

# **Monitor interior Android de 10 pulgadas**

## **Guía de inicio rápido**



# Prefacio

## General

Este documento presenta principalmente la estructura, el proceso de instalación y la configuración básica del monitor de interior Android de 10 pulgadas (en adelante, el "monitor de interior").

## Las instrucciones de seguridad

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

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

## Revisión histórica

Versión	Contenido de la revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento	Enero 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 actualizará de acuerdo con las últimas leyes y regulaciones de las regiones 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 tiene alguna duda o disputa, consulte nuestra 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, comuníquese con el proveedor o con el servicio de atención al cliente si se produce algún problema al utilizar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

# Advertencias y medidas de seguridad importantes

La siguiente descripción es el método de aplicación correcto del dispositivo. 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.

## Requisito de funcionamiento

- 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 que contenga líquido para evitar que fluyan al 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.

## Requisitos de energía

- El producto utilizará cables eléctricos (cables de alimentación) recomendados por esta área, que se utilizarán dentro de su especificación nominal.
- 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. La fuente de alimentación se puede cortar solo después de que el dispositivo haya completado la actualización y se haya reiniciado.

# Tabla de contenido

<b>Prólogo</b> .....	<b>YO Advertencias y salvaguardias importantes</b> .....	<b>II 1 Introducción</b>
.....	.....	<b>1</b>
1.1 Resumen .....		1
1.2 Características .....		1
1.3 Dimensiones .....		2
1.4 Conexiones de cables .....		3
<b>2 Instalación</b> .....		<b>4</b>
<b>3 Configuración</b> .....		<b>6</b>
3.1 Descripción general de la configuración .....		6
3.2 Configuración del monitor interior .....		6
3.2.1 Inicialización .....		6
3.2.2 Configuración de red .....		9
3.2.3 Configuración del proyecto .....		10
3.3 Puesta en servicio .....		14
3.3.1 Ver video de monitoreo .....		14
3.3.2 Verificación de mensajes .....		15
3.3.3 Realizar llamadas .....		15
3.3.4 Visualización de registros de alarmas .....		15
<b>Apéndice 1 Recomendaciones de ciberseguridad</b> .....		<b>dieciséis</b>

# 1. Introducción

## 1.1 Resumen

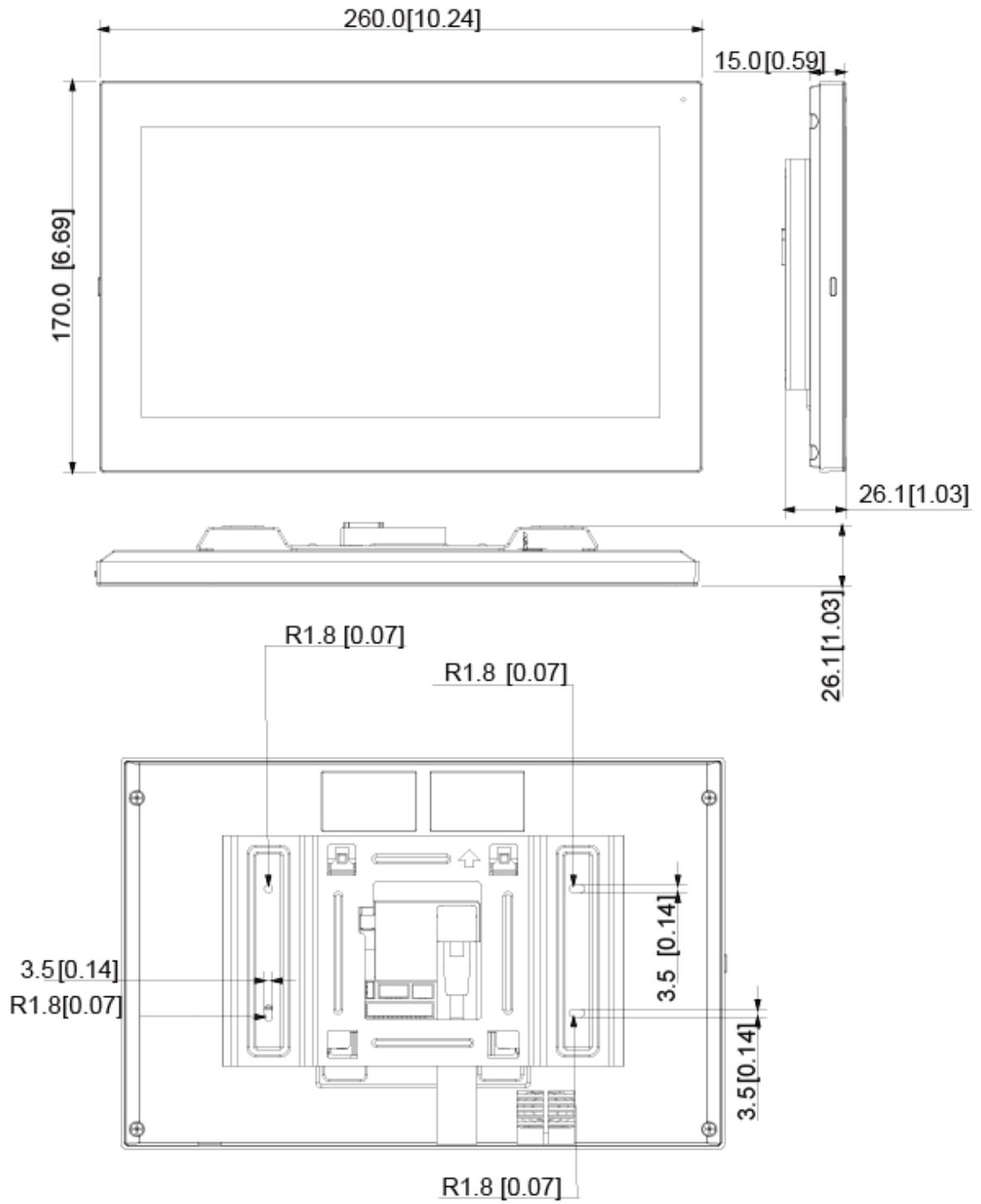
El monitor interior Android digital de 10 pulgadas, ampliamente utilizado en edificios inteligentes, integra funciones de monitoreo, comunicación por voz y desbloqueo. Se aplican tecnologías como la tecnología integrada, los métodos de comunicación IP, el protocolo simple de administración de red (SNMP), el cifrado de red y más para hacer que todo el sistema sea más estable, más seguro y más fácil de administrar.

