

Caja de juego distribuida

Guía de inicio rápido



Prefacio

General

Este manual presenta la instalación, las funciones y las operaciones de la caja de juego distribuida (en lo sucesivo, "la caja"). Lea detenidamente antes de usar la caja 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	Sentido
 DANGER	Indica un peligro de alto potencial que, si no se evita, provocará la muerte o lesiones graves.
 WARNING	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 CAUTION	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, reducción del rendimiento o resultados impredecibles.
 TIPS	Proporciona métodos para ayudarlo a resolver un problema o ahorrar tiempo.
 NOTE	Proporciona información adicional como suplemento al texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.1	Importante actualizado Salvaguardias y Advertencias.	abril 2022
V1.0.0	Primer lanzamiento.	marzo 2022

Aviso de protección de privacidad

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

Sobre el Manual

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

la versión electrónica y la versión en papel.

- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede haber errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, póngase en contacto con el proveedor o con el servicio de atención al cliente si se produce algún problema durante el uso del dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

Medidas de seguridad y advertencias importantes

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

requerimientos de instalación



- El uso inadecuado de la batería puede provocar un incendio o una explosión.
- Asegúrese de usar el mismo modelo cuando reemplace la batería.
- Utilice el adaptador de corriente estándar. No asumiremos ninguna responsabilidad por los problemas causados por el uso de un adaptador de corriente no estándar.
- Utilice los cables de alimentación recomendados para la región y cumpla con las especificaciones de potencia nominal.



- No coloque la caja en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga la caja alejada de la humedad, el polvo y el hollín.
- Instale la caja en una superficie estable para evitar que se caiga.
- Coloque la caja en un lugar bien ventilado y no bloquee su ventilación.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en el estándar IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de la fuente de alimentación están sujetos a la etiqueta del dispositivo.
- El dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectada a una toma de corriente con protección a tierra.
- El acoplador del aparato es un dispositivo de desconexión. Manténgalo en un ángulo conveniente cuando lo use.

Requisitos de operación



- No deje caer ni salpique líquido sobre la caja y asegúrese de que no haya ningún objeto lleno de líquido sobre la caja para evitar que el líquido fluya hacia ella.
- Opere la caja dentro del rango nominal de entrada y salida de energía.
- No desmonte la caja.
- Utilice la caja en condiciones de humedad y temperatura permitidas. Temperatura de funcionamiento: -10 °C a +55 °C (14 °F a 113 °F).

Tabla de contenido

Prefacio.....	YO Medidas de
seguridad y advertencias importantes.....	III 1. Introducción
.....	1
2 lista de embalaje.....	2
3 Estructura.....	3
3.1 Dimensiones.....	3
3.2 Puertos.....	3
4 Inicialización.....	5
5 Iniciar sesión.....	7
6 Barra de herramientas rápida.....	8
Apéndice 1 Recomendaciones sobre ciberseguridad.....	9

1. Introducción

La caja de reproducción es una nueva generación de terminal de información en la nube inteligente integrada con publicación de información multimedia, publicación de anuncios, amplificador de potencia de audio y acceso a la red. Basado en un esquema de diseño industrial, se combina con la plataforma de gestión de liberación de información que presenta una arquitectura B/S. La caja puede reproducir imágenes, videos y subtítulos de desplazamiento tanto en pantalla completa como en pantalla dividida. Puede configurar múltiples modos de reproducción en la plataforma, como bucle, reproducción cronometrada, reproducción intercortada y reproducción en tiempo de inactividad para un control multidimensional y flexible sobre el tiempo de reproducción de los videos, su secuencia, contenido y posición.

La caja es muy adecuada para su uso en comunidades residenciales, fábricas, escuelas y más. También se puede utilizar en diversas industrias, como ascensores, finanzas, catering, medios de comunicación, hotelería, transporte y educación.

2 lista de embalaje

Compruebe si hay algún daño evidente en la caja del paquete. Desembale la caja y compruebe si los componentes están completos según la lista de embalaje.

