Traducido del inglés al español - www.onlinedoctranslator.com

Panel de control de alarma

Manual de usuario

ZHEJIANG DAHUA VISIÓN TECNOLOGÍA CO., LTD. V2.1.0

Prefacio

General

Este manual presenta la instalación, funciones y operaciones del panel de control de alarma (en adelante denominado "el panel de control"). 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, menor rendimiento o resultados impredecibles.
TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrarle tiempo.
NOTE	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V2.1.0	• Características del producto actualizadas. • Configuración de zona actualizada. • Funciones de relé actualizadas. • Configuración de alarma actualizada. • Gestión de cuentas actualizada. • Se agregó administración de dispositivos periféricos.	abril 2023
V2.0.0	• Se agregaron 3 funciones, que incluyen armar y desarmar mediante SMS, anular y aislar zonas mediante SMS e instrucción de voz. • Configuraciones de zona y subsistema actualizadas, y funciones de subsistema público agregadas.	abril 2022

Versión	Contenido de revisión	Tiempo de liberación
V1.1.0	● Guía de configuración actualizada, restablecimiento de contraseña, función de audio, manejo de fallas, configuración del centro receptor de alarmas, módulos 2G/4G, configuración de hora, inicialización de teclado. ● Se actualizaron las descripciones de todos los capítulos. ● Imágenes actualizadas.	diciembre 2021
V1.0.0	Primer lanzamiento.	julio 2021

Aviso de protección de privacidad

Como usuario del dispositivo o panel de control de datos, puede recopilar datos personales de otras personas, 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 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, cumpla con las pautas al usarlo y guarde el manual en un lugar seguro para consultarlo en el futuro.

Requisitos de operación

- Asegúrese de que la fuente de alimentación del dispositivo funcione correctamente antes de usarlo.
- No desconecte el cable de alimentación del dispositivo mientras esté encendido.
- Utilice el dispositivo únicamente dentro del rango de potencia nominal.
- Transporte, utilice y almacene el dispositivo en las condiciones permitidas de humedad y temperatura.
- Evite que los líquidos salpiquen o goteen sobre el dispositivo. Asegúrese de que no haya objetos llenos de líquido encima del dispositivo para evitar que fluyan líquidos hacia él.
- No desmonte el dispositivo.

requerimientos de instalación

- Conecte el dispositivo al adaptador antes de encenderlo.
- Cumpla estrictamente con los estándares locales de seguridad eléctrica y asegúrese de que el voltaje en el área sea estable y se ajuste a los requisitos de energía del dispositivo.
- No conecte el dispositivo a más de una fuente de alimentación. De lo contrario, el dispositivo podría dañarse.

- Observe todos los procedimientos de seguridad y use el equipo de protección requerido proporcionado para su uso mientras trabaja en alturas.
- No exponga el dispositivo a la luz solar directa ni a fuentes de calor.
- No instale el dispositivo en lugares húmedos, polvorientos o con humo.
- Instale el dispositivo en un lugar bien ventilado y no bloquee el ventilador del dispositivo.
- Utilice el adaptador de corriente o la fuente de alimentación del estuche proporcionada por el fabricante del dispositivo.
- 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.
- Conecte los aparatos eléctricos de clase I a una toma de corriente con protección a tierra.

Tabla de contenido

Prefacio..... I Medidas de seguridad y advertencias importantes..... III 1
Descripción general del producto..... 1
1.1 Introducción..... 1
1.2 Características..... 1
2 Desembalar y comprobar..... 2
3 Dimensiones y puertos de la placa base..... 3
3.1 Dimensiones.....3
3.2 Puertos de la placa base..... 3
4 Instalación y cableado.....6
4.1 Montaje en pared..... 6
4.2 Conexión de cables.....6
4.2.1 Requisitos de cables..... 6
4.2.2 Conexión del cable de entrada de alarma local..... 7
4.2.3 Conexión del cable de salida de alarma local..... 7
4.2.4 Conexión del cable RS-485.....8
4.2.5 Conexión del cable del teclado.....8
4.2.6 Conexión del cable de la impresora.....9
4.2.7 Conexión del cable de la sirena.....9
4.2.8 Conexión del cable del módulo de expansión..... 9
5 Operaciones Web..... 11
5.1 Iniciar el dispositivo..... 11
5.1.1 Inicializando el Panel de Control.....11
5.1.2 Iniciar sesión en Web Manager..... 12
5.1.3 Guía de configuración.....13
5.1.4 Restablecer la contraseña..... 22
5.2 Configuración de alarma.....24
5.2.1 Zona.....24
5.2.2 Subsistema.....24
5.2.3 Sirena.....24
5.2.4 Relé..... 25
5.2.5 Impresora.....25
5.2.6 Zumbador.....26
5.2.7 Audio..... 27
5.2.8 Manejo de fallas..... 28
5.2.9 Enlace SMS.....29
5.2.10 Vinculación CID.....30

5.2.11 Central Receptora de Alarmas..... 30
5.3 Gestión de alarmas..... 31
5.3.1 Subsistema..... 31
5.3.2 Zona..... 31
5.3.3 Salida de relé..... 32
5.3.4 Sirena..... 33
5.4 Gestión de red..... 34
5.4.1 TCP/IP..... 34
5.4.2 Puerto..... 35
5.4.3 Servicios Básicos..... 36
5.5 Información del dispositivo..... 36
5.6 Gestión del sistema..... 37
5.6.1 Cuenta..... 37
5.6.2 Configuración de hora..... 44
5.6.3 Mantenimiento del dispositivo..... 45
5.6.4 Actualización del sistema..... 47
5.6.5 Detección del sistema..... 48
5.6.6 Gestión de periféricos..... 49
5.7 Registro..... 54
5.7.1 Visualización y copia de seguridad de registros..... 54
5.7.2 Registro remoto..... 54
5.7.3 Raspado de troncos..... 55
5.8 Seguridad..... 55
5.8.1 Estado de seguridad..... 55
5.8.2 Configuración del servicio del sistema..... 56
5.8.3 Configuración de la defensa contra ataques..... 58
5.8.4 Advertencia de seguridad..... 61
6 Operaciones del teclado..... 62
6.1 Inicialización..... 62
6.2 Modo de operación y contraseñas de usuario..... 62
6.3 Permiso de usuario..... 62
6.4 Modo Global..... 63
6.4.1 Armado y Desarmado..... 63
6.4.2 Cancelar alarma..... 64
6.4.3 Anulación y aislamiento..... 64
6.4.4 Relé..... sesenta y cinco
6.4.5 Prueba PSTN..... sesenta y cinco
6.4.6 Reiniciar el Panel de control..... 66
6.4.7 Inicialización del panel de control..... 66
6.4.8 Restauración a los valores predeterminados..... 67

Apéndice 1 Glosario..... 68

Apéndice 2 Recomendaciones de ciberseguridad..... 71

1 Descripción general del producto

1.1 Introducción

Este panel de control de alarma de alto rendimiento está especialmente diseñado para escenarios de aplicación de alarma basados en plataforma integrada. El panel de control adopta tecnología de control avanzada y tiene poderosas capacidades de transmisión de datos. Funciona de manera estable en su conjunto.

Con alta seguridad y confiabilidad, el panel de control puede funcionar de forma independiente o conectarse a un software de vigilancia profesional (DSS Professional) para formar una red de seguridad, mostrando su poderosa función de monitoreo remoto.

El panel de control es aplicable para uso con seguridad y protección en áreas como escuelas, tiendas, fábricas, institutos financieros, autoridades judiciales y áreas residenciales inteligentes.

1.2 Características

- Están disponibles una entrada de alarma local de 8/16 canales (se puede ampliar a 72/80/256) y una salida de 4 canales (se puede ampliar a 84/256).
- Conexiones con detectores normalmente abiertos o cerrados y alarmas de manipulación, cortocircuito y enmascaramiento.
- Enciende o apaga de forma forzada y automática el panel de control y el enlace de alarma.
- Hay varios tipos de zonas disponibles, como zona de tiempo real, zona de retardo de tiempo y zona de silencio de 24 horas.
- Proporciona protección para el circuito del puerto de entrada y salida de alarma.
- Las alarmas de falla incluyen alarma de manipulación para el panel de control y el teclado, alarma de falla de energía para el adaptador y la batería de almacenamiento, alarma de bajo voltaje de la batería de almacenamiento, alarma PSTN fuera de línea, alarma de desconexión de red, alarma de conflicto de direcciones IP o MAC, y más.
- Conexión abierta para 2 canales de RS-485, hasta 32 canales para teclado, impresora y módulos de extensión.
- Alarmas de pánico como alarmas de incendio, médicas y de coacción.
- Protocolos PSTN y Contact ID.
- SMS y red disponibles en el modelo G.
- Módulo 4G opcional, audio TTS, red y SMS.
- Opere en el panel de control mediante comandos de teclado (siguiendo instrucciones de audio) en una llamada telefónica.
- Configurar por teclado y página web. Admite guía de configuración rápida, configuración remota y búsqueda.
- armar y desarmar zona única y subsistema (8 como máximo) mediante teclado, control remoto, tarjeta IC, SMS (modelo G) y más.
- Estrategia de carga de datos para múltiples centrales receptoras de alarmas.
- Búsqueda masiva de registros.
- Actualización remota.
- Múltiples métodos de restauración.
- Puertos de red duales. Dos centrales de alarma cableadas y dos centrales de alarma inalámbricas.
- Acceso a 16 módulos de red y 64 dispositivos inalámbricos.

2 Desempacar y verificar

Cuando reciba el panel de control, compruébelo con la siguiente lista de verificación. Si alguno de los artículos falta o está dañado, comuníquese con el minorista local o con el personal del servicio posventa de inmediato.

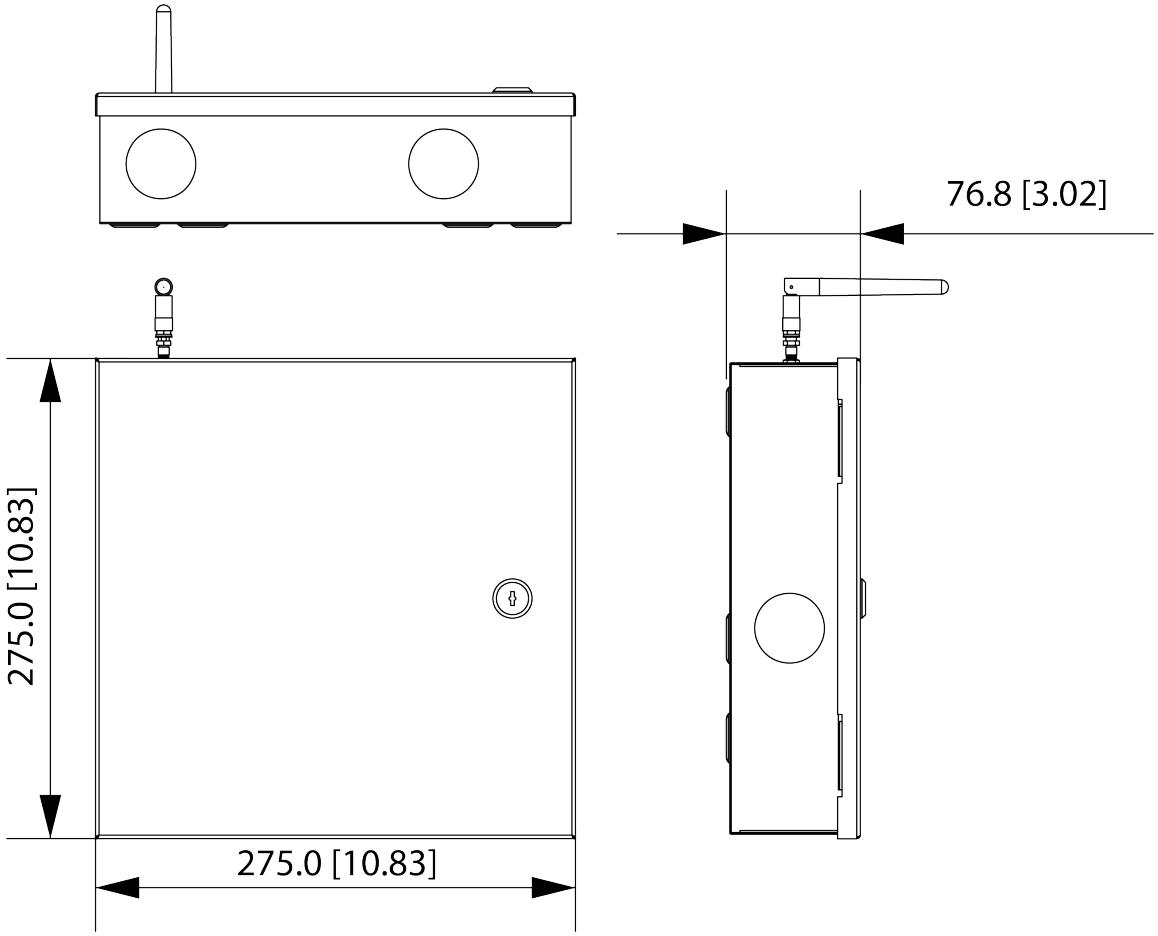
Tabla 2-1 Lista de verificación

No.	Artículo		Contenido
1	Paquete completo	Apariencia	Ningún daño evidente.
		Paquete	Compruebe si hay signos de impacto accidental.
		Accesorio	Compruebe si todos los accesorios están presentes.
2	Caja	Apariencia	Ningún daño evidente.
		Cables de datos, alimentación. Cables, cables de ventilador y placa principal.	Sin conexiones sueltas. Póngase en contacto con el servicio posventa inmediatamente si alguno de los cables o líneas está suelto.
3	Manual de usuario	—	Compruebe si hay 1 manual de usuario.
4	Resistencia		Compruebe si hay 32 resistencias.

3 dimensiones y puertos de placa base

3.1 Dimensiones

Figura 3-1 Dimensiones (mm [pulgadas])



3.2 Puertos de la placa base

Esta sección utiliza los puertos de la placa base de la serie ARC9016C como ejemplo.

En comparación con la serie ARC9016C, las series ARC2016C y ARC2008C no tienen módulo MBUS.
La serie ARC2008C admite entrada de alarma local de 8 canales y salida de alarma de 4 canales.

Figura 3-2 Puertos de la placa base

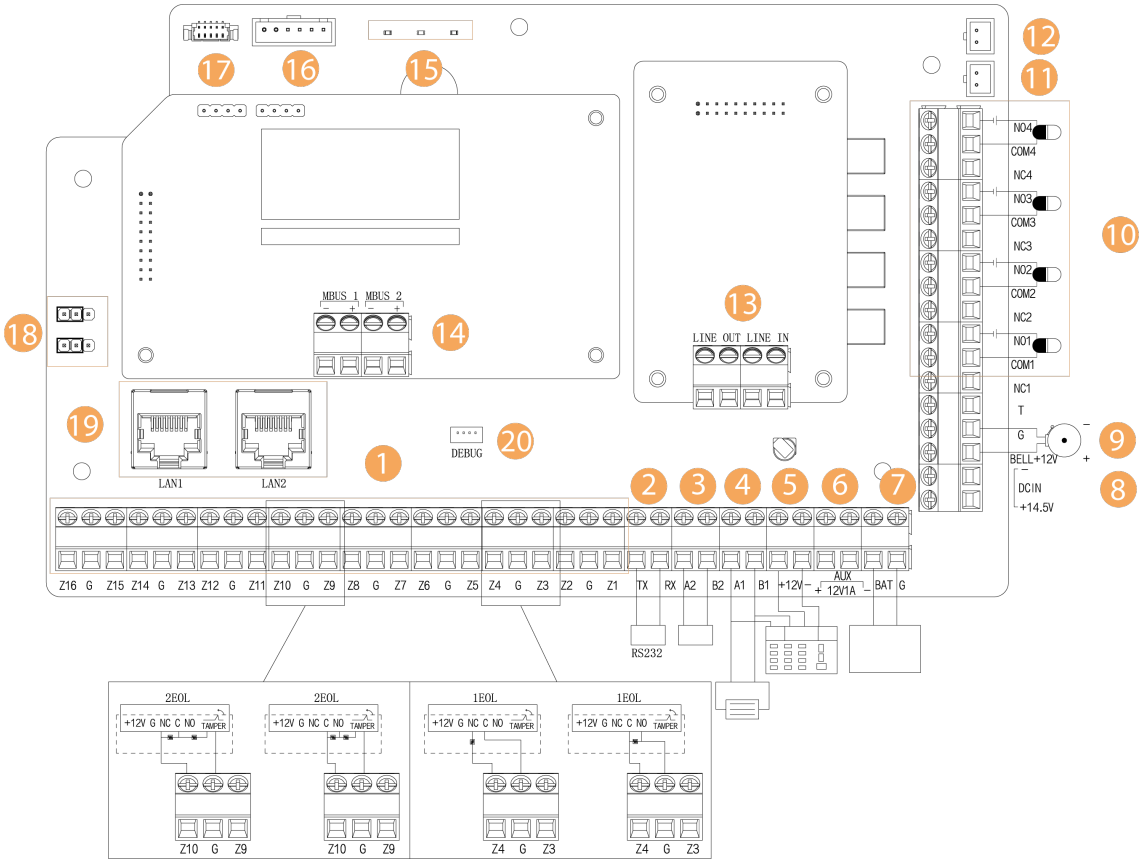


Tabla 3-1 Descripción de los puertos de la placa base

No.	Descripción
1	Puerto de entrada de alarma local. Admite entrada de alarma local de 16 canales. La serie ARC2008C admite entrada de alarma local de 8 canales.
2	RS-232.
3	A2, B2: Se conecta a módulos de entrada y salida de alarma de extensión RS-485.
4	A1, B1: Se conecta a la impresora o al teclado.
5	+ 12 VDC, –: Se conecta a la fuente de alimentación del teclado de programación de alarmas.
6	Fuente de alimentación auxiliar de 12 VCC, que alimenta otros módulos de dispositivos.
7	Puerto para batería de almacenamiento de plomo-ácido de 12 VCC.
8	Puerto de alimentación de 14,5 VCC.
9	• BELL, G: Sirena. • T: Sirena de manipulación.
10	Puerto de salida de alarma local. Admite salida de alarma de 4 canales.
11	Puerto de manipulación de caja.
12	Puerto de manipulación de pared.

No.	Descripción
13	• SALIDA DE LÍNEA: Puerto telefónico. • LINE IN: Puerto de línea de usuario.
14	Puerto M-BUS. Admite módulos de extensión de 2 canales. Las series ARC2016C y ARC2008C no tienen módulo M-BUS.
15	Indicador de estado. Izquierda: Batería colocada o subtensión. Medio: Descarga de batería. Derecha: Poder.
dieciséis	Puerto del módulo 2G.
17	Puerto del módulo 4G.
18	Restaurar la configuración de fábrica y restablecer los puertos de contraseña.
19	Puerto de red. La dirección IP predeterminada de LAN1 es 192.168.1.108 y LAN2 es 192.168.2.108.
20	Puerto de depuración. Utilizado para depurar.

4 Instalación y cableado

4.1 Montaje en pared

Asegúrese de que la distancia entre la pared y el panel de control no sea inferior a 15 mm para la circulación del aire.

Procedimiento

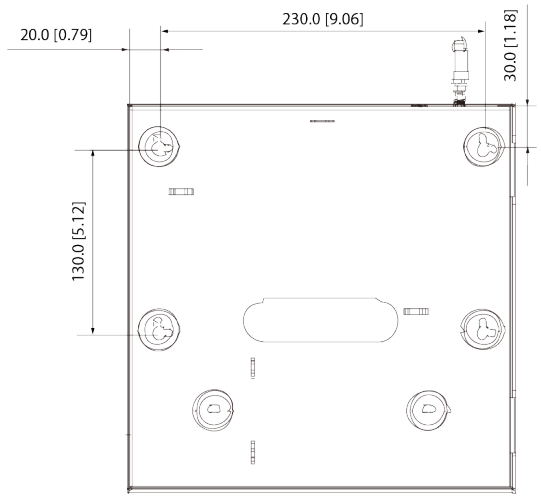
Paso 1 Abra la caja del paquete, saque el tubo de expansión de plástico y los tornillos autorroscantes.

Paso 2 Haz 4 agujeros en la pared.

Paso 3 Inserte el tubo de expansión de plástico en los orificios y luego inserte los 4 tornillos autorroscantes.

Etapa 4 Cuelgue el panel de control de los tornillos.

Figura 4-1 Instalación (mm [pulgadas])



4.2 Conexión de cables

4.2.1 Requisitos de cables

Tabla 4-1 Especificaciones para el cable recomendado del panel de control de alarma ARC

Dispositivo	Materiales de alambre	Área de sección (mm2)	Recomendado distancia (m)
Cable de red	CAT-5	—	≤ 100 metros
Detector	RVV	0,75	≤ 200 metros
Línea de señal RS-485	RVS	1.0	≤ 1.000m
Campana	RVV	0,75	≤ 200 metros
Línea de señal M-BUS	RVVP	1.5	≤ 2.400m

4.2.2 Conexión del cable de entrada de alarma local

Esta sección utiliza una entrada de alarma de 16 canales como ejemplo, los puertos correspondientes son Z1 a Z16. 0 o 1 EOL, 2 EOL y 3 EOL están disponibles para detectores que normalmente están abiertos y cerrados. Configure el panel de control en 0 o 1 EOL cuando no se requiere la alarma de manipulación del detector, 2 EOL para alarma de manipulación y 3 EOL para alarmas de manipulación y de máscara.

Figura 4-2 Cableado del detector (normalmente abierto)

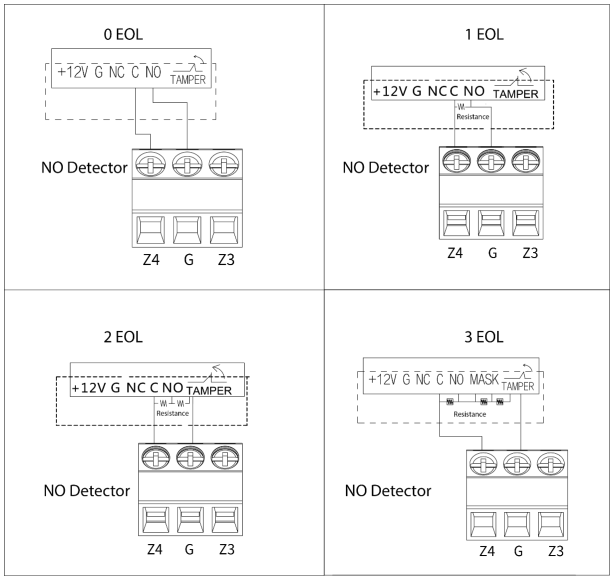
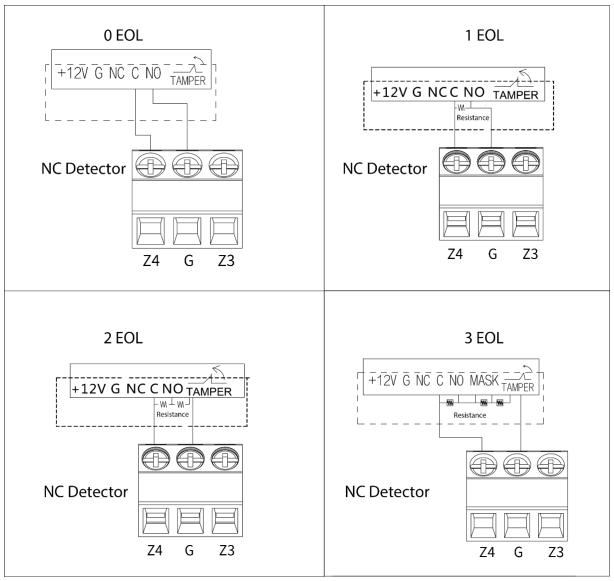


Figura 4-3 Cableado del detector (normalmente cerrado)



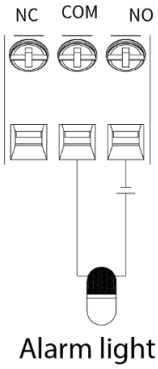
4.2.3 Conexión del cable de salida de alarma local

Para evitar daños al relé por sobrecorriente, no conecte el puerto de salida de alarma del panel de control donde puedan recibir grandes cargas de energía (no más de 1 VCA). Si necesita utilizar grandes cargas de potencia, utilice un contactor.

Las salidas de alarma de 4 canales corresponden a los puertos NC1–NC4, C1–C4 y NO1–NO4.

- NC: Puerto normalmente cerrado.
- C: Puerto común (COM).
- NO: Puerto normalmente abierto.

Figura 4-4 Conexión del cable de salida de alarma local

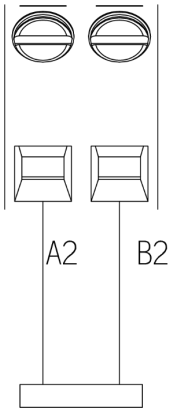


Los dispositivos externos necesitan una fuente de alimentación adicional. La capacidad de carga de la luz de alarma no supera los 12 VCC y 1 VCA.

4.2.4 Conexión del cable RS-485

Puerto RS-485. Se utiliza para conectar a módulos de entrada o salida de alarma de extensión RS-485.

Figura 4-5 Conexión del cable RS-485

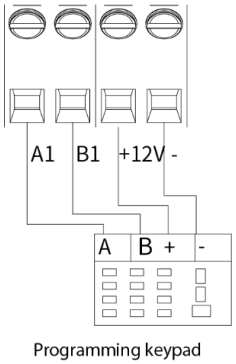


RS-485 extension module

4.2.5 Conexión del cable del teclado

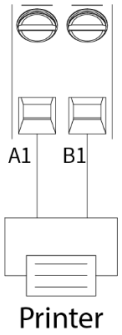
Conecte el puerto B y A del teclado a los puertos B y A del panel de control, el puerto – y + a GND– y + 12 VDC del panel de control.