## 1.2 Características

- Wi-Fi: proporciona una red inalámbrica para dispositivos.
- Llamada de voz: puede realizar llamadas desde las estaciones exteriores a los monitores interiores.
- Monitoreo: los videos capturados por estaciones de cerca, estaciones al aire libre, cámaras IP y más se pueden ver en el monitor interior.
- Llamada de emergencia: las llamadas de emergencia se pueden realizar en el monitor interior.
- Instantánea automática: durante las llamadas o durante el monitoreo, se pueden capturar imágenes y las imágenes se pueden almacenar en la tarjeta SD o FTP.
- No molestar: puede establecer un período en el que no desea que lo molesten. Desbloqueo remoto: puede desbloquear puertas de forma remota.
- Armar y desarmar: puede establecer zonas de protección y luego armar y desarmar. Búsqueda de registros: se pueden ver registros de llamadas y registros de alarmas.
- Verificación de mensajes: puede verificar los mensajes de texto y los videos que dejan los visitantes o los avisos públicos publicados por el centro de administración.
- Aplicación: puede instalar la aplicación en su teléfono móvil.

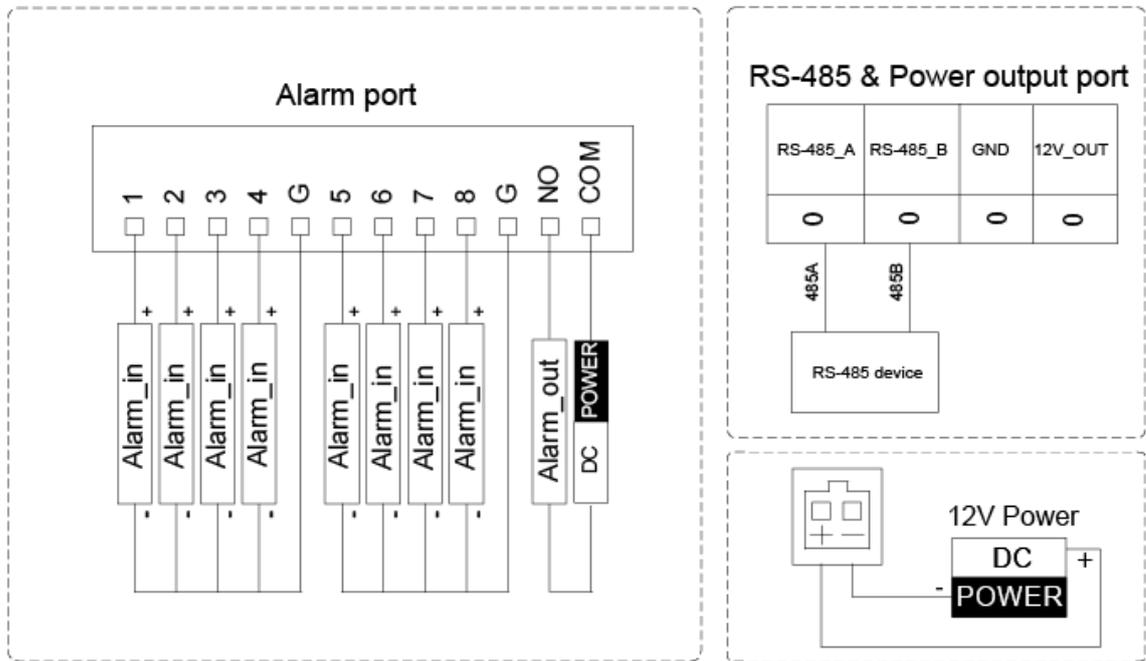
# 1.3 Dimensiones

Figura 1-1 Dimensiones (mm [pulgadas])



# 1.4 Conexiones de cables

Figura 1-2 Conexión de cables



## 2 Instalación

Figura 2-1 Instalación

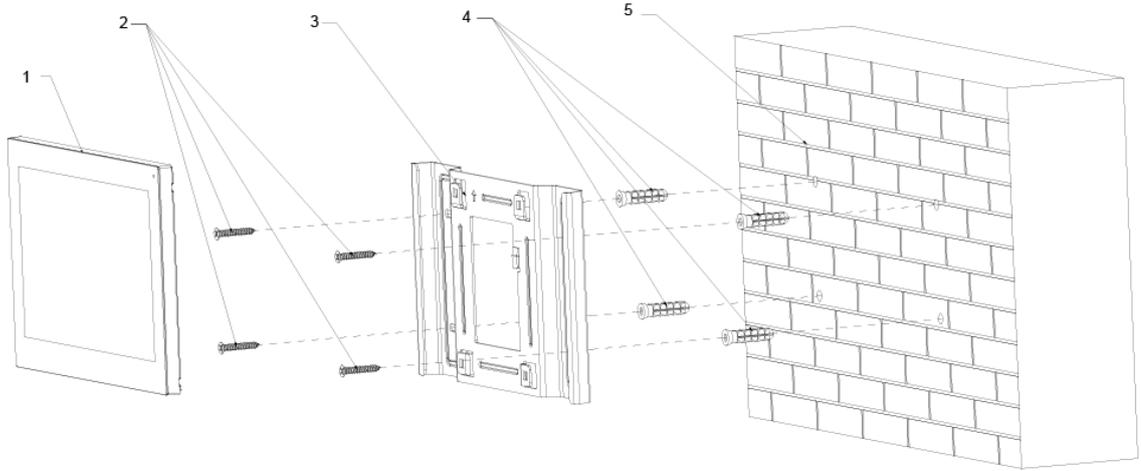


Tabla 2-1 Componentes

No.	Nombre
1	Monitor interior
2	Tornillos autorroscantes ST3
3	Soporte
4	Perno de ancla
5	pared

