono.**

Figura 4-10 Tono de llamada



4.6.2.2 Tono de la pantalla táctil

Puede activar / desactivar el tono de la pantalla táctil en **Config> Sonido> Touch Ring.**

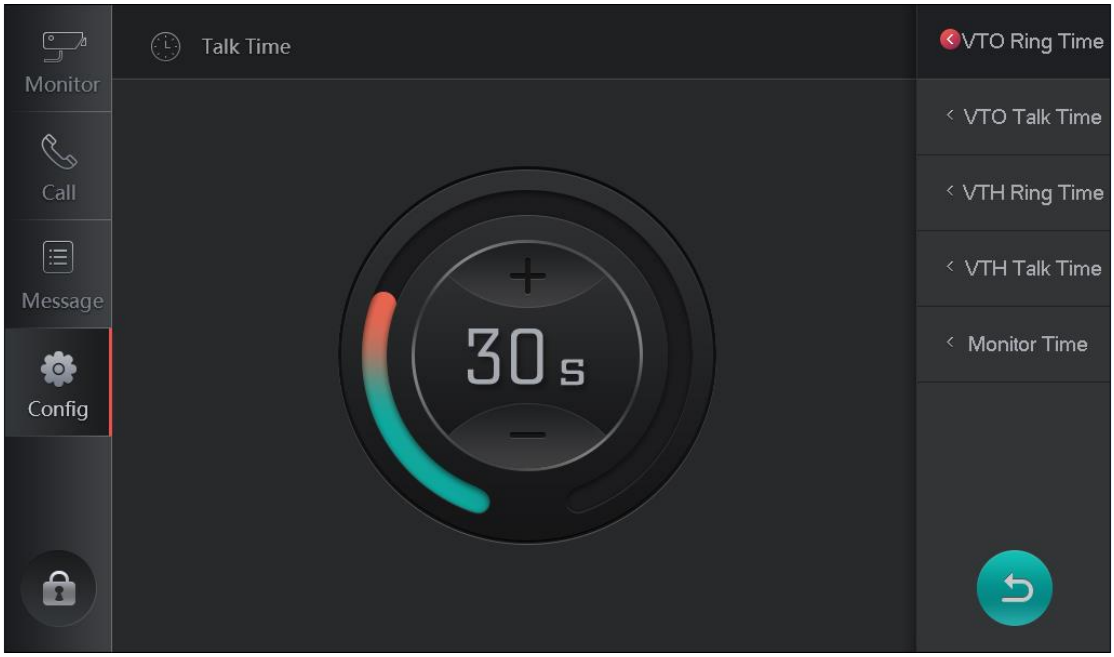
4.6.2.3 Volumen

Puede ajustar el volumen de voz de las personas en **Config> Sonido> Volumen.**

4.6.3 Duración de la llamada

Puedes ir a **Config> Tiempo de conversación,** establezca la duración de la llamada con estaciones de puerta (VTO), el tiempo de timbre del monitor interior (VTH) y más.