Figura 4-6 Conexión del cable del teclado



4.2.6 Conexión del cable de la impresora

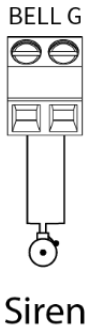
Figura 4-7 Conexión del cable de la impresora



4.2.7 Conexión del cable de la sirena

La capacidad de carga del puerto de sirena es de 12 VDC y 1 VAC.

Figura 4-8 Conexión del cable de sirena



4.2.8 Conexión del cable del módulo de expansión

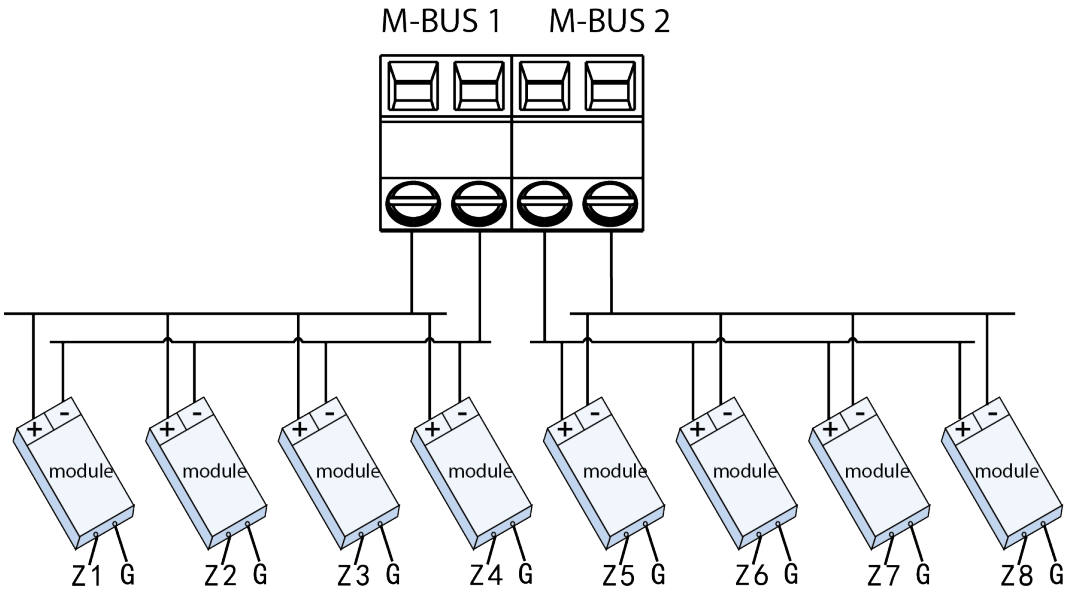
Proporciona puerto M-BUS de 2 canales.

- El valor de la resistencia de final de línea de la entrada del módulo de extensión es de 10 kΩ.
- El rango del código DIP de dirección del módulo de extensión es 0–254. Según el módulo de extensión (ARM801, ARM802, ARM911, ARM808), consulte "4.2.1 Requisitos del cable" para ver detalles sobre el

Requisitos de conexión de cables. El módulo M-BUS de un solo canal admite una distancia de comunicación de 2,4 km.

- El número de módulos a los que se puede conectar cada M-BUS es el siguiente.
  - ◇ El módulo 801 es un canal de entrada de zona única que admite 120 módulos.
  - ◇ El módulo 802 es el canal de entrada de 2 zonas que admite 60 módulos.
  - ◇ El módulo 911 es un canal de entrada de zona única con una salida, que admite 60 módulos. El
  - ◇ módulo 808 es el canal de entrada de 8 zonas con una salida, que admite 15 módulos.
- La dirección del módulo de extensión no se puede repetir; de lo contrario, es posible que el panel de control no pueda detectar el módulo de extensión o que no pueda reconocer si el módulo de extensión está en línea o fuera de línea.

Figura 4-9 Conexión del cable del módulo de extensión



5 operaciones web

5.1 Iniciar el dispositivo

5.1.1 Inicializando el Panel de Control

Información de contexto

Cuando utilice el panel de control por primera vez después de la instalación o después de restaurar la configuración de fábrica, configure la contraseña de inicio de sesión para la cuenta de administrador. Además, configure una dirección de correo electrónico en caso de que necesite restablecer la contraseña de inicio de sesión para la cuenta de administrador.

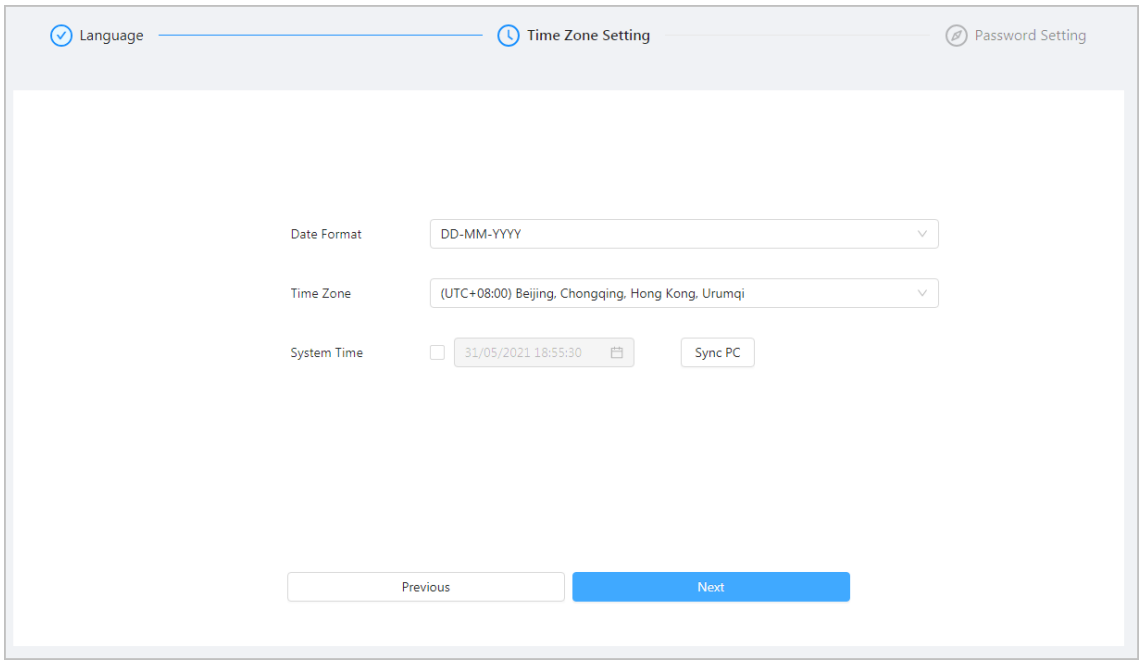
- Para proteger su dispositivo, mantenga segura su contraseña de inicio de sesión de administrador después de completar los pasos de inicialización y cambie la contraseña periódicamente.
- La dirección IP predeterminada de LAN1 es 192.168.1.108 y LAN2 es 192.168.2.108.

Procedimiento

Paso 1 Abra el navegador, ingrese la dirección IP predeterminada del panel de control y luego presione la tecla Enter.

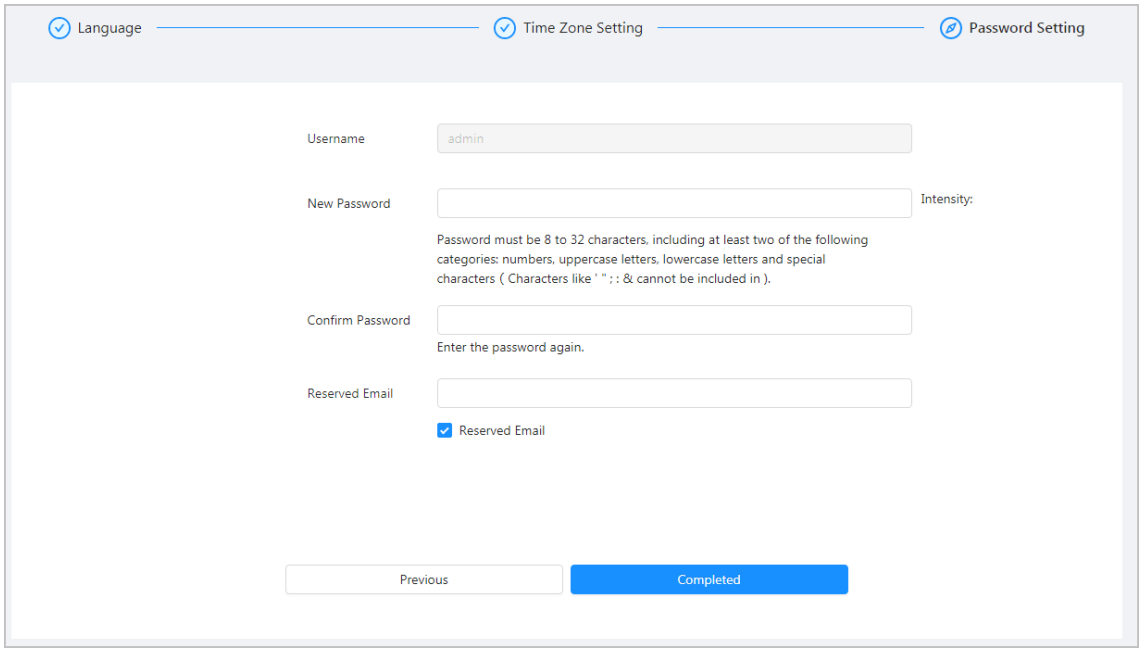
Paso 2 Colocar**Idioma**(compatible con inglés, ruso, latinoamericano, árabe),**Zona horaria**y**Hora del sistema**y luego haga clic en**Próximo**.

Figura 5-1 Inicializar



Paso 3 Establezca la contraseña de inicio de sesión para el administrador.

Figura 5-2 Establecer contraseña de administrador



Etapa 4 Seleccionar**Correo electrónico reservado**y luego ingrese la dirección de correo

Paso 5 electrónico. Hacer clic**Terminado**.

Se muestra un mensaje de inicialización exitosa y luego se muestra la página de inicio de sesión.

5.1.2 Iniciar sesión en Web Manager

Información de contexto

Asegúrese de que la computadora local y el panel de control estén en el mismo segmento de red.

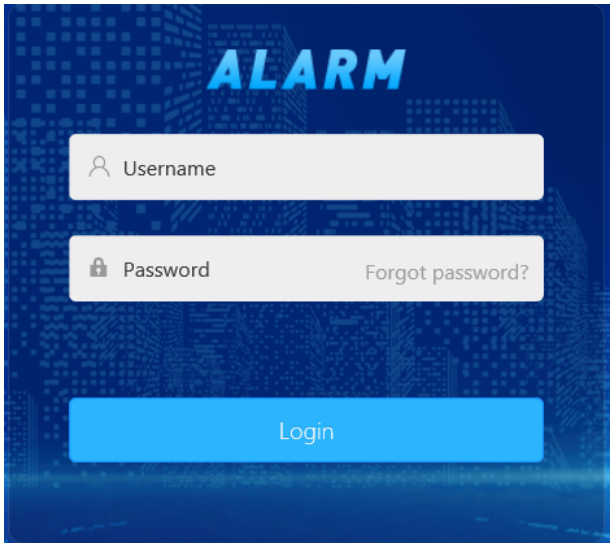
- La dirección IP predeterminada de LAN1 es 192.168.1.108 y LAN2 es 192.168.2.108.
- Se recomienda que la versión del navegador sea Chrome 41.0 o posterior, IE9.0 o posterior, o Firefox 50.0 o posterior.

Procedimiento

Paso 1 Ingrese la dirección IP del dispositivo en la barra de direcciones del navegador y luego presione Entrar.

Paso 2 Ingrese el nombre de usuario y la contraseña y luego haga clic en**Acceso**.

Figura 5-3 Iniciar sesión



5.1.3 Guía de configuración

El Asistente de configuración está disponible para una configuración rápida de parámetros relacionados para el armado y desarmado básico de una sola zona y subsistema, y para configurar la alarma de salida y los ajustes del centro receptor de alarmas.

5.1.3.1 Configuración de zona y subsistema

5.1.3.1.1 Configuración de zona

Configure el método de detección de sensores, tipo de zona y tipo de sensor de cada zona.

Procedimiento

Paso 1 Hacer clic en la esquina superior derecha de la página de inicio.

Paso 2 Hacer clic para configurar los parámetros de la zona.

Figura 5-4 Configurar zona

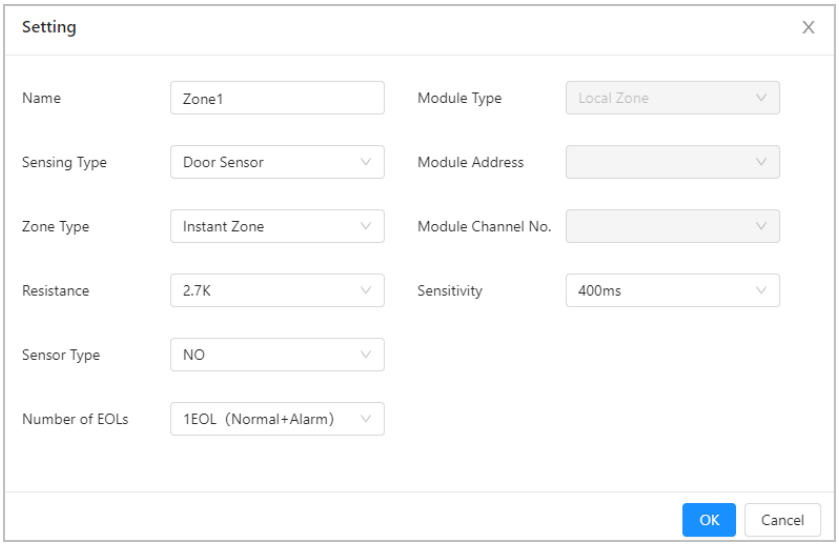


Tabla 5-1 Descripción de los parámetros de zona

Parámetro	Descripción
Nombre	Nombre de zona personalizado.
Tipo de detección	Seleccione según el tipo de detector conectado.
Tipo de zona	Seleccione la zona según sea necesario. Para obtener más información, consulte el "Apéndice 1 Glosario".
Resistencia	Seleccione 10 K para el módulo M-BUS y otros según sea necesario. 2,7 K, 4,7 K, 6,8 K, 10 K (M-BUS).
Tipo de sensor	Seleccionar**NO**o**CAROLINA DEL NORTE**según el tipo de sensor. ● NO: Normalmente abierto. ● NC: Normalmente cerrado.
Número de EOL	● 0 EOL (Normal + Alarma): Sin resistencia. ● 1 EOL (Normal + Alarma): Predeterminado. ● 2 EOL (Normal + Alarma + Cortocircuito + Sabotaje): Soporta alarmas de cortocircuito y sabotaje. ● 3 EOL (Normal + Alarma + Cortocircuito + Sabotaje + Enmascarado): Admite alarma de máscara.
Tipo de módulo	Seleccione el módulo correspondiente. ● Zona Local ● MBUS ● RS-708 ● RS-808 ● Módulos de red ● Dispositivos inalambricos
Dirección del módulo	Ingrese la dirección según sea necesario. Recomendamos configurar la dirección en secuencia comenzando desde 0. ● **ARM801**,**ARM802**y**ARM911**: 0–254. ● **ARM808**:0–127. ● **RS-808**y**RS-808**: 0–15. ● **Módulos de red**:1–16. ● **Dispositivos inalambricos**:1–70.
Canal del módulo No.	Ingrese según sea necesario. ● **ARM801**y**ARM911**: 1. ● **ARM802**:1–2. ● **ARM808**,**RS-708**y**RS-808**: 1–8. ● **Módulos de red**:1–8. ● **Dispositivos inalambricos**:1–2.
Sensibilidad	● Establezca el valor de sensibilidad. Puede seleccionar entre 200 ms, 400 ms, 600 ms u 800 ms. El valor de sensibilidad es de 400 ms de forma predeterminada. ● Admite la configuración del valor de sensibilidad para una sola zona. ● Admite la modificación de los valores de sensibilidad de los siguientes módulos de expansión: RS-808, RS-708 y RS-816.

Paso 3 Hacer clic**DE ACUERDO**.

Etapa 4 Hacer clic**Próximo**.

5.1.3.1.2 Configuración del subsistema

Configure el horario, la hora y el modo de armado y desarmado diario para el subsistema.

Procedimiento

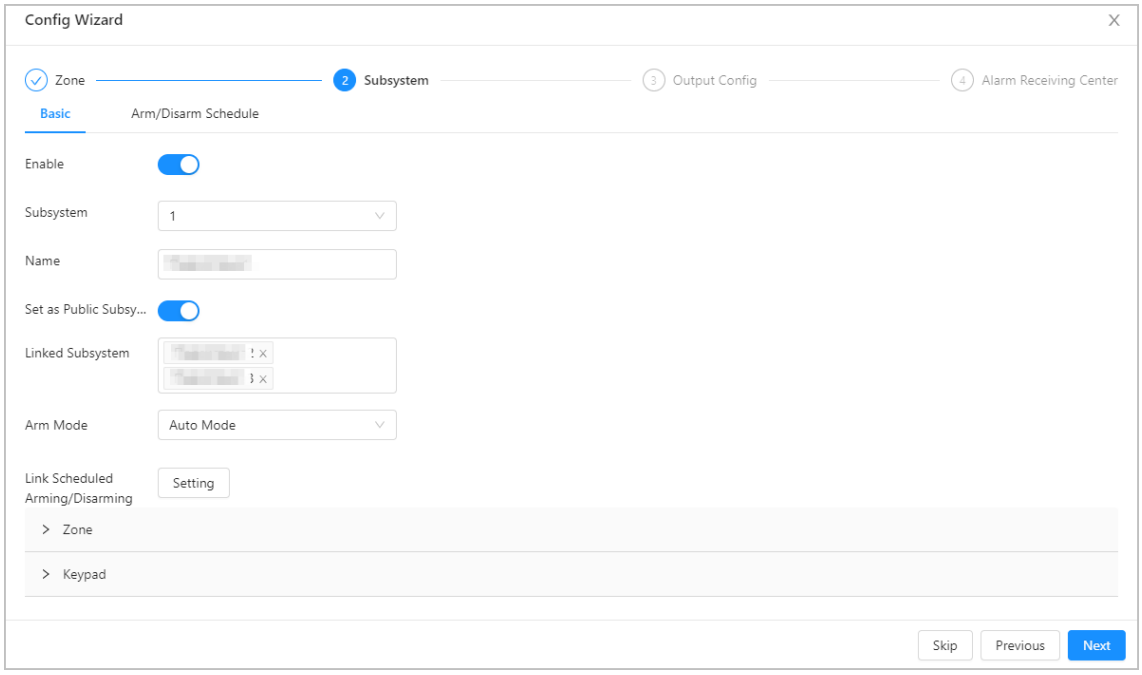
Paso 1 En el**Subsistema**, seleccione un subsistema de la lista desplegable.

si estableces**Subsistema**a 1, puede configurarlo como un subsistema público. Una vez configurado, puede vincular el subsistema 1 a otros subsistemas, zonas y el teclado. También puede configurar modos de armado y horarios para armar y desarmar el subsistema público.

1. Haga clic junto a**Establecer como subsistema público**para permitir el funcionamiento del subsistema público.
2. Seleccione los subsistemas vinculados.

- Además del subsistema 1, puede seleccionar al menos 2 subsistemas.
- Si todos los subsistemas vinculados están armados, el sistema público se armará automáticamente. Si todos los subsistemas vinculados están desarmados, el sistema público se desarmará automáticamente.
- Colocar**Modo armado**a**Modo automático**o**Modo forzado**.

Figura 5-5 Configuración de armado/desarmado



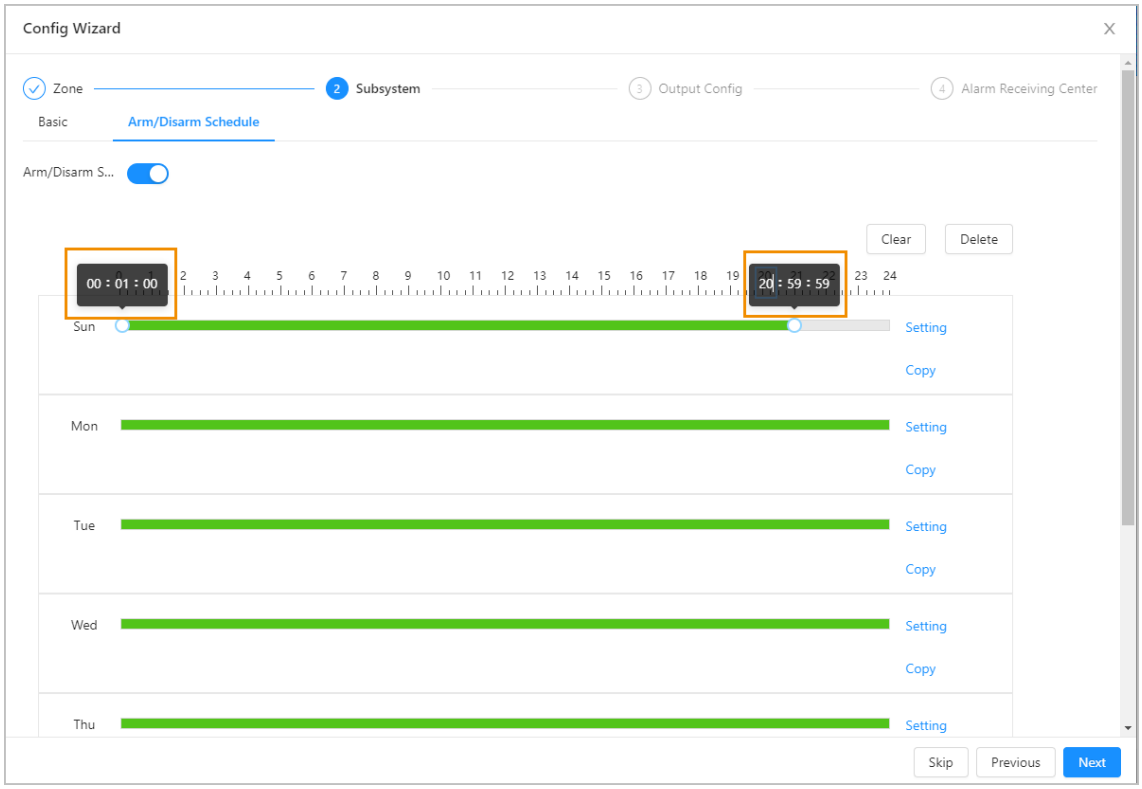
Paso 2 Seleccionar**programar armar y desarmar**, configure el tiempo de armado/desarmado.

El área verde en el control deslizante indica que el sistema estará armado durante los períodos definidos.

- Haga clic y mantenga presionado el control deslizante y ajuste ambos extremos para configurar el tiempo de armado y desarmado.
- Haga clic en el control deslizante, ingrese una hora específica en el cuadro de texto de hora de inicio y finalización para configurar el período de armado y desarmado.

Hacer clic**Copiar**para copiar el horario a otros días.

Figura 5-6 cronograma de armado y desarmado



Paso 3 Hacer clic**Configuración**para configurar el período de armado y desarmado y su modo.

De forma predeterminada, la hora de inicio es la hora de armado y la hora de finalización es la de desarmado.

Figura 5-7 Configuraciones de armado/desarmado

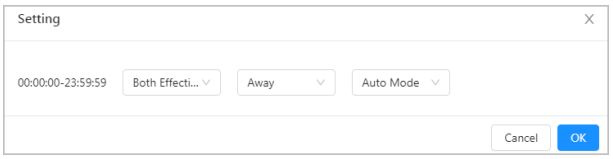


Tabla 5-2 Descripción del parámetro de armado

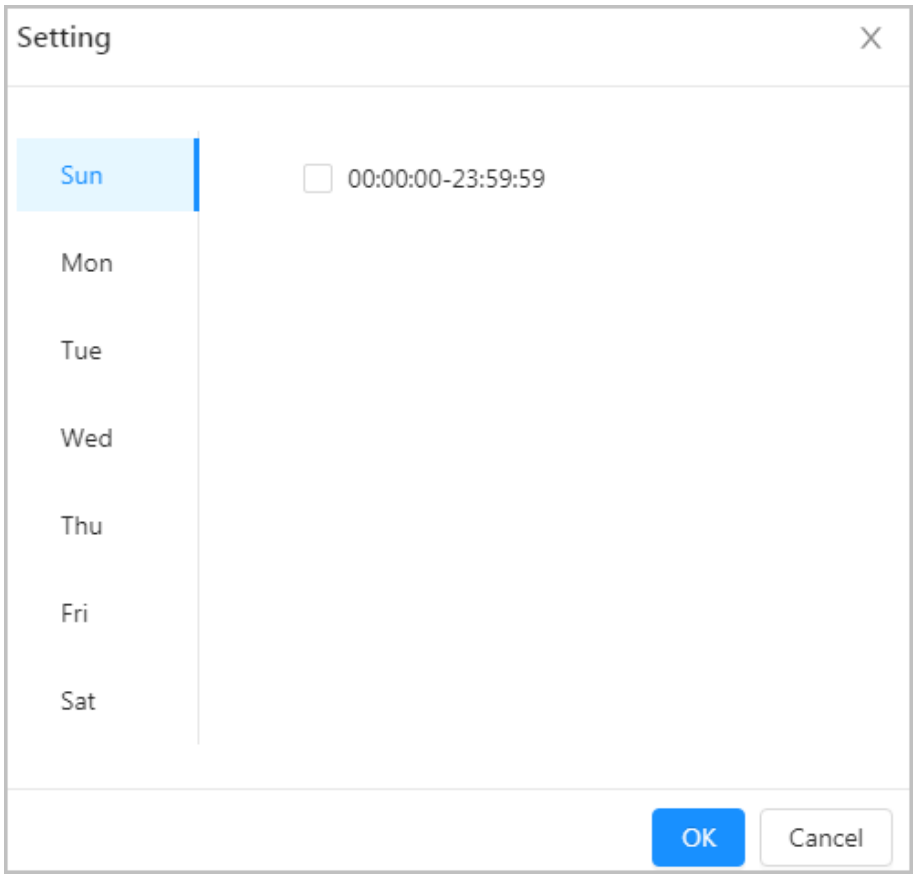
Parámetro	Descripción
Hora de inicio efectiva	Arma el sistema al momento de inicio, pero no lo desarma al momento de finalizar.
Hora de finalización efectiva	Desarma el sistema al finalizar.
Ambos efectivos	Arma el sistema a la hora de inicio y lo desarma a la hora de finalización.
Modo automático	Se arma/desarma automáticamente en el momento definido cuando no ocurren errores (predeterminado). No se arma automáticamente cuando ocurre un error.