Figura 2-2 Distancias y diámetros de los orificios de los tornillos

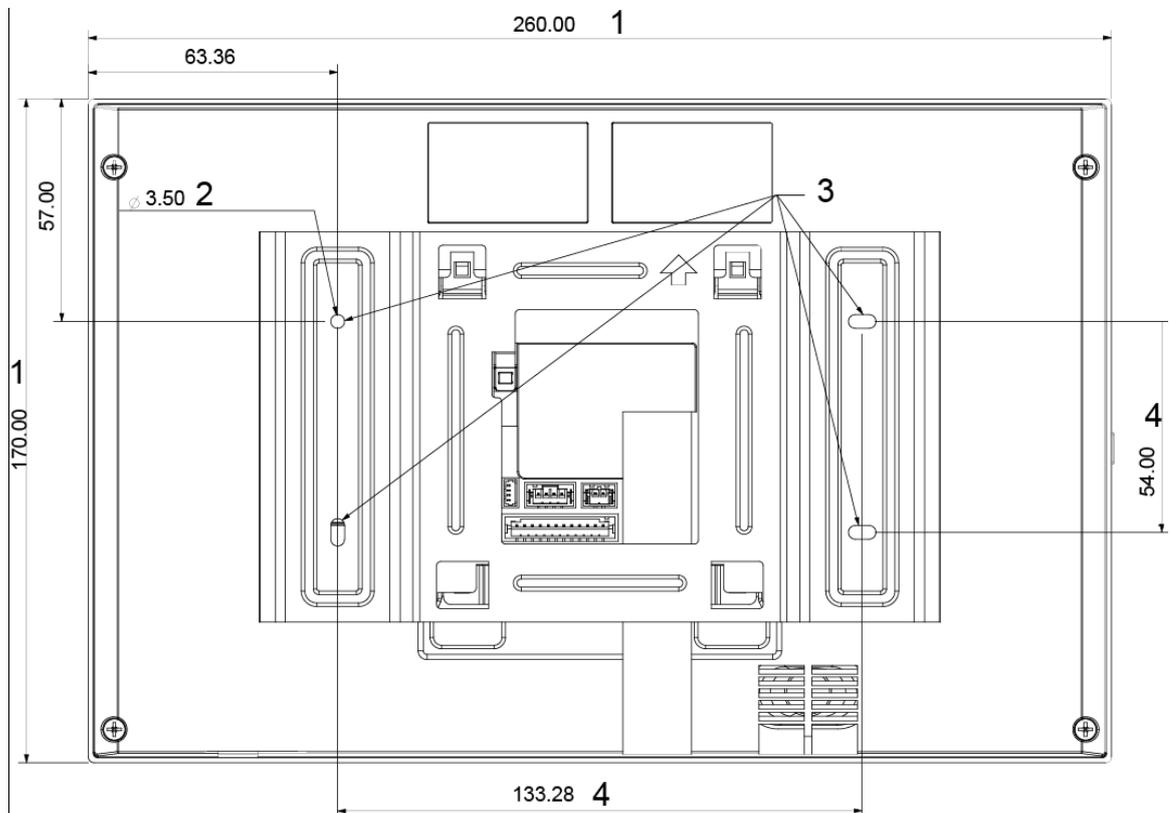


Tabla 2-2 Descripción de las distancias y los diámetros de los orificios de los tornillos

No.	Descripción
1	Dimensión del monitor interior
2	Diámetro del orificio del tornillo del soporte
3	Posición del orificio ovalado del soporte Distancia
4	del orificio del tornillo

Paso 1 Taladre cuatro orificios para tornillos en la pared de acuerdo con los orificios del soporte.

Paso 2 Coloque pernos de anclaje en los orificios de los tornillos.

Paso 3 Fije el monitor interior en la pared con tornillos.

Paso 4 Conecte los cables (cable de alimentación, cables de red y más).

La instalación está completa.

# 3 Configuración

Debe configurar IP, Wi-Fi, parámetro de estación de puerta, servidor SIP y más en el monitor interior, y luego el monitor interior puede comunicarse con las estaciones de puerta y el centro de gestión.

## 3.1 Descripción general de la configuración

Paso 1 Planifique la ubicación del servidor SIP y planifique la IP y los números de cada estación de puerta y monitores interiores.

Paso 2 Asegúrese de que no haya cortocircuito ni circuito abierto. Configure los parámetros

Paso 3 para las estaciones de puerta.

Paso 4 Agregue monitores interiores al servidor SIP. Configure los

Paso 5 parámetros para los monitores de interior. Puesta en servicio.

Paso 6

## 3.2 Configuración del monitor interior

### 3.2.1 Inicialización

Establecer contraseña y correo electrónico.

- Contraseña: se utiliza cuando los administradores necesitan pasar al modo de proyecto. Correo electrónico: se utiliza cuando necesita restablecer la contraseña.



La dirección IP predeterminada del monitor interior es 192.168.1.108.

Paso 1 Conecte el monitor interior a la fuente de alimentación.