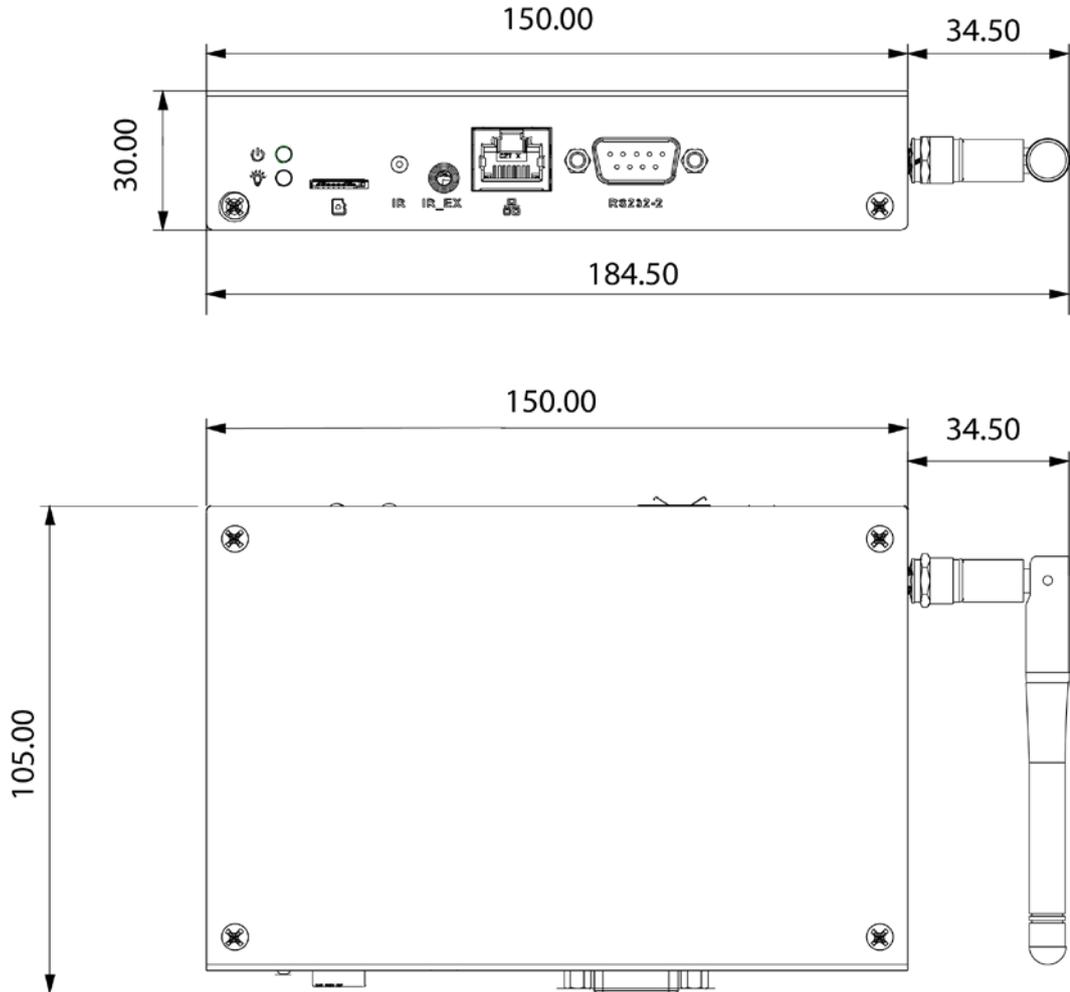
Tabla 2-1 Lista de embalaje

Nombre	Cantidad	Nombre	Cantidad
Caja de juego distribuida	1	Adaptador de corriente	1
Control remoto	1	Soporte de base fija	1
antena wifi	1	Guía de inicio rápido	1

3 Estructura

3.1 Dimensiones

Figura 3-1 Dimensiones (mm [pulgadas])



3.2 Puertos

Figura 3-2 Puertos (1)