Figura 4-11 Tiempo de conversación



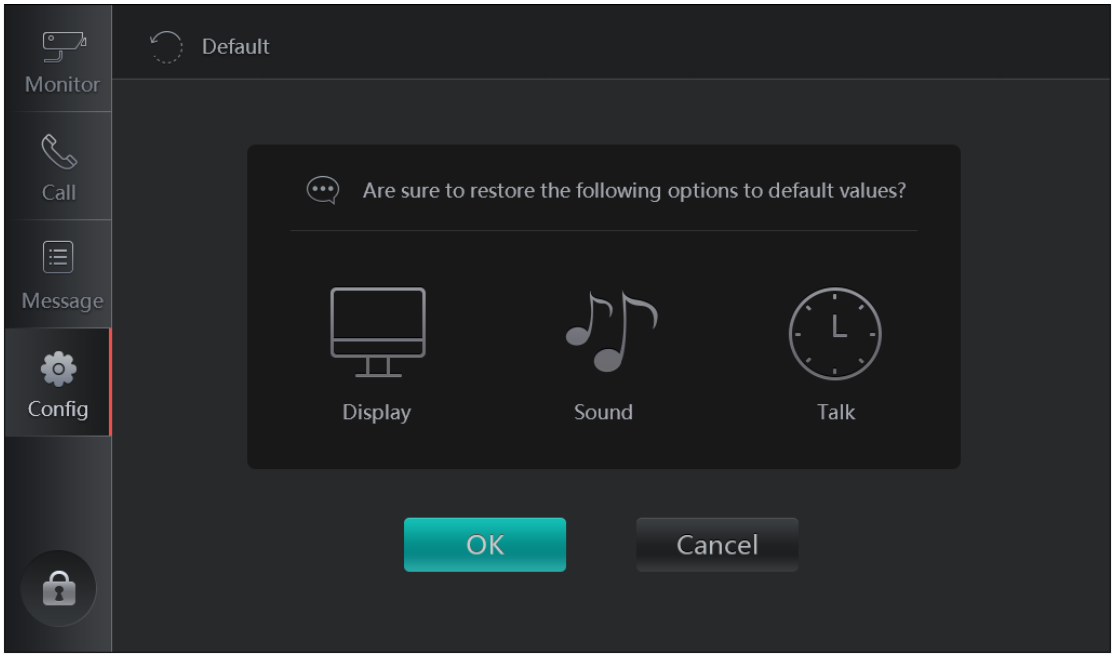
4.6.4 Tarjeta SD

Seleccione **Config> Tarjeta SD,** y luego toque Tarjeta SD para ver el espacio libre o formatear la tarjeta SD.

4.6.5 Por defecto

Grifo **Defecto** sobre el **Config** interfaz para restaurar la configuración de pantalla, el sonido y la duración de la llamada a la configuración predeterminada.

Figura 4-12 Predeterminado



Apéndice 1 Recomendaciones de ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que pertenece a todos los dispositivos que están conectados a Internet. La videovigilancia IP no es inmune a los riesgos cibernéticos, pero tomar medidas básicas para proteger y fortalecer las redes y los dispositivos en red los hará menos susceptibles a los ataques. A continuación, se muestran algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias que deben tomarse para la seguridad de la red de equipos básicos:

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Actualice el firmware y el software cliente a tiempo

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su equipo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el equipo está conectado a la red pública, se recomienda habilitar la función de “búsqueda automática de actualizaciones” para obtener información oportuna de las actualizaciones de firmware publicadas por el fabricante.

- Le sugerimos que descargue y utilice la última versión del software cliente.

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

1. Protección física

Le sugerimos que realice protección física a los equipos, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en una sala de computadoras especial y gabinete, e implemente permisos de control de acceso bien hechos y administración de claves para evitar que el personal no autorizado lleve a cabo contactos físicos como daños en el hardware, conexión no autorizada de equipos 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 ser adivinado o descifrado.

3. Establecer y actualizar contraseñas Restablecer información a tiempo

El equipo 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 las preguntas de protección por contraseña, se sugiere no utilizar aquellas que se puedan adivinar fácilmente.

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. **Habilitar HTTPS**

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

7. **Habilitar lista blanca**

   Le sugerimos que habilite la función de lista blanca para evitar que todos, excepto aquellos con direcciones IP específicas, accedan al sistema. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del equipo adjunto a la lista blanca.

8. **Enlace de dirección MAC**

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

9. **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.

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

11. **Transmisión encriptada de audio y video**

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

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

12. **Auditoría segura**

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

13. **Registro de red**

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

14. **Construya un entorno de red seguro**

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

    - Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde una red externa.
    - La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, es

sugirió utilizar VLAN, red GAP y otras tecnologías para particionar 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.
- Se recomienda que habilite el firewall de su dispositivo o la función de lista negra y lista blanca para reducir el riesgo de que su dispositivo sea atacado.