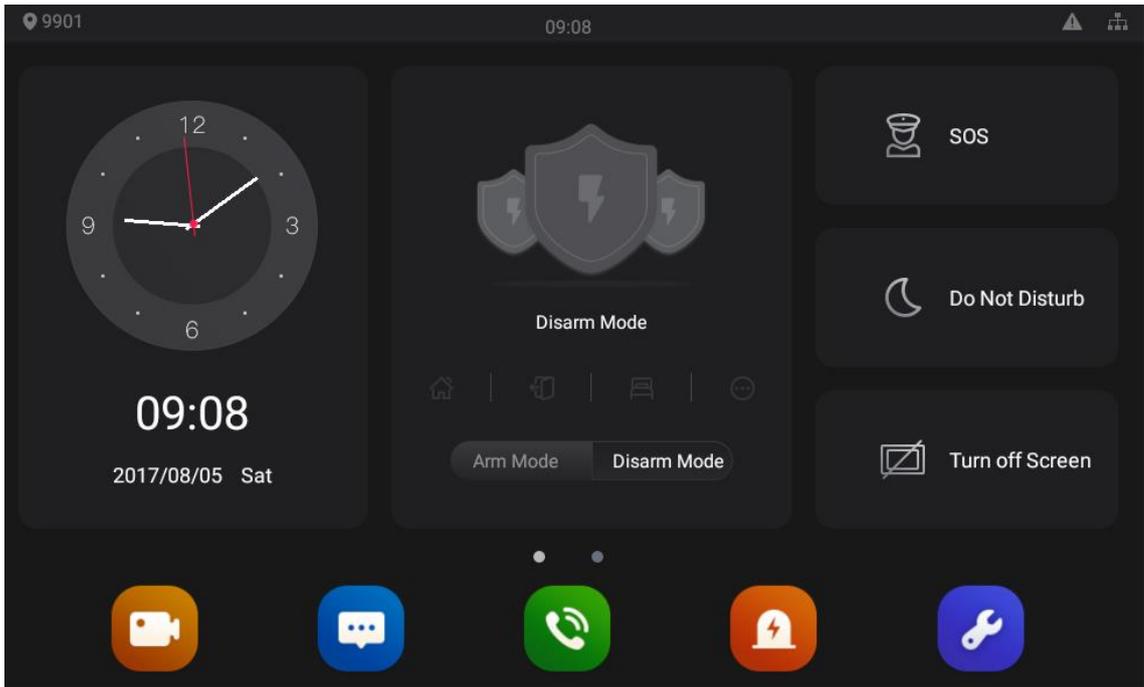
**BIENVENIDOS** Se muestra, y luego se muestra la interfaz de inicialización.

Paso 2 Ingrese la contraseña, confirme la contraseña y el correo electrónico.

Paso 3 Toque **OKAY**.

El menú principal es mostrado.

Figura 3-1 Menú principal



Habitación no.

Room No. se muestra en la esquina superior izquierda del menú principal.

## Hora y fecha

En el menú principal, se muestran la fecha y la hora.

## Modo de armado / modo de desarmado

Aquí se muestran los iconos de acceso directo para armar o desarmar. Los cuatro íconos representan el modo de inicio, fuera del modo de inicio, el modo de suspensión y el modo personalizable. Seleccione **Modo de armado** o **Modo desarmar** primero, y luego toque los íconos para armar o desarmar.

## Estado de la red

El estado de la red y el estado del servidor SIP se muestran en la esquina superior derecha del menú principal.



Si el servidor SIP funciona normalmente, el  El icono desaparecerá.

## llamada de socorro

Toque el icono SOS, el monitor interior llamará al centro de gestión.

## No molestar

Toque el icono y, a continuación, podrá establecer el período de no molestar. Primero debe habilitar el período DND,

y luego puede realizar la configuración de no molestar. Para obtener más detalles, consulte DND tocando



## Apagar la pantalla

Toque el icono y luego la pantalla se apagará.

## Ajustes de usuario

Grifo , y luego se muestra la interfaz de configuración del usuario. Puede seleccionar tonos de llamada para diferentes

estaciones exteriores, período de No molestar, modo de desvío de llamadas (hay tres opciones: Siempre, Ocupado y Sin respuesta) y otras configuraciones.

### anillo

En esta interfaz, puede seleccionar tonos de llamada para diferentes estaciones al aire libre.

### DND

Habilitar **Período DND** primero, y luego puede establecer el período de no molestar para cada día.

### Adelante

Cuando entren llamadas, se reenviarán al centro de gestión durante las horas que haya establecido. Hay tres opciones: Siempre, Ocupado y Sin respuesta.

- Siempre: siempre que entren llamadas, siempre se reenviarán.
- Ocupado: si entran llamadas cuando está hablando con otras personas a través del monitor interior, las llamadas se desviarán.
- Sin respuesta: cuando no se responda a las próximas llamadas, se reenviarán.

### General

Sobre el **General** interfaz, puede establecer nuevas contraseñas para armar y desarmar, registrar nuevos usuarios y descargar aplicaciones escaneando códigos QR y estableciendo otros parámetros.

- Tiempo de monitorización: Puede ver imágenes de monitorización desde el monitor interior durante un máximo de 300 segundos por vez.
- Tiempo (s) de grabación: puede grabar como máximo archivos de audio de 300 segundos a la vez en el monitor interior.
- Tiempo (s) de mensajes VTO: los visitantes solo pueden dejar un mensaje de 90 segundos como máximo por vez en la estación exterior (VTO).
- Tiempo (s) de conversación VTO: los visitantes pueden hablar con usted a través de la estación exterior (VTO) durante un máximo de 300 segundos por vez.
- Duración de la llamada interna: puede hablar con otros monitores interiores durante un máximo de 60 segundos por vez. Llamada interna:
- después de habilitar la llamada interna, puede llamar a otros monitores interiores desde el monitor interior que está operando.
- Captura automática: una vez habilitada la función de captura automática, si un visitante lo llamó pero usted no respondió la llamada, la estación exterior (VTO) tomaría tres imágenes del visitante parado frente a la estación exterior.

## Temas

Puede seleccionar un tema para su monitor interior. Hay dos opciones: modo blanco y modo negro.

## Calendario

Puede ver la fecha a través del monitor interior y crear notas, horarios y planes.