Parámetro	Descripción
Modo forzado	Forzar el armado del subsistema.

Etapa 4 Hacer clic para habilitar el cronograma de armado y desarmado.

Paso 5 Seleccionar**Básico**>**Configuración**y luego seleccione el día para configurar la hora para habilitar el horario.

Figura 5-8 Configuración básica



Paso 6 Hacer clic**DE ACUERDO**.

Paso 7 Hacer clic**Próximo**para configurar el relé y la sirena.

5.1.3.2 Configuración de salida

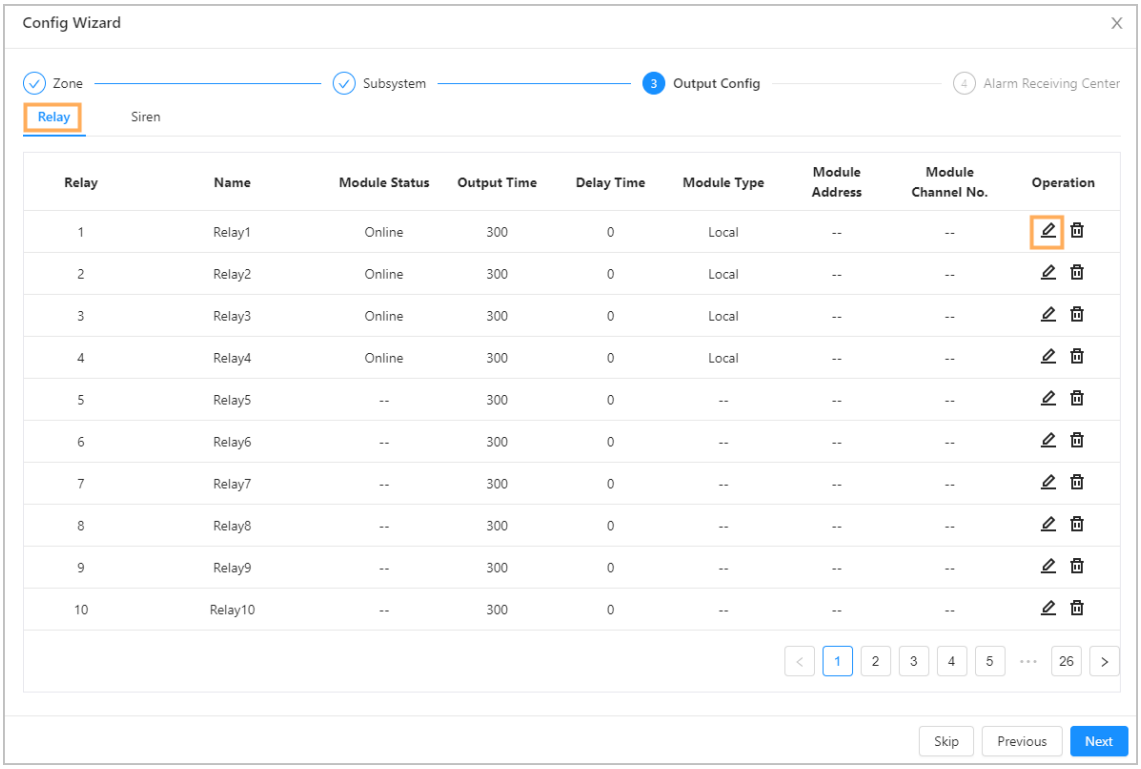
5.1.3.2.1 Configuración de retransmisión

Establece el estado de salida del relé de cada canal. Cuando se activa una alarma, el panel de control vincula el relé a la salida.

Procedimiento

Paso 1 En el**Configuración de salida**sección, seleccione**Relé**y luego haga clic en .

Figura 5-9 Relé



Paso 2 Configure los parámetros.

Figura 5-10 Configuración

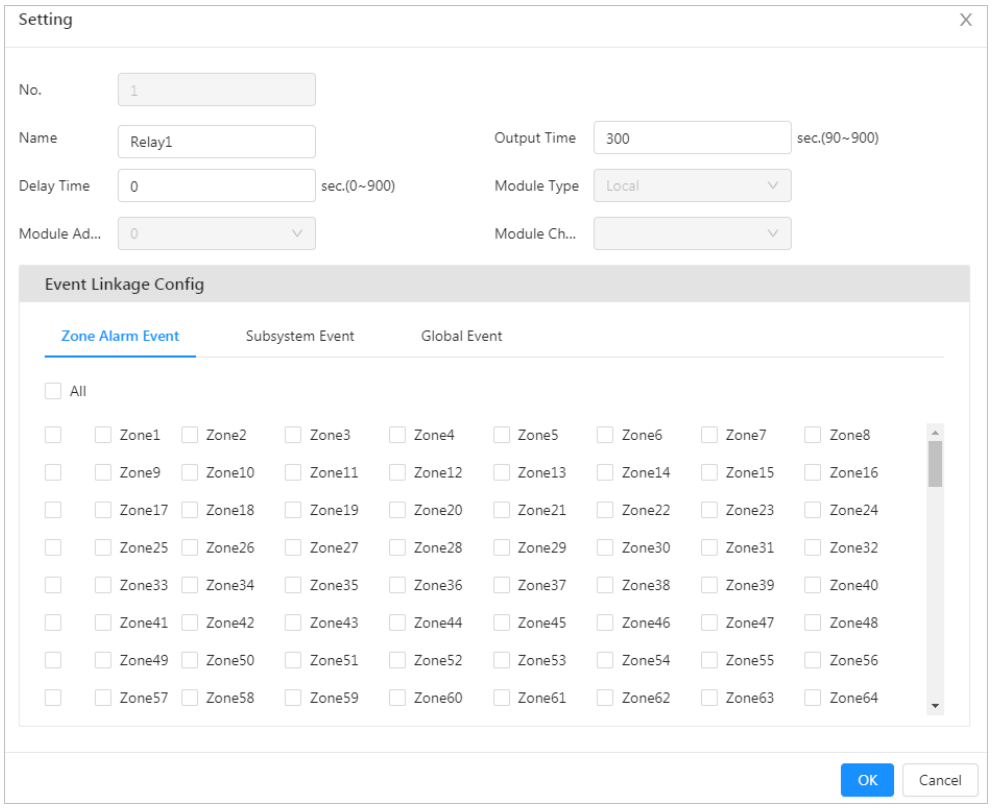


Tabla 5-3 Descripción de los parámetros del relé

Parámetro	Descripción
Nombre	Introduzca el nombre del relé.
Tiempo de salida	El período en el que el relé vuelve al estado desconectado.
Tiempo de retardo	El período que el relé demora antes de volver a emitir otra salida.
Configuración de vinculación de eventos	Cuando ocurre un evento, el panel de control vincula el relé a la salida. ● **Evento de alarma de zona**:Seleccione las zonas a configurar. ● **Evento del subsistema**:La salida vinculada después de que el subsistema esté armado o desarmado. Por ejemplo, después de que se arma el subsistema 1, el panel de control vincula el relé 1 a la salida. ● **Evento Mundial**:Cuando ocurre un evento del sistema o un evento de emergencia, el panel de control vincula el relé a la salida.
Tipo de módulo	Seleccione según los módulos reales (no se necesita configuración para los 4 relés locales). ● **Local**. ● **MBUS**. ● **RS-708**. ● **RS-808**.
Dirección del módulo	Ingrese la dirección según sea necesario. Recomendamos configurar la dirección a partir de 0. ● **ARM801**,**ARM802**y**ARM911**: 0–254. ● **ARM808**:0–127. ● **RS-708**y**RS-808**: 0–15. ● **Módulos de red**:1–16.
Número de canal del módulo	● **ARM808**y**ARM911**: 1. ● **RS-708**:1–8. ● **RS-808**:1–2. ● **Módulos de red**:1–2.

Paso 3 Hacer clic**DE ACUERDO**.

5.1.3.2.2 Configuración de la sirena

Configure el estado de salida del relé para cada canal. Cuando ocurre un evento de alarma, el panel de control vincula la sirena a la salida.

Procedimiento

Paso 1 Sobre el**Configuración de salida**sección, seleccione**Sirena**y luego haga clic

Paso 2 en . Configure los parámetros.

Figura 5-11 Sirena

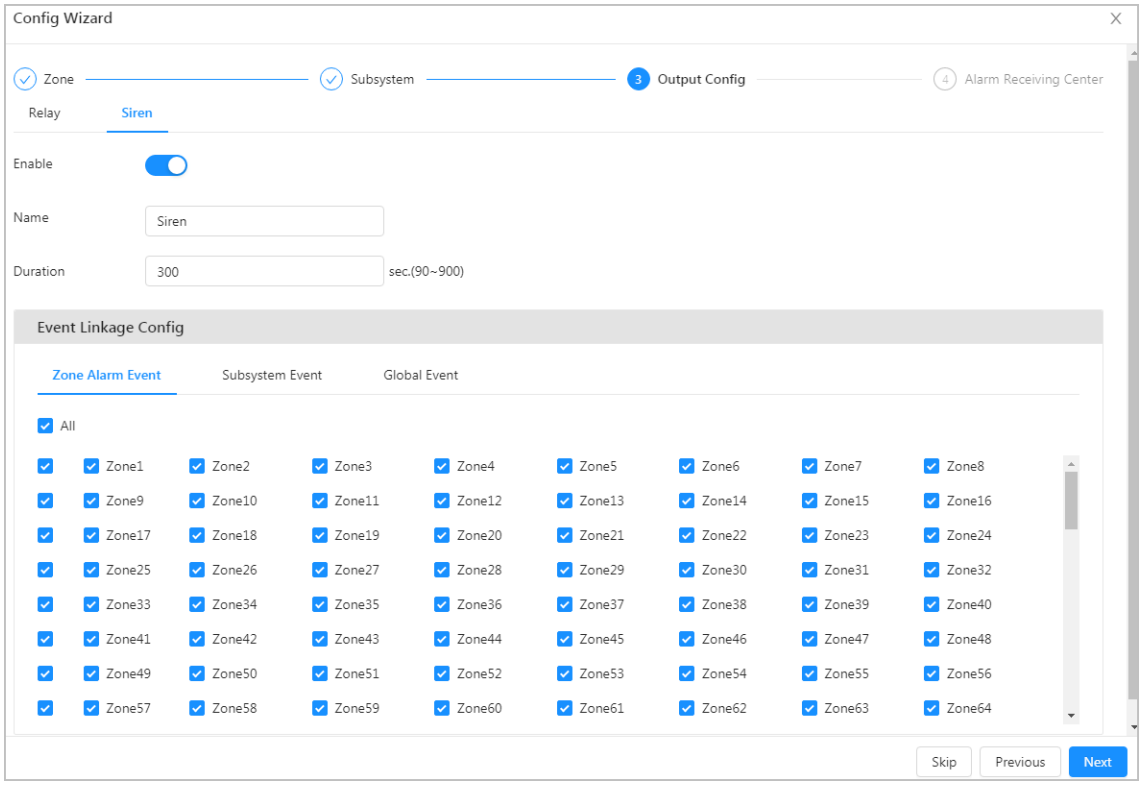


Tabla 5-4 Descripción

Parámetro	Descripción
Nombre	Ingrese el nombre de la sirena.
Duración	La duración de salida de la sirena.
Configuración de vinculación de eventos	• **Evento de alarma de zona**:Seleccione las zonas a configurar. • **Evento del subsistema**:La salida vinculada después de que el subsistema esté armado o desarmado. Por ejemplo, después de que se arma el subsistema1, el panel de control vincula la sirena a la salida. • **Evento Mundial**:Cuando ocurre un evento del sistema o un evento de emergencia, el panel de control vincula la sirena a la salida.

Paso 3 Hacer clic**Próximo**.

5.1.3.3 Configuración del centro receptor de alarmas

Configure el método de transmisión de alarma. Cuando se activa una alarma, el panel de control envía un mensaje a la central receptora de alarmas.

Procedimiento

Paso 1 Sobre el**Centro Receptor de Alarmas**sección, configure los parámetros.

Figura 5-12 Configuración del centro receptor de alarmas

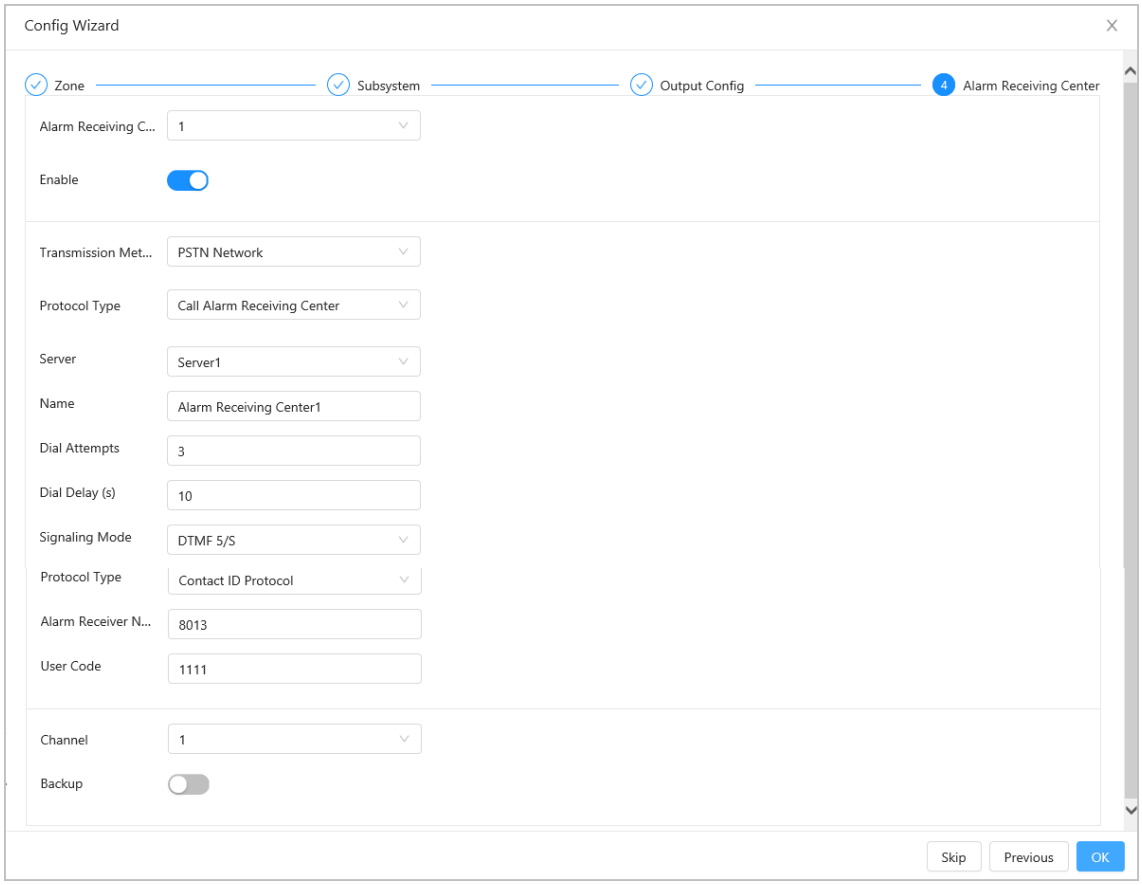


Tabla 5-5 Descripción de los parámetros del centro receptor de alarmas

Parámetro	Descripción
Central Receptora de Alarmas No.	Hacer clic para habilitar la central receptora de alarmas según sea necesario.
Método de transmisión	• **Red PSTN**:Envía mensajes CID al centro receptor de alarmas de llamadas. • **Red celular**,**NIC 1**o**NIC 2**: Envía mensajes de red al centro receptor de alarmas de red.

Parámetro	Descripción
Tipo de protocolo	● Ninguno ● Llamar a central receptora de alarmas ◇ **Servidor**:Seleccione entre el servidor 1 y el servidor 2 según sea necesario. ◇ **Nombre**:Introduzca el nombre del centro. ◇ **Intentos de marcación**:Intenta enviar datos para llamar al centro receptor de alarmas. Si falla 3 veces, el panel de control no enviará mensajes CID. ◇ **Retardo de marcado (s)**:Funciona con**Intentos de marcación**. El tiempo necesario antes de volver a marcar después de un error de marcación. ◇ **Modo de señalización**:Déjalo por defecto. ◇ **Tipo de protocolo**:Es**Protocolo de identificación de contacto**por defecto. ◇ **Número de receptor de alarma**:El número del centro receptor de alarmas de llamadas. ◇ **Codigo de usuario**:Único código utilizado cuando la central envía mensajes a la central receptora de alarmas de llamadas. Es 0000 por defecto. ● Registro ◇ **ID del dispositivo**:ID del dispositivo asignado por el servidor y consistente con el ID registrado en el servidor. ◇ **Servidor**:Servidor 1 y servidor 2. Seleccione según sea necesario. ◇ **DIRECCIÓN**:La dirección IP del servidor en el que debe registrarse. ◇ **Puerto**:El puerto para el registro automático. ● central de alarmas ◇ **Servidor**:Seleccione entre el servidor 1 y el servidor 2 según sea necesario. ◇ **DIRECCIÓN**:La dirección IP del servidor en el que debe registrarse. ◇ **Puerto**:Número de puerto del servidor. ● Puedes configurar**Llamar a la central receptora de alarmas**o**Ninguno**como**Tipo de protocolo**cuando el**Método de transmisión**se establece en**Red PSTN**. ● Puedes configurar**Registro**,**Centro de alarma**o**Ninguno**como**Tipo de protocolo** cuando el**Método de transmisión**se establece en**Red celular**, **NIC 1**o**NIC 2**.
Canal de respaldo	Hacer clic para habilitar el canal de respaldo 1 o 2. Cada centro puede configurar un canal principal y canal de respaldo. El canal de respaldo solo se puede habilitar cuando falla la comunicación con el canal principal.

Paso 2 Hacer clic**DE ACUERDO**.

5.1.4 Restablecer la contraseña

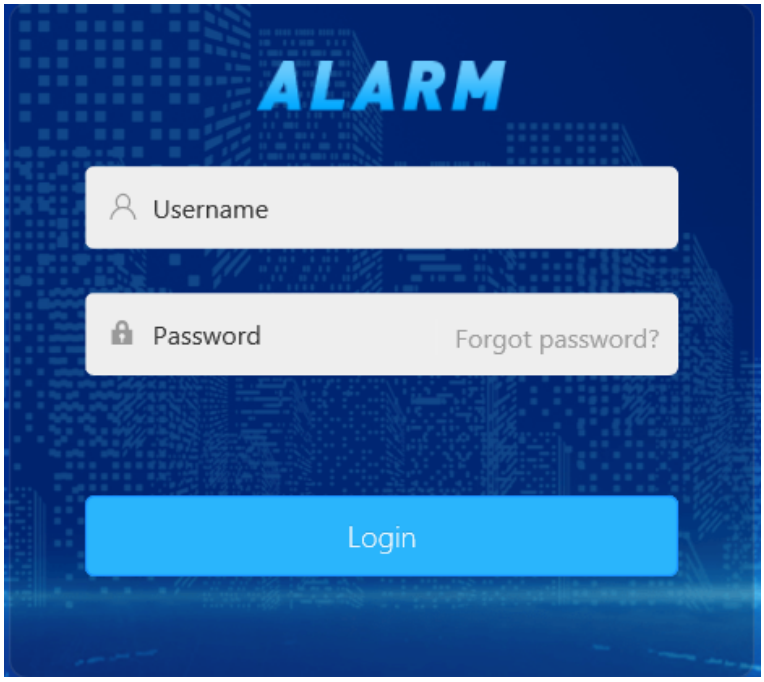
Requisitos previos

- Durante la inicialización del dispositivo, configure un correo electrónico asociado. Para obtener más información, consulte "5.1.1 Inicialización del Panel de control".
- Asegúrese de haber habilitado el**Restablecimiento de contraseña**función en el**Sistema**>**Cuenta**.

Procedimiento

Paso 1 En la página web, haga clic en**¿Has olvidado tu contraseña?**.

Figura 5-13 ¿Olvidé mi contraseña?



Paso 2 Hacer clic**DE ACUERDO**.

Paso 3 Escanea el código QR y obtendrás el código de seguridad.

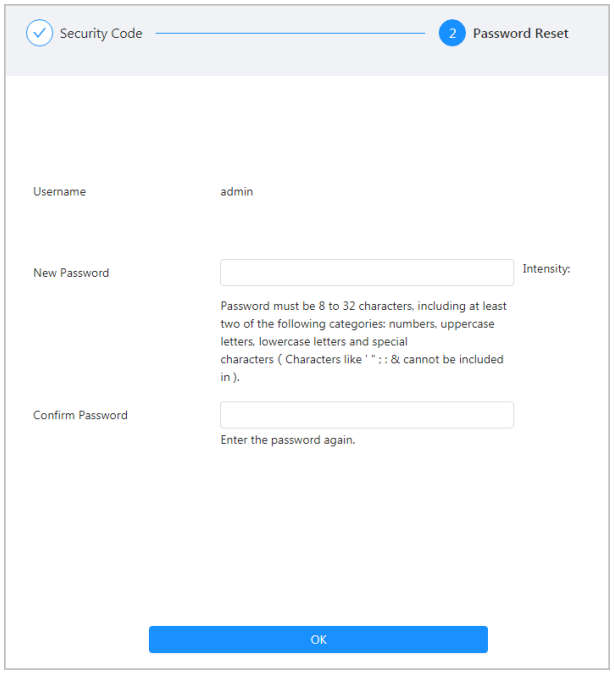
Etapa 4 Ingrese el código de seguridad recibido en el**Código de seguridad**cuadro de texto y luego haga clic en**Próximo**.

Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, no será válido.

Paso 5 Establezca y confirme la nueva contraseña.

La contraseña puede contener de 8 a 32 caracteres no vacíos y debe tener al menos 2 tipos de los siguientes caracteres: letras mayúsculas, minúsculas, números y caracteres especiales (excluidos ' " ; , : &). La contraseña de confirmación debe ser la misma que la nueva contraseña. Utilice el mensaje de seguridad de la contraseña como guía para establecer una contraseña segura.

Figura 5-14 Restablecimiento de contraseña



Paso 6 Hacer clic**DE ACUERDO**.

5.2 Configuración de alarma

Configure funciones básicas como armado/desarmado de zona única y subsistema, salida de alarma y central receptora de alarmas.

5.2.1 Zona

Inicie sesión en la web y luego seleccione**Configuración de alarma**>**Zona**. Para obtener más información, consulte "5.1.3.1.1 Configuración de zona".

5.2.2 Subsistema

Inicie sesión en la web y luego seleccione**Configuración de alarma**>**Subsistema**. Para obtener más información, consulte "5.1.3.1.2 Configuración del subsistema".

5.2.3 Sirena

- Un panel de control de alarma puede admitir hasta 6 conexiones de sirena inalámbrica.
- La duración máxima de la sirena inalámbrica es de 180 s ya que utiliza batería como fuente de alimentación de forma predeterminada.

Procedimiento

Paso 1 Inicie sesión en la página web del panel de control de alarma y luego seleccione**Configuración de alarma**>**Sirena**.

Paso 2 Seleccione la sirena que debe configurarse y haga clic en para habilitar la sirena, y luego configurar parámetros.

Figura 5-15 Configurar sirena

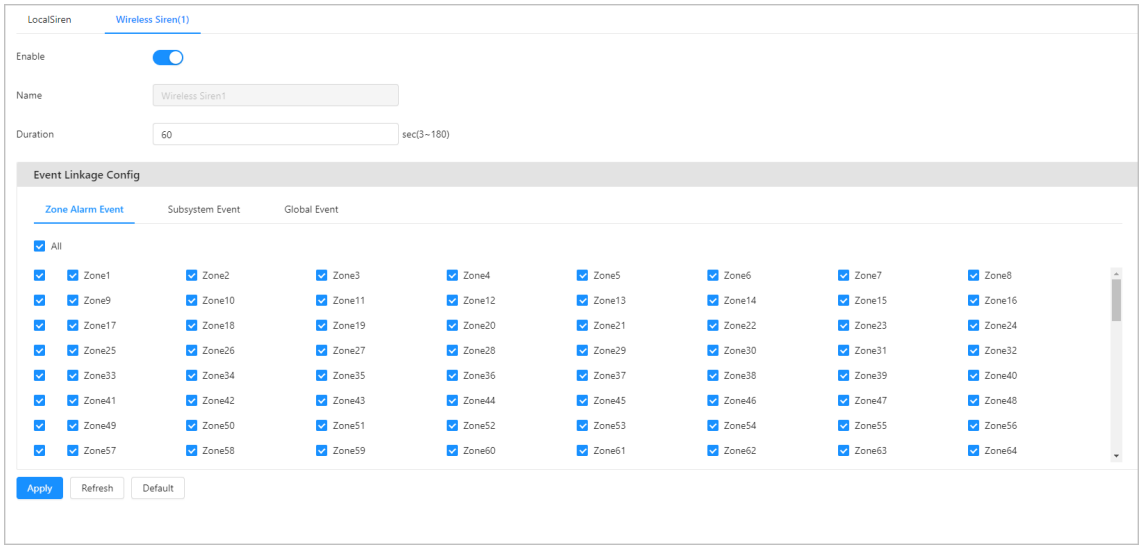


Tabla 5-6 Descripción del parámetro de sirena

Parámetro	Descripción
Nombre	Nombre de sirena personalizado.
Duración	Salida de la hora de la alarma o la duración del sonido de la alarma.
Configuración de vinculación de eventos	Después de la configuración del evento de vinculación, el panel de control de alarma emitirá una señal de alarma de vinculación cuando ocurra un evento de alarma. ● **Evento de alarma de zona**: Seleccione una zona que ya haya sido configurada para eventos de alarma. Cuando ocurre un evento de alarma en la zona de defensa, se emite la señal de alarma de enlace. ● **Evento del subsistema**: La salida vinculada después de que el subsistema esté armado o desarmado. Por ejemplo, después de que se arma el subsistema1, el panel de control vincula la sirena a la salida. ● **Evento Mundial**:Cuando ocurre un evento del sistema o un evento de emergencia, el panel de control vincula la sirena a la salida.