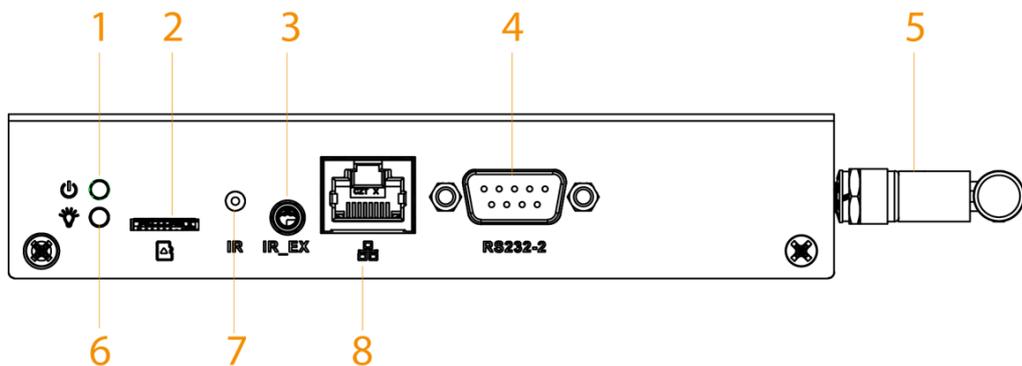


Figura 3-3 Puertos (2)

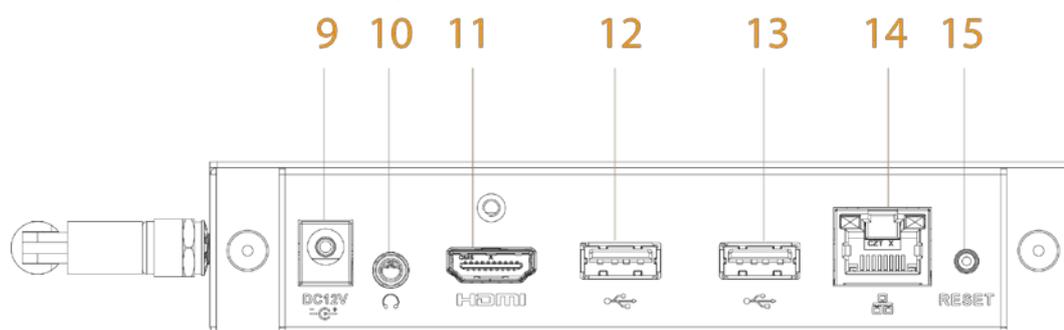


Tabla 3-1 Descripción del puerto

No.	Nombre	Descripción
1	Luz indicadora de poder	La luz se enciende cuando la caja está encendida.
2	Ranura para tarjetas TF	<p>Inserte una tarjeta TF en la ranura para almacenar datos.</p> <p>La capacidad máxima de almacenamiento es de 128 GB. Cuando el sistema Android repite el reinicio debido a operaciones anormales, o la caja no puede iniciarse, puede usar la tarjeta TF para forzar la actualización del sistema.</p> <p></p> <p>Para forzar la actualización del sistema, póngase en contacto con el cliente servicio para obtener el paquete de actualización. Después de insertar el Tarjeta TF que contiene el paquete de actualización correcto en el ranura, apague y luego reinicie la caja. El sistema actualizar automáticamente.</p>
3	Puerto IREX	Se conecta al cable de extensión de infrarrojos.
4	Puerto RS-232	Puerto serial DB9 RS-232 para comunicación y depuración.
5	antena wifi	Recibe señales wifi.
6	Estado de la operación luz indicadora	<ul style="list-style-type: none"> ● La luz se enciende cuando la caja funciona normalmente. ● La luz parpadea cuando la caja no funciona correctamente.
7	puerto de infrarrojos	Recibe señales IR del control remoto.
8	Puerto RS-232	Puerto serial RJ-45 RS-232 para comunicación y depuración.
9	Puerto de alimentación	Se conecta a un adaptador de corriente de 12 VDC.
10	Conector de audio	Se conecta a un auricular de 3,5 mm para emitir señales de audio.
11	puerto HDMI	Envía señales a dispositivos compatibles con HDMI para reproducir proyectos.
12	USB 2.0/OTG	Se conecta al mouse, dispositivos de almacenamiento USB y otros tipos de dispositivos. Puede cambiar el modo USB a OTG.
13	USB 2.0	Se conecta a mouse, dispositivos de almacenamiento USB y otros dispositivos.
14	puerto de red	Se conecta al cable de red.
15	Botón de reinicio	Póngase en contacto con el servicio de atención al cliente para usar el botón para restaurar la caja a su configuración de fábrica o restablecer la contraseña.