## Galería

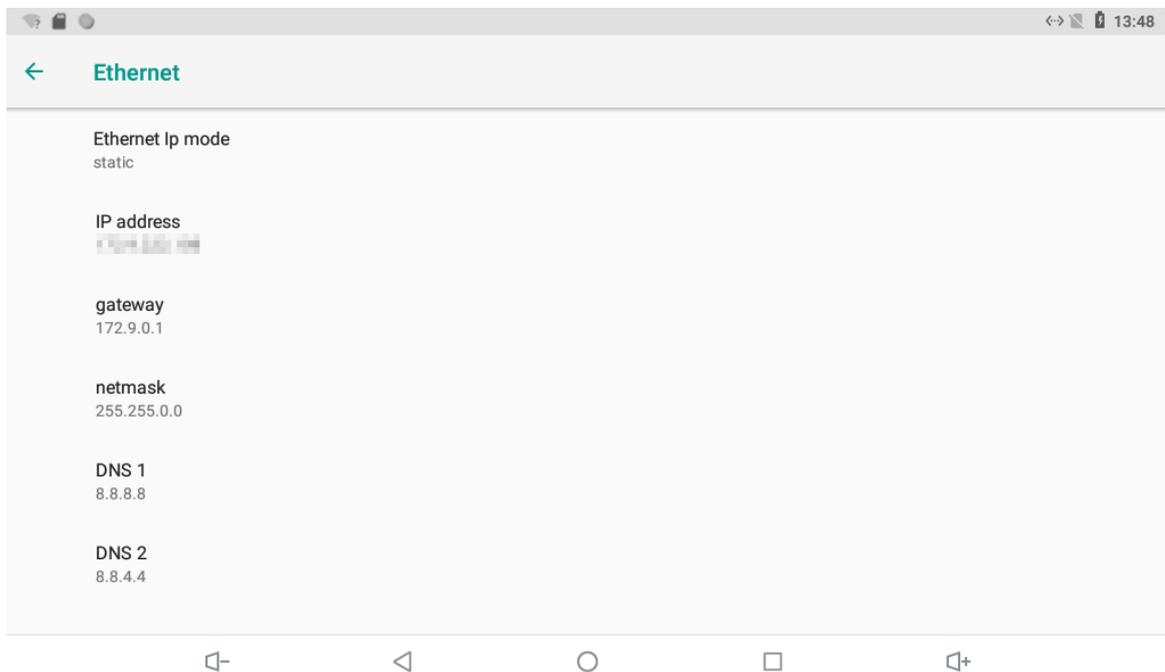
Puede ver imágenes capturadas por estaciones exteriores (VTO) o cámaras IP.

## 3.2.2 Configuración de red

**Paso 1** Toque el **Configuraciones** interfaz.

Se muestra la interfaz de configuración.

Figura 3-2 Configuración



**Paso 2** Configure los parámetros.

Tabla 3-1 Descripción de los parámetros

Parámetro	Descripción
Red & Internet	<p>Puede elegir habilitar Wi-Fi o no presionando .</p> <ul style="list-style-type: none"><li>Grifo , y luego se mostrará la red Wi-Fi disponible.</li><li>Puede seleccionar el modo IP de Ethernet. Hay dos opciones: estática y DHCP.</li></ul>
Aplicaciones Y notificaciones	<p>Puede ver las aplicaciones abiertas recientemente, las aplicaciones abiertas de forma predeterminada, los permisos de las aplicaciones (aplicaciones que usan ubicación, micrófono y cámara), notificaciones de aplicaciones y acceso a aplicaciones especiales.</p>

Parámetro	Descripción	
Monitor	Puede ajustar el brillo de la pantalla, la duración de la suspensión, el tamaño de la fuente y el tamaño de la pantalla.	
Sonido	Puede ajustar el volumen de los medios y el volumen de las notificaciones. También puede optar por utilizar el sonido de notificación predeterminado y el sonido de alarma predeterminado.	
Almacenamiento	Se pueden visualizar los espacios utilizados y los espacios que quedan. Puede eliminar archivos no deseados según sea necesario.	
Sistema	Idiomas & Entrada	Idiomas: puede seleccionar los idiomas que necesite. Teclado y entradas: hay dos opciones: teclado virtual y teclado físico.  Asistencia de entrada: puede usar el corrector ortográfico, el servicio de autocompletar (no disponible en este momento), el diccionario personal y la salida de texto a voz según sea necesario. También se puede ajustar la velocidad del puntero.
	Apoyo	Puede usar el almacenamiento de respaldo según sea necesario.
	Reiniciar opciones	Puede restablecer las preferencias de aplicaciones, Wi-Fi, móvil y Bluetooth. También puede borrar todos los datos, lo que significa restaurar el monitor interior a la configuración de fábrica.
	Acerca de la tableta	Puede ver detalles (estado de la batería, estado de la red, información legal, modelo, versión de Android, nivel de parche de seguridad de Android, versión de banda base, versión de Kernel, número de compilación y más) sobre el monitor interior.

#### Grabadora de sonido

Puede grabar sus mensajes de voz en la tarjeta SD o en el monitor interior.

#### Calculadora

Puedes hacer cálculos a través de la calculadora.