Paso 3 Hacer clic**Aplicar**.

5.2.4 Relé

Inicie sesión en la web y luego seleccione**Configuración de alarma**>**Relé**. Para obtener más información, consulte "5.1.3.2.1 Configuración de la retransmisión".

5.2.5 Impresora

Configure la impresora para que imprima información del evento cuando ocurra el evento definido.

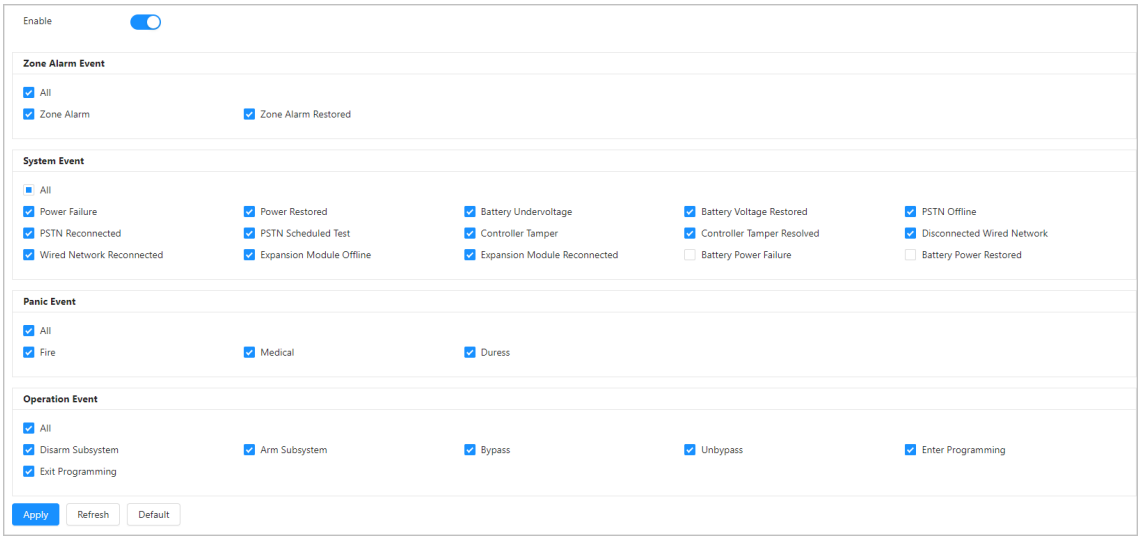
Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Configuración de alarma**>**Impresora**.

Paso 2 Hacer clic**Permitir**.

Paso 3 Seleccione un evento para vincularlo a la impresora.

Figura 5-16 Configuración de la impresora



Etapa 4 Hacer clic**Aplicar**.

5.2.6 Zumbador

Configure el timbre para que suene cuando ocurra el evento definido.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Configuración de alarma**>**Zumbador**.

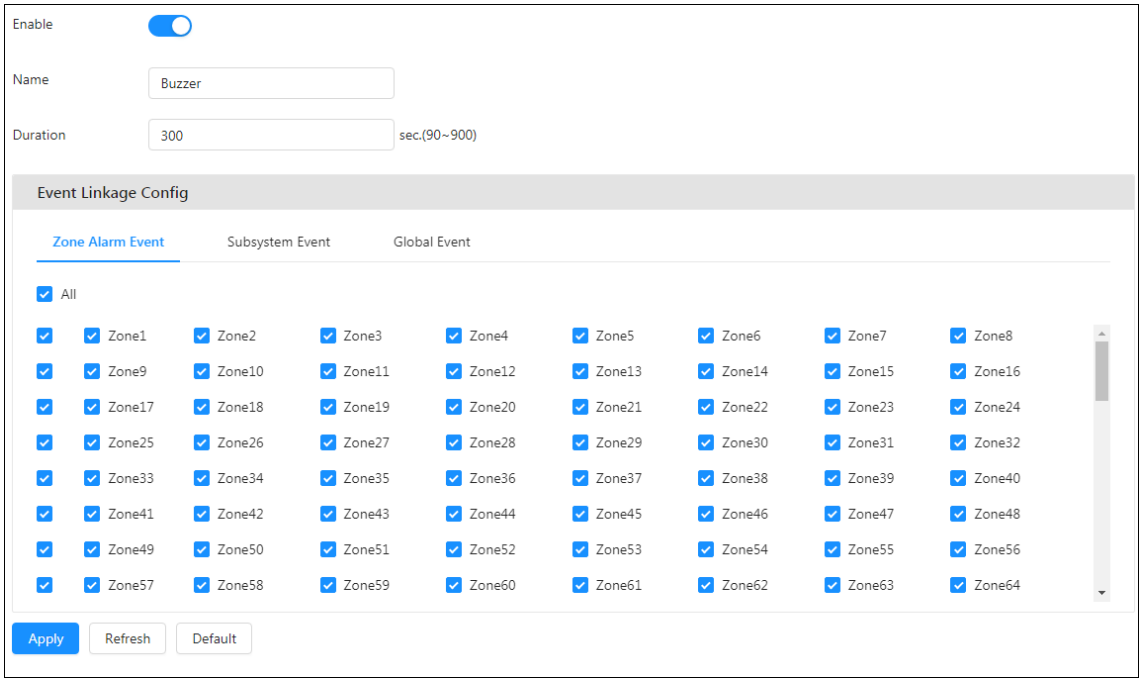
Paso 2 Hacer clic**Permitir**.

Paso 3 Ingrese el nombre del timbre y establezca la duración.

Etapa 4 Seleccione un evento para vincularlo al timbre.

Los parámetros del timbre son los mismos que los de la sirena. Para obtener detalles sobre los parámetros, consulte la Tabla 5-4.

Figura 5-17 Configuración del zumbador



Paso 5 Hacer clic**Aplicar**.

5.2.7 Audio

Información de contexto

Establezca el evento de vinculación. Cuando ocurre un evento definido, se activará una alarma sonora.

- No se admiten caracteres especiales porque son difíciles de reconocer.
- La transmisión de voz TTS no admite otros idiomas además del inglés y el chino.

Procedimiento

Paso 1 Inicie sesión en la web y seleccione**Configuración de alarma**>**Audio.**

Paso 2 Hacer clic**Estrategia de envío**y luego seleccione de la lista desplegable.

- **Sólo PSTN**:Los mensajes de audio sólo se pueden enviar a través del módulo PSTN.
- **Sólo 2G/4G**:Los mensajes de audio sólo se pueden enviar a través del módulo 2G/4G.
- **PSTN preferido**:Seleccione 2G/4G cuando la PSTN no esté disponible.
- **Preferido 2G/4G**:Seleccione PSTN cuando 2G/4G no esté disponible.

Al configurar el**Estrategia de envío**a**Sólo 2G/4G**o**Preferido 2G/4G**, asegúrese de que el panel de control admita el módulo 2G/4G.

Paso 3 Subiendo archivos de audio.

1. Seleccione el archivo de audio para cargar.

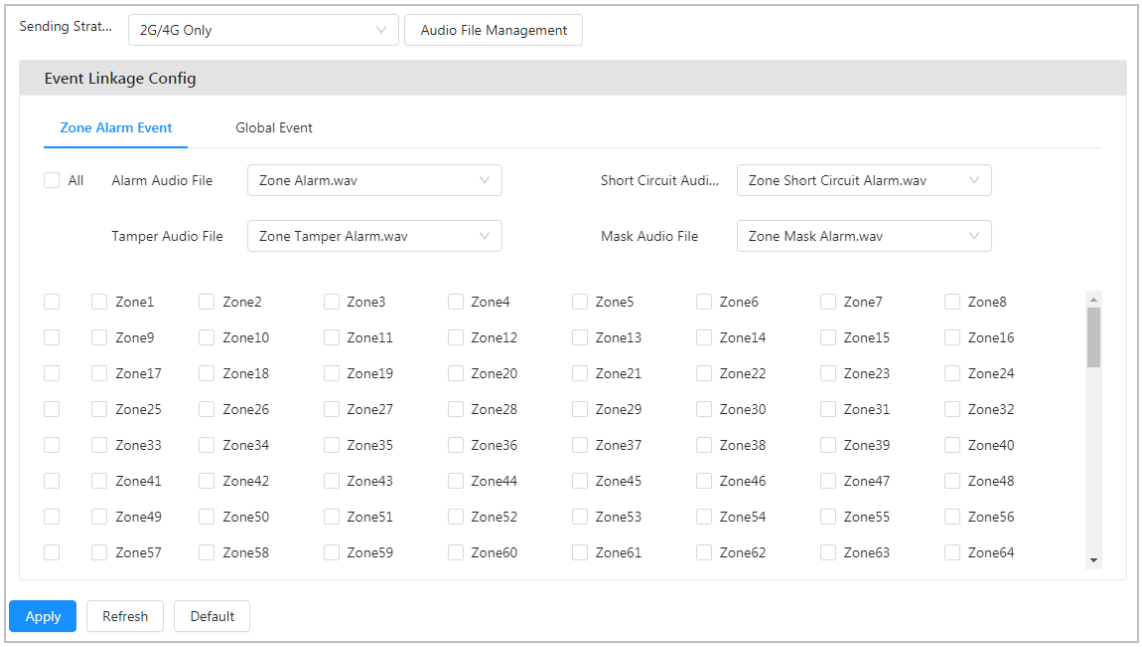
Puede cargar paquetes de audio de hasta 3 M de tamaño, en formato .wav. Un solo archivo de audio puede tener hasta 500 k.

2. Haga clic**DE ACUERDO**.

Etapa 4 Seleccione archivos de audio del**Archivo de audio**lista.

Paso 5 Seleccione un evento para vincularlo al audio.

Figura 5-18 Configuración de audio



Paso 6 Hacer clic**Aplicar**.

5.2.8 Manejo de fallas

Configure el evento de detección para el panel de control. Cuando ocurre el evento definido, se activa una alarma y luego el teclado vinculado responde encendiendo el indicador o emitiendo un mensaje de audio.

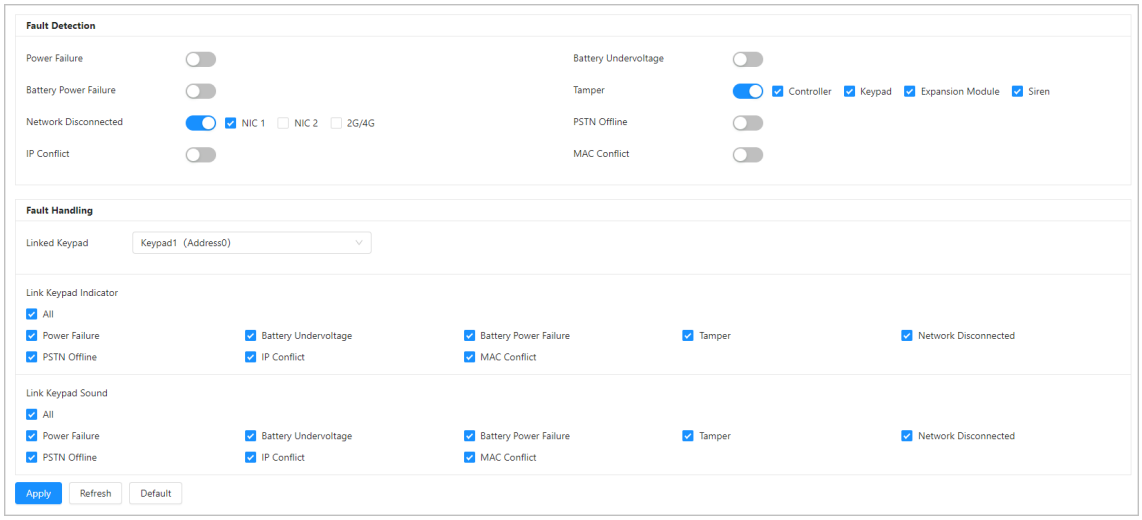
Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Configuración de alarma**>**Manejo de fallas**.

Paso 2 Habilitar la detección de eventos.

Lo siguiente está habilitado de forma predeterminada: eventos de alarma de manipulación desde el panel de control y el teclado, y eventos de desconexión de red desde la NIC 1.

Figura 5-19 Configuraciones para el manejo de fallas



Paso 3 Seleccione el teclado para vincularlo.

- Configure el evento que activa el indicador del teclado cuando se detecta.
- Configure el evento que activa el mensaje de audio del teclado cuando se detecta.

Etapa 4 Hacer clic**Aplicar**.

5.2.9 Vinculación de SMS

El panel de control admite SMS. Puede vincular un número de teléfono para recibir mensajes cuando ocurre una excepción en la batería de almacenamiento, la fuente de alimentación o la red, o si se activa una alarma, el panel de control le enviará un SMS.

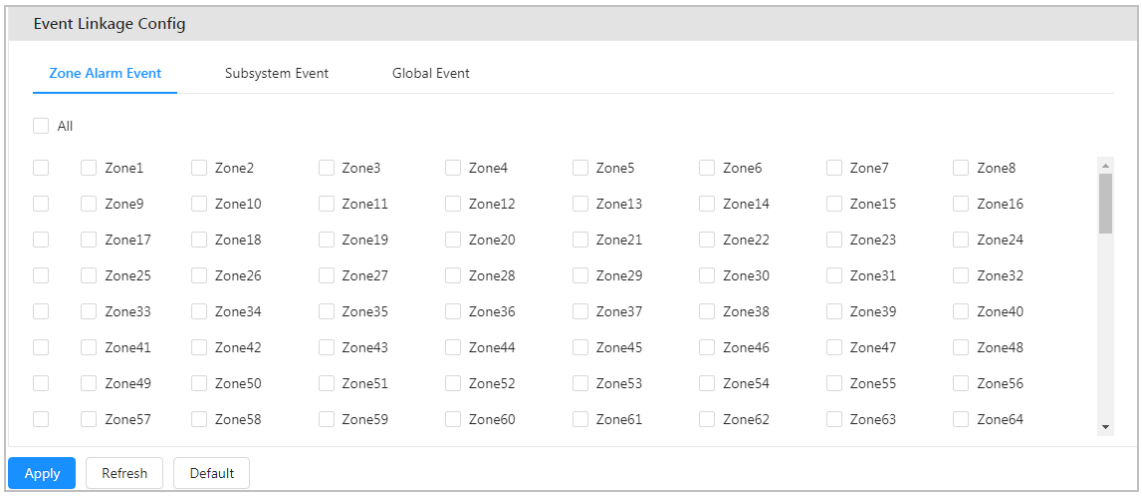
Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Configuración de alarma**>**Enlace SMS**.

Paso 2 Seleccione la zona y el evento a vincular.

Los parámetros del enlace SMS son los mismos que los de la sirena. Para obtener detalles sobre los parámetros, consulte la Tabla 5-4.

Figura 5-20 Configuración de vinculación de SMS



Paso 3 Hacer clic**Aplicar**.

5.2.10 Vinculación CID

Configure el evento para vincularlo con el centro receptor de alarmas. Cuando ocurre el evento definido, el centro vinculado recibe el mensaje de alarma.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Configuración de alarma**>**Vinculación CID.**

Paso 2 Seleccione y habilite la central receptora de alarmas para cada evento según sea necesario.

Paso 3 Permitir**Informar evento restaurado**.

Figura 5-21 Configuración de vinculación de CID

No.	Event Name	Event Code	Alarm Receiving Center1	Alarm Receiving Center2	Report Restored Event
1	General Zone Alarm	140			
2	Zone Tamper Alarm	383			
3	Zone Fault Alarm	380			
4	Bypassed Zone	570			
5	Fast Arming	408			
6	Key Zone Arming/Disarming	409			
7	Remote Arming/Disarming	400			
8	Scheduled Arming/Disarming	403			
9	Keyfob Arming/Disarming	407			
10	User Arming/Disarming	401			
11	Partial Arming/Disarming	401			
12	Controller Tamper	137			
13	Power Failure	301			
14	Battery Undervoltage	302			
15	Battery Power Failure	309			
16	Phone Offline	351			

5.2.11 Centro Receptor de Alarmas

Configure el método de transmisión del centro receptor de alarmas, el período de informe para los informes de prueba y el enlace para llamar al centro receptor de alarmas.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Configuración de alarma**>**Centro Receptor de Alarmas**. Después

Paso 2 de configurar**Estrategia de envío**,hacer clic**Informe de prueba**.

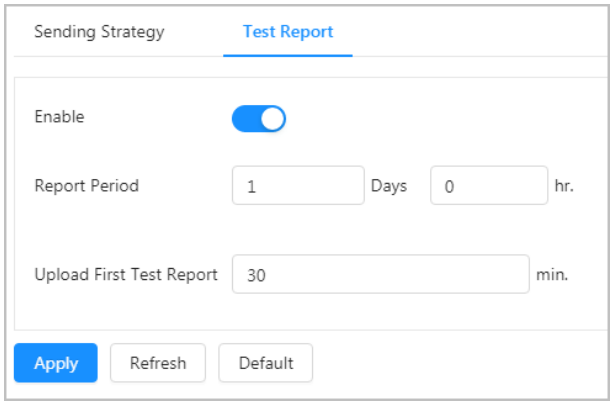
Configure y haga una copia de seguridad del método de transmisión de la central receptora de alarmas. Para obtener más información, consulte "5.1.3.3 Configuración del centro receptor de alarmas".

Paso 3 Hacer clic**Permitir**.

Etapa 4 Configure los parámetros.

- **Período del informe**:Establezca el intervalo de tiempo para cargar los informes de prueba.
- **Cargar el primer informe de prueba**:Establezca el tiempo necesario para cargar el primer informe de prueba después de habilitarlo.

Figura 5-22 Informe de prueba



5.3 Gestión de alarmas

5.3.1 Subsistema

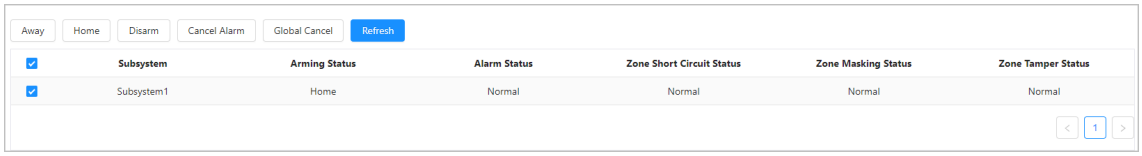
Arma y desarma subsistemas y puedes cancelar alarmas que ocurrieron en los subsistemas.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Gestión de alarmas**>**Subsistema.**

Paso 2 Seleccione un subsistema.

Figura 5-23 Configuración del subsistema



Paso 3 Hacer clic**Lejos**,**Hogar**,**Desarmar**o**Cancelar alarma**.

El estado de armado del subsistema cambia después de las operaciones de armado/desarmado.

Cancelación globalno requiere seleccionar datos del subsistema. Haga clic en él para cancelar todas las alarmas vinculadas de los subsistemas.

5.3.2 Zona

Puede armar, desarmar y anular la zona.

Procedimiento

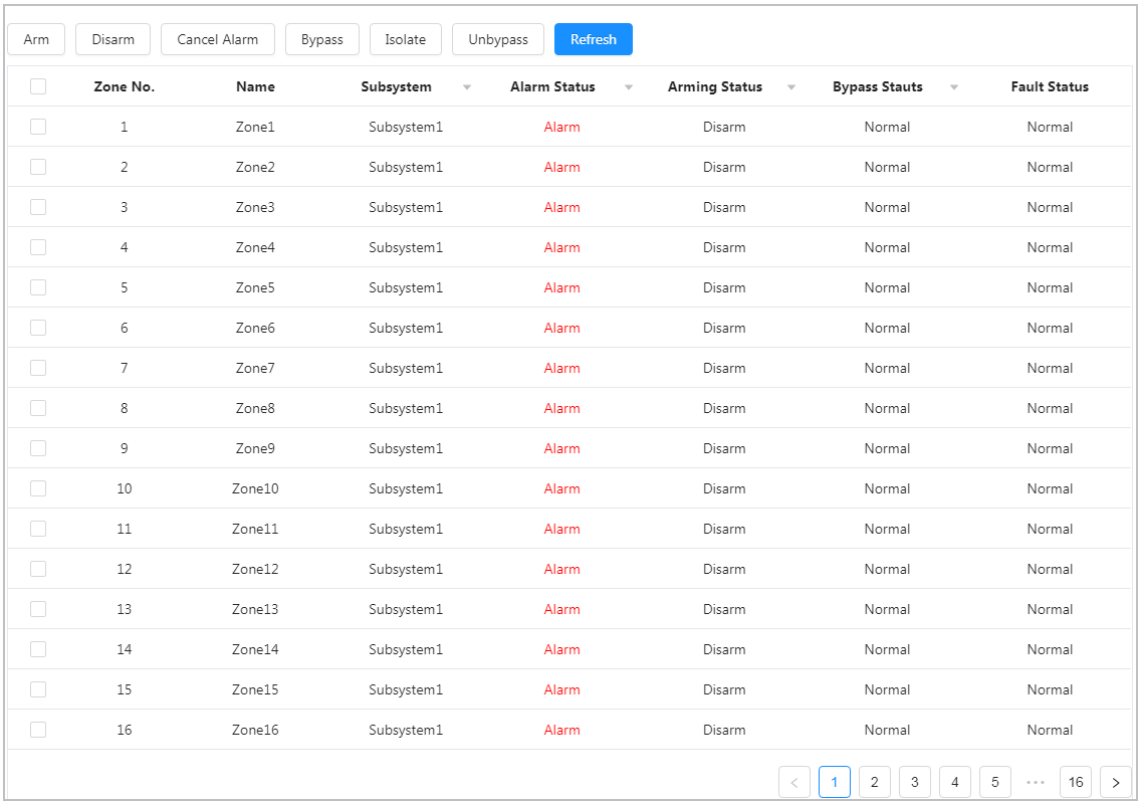
Paso 1 Inicie sesión en la web y luego seleccione**Gestión de alarmas**>**Zona**. Seleccione

Paso 2 una zona.

Paso 3 Hacer clic**Brazo**,**Desarmar**,**Cancelar alarma**,**Derivación**,**Aislar**o**desviar**.

El estado de armado y anulación de la zona cambia después de las operaciones de armado y desarmado y de anulación.

Figura 5-24 Configuración de zona



Zone No.	Name	Subsystem	Alarm Status	Arming Status	Bypass Stauts	Fault Status
1	Zone1	Subsystem1	Alarm	Disarm	Normal	Normal
2	Zone2	Subsystem1	Alarm	Disarm	Normal	Normal
3	Zone3	Subsystem1	Alarm	Disarm	Normal	Normal
4	Zone4	Subsystem1	Alarm	Disarm	Normal	Normal
5	Zone5	Subsystem1	Alarm	Disarm	Normal	Normal
6	Zone6	Subsystem1	Alarm	Disarm	Normal	Normal
7	Zone7	Subsystem1	Alarm	Disarm	Normal	Normal
8	Zone8	Subsystem1	Alarm	Disarm	Normal	Normal
9	Zone9	Subsystem1	Alarm	Disarm	Normal	Normal
10	Zone10	Subsystem1	Alarm	Disarm	Normal	Normal
11	Zone11	Subsystem1	Alarm	Disarm	Normal	Normal
12	Zone12	Subsystem1	Alarm	Disarm	Normal	Normal
13	Zone13	Subsystem1	Alarm	Disarm	Normal	Normal
14	Zone14	Subsystem1	Alarm	Disarm	Normal	Normal
15	Zone15	Subsystem1	Alarm	Disarm	Normal	Normal
16	Zone16	Subsystem1	Alarm	Disarm	Normal	Normal

5.3.3 Salida de relé

Activar o desactivar relés.