4 Inicialización

Cuando inicia sesión por primera vez o después de restaurar la configuración de fábrica, debe inicializar el cuadro. Después de eso, puede configurar y operar la caja.

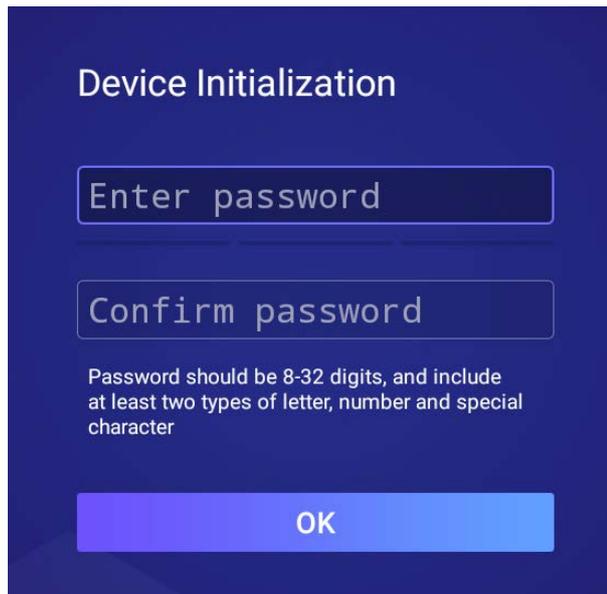
Paso 1 Encienda la caja.

Paso 2 Seleccione el idioma y luego haga clic en **Guardar y Siguiente**. Lea el acuerdo

Paso 3 de licencia del software y luego haga clic en **próximo**. Introduzca y confirme

Paso 4 la contraseña y, a continuación, haga clic en **OK**.

Figura 4-1 Introducir contraseña



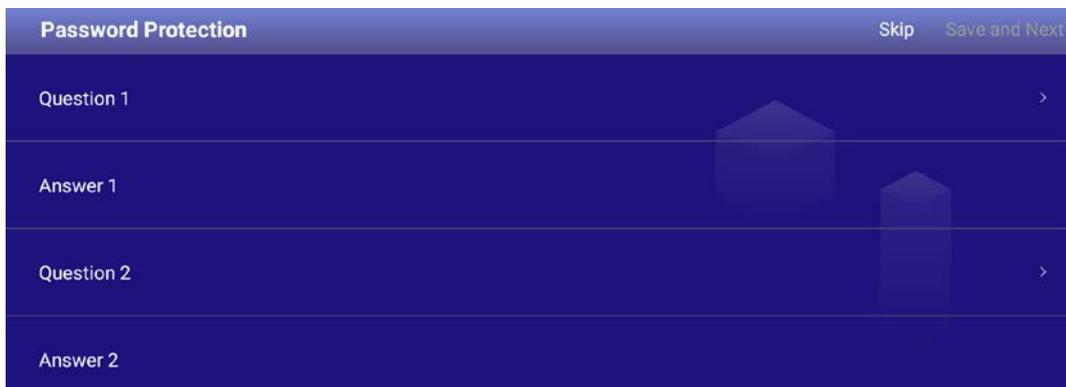
Paso 5 Establezca sus preguntas de seguridad.



Hacer clic **Saltar** si no desea configurar las preguntas de seguridad.