#### Archivos

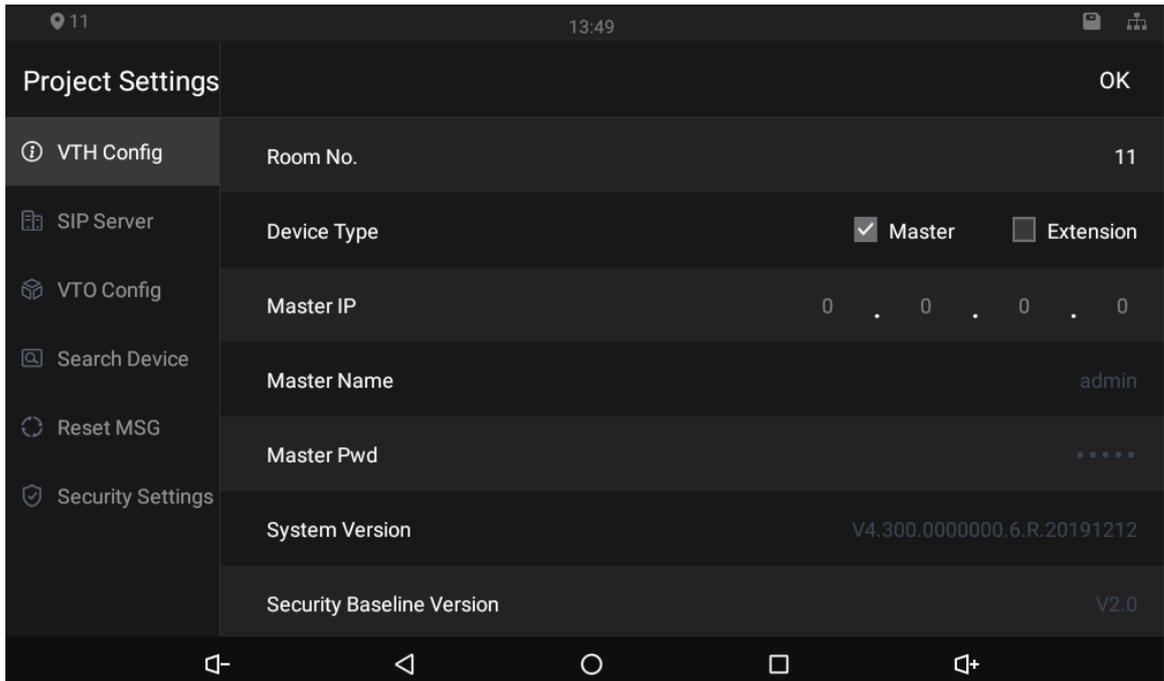
Puede ver archivos como imágenes, videos, audio y archivos producidos recientemente.

### 3.2.3 Configuración del proyecto

Toque y mantenga  durante más de 5 segundos, introduzca la contraseña (123456 por defecto), y luego la

**Configuración del proyecto** Se mostrará la interfaz.

Figura 3-3 Configuración del proyecto



### Configuración VTH

- Room No .: No. de la habitación donde está instalado el monitor interior. Tipo de
- dispositivo: hay dos opciones: maestro y extensión.
  - Maestro: si el monitor interior que está operando funciona como la estación maestra, debe seleccionar **Maestro**.
  - Extensión: si el monitor interior funciona como una extensión, debe seleccionar Extensión. IP maestra: cuando el
- monitor interior funciona como una extensión, debe ingresar la dirección IP de la estación maestra.
- Nombre maestro: mantenga el valor predeterminado. Master
- Pwd: Conserva el valor predeterminado.
- Versión del sistema: puede ver la versión del sistema del monitor interior.
- Versión de referencia de seguridad: puede ver la versión de referencia de seguridad del monitor interior.

### Servidor SIP

Debe ingresar la información del servidor SIP, y luego todo el sistema de videoportero puede comunicarse entre sí.

Grifo **Servidor SIP**, y luego se muestra la interfaz del servidor SIP.

Figura 3-4 Servidor SIP (1)