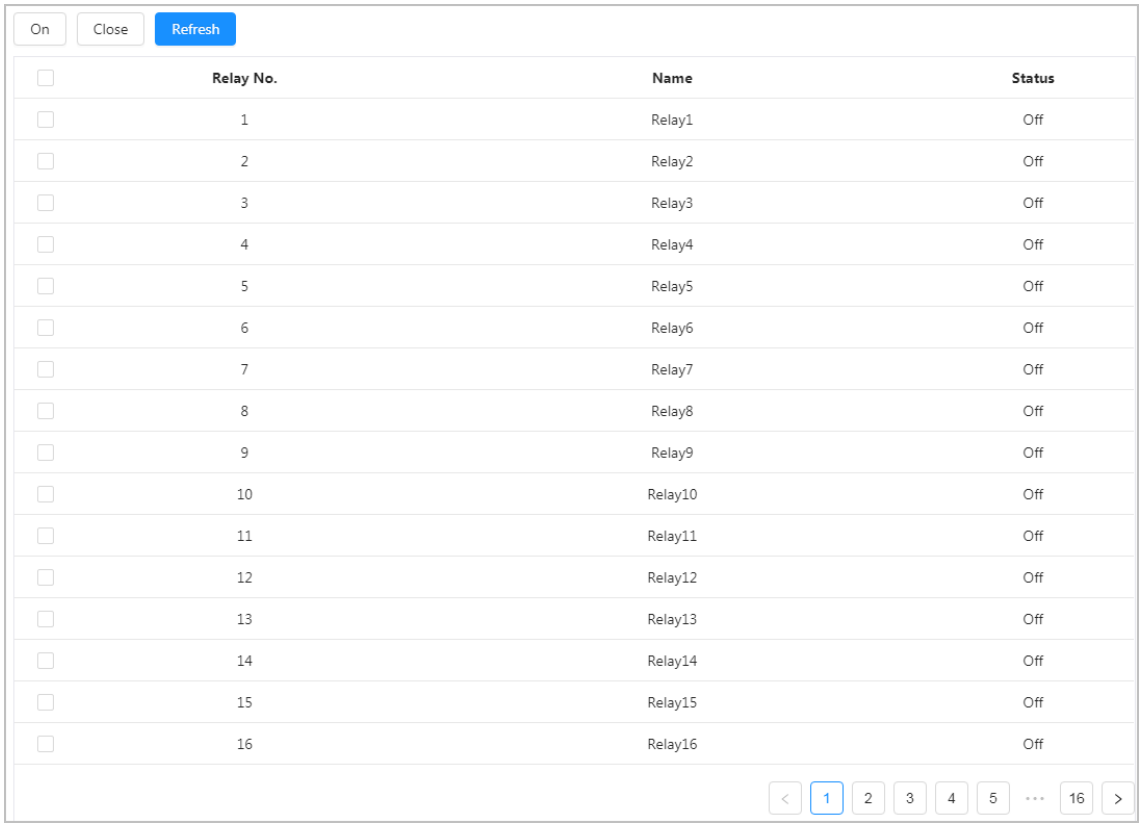
Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Gestión de alarmas**>**Relé**.

Paso 2 Seleccione un relé.

Paso 3 Hacer clic**En**o**Cerca**para encender o apagar el relé.

Figura 5-25 Configuración del relé



5.3.4 Sirena

Enciende o apaga una sirena.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Gestión de alarmas**>**Sirena**.

Paso 2 Seleccione una sirena.

Paso 3 Hacer clic**En**o**Cerca**para encender o apagar la sirena.

Figura 5-26 Sirena

5.4 Gestión de red

5.4.1 TCP/IP

Puede configurar la dirección IP, el servidor DNS (Sistema de nombres de dominio) y más según el plan de red.

Requisitos previos

El panel de control está conectado a la red.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Red**>**TCP/IP**.

Paso 2 Configure los parámetros TCP/IP.

Figura 5-27 TCP/IP

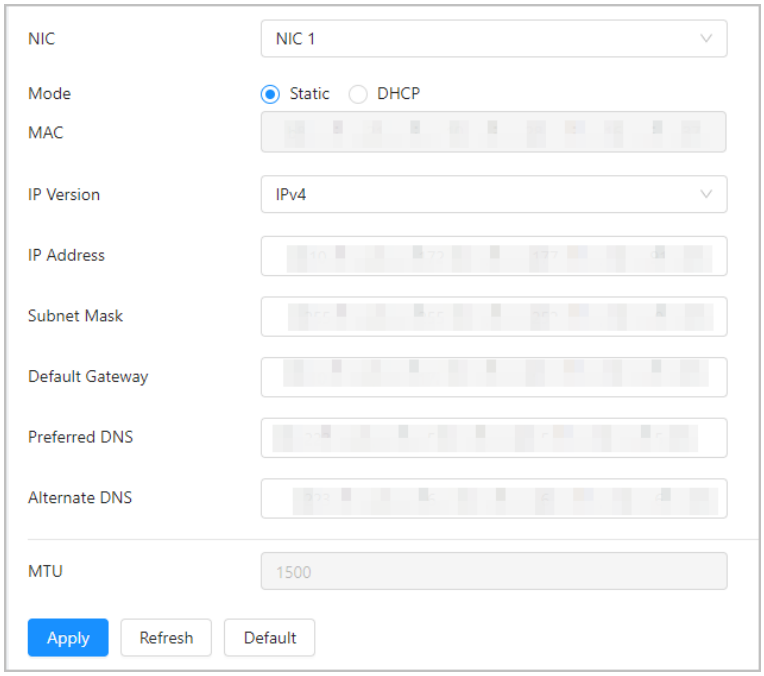


Tabla 5-7 Descripción de los parámetros TCP/IP

Parámetro	Descripción
tarjeta de red	Seleccionar**NIC1**o**NIC2**para dispositivos con dos tarjetas de red. La dirección IP predeterminada de LAN1 es 192.168.1.108 y LAN2 es 192.168.2.108.
Modo	● **Estático**:Configurar**Dirección IP**,**Máscara de subred**, y**Puerta de enlace predeterminada** manualmente y luego haga clic en**Ahorrar**, se muestra la página de inicio de sesión con la dirección IP configurada. ● **DHCP (Protocolo de configuración dinámica de host)** Si hay un servidor DHCP en la red, seleccione**DHCP**, y el panel de control adquiere la información de la red, como la dirección IP, automáticamente.
Dirección MAC	Muestra la dirección MAC (Control de acceso a medios) del panel de control.

Parámetro	Descripción
Versión IP	Seleccionar**IPv4**o**IPv6**.
Dirección IP	Seleccionar**Estático**en**Modo**e ingrese la dirección IP y la máscara de subred que necesita. ● IPv6 no tiene máscara de subred. ● La puerta de enlace predeterminada debe estar en el mismo segmento de red que la IP DIRECCIÓN.
Máscara de subred	
Puerta de enlace predeterminada	
DNS preferido	Dirección IP del DNS preferido.
DNS alternativo	Dirección IP del DNS alternativo.
MTU	Ajuste el valor de MTU según el entorno de la red y las condiciones de comunicación para obtener una buena velocidad de transmisión. El valor de MTU predeterminado es 1500 bytes. Los valores de MTU recomendados para diferentes situaciones son los siguientes. ● 1500: Por defecto. Es la configuración típica para conexiones de red que no tienen PPPOE ni VPN. También es la configuración predeterminada de algunos enrutadores, adaptadores de red y conmutadores. ● 1492: El valor óptimo para PPPOE. ● 1468: El valor óptimo para DHCP. ● 1450: el valor óptimo para VPN.

Paso 3 Hacer clic**Aplicar**.

5.4.2 Puerto

Configure los números y valores máximos de puerto.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Red**>**Puerto**.

Paso 2 Configure cada puerto del panel de control.

Excepto**Conexión máxima**, las modificaciones de otros parámetros entrarán en vigor después del reinicio.

Figura 5-28 Puerto

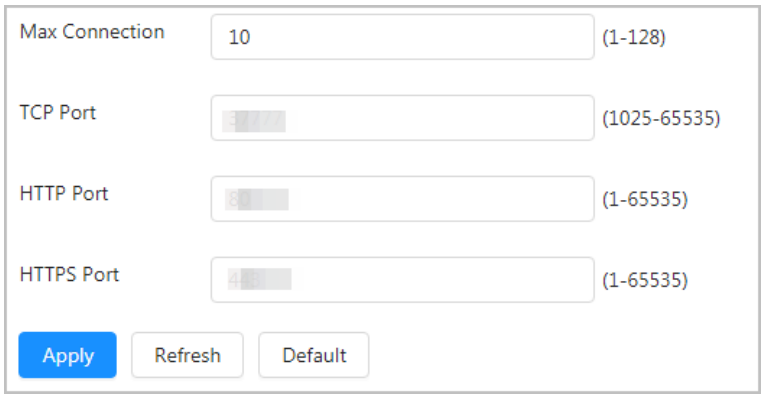


Tabla 5-8 Descripción de los parámetros del puerto

Parámetro	Descripción
Máx. Conexión	La cantidad máxima de clientes que acceden al Dispositivo al mismo tiempo, como clientes que acceden a través de la web, la plataforma y el teléfono móvil.
puerto tcp	Puerto de servicio TCP. Puede ingresar el valor según sea necesario. Es 37777 por defecto.
El puerto UDP	Puerto de protocolo de datagramas de usuario. Puede ingresar el valor según sea necesario. Es 37778 por defecto.
Puerto HTTP	Puerto de comunicación HTTP. Puede ingresar el valor según sea necesario. Es 80 por defecto. Si ingresa otros valores, ingrese el número de puerto modificado después de la dirección IP al iniciar sesión en el Dispositivo en el navegador.
Puerto HTTPS	Puerto de comunicación HTTPS. Puede ingresar el valor según sea necesario. Es 443 por defecto.

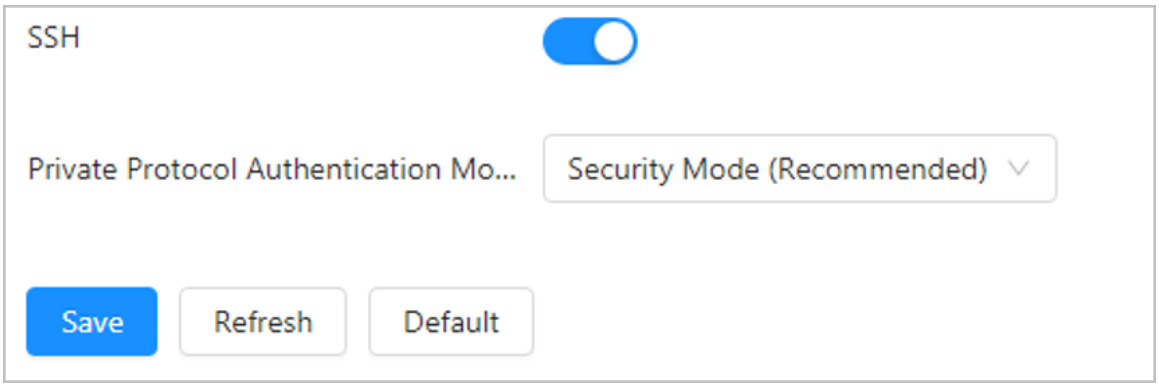
Paso 3 Hacer clic**Aplicar**.

5.4.3 Servicios Básicos

El protocolo SSH (Secure Shell) proporciona protección de seguridad para el inicio de sesión de diálogo remoto y los servicios de red. Mediante la configuración de los servicios del sistema, puede proteger el sistema. Está deshabilitado de forma predeterminada y necesita autenticación después de habilitarse para acceder a la administración de seguridad y cifrar datos durante la transmisión. **modo de seguridad**se recomienda para**Modo de autenticación de protocolo privado**.

Inicie sesión en la web y luego seleccione**Red**>**Servicios basicos**.

Figura 5-29 Servicios básicos



5.5 Información del dispositivo

Inicie sesión en la web, seleccione**Información del dispositivo**, y luego se mostrarán las características del panel de control, versión, estado del sistema, módulo e información legal.

- **Características**:Muestra el número de entradas de alarma, salidas de alarma y sirenas.
- **Versión**:Muestra el modelo del dispositivo, SN, versión del sistema y otra información.
- **Estado del sistema**:Muestra el estado de subtensión, el estado de la batería, la fuente de alimentación, la manipulación del panel de control, PSTN fuera de línea y otra información.
- **Módulo**:Muestra información en el teclado y módulo RS-485 de la central.
- **Información legal**:El acuerdo de software de código abierto del panel de control.

5.6 Gestión del sistema

5.6.1 Cuenta

5.6.1.1 Usuario web

Puede agregar, editar y eliminar cuentas de usuario que pueden iniciar sesión en la página web del panel de control.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Sistema**>**Cuenta**>**Usuario Web**. Hacer

Paso 2 clic**Agregar**.

Paso 3 Configure los parámetros.

- Nombre de usuario del instalador: Instalador; Contraseña predeterminada: Installer9090.
- Nombre de usuario del fabricante del equipo: Fabricante; Contraseña predeterminada: Fabricante2008.

Figura 5-30 Agregar usuario web

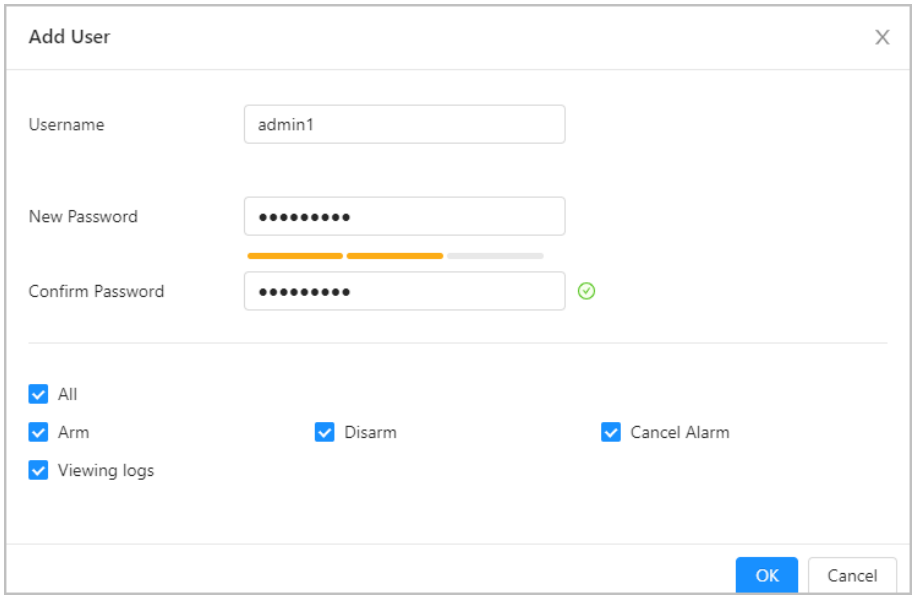


Tabla 5-9 Descripción de los parámetros del usuario web

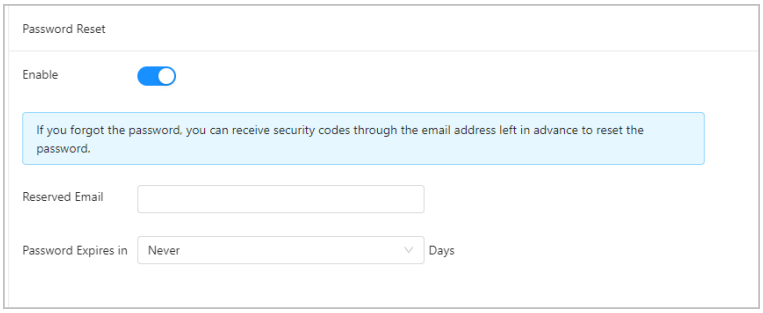
Parámetro	Descripción
Nombre de usuario, Nueva contraseña, Confirmar contraseña	Ingrese el nombre de usuario y la contraseña y confirme la contraseña.
Permisos de usuario	Otorgue permisos al usuario para armar, desarmar y cancelar alarmas y ver registros.

Etapa 4 Hacer clic**DE ACUERDO**.

Paso 5 (Opcional) Restablezca la contraseña después de agregar usuarios web.

1. Haga clic para habilitar la función.
2. Ingrese el correo electrónico reservado y seleccione el período de caducidad de la contraseña.

Figura 5-31 Restablecer contraseña



Paso 6 Hacer clic**Aplicar**para guardar la configuración.

5.6.1.2 Usuario del teclado

El usuario del teclado puede ejecutar operaciones como armar/desarmar, cancelar alarmas y ver registros a través del teclado.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Sistema**>**Cuenta**>**Usuario del teclado**. Hacer clic

Paso 2 **Agregar**.

Paso 3 Configure los parámetros.

Figura 5-32 Agregar usuario del teclado

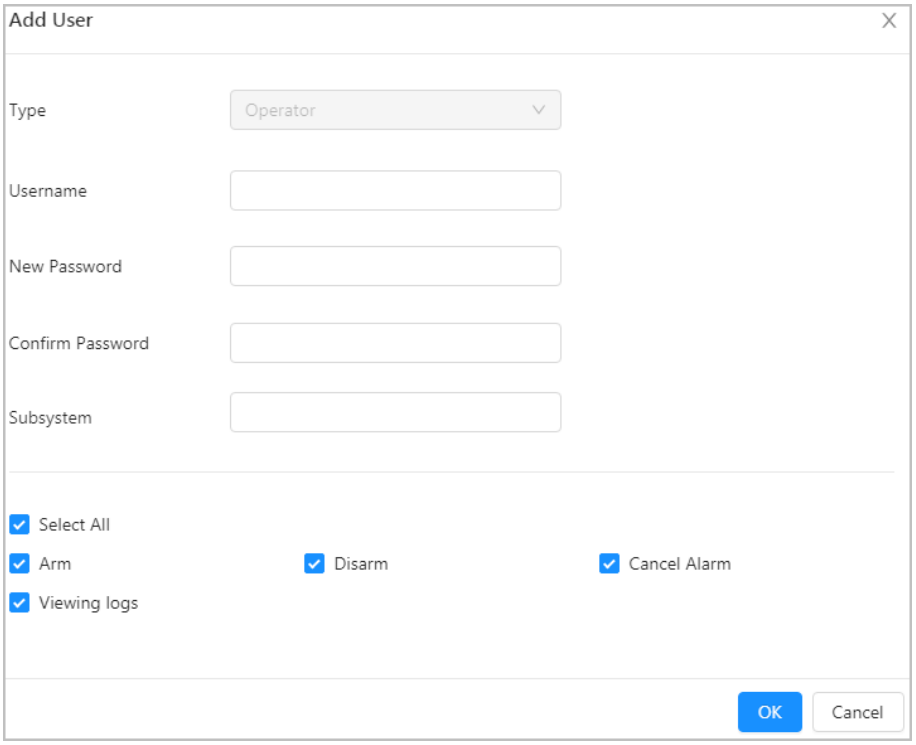


Tabla 5-10 Descripción de los parámetros de usuario del teclado

Parámetro	Descripción
Tipo	Es**Operador**por defecto.

Parámetro	Descripción
Nombre de usuario, Nueva contraseña, Confirmar contraseña	Ingrese el nombre de usuario, contraseña y confirme la contraseña.
Subsistema	Vincular subsistemas del usuario del teclado. Hay varias selecciones disponibles.
Permisos de usuario	Otorgue permisos al usuario para armar, desarmar y cancelar alarmas y ver registros.

Etapa 4 Hacer clic**DE ACUERDO**.

5.6.1.3 Usuario del mando

Puede armar y desarmar el panel de control y cargar la alarma de pánico a través del llavero.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Sistema**>**Cuenta**>**Usuario de llavero**.

Paso 2 Hacer clic**Agregar**y luego presione y mantenga presionado el control remoto hasta que se encienda el indicador. La central obtiene automáticamente el SN del mando.

Paso 3 Configure los parámetros.

Figura 5-33 Agregar usuario de llavero

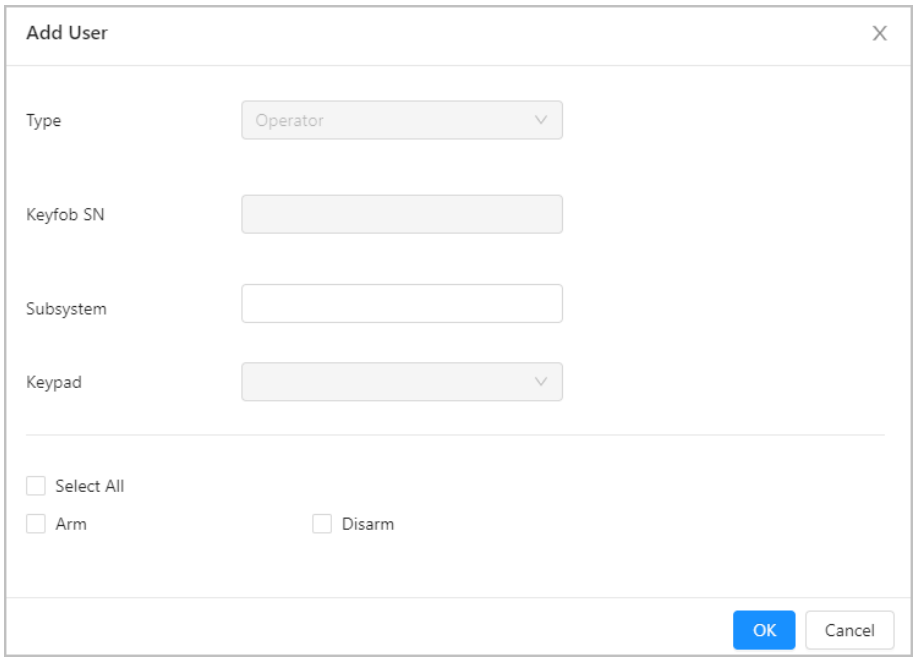


Tabla 5-11 Descripción de los parámetros de usuario del llavero

Parámetro	Descripción
Tipo	Es**Operador**por defecto.
Llavero SN	Se obtiene automáticamente del llavero después de encenderlo.
Subsistema	Vincular subsistemas del usuario del llavero. Hay varias selecciones disponibles.
Teclado	El panel de control se puede emparejar con hasta 32 teclados diferentes, pero cada mando solo se puede vincular a un teclado. No puede cambiar el teclado que está vinculado al llavero.

Parámetro	Descripción
Permisos de usuario	Otorgue permisos al usuario del mando para armar (como armado local y armado ausente) y desarmar.

Etapa 4 Hacer clic**DE ACUERDO**.

Paso 5 Prensa**Hogar**,**Lejos**,**Desarmar**o**LLAMADA DE SOCORRO**en el llavero.

5.6.1.4 Propietario de la tarjeta

El propietario de la tarjeta IC puede armar y desarmar el panel de control después de agregarla al sistema.

Información de contexto

Conecte un teclado al panel de control de alarma.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Sistema**>**Cuenta**>**Titular**.

Paso 2 Hacer clic**Agregar**y luego pase la tarjeta por el teclado para leer su número de tarjeta.

Paso 3 Configure los parámetros.

Figura 5-34 Agregar propietario de la tarjeta

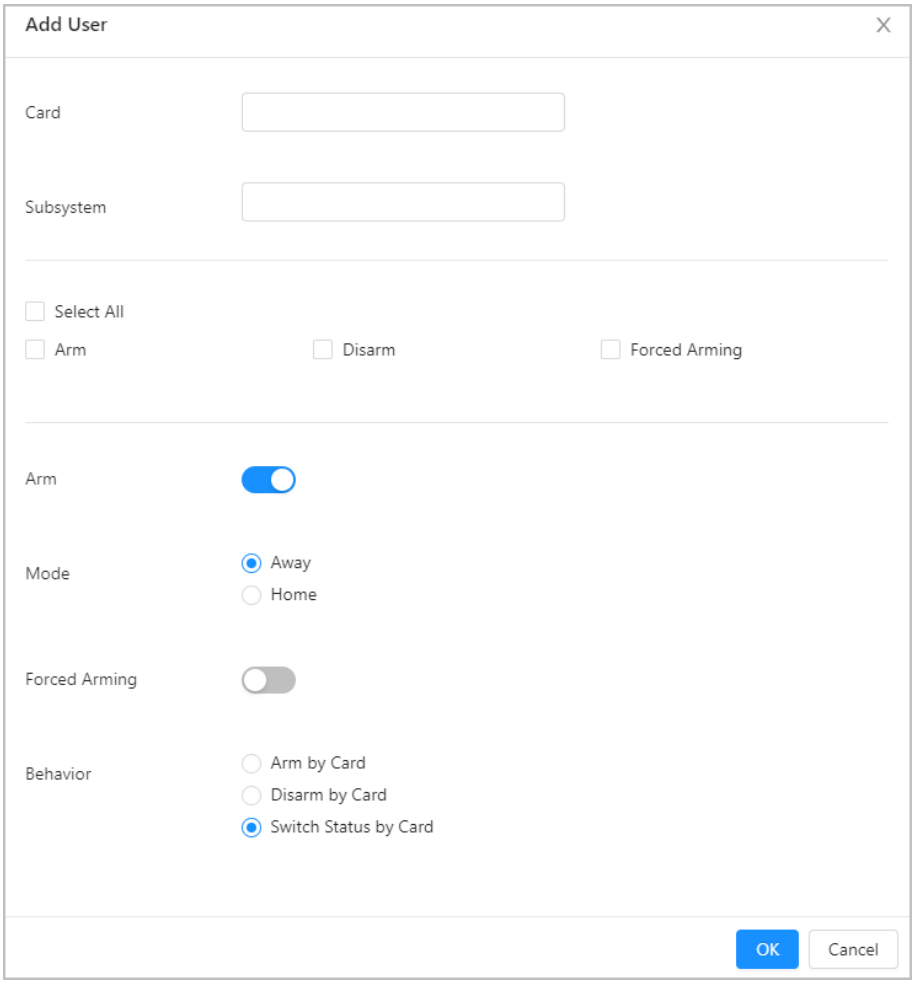


Tabla 5-12 Descripción de los parámetros Agregar propietario de tarjeta

Parámetro	Descripción
Tarjeta	Obtenido automáticamente por el panel de control al deslizarlo en el teclado.
Subsistema	Subsistemas de enlace del titular de la tarjeta. Hay varias selecciones disponibles.
Permisos de usuario	Otorgue permisos al propietario de la tarjeta para armar y desarmar.
Brazo	Habilitar brazo. ● **Modo**:Seleccione entre**Hogar**y**Lejos**. ● **Armado forzado**:Puede armar el subsistema cuando se activa una alarma. ● Comportamiento ◇ **Armar por Tarjeta**:Brazo. ◇ **Desarmar por Tarjeta**:Desarmar. ◇ **Cambiar estado por tarjeta**:Cambie el estado de armado actual del panel de control deslizando la tarjeta.

Etapa 4 Hacer clic**DE ACUERDO**.

5.6.1.5 Usuario móvil

Puede armar y desarmar el panel de control y reportar una alarma a través de su teléfono móvil después de agregarlo al sistema.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Sistema**>**Cuenta**>**Usuario móvil.** Hacer clic

Paso 2 **Agregar**.

Paso 3 Configure los parámetros.