1. Seleccione las preguntas de seguridad y luego configure las respuestas correspondientes.
2. Haga clic en **Guardar y Siguiente**.

Figura 4-2 Protección por contraseña



Paso 6 Configure el nombre del dispositivo.

1. Haga clic para  establecer el nombre del dispositivo.
2. Haga clic en **Guardar y Siguiente**.

Paso 7 Configure los ajustes de red.



Hacer clic **Saltar** si no desea configurar los ajustes de red.

1. Seleccione un tipo de red y luego configure los ajustes de red.

Tabla 4-1 Configuración de red

Tipo de red	Descripción
WiFi	<p>Hacer clic  cuando Wi-Fi esté disponible cerca de la caja.</p> <ul style="list-style-type: none"> ● Búsqueda automática: haga clic en una red Wi-Fi, ingrese su contraseña y luego haga clic en Conectar. ● Conéctese al Wi-Fi manualmente: Haga clic en  luego en el Agregar red página, ingrese el SSID de la red, seleccione una opción de seguridad y luego haga clic en Ahorrar. <p> Le recomendamos que elija un método de autenticación seguro para conectarse a la red wifi.</p>
ethernet	<p>Conecte la caja a la red por Ethernet. Hay 2 métodos para establecer la dirección IP de la caja.</p> <ul style="list-style-type: none"> ● DHCP: cuando haya un servidor DHCP en la red, seleccione DHCP para permitir que la caja obtenga una dirección IP del servidor DHCP automáticamente. ● IP estática: después de seleccionar IP estática, configurar Dirección IP, Puerta, y máscara de red según su plan de red.

2. Haga clic en **Guardar y Siguiente**.

Paso 8 Registrar la caja a la plataforma.



Hacer clic **Saltar** para omitir el registro de la plataforma.

1. Ingrese la dirección IP o el nombre de dominio, el puerto de la plataforma (MPS o ICC) y el ID del departamento.

Figura 4-3 Registro de plataforma



2. Haga clic en **Completo**.

5 Iniciar sesión

Debe iniciar sesión en el sistema para realizar operaciones cuando ocurra alguna de las siguientes situaciones.

- Es su primer uso después de la inicialización.
- Bloquee la pantalla manualmente.
- La pantalla bloqueó la pantalla automáticamente después de un largo período de inactividad. Paso

1 Haga clic en cualquier posición en la pantalla.

Paso 2 Ingrese la contraseña y luego haga clic en **OK**.

Se muestra la página de inicio o la página que estaba abierta antes de que se bloqueara la pantalla.



Después de 5 intentos de inicio de sesión fallidos consecutivos, el sistema le indicará **Cuenta bloqueada, reiniciar o vuelve a intentarlo 5 minutos después.**

6 Barra de herramientas rápida

La barra de herramientas rápida puede ayudar a mejorar la eficiencia de su operación. Apunte a la parte inferior de la página y luego se mostrará la barra de herramientas rápida.

Figura 6-1 Barra de herramientas rápida



Tabla 6-1 Descripción de la barra de herramientas rápida

Icono	Descripción
	Indica si la casilla está registrada en la plataforma.
	Ve a la página principal.
	Ajusta el volumen.
	Ajuste el brillo de la retroiluminación.
	Bloquea la pantalla.
	Desconecte su unidad USB de la caja.

Apéndice 1 Recomendaciones sobre ciberseguridad

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

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su 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 de "comprobación automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

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

1. Protección Física

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

2. Cambie las contraseñas regularmente

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

3. Establecer y actualizar contraseñas Restablecer información a tiempo

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

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilitar HTTPS

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

7. Enlace de dirección MAC

Le recomendamos vincular la dirección IP y MAC de la puerta de enlace al dispositivo, reduciendo así

el riesgo de suplantación de ARP.

8. Asigne cuentas y privilegios de manera razonable

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios razonablemente y 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 los riesgos.

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

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

10 Transmisión encriptada de audio y video

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

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

11 Auditoría segura

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

12 Registro de red

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

13 Construir un entorno de red seguro

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

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