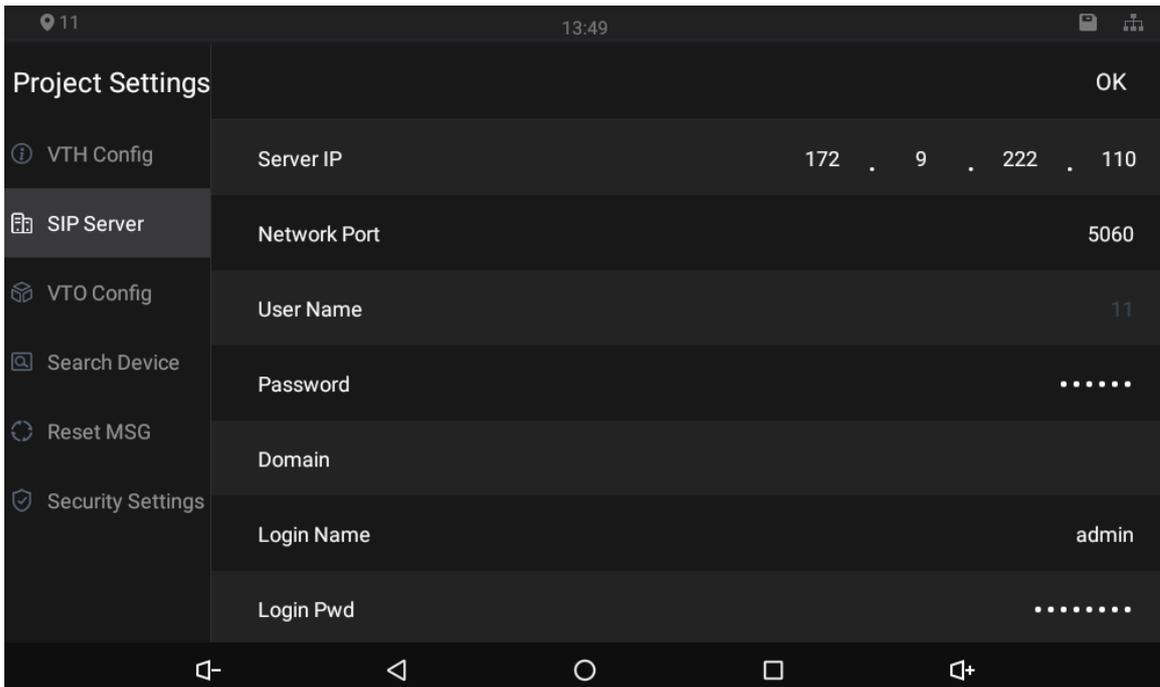


Tabla 3-2 Descripción del servidor SIP

Parámetro	Descripción
Servidor IP	<ul style="list-style-type: none"> <li>Cuando la plataforma funciona como servidor SIP, la IP del servidor es la dirección IP de la plataforma de gestión.</li> <li>Cuando una estación exterior funciona como servidor SIP, la IP del servidor es la dirección IP de la estación exterior.</li> </ul>
Puerto de red	<ul style="list-style-type: none"> <li>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.</li> </ul>
Nombre de usuario	Utilice el valor predeterminado.
Contraseña	
Dominio	Dominio de registro del servidor SIP, que puede ser nulo. Cuando VTO funciona como servidor SIP, el dominio de registro del servidor SIP será VDP.
Nombre de inicio de sesión	Nombre de usuario y contraseña para iniciar sesión en la página web del servidor SIP.
Iniciar sesión Pwd	
Estado	Habilite el estado del servidor SIP y, a continuación, el servidor SIP puede comenzar a funcionar.

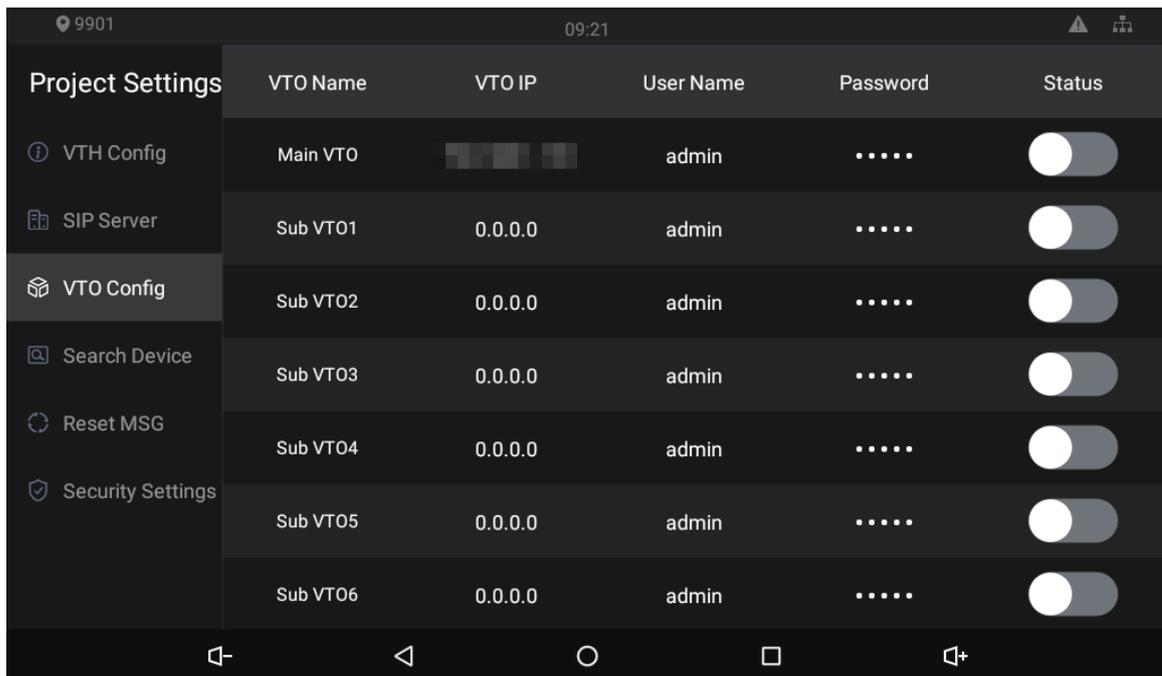
## Configuración VTO

Necesita agregar estaciones exteriores al monitor interior.

**Paso 1** Toque VTO Config.

los **Configuración VTO** se muestra la interfaz.

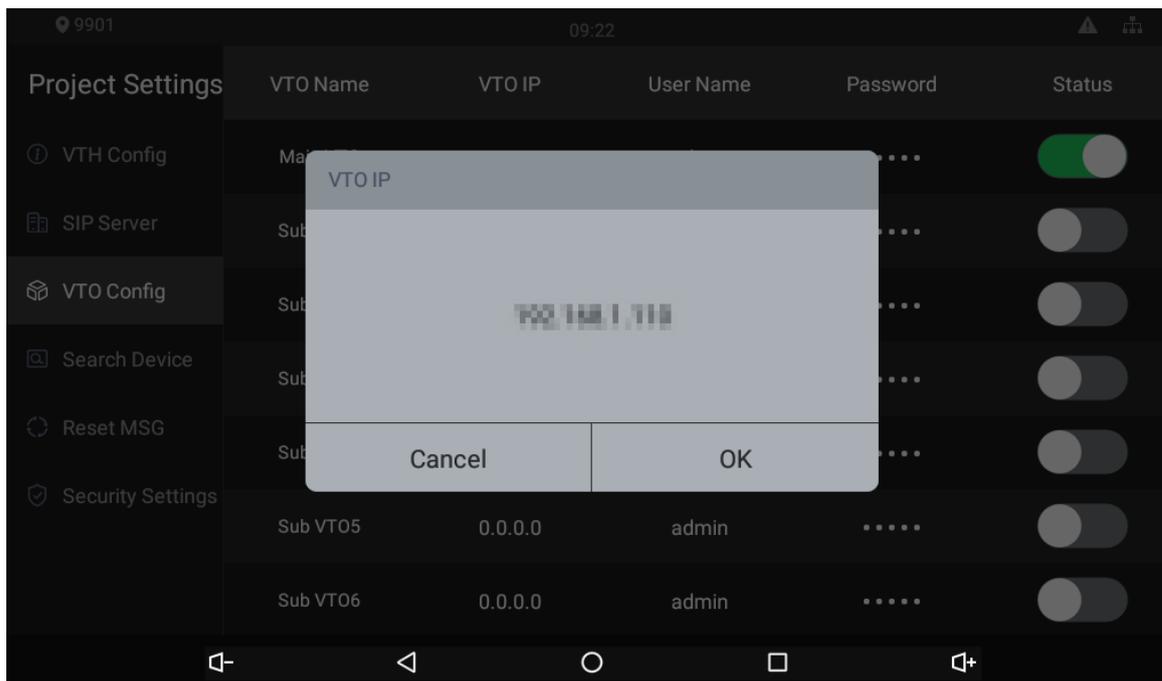
Figura 3-5 Configuración de la estación exterior (VTO)



**Paso 2** Toque una estación exterior (VTO).

los **IP VTO** se muestra la interfaz.