Figura 5-35 Agregar usuario móvil

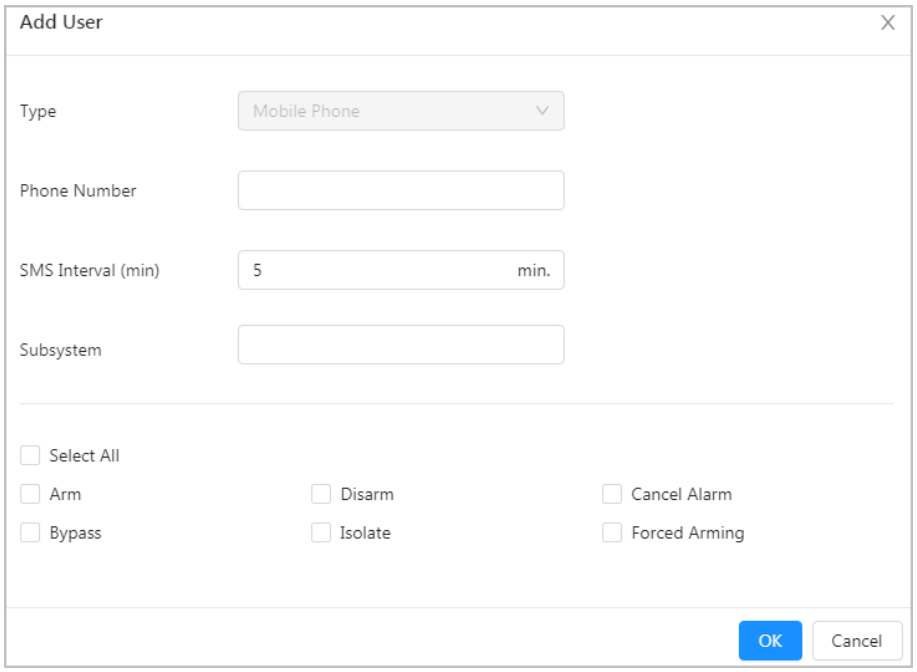


Tabla 5-13 Descripción de los parámetros del usuario móvil

Parámetro	Descripción
Tipo	Es**Teléfono móvil**por defecto.
Número de teléfono	Introduzca el número de teléfono móvil.
Intervalo de SMS (min)	El intervalo de tiempo durante el cual se envía el mismo SMS de alarma a su teléfono móvil. Debe ser un número entero entre 0 y 5.
Subsistema	Seleccione el subsistema al que pertenece el usuario móvil. Hay varias selecciones disponibles.
Permiso de usuario	Otorgue permiso al usuario para armar, desarmar y cancelar alarmas, anularlas y más.

Etapa 4 Hacer clic**DE ACUERDO**.

5.6.1.6 Usuario clave

Agregue usuarios clave y vincúlelos a zonas clave, y luego estos usuarios clave podrán armar y desarmar los subsistemas de la zona.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Sistema**>**Cuenta**>**Usuario clave.** Hacer clic

Paso 2 **Agregar**.

Paso 3 Configure los parámetros.

Figura 5-36 Agregar usuario clave

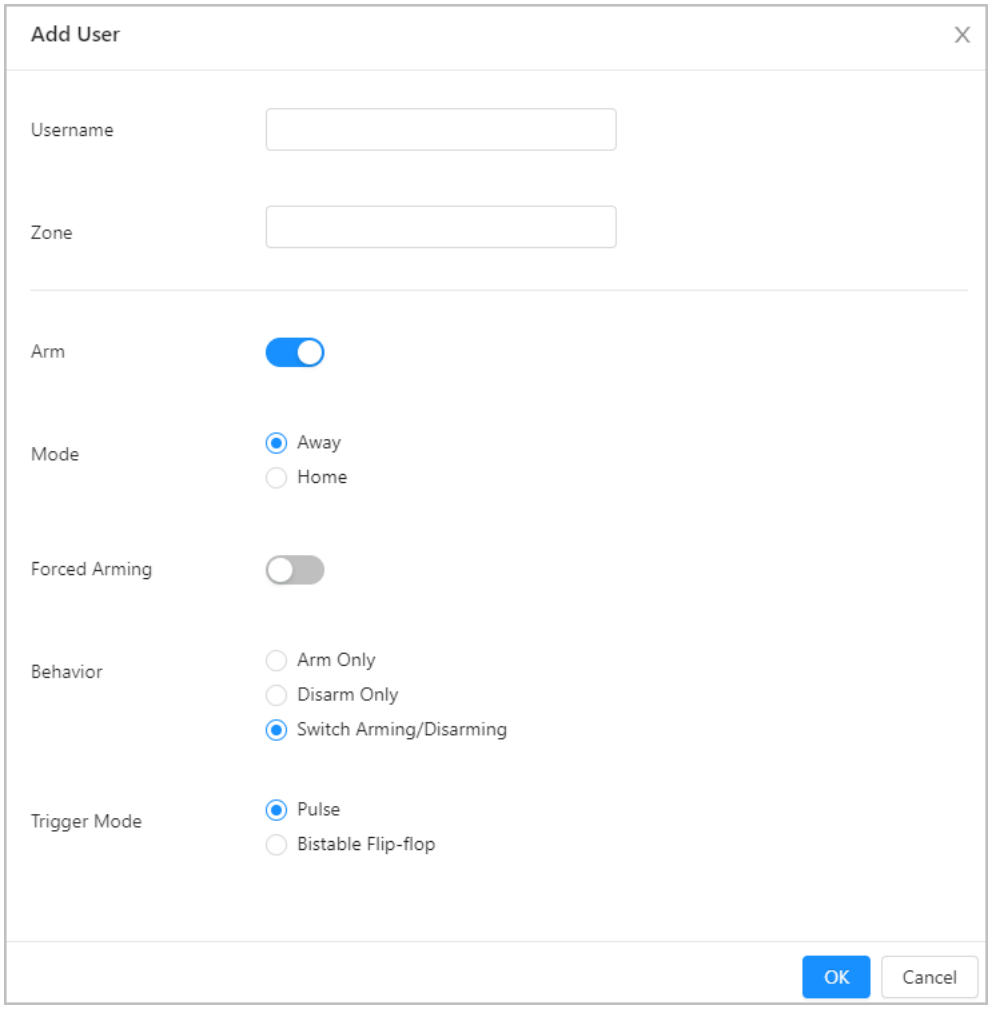


Tabla 5-14 Descripción de Agregar parámetros clave de usuario

Parámetro	Descripción
Nombre de usuario	Ingrese el nombre de usuario.
Zona	Vincula la zona al usuario clave. Hay varias selecciones disponibles.

Parámetro	Descripción
Brazo	Habilitar brazo. ● **Modo**:Seleccione entre**Hogar**y**Lejos**. ● **Armado forzado**:Puede armar el subsistema cuando ocurren errores en zonas bajo el subsistema. ● Comportamiento ◇ **Sólo Armar**:Brazo. ◇ **Sólo desarmar**:Desarmar. ◇ **Interruptor de armado/desarmado**:Cambia el estado de armado del subsistema correspondiente a la zona clave. ● Modo de disparo ◇ **Legumbres**:Tipo variable. El estado de la zona clave desde antes del disparo hasta activado. ◇ **Flip-flop biestable**:Tipo fijo. Desarmar cuando la zona clave cambia de activado a antes de activar, y armar cuando cambia de antes de activar a activado.

Etapa 4 Hacer clic**DE ACUERDO**.

5.6.2 Configuración de hora

Configure la fecha y zona horaria, DST y otros parámetros del Dispositivo.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Sistema**>**Tiempo**.

Paso 2 Configure los parámetros.

Figura 5-37 Configuración de hora

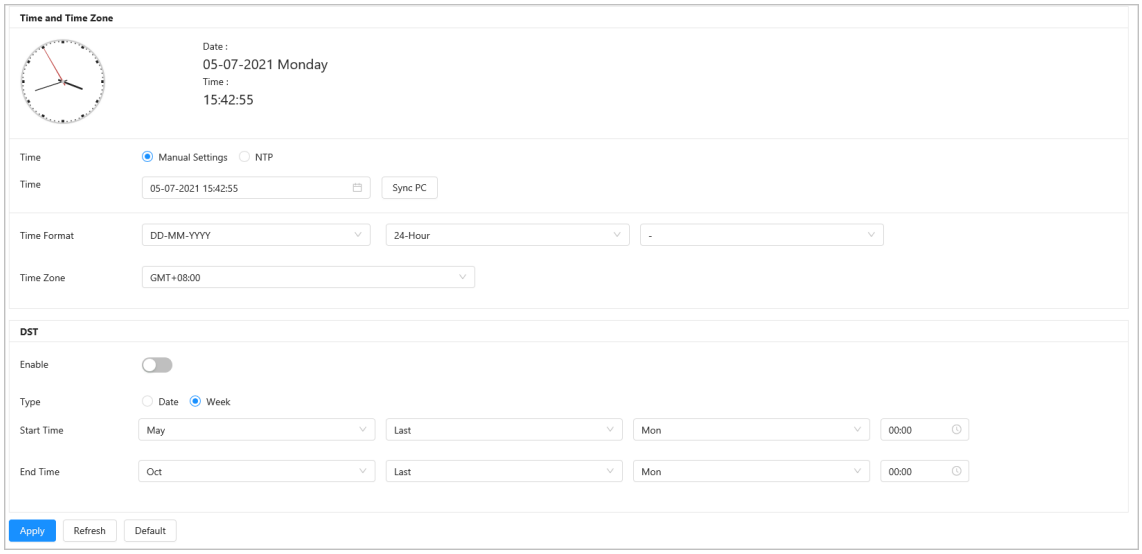


Tabla 5-15 Descripción del parámetro de configuración de tiempo

Parámetro	Descripción
Tiempo	Seleccionar**Ajustes manuales**o**NTP**.

Parámetro	Descripción
Ajustes manuales	Configure la hora manualmente. Establezca la fecha y hora del sistema actual para el Dispositivo. Hacer clic**Sincronizar computadora local**para sincronizar con la hora de la computadora local.
NTP	Habilite la función NTP para sincronizar la hora del panel de control con el servidor NTP. ● **Servidor**:Ingrese la dirección IP del servidor que tiene instalados los servicios NTP o haga clic en**Actualización manual**para sincronizar la hora del dispositivo con el servidor NTP. ● **Puerto**:El sistema solo admite el protocolo TCP y la configuración predeterminada es 123 (1–65535). ● **Intervalo**:Ingrese el intervalo de tiempo en el que desea que el panel de control sincronice su hora con el servidor NTP. El valor máximo es 65535 minutos.
Formato de tiempo	● Seleccione un formato de fecha, incluido**AAAA-MM-DD**,**MM-DD-AAAA**, y **DD-MM-AAAA**. ● Seleccionar**24 horas**o**12 horas**. ● Establezca un separador para el formato de hora.
Zona horaria	Seleccione una zona horaria según la ubicación del panel de control.
horario de verano	Algunos países o regiones adoptan el sistema DST. Puede habilitar esta función según sea necesario. 1. Habilitar**horario de verano**. 2. Seleccione el tipo de**Fecha**o**Semana**. 3. Establezca la hora de inicio y la hora de finalización.

Paso 3 Hacer clic**Aplicar**.

5.6.3 Mantenimiento del dispositivo

5.6.3.1 Mantenimiento del dispositivo

Reinicio automático

Seleccionar**Sistema**>**Mantenimiento**>**Mantenimiento**para configurar la semana y la hora del reinicio automático. Hacer clic **Aplicar**para guardar las configuraciones. El sistema se reinicia automáticamente a la hora establecida.

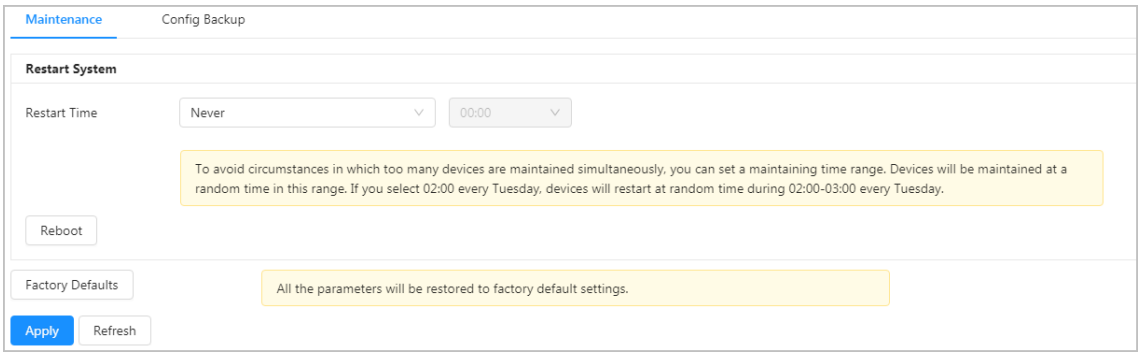
Reinicio manual

Seleccionar**Sistema**>**Mantenimiento**>**Mantenimiento**y luego haga clic en**Reiniciar**. El sistema se reinicia inmediatamente cuando usted confirma que desea reiniciar según se le solicite.

Restaurar valor predeterminado

Seleccionar**Sistema**>**Mantenimiento**>**Mantenimiento**y luego haga clic en**Fallas de fábrica**,ingrese la contraseña de la cuenta de administrador y luego haga clic**DE ACUERDO**. El sistema se reinicia y restaura todos los parámetros (excepto IP) a los valores predeterminados de fábrica después de que usted confirme hacerlo cuando se le solicite.

Figura 5-38 Mantenimiento



5.6.3.2 Configurar la copia de seguridad

Importe o exporte un perfil del sistema. Puede aplicar los mismos parámetros a varios dispositivos utilizando un archivo de copia de seguridad de configuración.

Procedimiento

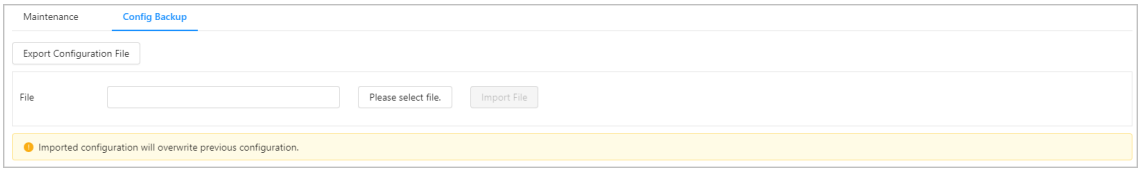
Paso 1 Inicie sesión en la web y luego seleccione**Sistema**>**Mantenimiento**>**Mantenimiento**>**Copia de seguridad de configuración**.

Paso 2 Hacer clic**Por favor seleccione archivo**para seleccionar un perfil para importar. Hacer clic

Paso 3 **Importar archivo**para completar la importación de los datos de la copia de seguridad.

Etapa 4 Hacer clic**Exportar archivo de configuración**para guardar todos los perfiles en la web localmente cuando se le solicite.

Figura 5-39 Configurar copia de seguridad



5.6.3.3 Prueba de caminata (instalador)

Pruebe el estado de funcionamiento de los detectores instalados y la reacción del panel de control al activar o apagar el detector. El modo de prueba de caminata puede probar la validez de uno o más detectores.

La función de prueba de caminata solo está disponible para el instalador.

Procedimiento

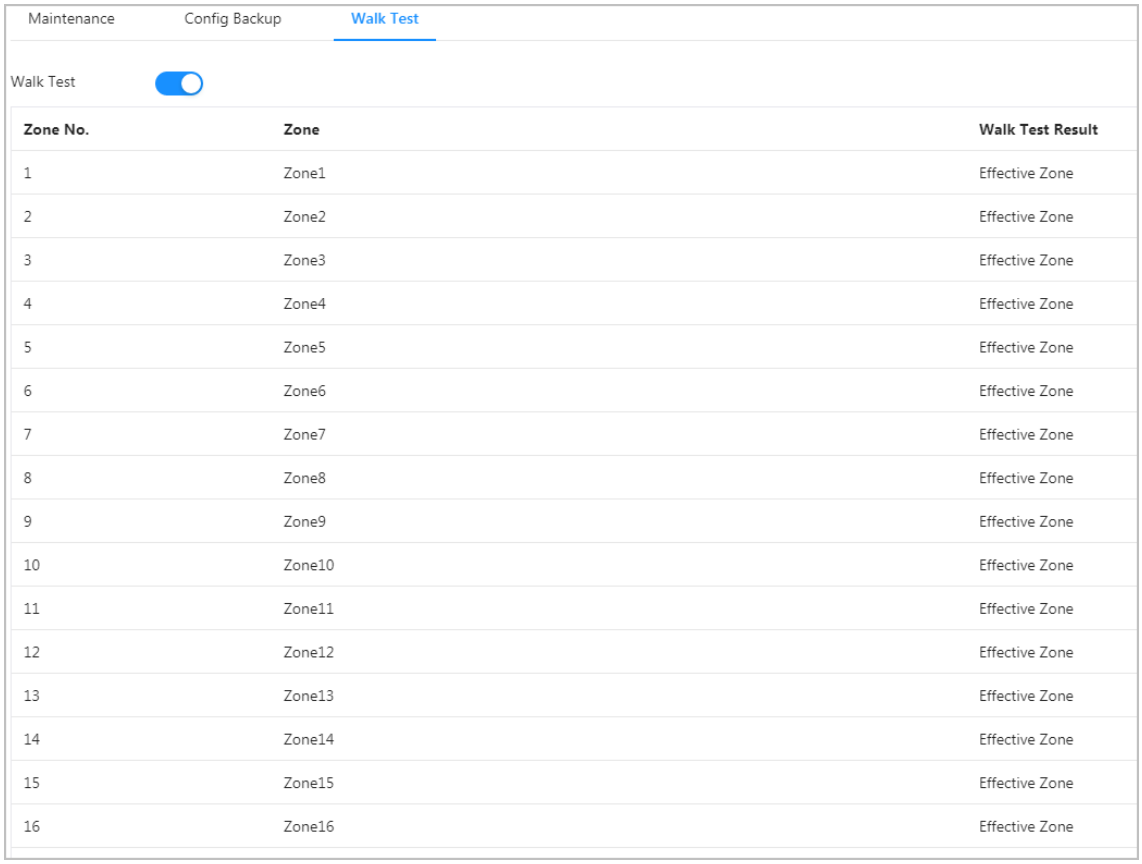
Paso 1 Inicie sesión en la web y luego seleccione**Sistema**>**Mantenimiento**>**Prueba de caminata**.

Inicie sesión en la página web a través de la cuenta y contraseña del instalador.

Paso 2 Permitir**Prueba de caminata**y luego verifique los resultados de la prueba.

- **Zona efectiva**:Se activaron los detectores.
- **Zona ineficaz**:Los detectores no se activaron.

Figura 5-40 Prueba de caminata



5.6.4 Actualización del sistema

Información de contexto

- Sólo el administrador y el fabricante pueden realizar actualizaciones del sistema. La zona debe estar desarmada cuando se actualiza el sistema.
- Durante una actualización, no apague, reinicie ni apague el panel de control, ni desconecte el sistema de la red.
- Seleccione los archivos de actualización correctos. Actualizar el programa incorrecto hará que el panel de control se comporte de manera anormal.

Procedimiento

Paso 1 Inicie sesión en la web con la cuenta del fabricante y luego seleccione**Sistema**>**Actualizar**.

Paso 2 Configure los parámetros.

Figura 5-41 Actualización del sistema

Tabla 5-16 Descripción del parámetro de actualización de archivos

Parámetro	Descripción
Por favor seleccione el tipo	Seleccione el método de actualización según sea necesario.
DIRECCIÓN	Solo los siguientes tres tipos de actualización requieren dirección. ● **Teclado de alarma**:Dirección del teclado. ● **Módulo ARM808-RS**:Dirección DIP. ● **Módulo ARM708-RS**:Dirección DIP. ● **Módulo de red**:ID del dispositivo. ● **Dispositivo inalámbrico**:ID del dispositivo.

Paso 3 Hacer clic**Navegar**y luego seleccione el archivo de actualización (archivo .bin) que desea importar.

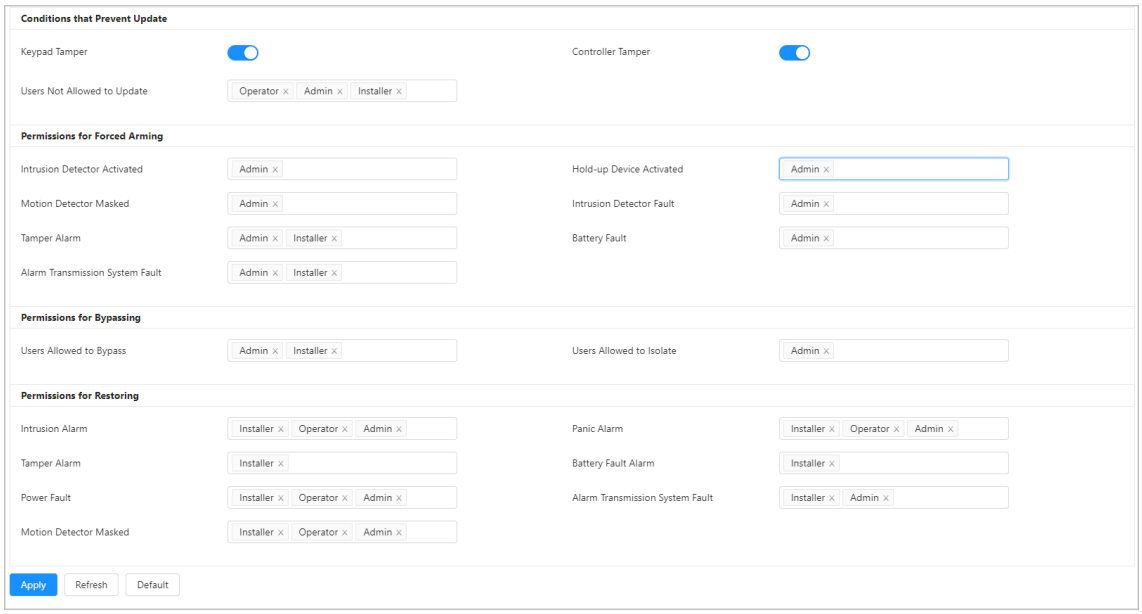
Etapa 4 Hacer clic**Actualizar**para actualizar el sistema.

Una vez completada la actualización, el panel de control y el administrador web se reiniciarán.

5.6.5 Detección del sistema

Después de habilitar la función de detección del sistema, toda la lógica empresarial del panel de control cumple con los estándares. Se recomiendan los valores predeterminados.

Figura 5-42 Detección del sistema



5.6.6 Gestión de periféricos

5.6.6.1 Inicialización del módulo de red

Información de contexto

La inicialización solo se admite cuando el panel de control de alarma y el dispositivo están conectados al mismo enrutador.

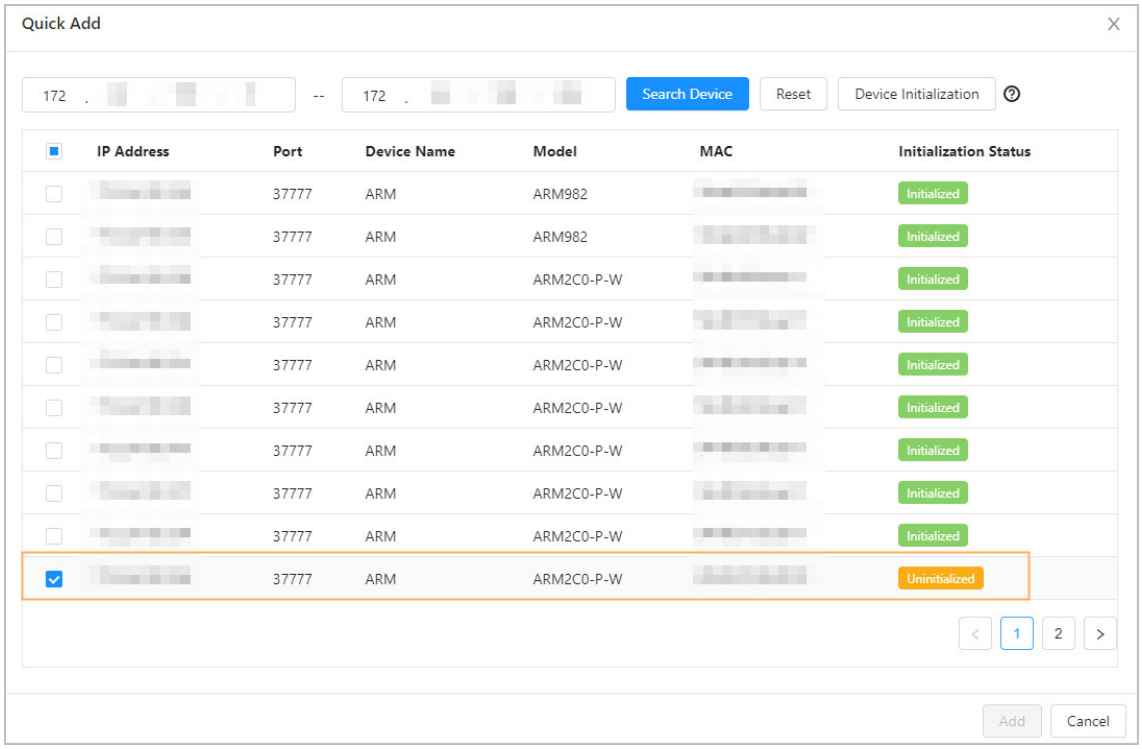
Procedimiento

Paso 1 Inicie sesión en la página web y seleccione**Sistema**>**Periférico**>**Módulo de red**>**Agregar rápido**.

Paso 2 Hacer clic**Agregar rápido**,e ingrese el segmento IP, y luego haga clic en**Dispositivo de búsqueda**. Seleccione

Paso 3 los dispositivos que no están inicializados y luego haga clic en**Inicialización del dispositivo**.

Figura 5-43 Inicialización



Etapa 4 Siga las instrucciones en pantalla para cambiar la contraseña y la dirección IP del dispositivo.

5.6.6.2 Agregar módulos de red

Los módulos de red se pueden agregar mediante adición rápida o adición manual.

5.6.6.2.1 Agregar rápido

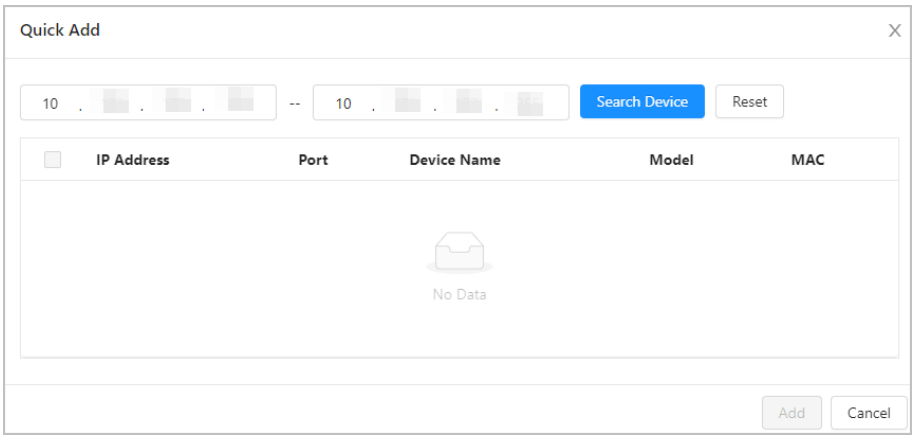
Procedimiento

Paso 1 Inicie sesión en la página web del panel de control de alarma y seleccione**Sistema**>**Periférico**>**Módulo de red**.

Paso 2 Hacer clic**Agregar rápido**,e ingrese la IP inicial y la IP final, y luego haga clic en**Dispositivo de búsqueda**.

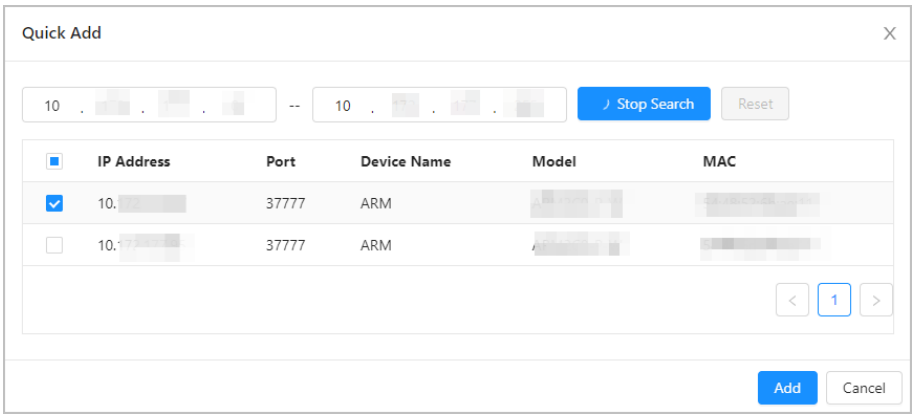
Los dispositivos cuya IP está dentro de este rango de IP aparecen en la lista.

Figura 5-44 Adición rápida(1)



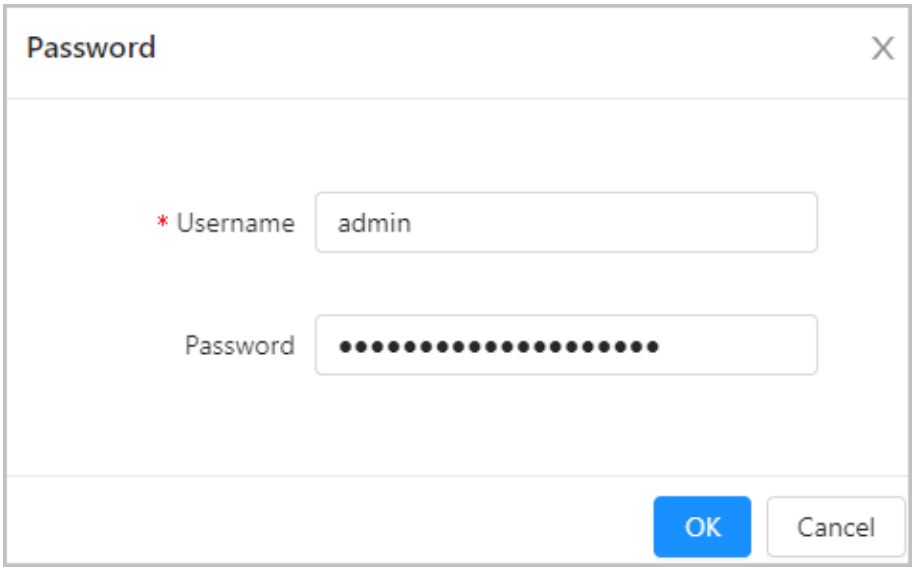
Paso 3 Seleccione el dispositivo de la lista y luego haga clic en**Agregar**.

Figura 5-45 Adición rápida (2)



Etapa 4 Ingrese el nombre de usuario y la contraseña del dispositivo y luego haga clic en**DE ACUERDO**para finalizar la configuración.

Figura 5-46 Ingresar contraseña



5.6.6.2.2 Agregar manualmente

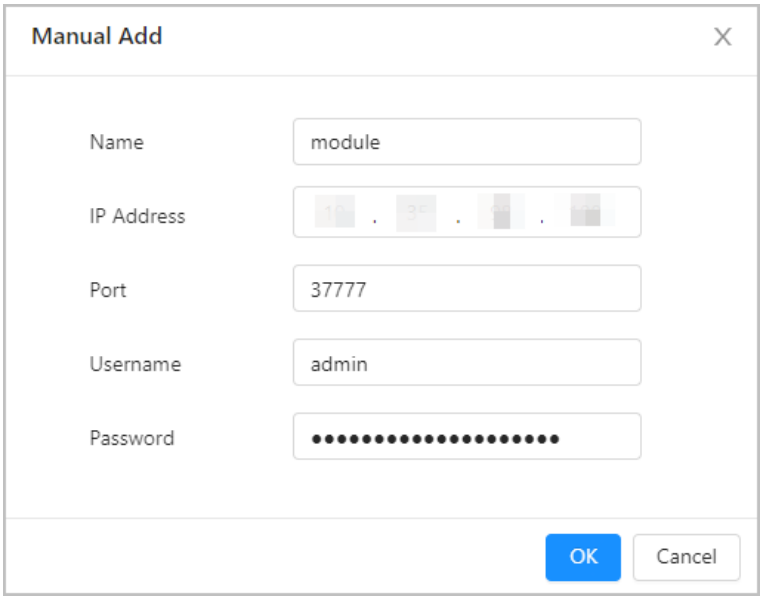
Procedimiento

Paso 1 Inicie sesión en la página web del panel de control de alarma y seleccione**Sistema**>**Periférico**> **Módulo de red**.

Paso 2 Hacer clic**Agregar manualmente**.

Paso 3 Configure el nombre, dirección IP, número de puerto, nombre de usuario y contraseña del módulo y luego haga clic en**DE ACUERDO**.

Figura 5-47 Agregar manualmente



5.6.6.3 Agregar dispositivos inalámbricos

Los dispositivos inalámbricos se agregan mediante métodos de emparejamiento, incluido el emparejamiento web y el emparejamiento físico.

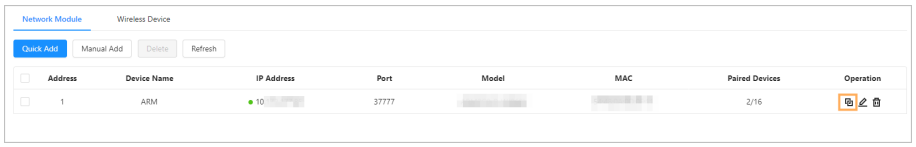
5.6.6.3.1 Emparejamiento web

Procedimiento

Paso 1 Inicie sesión en la página web del panel de control de alarma y seleccione**Sistema**>**Periférico** > **Módulo de red**.

Paso 2 Seleccione el dispositivo que desea emparejar y haga clic en .

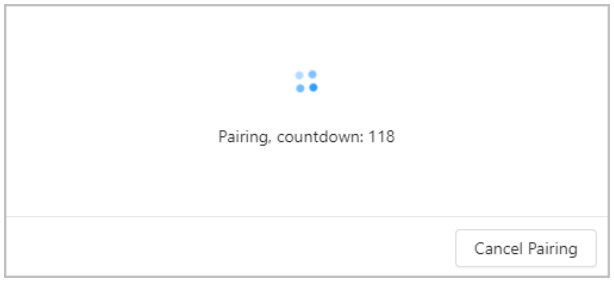
Figura 5-48 Emparejamiento inalámbrico



Paso 3 Después de que el módulo comienza a emparejarse, la luz indicadora de emparejamiento parpadea y el dispositivo inalámbrico que se va a emparejar se configura para ingresar al modo de emparejamiento.

Cada dispositivo inalámbrico tiene un modo de emparejamiento diferente. Consulte el manual de cada dispositivo inalámbrico para obtener una introducción detallada.

Figura 5-49 Cuenta regresiva de emparejamiento



Etapa 4 Hacer clic**DE ACUERDO**para existir el emparejamiento terminado, o**Próximo**para continuar con el emparejamiento.

También puedes hacer clic**Cancelar emparejamiento**si desea salir del proceso de emparejamiento actual.

5.6.6.3.2 Emparejamiento físico

Procedimiento

Paso 1 presione el**Par**botón en el módulo de red.

Si el panel de control de alarma está armado, el módulo está fuera de línea u otros módulos de red en el panel de control de alarma están emparejados, no se admite el emparejamiento físico.

Paso 2 Espere a que el dispositivo pase al modo de emparejamiento.

El modo de emparejamiento físico para diferentes dispositivos varía; consulte el manual de cada dispositivo inalámbrico para obtener una introducción detallada.

Paso 3 Inicie sesión en la página web del panel de control de alarma, seleccione**Sistema**>**Periférico**>**Dispositivo inalámbrico**para ver si el dispositivo inalámbrico se agregó correctamente.

5.6.6.4 Comprobación de la intensidad de la señal para dispositivos inalámbricos

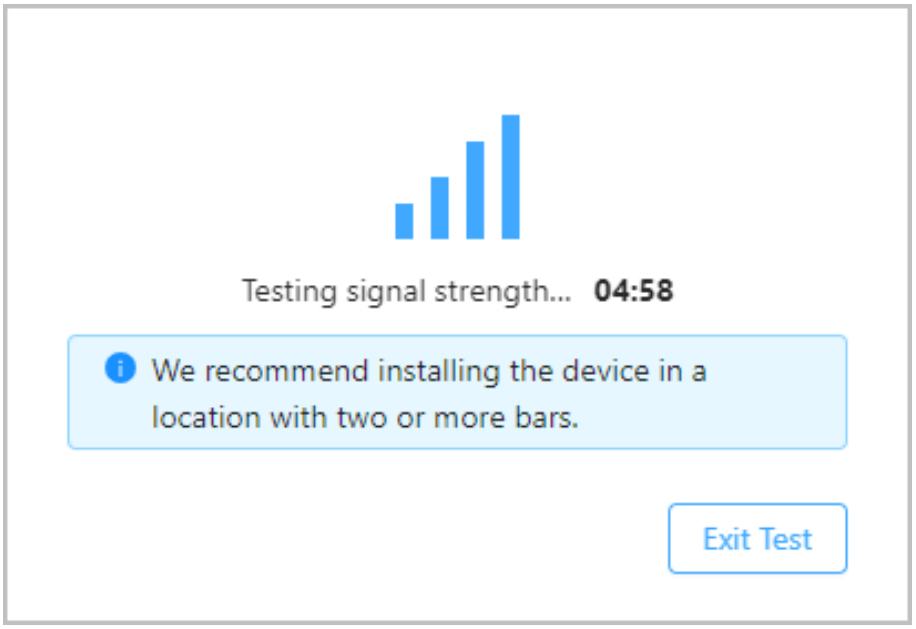
Antes de instalar y reparar el dispositivo, realice pruebas de la señal del dispositivo inalámbrico para encontrar la ubicación óptima para la instalación.

Procedimiento

Paso 1 Inicie sesión en la página web del panel de control de alarma y luego seleccione**Sistema**>**Periférico**>**Módulo de red**.

Paso 2 Seleccione los dispositivos que ya se agregaron y luego haga clic en Check.

Figura 5-50 Prueba de intensidad de la señal



Paso 3 Mueva el dispositivo inalámbrico a la ubicación de instalación de destino para ver la intensidad de la señal.

5.6.6.5 Edición de dispositivos inalámbricos

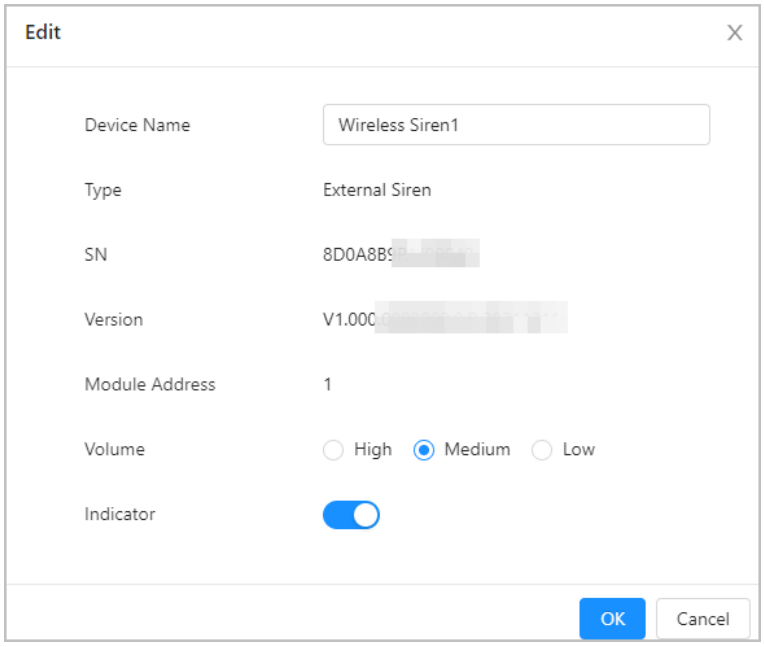
Cada dispositivo inalámbrico admite la modificación de algunos parámetros inalámbricos a través de la configuración web, como la habilitación de LED, la sensibilidad PIR, el volumen de la alarma y más. Esta sección toma la sirena como ejemplo para introducir la modificación de dispositivos inalámbricos.

Procedimiento

Paso 1 Inicie sesión en la página web del panel de control de alarma y luego seleccione**Sistema**>**Periférico**> **Dispositivo inalámbrico**.

Paso 2 Seleccione un dispositivo inalámbrico que se agregó y luego haga clic en para modificar los parámetros.

Figura 5-51 Modificar parámetros del dispositivo



Paso 3 Hacer clic**DE ACUERDO**.

5.7 Registro

5.7.1 Visualización y copia de seguridad de registros

Puede ver y realizar copias de seguridad de los registros.

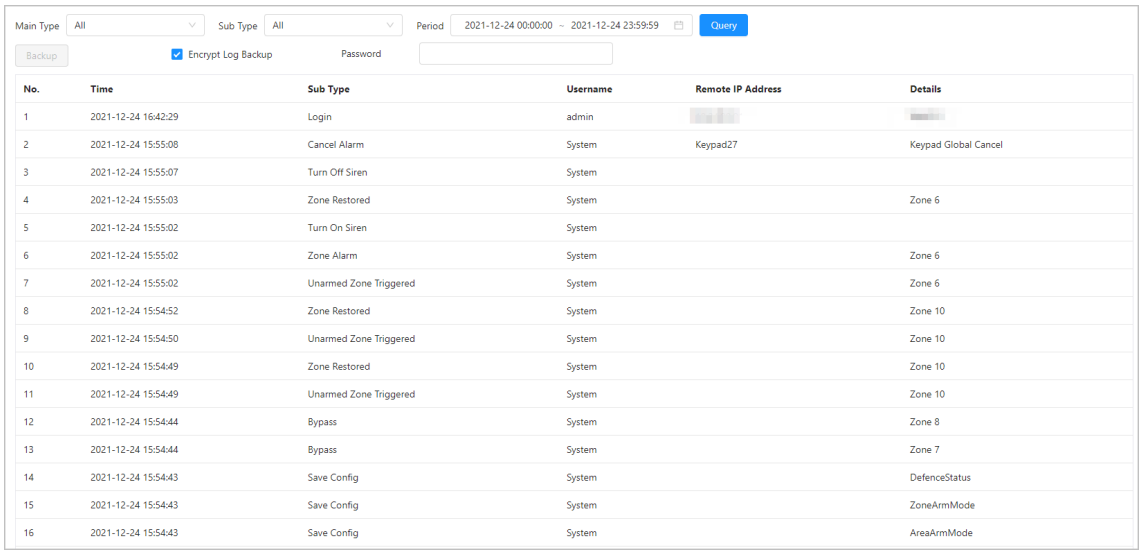
Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Registro**>**Registro**.

Paso 2 Colocar**Tipo principal**,**Subtipo**y**Período**. Hacer clic**Consulta**.

Paso 3

Figura 5-52 Registro



No.	Time	Sub Type	Username	Remote IP Address	Details
1	2021-12-24 16:42:29	Login	admin		
2	2021-12-24 15:55:08	Cancel Alarm	System	Keypad27	Keypad Global Cancel
3	2021-12-24 15:55:07	Turn Off Siren	System		
4	2021-12-24 15:55:03	Zone Restored	System		Zone 6
5	2021-12-24 15:55:02	Turn On Siren	System		
6	2021-12-24 15:55:02	Zone Alarm	System		Zone 6
7	2021-12-24 15:55:02	Unarmed Zone Triggered	System		Zone 6
8	2021-12-24 15:54:52	Zone Restored	System		Zone 10
9	2021-12-24 15:54:50	Unarmed Zone Triggered	System		Zone 10
10	2021-12-24 15:54:49	Zone Restored	System		Zone 10
11	2021-12-24 15:54:49	Unarmed Zone Triggered	System		Zone 10
12	2021-12-24 15:54:44	Bypass	System		Zone 8
13	2021-12-24 15:54:44	Bypass	System		Zone 7
14	2021-12-24 15:54:43	Save Config	System		DefenceStatus
15	2021-12-24 15:54:43	Save Config	System		ZoneArmMode
16	2021-12-24 15:54:43	Save Config	System		AreaArmMode

Etapa 4 Hacer clic**Respaldo**directamente, o haga clic**Cifrar copia de seguridad de registros**, introduzca la contraseña y luego haga clic en **Respaldo**para realizar copias de seguridad de los registros.

5.7.2 Registro remoto

Puede configurar el servidor syslog remoto para que se carguen los registros y luego podrá verlos en el servidor syslog.

Procedimiento

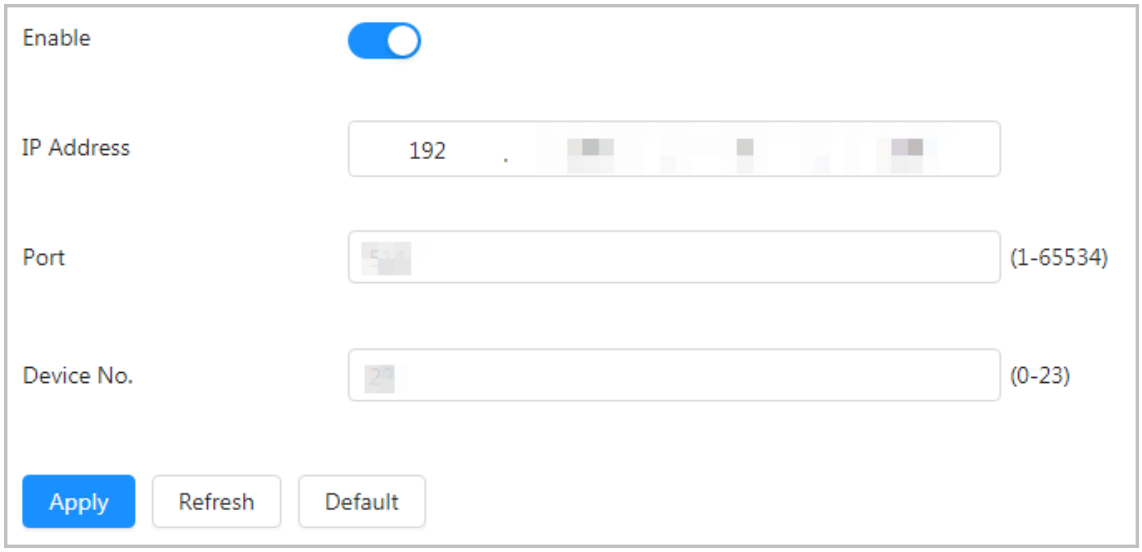
Paso 1 Inicie sesión en la web y luego seleccione**Registro**>**Registro remoto**.

Paso 2 Haga clic al lado de**Permitir**para habilitar la función.

Paso 3 Colocar**Dirección IP**,**Puerto**y**Dispositivo No.**del servidor remoto. Hacer

Etapa 4 clic**Aplicar**.

Figura 5-53 Registro remoto



5.7.3 Raspado de troncos

Puede aplicar la extracción de registros para ver y analizar problemas a través de registros.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Registro**>**Raspado de troncos**.

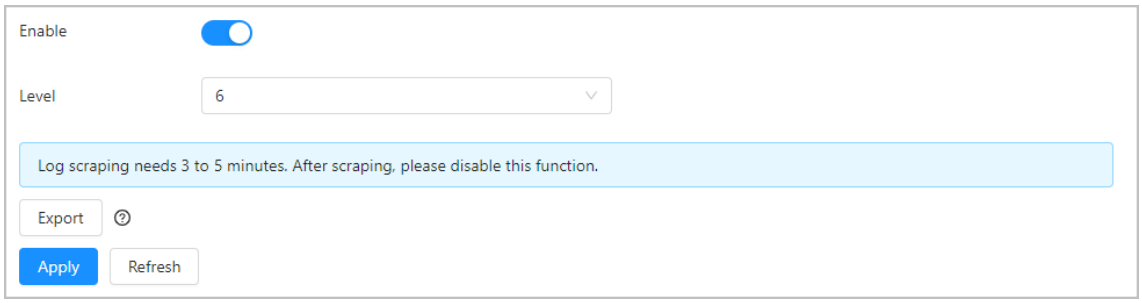
Paso 2 Haga clic al lado de**Permitir**para habilitar la función.

Cuanto mayor sea el nivel de la cuenta iniciada, mayor será la cantidad de información de registro disponible.

Paso 3 Hacer clic**Ahorrar**.

Etapa 4 Deshabilite la función, haga clic**Ahorrar**y luego haga clic**Exportar**para exportar troncos raspados.

Figura 5-54 Raspado de troncos



5.8 Seguridad

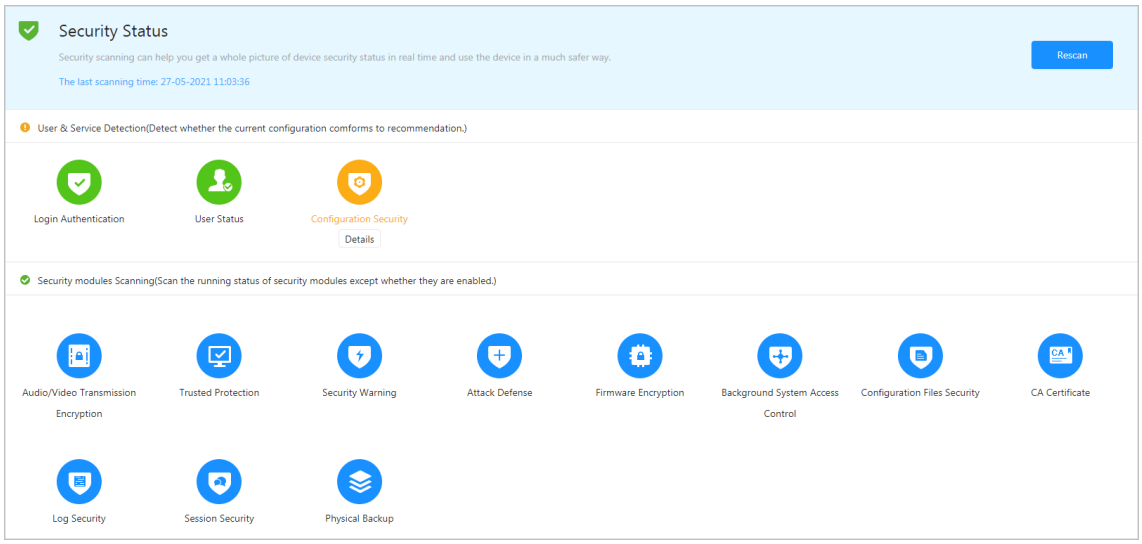
Ver el estado de seguridad del dispositivo y configurar funciones de seguridad.

5.8.1 Estado de seguridad

Lea el estado de seguridad actual del panel de control para usarlo de forma más segura, inicie sesión en la web y luego seleccione**Seguridad**>**Estado de seguridad**para comprobar si el dispositivo actual cumple con los

requisitos de las configuraciones recomendadas. Si no, haga clic**Detalles**para comprobar y optimizar. También puedes hacer clic**Volver a escanear**para actualizar el resultado del estado de seguridad.