Figura 3-6 VTO IP



**Paso 3** Toque la IP predeterminada y luego aparecerá el teclado en pantalla.

**Paso 4** Introduzca la IP de la estación exterior (VTO) que planificó.

**Paso 5** Toque **Okay** para guardar la configuración.



Puede agregar 20 estaciones exteriores (una estación exterior principal y 19 estaciones exteriores secundarias) al monitor interior.

## Dispositivo de búsqueda

Toque en el **Dispositivo de búsqueda** y luego el sistema comienza a buscar dispositivos automáticamente.

## Restablecer MSG

Puede cambiar la dirección de correo electrónico que utiliza para restablecer su contraseña.



Necesita habilitar el **Resst Contraseña** primero si desea restablecer la contraseña.

## Configuraciones de seguridad

Debe habilitar la lista de confianza y luego se pueden agregar los dispositivos de confianza. También puede usar Dshell para brindarle la capacidad de desarrollar módulos de análisis personalizados que lo ayuden a comprender los eventos de intrusión cibernética.

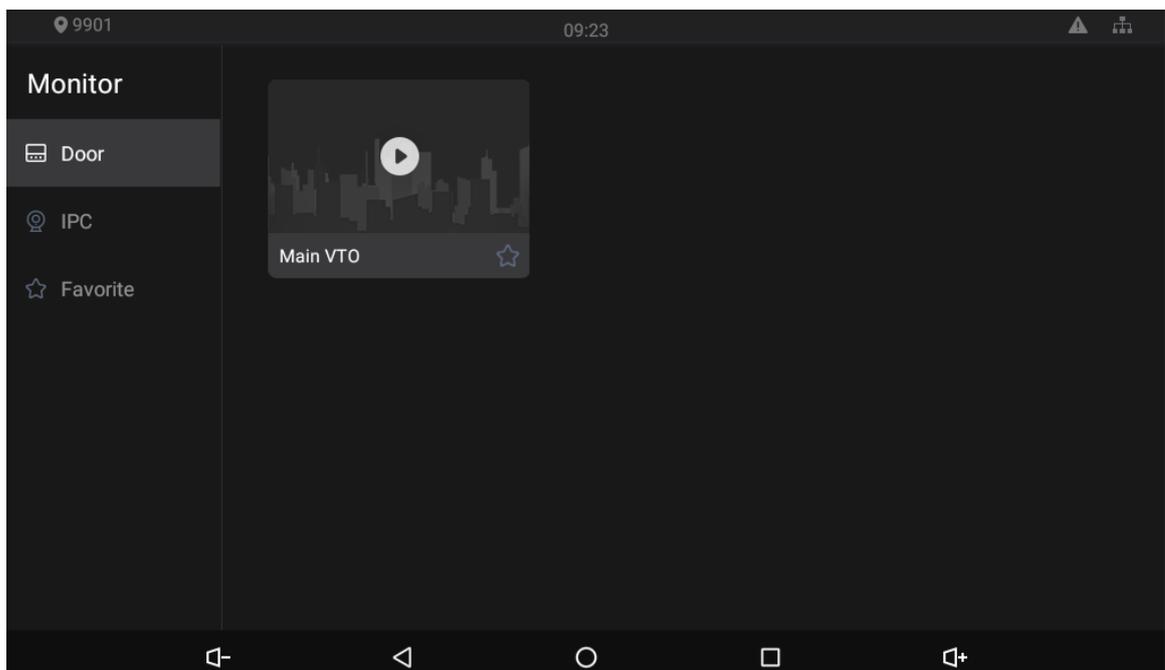
## 3.3 Puesta en servicio

### 3.3.1 Ver video de monitoreo

Grifo  se muestra la interfaz de Monitor.

En el monitor interior, puede ver videos de estaciones exteriores y cámaras IP. También puede colocar las estaciones exteriores y las cámaras IP que desee en el **Favorito** carpeta por toque  en el esquina inferior derecha de cada dispositivo.

Figura 3-7 Monitor



- : Toque el icono para bajar el volumen.

- : Toque el icono para ir a la página anterior.
- : Toque el icono para ir al menú principal.
- : Toque el icono y se mostrarán todas las miniaturas de las interfaces que ha abierto.  
 Seleccione una interfaz y deslícela hacia la izquierda o hacia la derecha para cerrar la interfaz.
- : Toque el icono para subir el volumen.

### 3.3.2 Verificación de mensajes

Grifo  y luego mensajes de texto y videos dejados por visitantes, o avisos públicos publicados por el Se mostrará el centro de gestión.

### 3.3.3 Realizar llamadas

Grifo  y luego puede hacer llamadas a otros monitores interiores y al centro de administración; y también puede ver los registros de llamadas y sus contactos en esta interfaz.

### 3.3.4 Visualización de registros de alarmas

Grifo  , y luego el **Alarma** se muestra la interfaz. Los módulos de alarma periféricos se pueden conectado al monitor interior. Puede ver registros de alarmas, realizar ajustes de alarma para 6 áreas según sea necesario. Hay 7 tipos de alarmas: infrarrojas, sensor de gas, sensor de humo, botón de urgencia, sensor de puerta, robo y perímetro.



Primero desarme todas las alarmas y luego podrá configurar las alarmas.

# 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 asigne 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.