Figura 5-55 Estado de seguridad



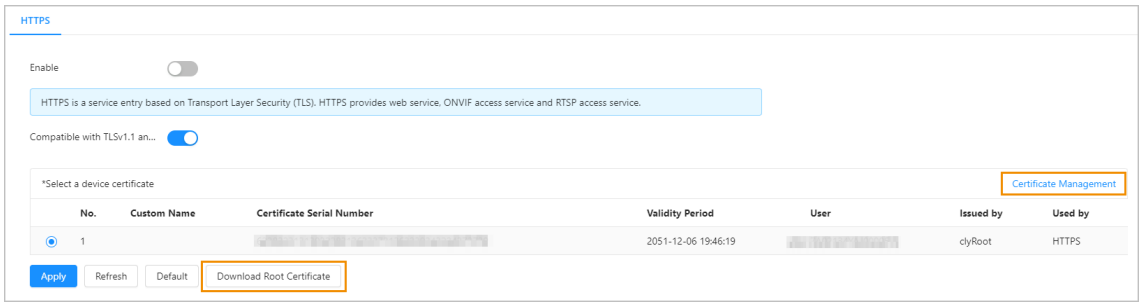
5.8.2 Configuración del servicio del sistema

Al instalar el certificado raíz, la computadora local puede iniciar sesión en el panel de control mediante HTTPS para garantizar la seguridad de los datos de comunicación y proteger la información del usuario y la seguridad del dispositivo con medidas tecnológicas estables.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Seguridad**>**Servicio del sistema**.

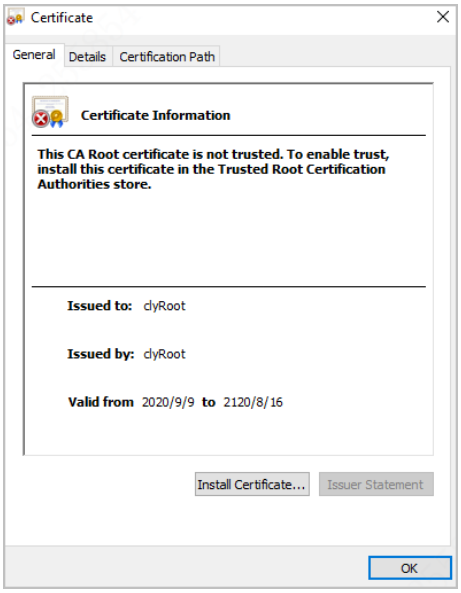
Figura 5-56 Servicio del sistema



Paso 2 Descargue e instale el certificado raíz.

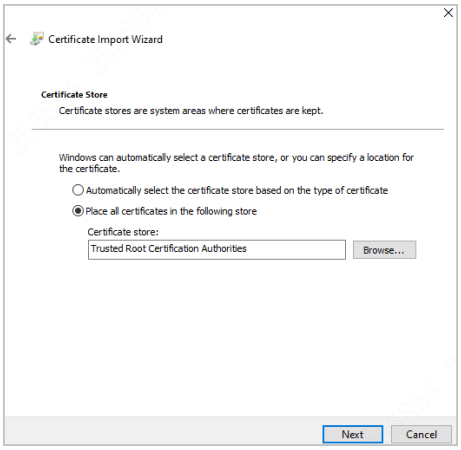
1. Haga clic**Descargar certificado raíz**y guarde el certificado raíz siguiendo las instrucciones de la página.
2. Haga doble clic en el descargado**RootCert.cer**archivo para abrir el certificado.
3. Haga clic**Instalar certificado**.

Figura 5-57 Certificado



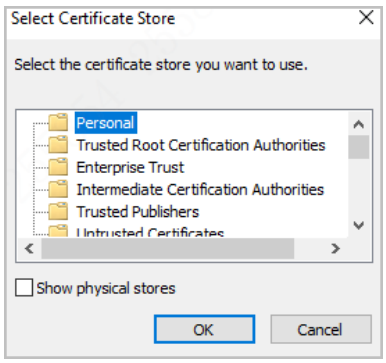
4. Haga clic**Próximo**en la ventana solicitada.
5. Seleccione**Coloque todos los certificados en la siguiente tienda.**,y luego haga clic**Navegar**.

Figura 5-58 Ubicación de almacenamiento del certificado



6. Seleccione**Autoridades de certificación raíz de confianza**y haga clic**DE ACUERDO**.

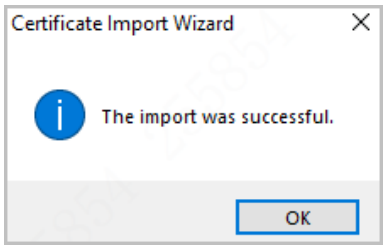
Figura 5-59 Seleccionar almacén de certificados



7. Haga clic**Próximo**y luego haga clic**Finalizar**.
8. Se completa la instalación del certificado.

Ingrese https://IP*DIRECCIÓN*en el navegador para abrir la página de inicio de sesión, lo que indica que se instaló el certificado. Si no hay ningún certificado instalado, el navegador mostrará un error de certificado.

Figura 5-60 Certificado importado exitosamente



Operaciones relacionadas

Hacer clic**Gestión de certificados**ir a**Certificado de CA**página.

5.8.3 Configuración de la defensa contra ataques

5.8.3.1 Configuración del cortafuegos

Configure la lista de bloqueo y la lista de permisos para restringir los derechos de acceso de los usuarios, salvaguardando así la seguridad de la puerta de enlace de la red.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Seguridad**>**Defensa de ataque**>**Cortafuegos**. Habilite la

Paso 2 lista de permitidos o la lista de bloqueo.

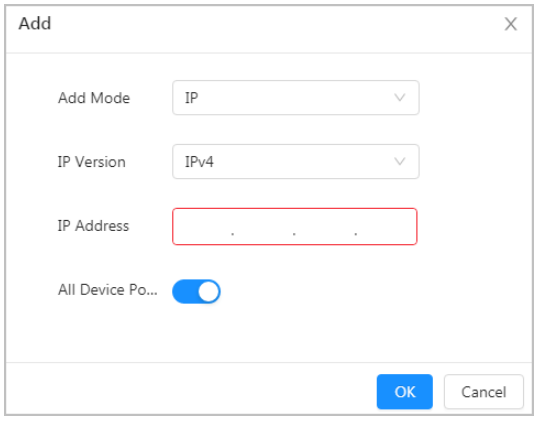
Paso 3 Colocar**Lista de permitidos**o**Lista de bloqueos**como el**Modo**. Hacer

Etapa 4 clic**Agregar**.

- **Lista de permitidos**:Sólo si la dirección IP o MAC del usuario está en la lista de permitidos, se puede acceder al Terminal. Si también se configura un puerto, el usuario solo podrá acceder al puerto especificado.
- **Lista de bloqueos**:Si la dirección IP o MAC del usuario está en la lista de bloqueo, no se podrá acceder al Terminal. Si también se configura un puerto, el usuario no puede acceder al puerto especificado.

- El dispositivo IP/MAC no se incluirá en la lista de bloqueo ni en la lista de permitidos.
- Al agregar la dirección MAC, no puede configurar el puerto.
- La verificación de la dirección MAC tiene efecto solo cuando la dirección IP del Terminal y la computadora local del usuario están en la misma LAN.
- Cuando se accede a la Terminal a través de WAN, el sistema solo puede verificar la dirección MAC del enrutador.

Figura 5-61 Agregar lista de permitidos o lista de bloqueo



Paso 5 Configure los parámetros.

Tabla 5-17 Descripción de los parámetros del firewall

Parámetro	Descripción
Agregar modo	• **IP**:Seleccione la versión de IP e ingrese la dirección IP del host. • **Segmento IP**:Seleccione la versión de IP y luego ingrese la dirección de inicio y la dirección de finalización del segmento. • **MAC**:Ingrese la dirección MAC que se agregará.
Dirección IP	La dirección IP de los dispositivos incluidos en la lista de permitidos o lista de bloqueo.
Agregar puertos de dispositivo	Configure el puerto de acceso. Controle las direcciones IP y MAC para acceder a los puertos designados. Puedes habilitar**Todos los puertos del dispositivo**,o deshabilite esta función y luego configure el**Puerto de inicio**y el**Puerto final**.
Puerto de inicio	
Puerto final	

Paso 6 Hacer clic**DE ACUERDO**.

El sistema vuelve a la**Cortafuegos**sección. Hacer

Paso 7 clic**Aplicar**.

5.8.3.2 Bloqueo de cuenta

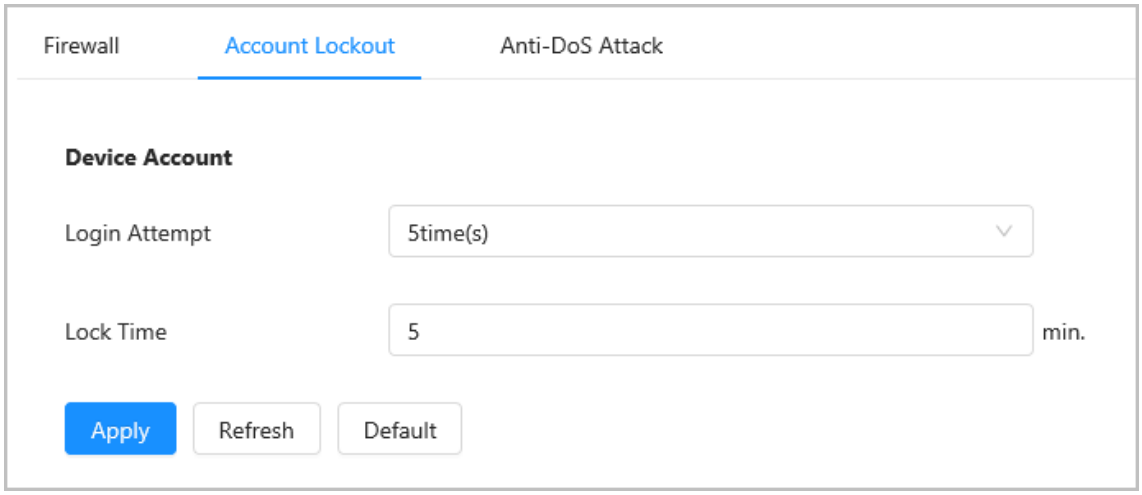
Establezca los tiempos permitidos de intentos de inicio de sesión y el tiempo de bloqueo para mejorar la seguridad.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Seguridad**>**Defensa de ataque**>**Bloqueo de cuenta**.

Paso 2 Selecciona el**Intentos de acceso**y**Tiempo de bloqueo**.

Figura 5-62 Configuración de bloqueo de cuenta



Paso 3 Hacer clic**Aplicar**.

5.8.3.3 Configuración del ataque Anti-DoS

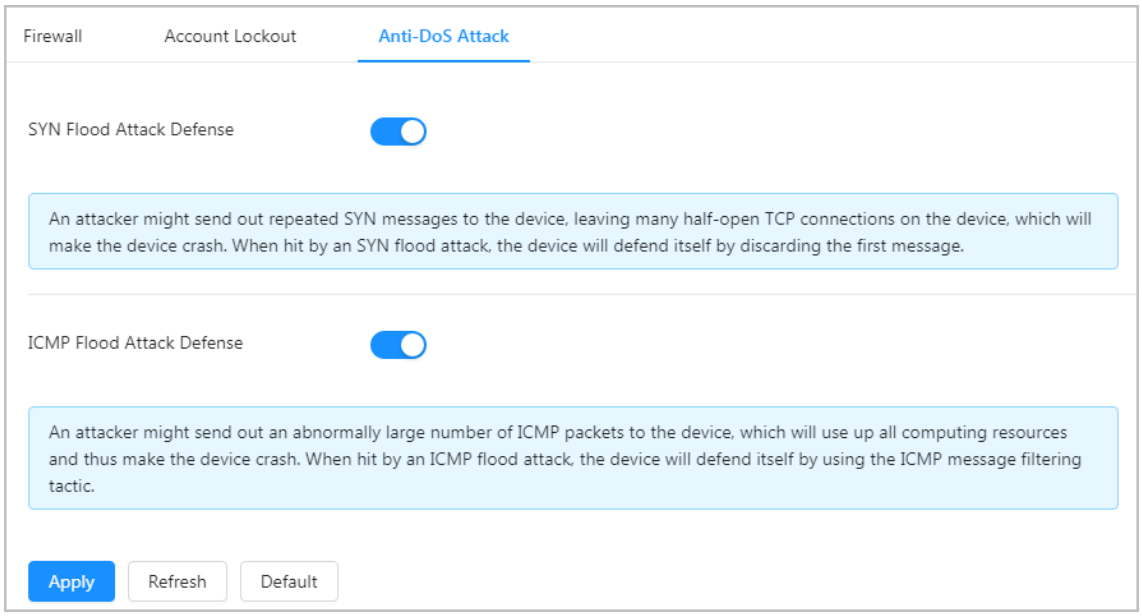
El ataque anti-DoS incluye defensa contra ataques contra inundaciones SYN y defensa contra ataques contra inundaciones ICMP.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Seguridad**>**Defensa de ataque**>**Ataque anti-DoS**.

Paso 2 Haga clic correspondiente a**Defensa contra ataques de inundación SYN**y**Defensa contra ataques de inundaciones ICMP**para permitir la defensa.

Figura 5-63 Ataque Anti-DoS



Paso 3 Hacer clic**Aplicar**.

5.8.4 Advertencia de seguridad

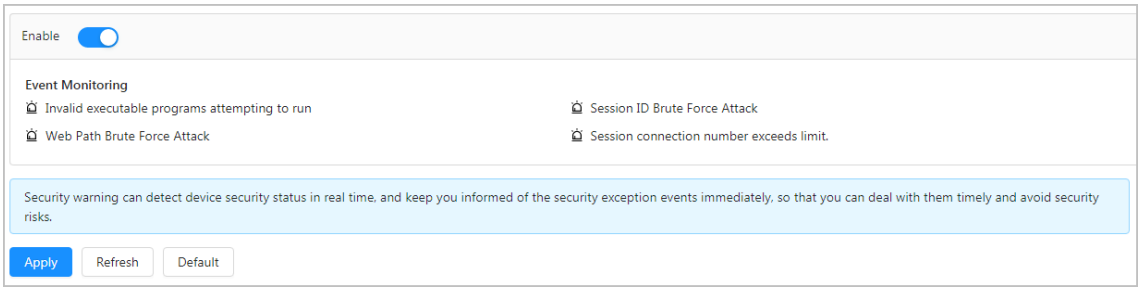
La advertencia de seguridad puede detectar el estado del dispositivo en tiempo real y mantenerlo informado de los eventos de excepción de seguridad de inmediato, para que pueda abordarlos oportunamente y evitar riesgos de seguridad.

Procedimiento

Paso 1 Inicie sesión en la web y luego seleccione**Seguridad**>**Advertencia de seguridad**.

Paso 2 Hacer clic**Permitir**.

Figura 5-64 Advertencia de seguridad



Paso 3 Hacer clic**Aplicar**.

6 operaciones del teclado

Esta sección presenta las funciones básicas del teclado. Para una operación específica, consulte el manual del usuario del teclado.

6.1 Inicialización

Requisitos previos

- El panel de control funciona normalmente.
- El panel de control y el teclado estaban conectados correctamente. Conectó exitosamente los puertos B y A del teclado a los puertos B y A del panel de control, el puerto – a GND– y el puerto + a +12 VCC del panel de control. Para obtener más información, consulte "4.2.5 Conexión del cable del teclado".

Procedimiento

Paso 1 Apague el teclado mientras el panel de control aún está encendido y verifique si el panel de control funciona normalmente.

Suministra energía independiente para cada uno de ellos cuando se conectan varios teclados.

Paso 2 Mantenga presionados ambos ENTER y ENTER teclas para encender el teclado. Liberar ENTER cuando el El teclado se ilumina y muestra las opciones de idioma de funcionamiento (chino e inglés).

Paso 3 Seleccione un idioma adecuado a través de ^ o v y luego presione ENTER.

Etapa 4 Seleccionar**Dirección RS-485**a través de ^ o v, presione ENTER, ingrese la dirección del teclado y luego la prensa ENTER.

Paso 5 Reinicie el teclado.

6.2 Modo de operación y contraseñas de usuario

Utilice el teclado ingresando directamente el comando en el modo de operación. El modo de operación se divide en modos de programación y prueba de caminata en los que no se puede iniciar sesión al mismo tiempo. Al salir del modo de programación, el teclado vuelve al modo global por defecto. Cuando no hay operaciones durante 3 minutos en el modo de programación, el teclado vuelve al modo global automáticamente.

La contraseña predeterminada es diferente para cada tipo de usuario, que incluye administrador, instalador, fabricante y operador.

- La contraseña predeterminada de administrador es 1234.
- La contraseña predeterminada del instalador es 9090.
- La contraseña predeterminada del fabricante 2008.

6.3 Permiso de usuario

Los permisos varían para diferentes usuarios.

Tabla 6-1 Descripción de los permisos de usuario

Usuario	Descripción
Administrador	Armar, desarmar, cancelar alarma, restaurar cancelación de alarma, anular, aislar, configurar armado forzado, administrar usuarios, agregar o editar parámetros de configuración.
Instalador	Todos los permisos del administrador (incluida la prueba de caminata) excepto el desarmado.
Fabricante	Administrar usuarios, editar programas básicos, como programas de actualización.
Operador	Armar, desarmar, cancelar alarma, restaurar cancelación de alarma.

6.4 Modo Global

- El número de zona contiene 3 dígitos, que van desde 001 a 256. Utiliza 0 como marcador de posición delante cuando hay menos de 3 dígitos (por ejemplo, 10 se convierte en 010).
- El número del subsistema contiene 2 dígitos, que van del 01 al 08. Utiliza 0 como marcador de posición delante cuando hay menos de 2 dígitos (por ejemplo, 8 se convierte en 08).
- El número de relé contiene 3 dígitos, que van desde 001 a 256. Utiliza 0 como marcador de posición delante cuando hay menos de 3 dígitos (por ejemplo, 10 se convierte en 010).
- Todos los objetos con la función de operación consecutiva admiten hasta 16 operaciones seguidas. Por ejemplo, la zona de anulación puede anular hasta 16 zonas al mismo tiempo.

6.4.1 Armado y Desarmado

Función

- Armado: Cuando el panel de control y los detectores funcionen correctamente, arme la zona y luego el panel de control responderá a las señales de alarma en la zona.
- Desarmado: Desarma la zona cuando está en estado armado.

Dominio

- Cambiar estado del sistema: ingrese la contraseña.
- Desarmar subsistema: Ingrese la contraseña + * + 2 + * + número de subsistema.
- Subsistema de armado ausente: Ingrese la contraseña + * + 3 + * + número del subsistema.
- Armado forzado del subsistema: Ingrese la contraseña + * + 4 + * + número del subsistema.
- Subsistema de armado en casa: Ingrese la contraseña + * + 5 + * + número del subsistema.
- Subsistema de armado local forzado: Ingrese la contraseña + * + 6 + * + número del subsistema.
- Armar zona única: Ingrese la contraseña + * + 10 + * + número de zona.
- Desarmar zona única: Ingresar contraseña + * + 11 + * + número de zona.

Cambiar el estado del sistema significa que puede cambiar el estado de armado/desarmado de cada subsistema activo. Por ejemplo, si el subsistema actual está en estado armado, ingrese el comando y el subsistema cambiará al estado desarmado.

Ejemplo

El administrador (el código de acceso predeterminado es 1234) realiza el armado remoto en el subsistema1.

1. En modo global, ingrese 1234 * 3 * 01.
2. Presione Entrar.

6.4.2 Cancelar alarma

Función

Cancele la alarma a través del teclado cuando se active una alarma.

Dominio

- Cancelar todas las alarmas: Ingrese la contraseña + * + 1.
- Cancelar alarma de zona: Ingrese la contraseña + * + 1 + * + número de zona.
- Cancelar la alarma del subsistema: Ingrese la contraseña + * + 23 + * + número del subsistema.

Ejemplo

El administrador (el código de acceso predeterminado es 1234) cancela todas las alarmas.

1. En modo global, ingrese 1234 * 1.
2. Presione Entrar.

6.4.3 Anulación y aislamiento

Función

Cuando todo el sistema no puede armarse debido a fallas en los detectores o actividades humanas en algunas zonas, se le permite omitir estas zonas eliminando selectivamente los detectores del sistema de seguridad. Por ejemplo, se puede pasar por alto un detector para armar el perímetro con una ventana abierta.

- Anular: Si una o más zonas son anuladas, quedan deshabilitadas durante un ciclo de armado. Después de un ciclo de armado, se desanulan automáticamente.
- Aislar: Si una o más zonas están aisladas, quedan deshabilitadas hasta que se desanulan.
- Desanular: Restaura manualmente una zona a su funcionamiento normal eliminando una condición de anulación.

Dominio

- Desanular: Ingrese la contraseña + * + 7 + * + número de zona.
- Anular: Ingrese la contraseña + * + 8 + * + número de zona.
- Aislar: Ingrese la contraseña + * + 9 + * + número de zona.

Ejemplo

Administrador (el código de acceso predeterminado es 1234) omite la zona 1.

1. En el modo global, ingrese 1234*8*001.
2. Presione Entrar.

6.4.4 Relé

Función

Enciende o apaga manualmente la salida de relé.

Dominio

- Encienda manualmente la salida de relé: Ingrese la contraseña + * + 13 + * + número de relé.
- Apague manualmente la salida de relé: Ingrese la contraseña + * + 14 + * + número de relé.

El número de retransmisión de 3 dígitos oscila entre 001 y 256 y utiliza 0 como marcador de posición delante cuando hay menos de 3 dígitos (por ejemplo, 10 se convierte en 010).

Ejemplo

El instalador (el código de acceso predeterminado es 1234) desactiva la función de salida del relé 1.

1. En modo global, ingrese 1234*14*001.
2. Presione Entrar.

6.4.5 Prueba RTPC

Función

- Con la configuración correcta, la central intenta enviar un mensaje de prueba a la central receptora de alarmas configurada después de ejecutar el comando de prueba manual PSTN. El mensaje de prueba exitoso solo significa que el comando se envió exitosamente, pero no que el centro receptor de alarmas recibió el mensaje.
- Después de ejecutar el SMS o el comando de prueba de llamada manual, el panel de control envía un mensaje de prueba o realiza una llamada de prueba al teléfono para verificar si el módulo 2G/4G o las funciones de SMS y llamada del panel de control están disponibles.

Dominio

- Prueba manual de PSTN: ingrese la contraseña + * + 15.
- Prueba manual de SMS: Ingrese la contraseña + * + 16 + * + número de teléfono.
- Llamar a prueba manual: Ingrese la contraseña + * + 17 + * + número de teléfono.

Ejemplo

El instalador (el código de acceso predeterminado es 1234) prueba manualmente PSTN.

1. En modo global, ingrese 1234*15.
2. Presione Entrar.

6.4.6 Reiniciar el panel de control

Función

Reinicie el panel de control de alarma.

Dominio

Ingrese la contraseña + * + 20.

Ejemplo

El administrador (el código de acceso predeterminado es 1234) reinicia el panel de control.

1. En modo global, ingrese 1234 * 20.
2. Presione Entrar.

6.4.7 Inicialización del panel de control

Función

Inicialice el panel de control de alarma.

Debido al inconveniente de ingresar letras en el teclado, la contraseña de la cuenta de administrador que inicializa el panel de control utiliza las siguientes reglas.

- Después de ejecutar el comando con un código de acceso digital (3 a 27 dígitos) para inicializar exitosamente el panel de control, el código de acceso real es admin + el código de acceso digital.
- Si el código de acceso es una combinación de números y letras (8 a 32), después de una inicialización exitosa, el código de acceso real es el código de acceso mixto.

Dominio

Ingrese el código de acceso * + 21 + * + código de acceso del administrador.

Ejemplo

El administrador (la contraseña predeterminada es 1234) inicializa el panel de control y establece el código de acceso del usuario administrador en admin123.

1. En modo global, ingrese 1234*21*123.
2. Presione Entrar.

6.4.8 Restauración a los valores predeterminados

Función

Restaure los parámetros a la configuración predeterminada, incluida alarma, salida de alarma, subsistema de alarma, teclado, armado y desarmado, falla de la batería principal, subtensión, alarma de manipulación, llamada al centro receptor de alarma, PSTN fuera de línea, estado del subsistema, desconexión de la red, conflicto de IP, conflicto de MAC y alarma de emergencia.

Dominio

Ingrese la contraseña + * + 22.

Ejemplo

El administrador (el código de acceso predeterminado es 1234) restaura el panel de control a la configuración predeterminada.

1. En el modo global, ingrese 1234*22.
2. Presione Entrar.

Apéndice 1 Glosario

Apéndice Tabla 1-1Glosario

Término	Descripción
Subsistema	El subsistema es un área independiente distribuida por el panel de control de alarma, el cual funciona como un sistema independiente que puede armar y desarmar el área.
Zona Auxiliar 24 horas	Se aplica frecuentemente al botón de emergencia, detector de fugas de agua, detector de temperatura y más. Los detectores que trabajan en esta zona están armados las 24 horas del día. Tampoco se ven afectados por las operaciones de armado y desarmado ni por derivación. Cuando se detecta un evento de alarma, la zona activa mensajes de alarma de luz y sonido en el teclado, activando una sirena si la conexión de sirena está habilitada. Mientras tanto, genera un informe de evento y lo envía a la central receptora de alarmas (el código de informe cargado difiere del de la zona audible de 24 horas). Puede ver el estado de alarma de la zona en el cliente.
Zona de vibración las 24 horas	Se aplica frecuentemente al botón de emergencia, al detector de humo y al detector de rotura de cristales. Aplicable para nosotros con cajeros automáticos y en otros escenarios. Los detectores que trabajan en esta zona están armados las 24 horas del día. Tampoco se ven afectados por las operaciones de armado y desarmado ni por derivación. Cuando se detecta un evento de alarma, la zona activa mensajes de alarma de luz y sonido en el teclado y activa la sirena si la conexión de sirena está habilitada. Mientras tanto, genera un informe de evento y lo envía a la central receptora de alarmas. Puede ver el estado de la alarma de la zona en el cliente.
Zona Audible las 24 horas	Se aplica frecuentemente al botón de emergencia, al detector de humo y al detector de rotura de cristales. Los detectores que trabajan en esta zona están en estado armado las 24 horas del día y no se ven afectados por las operaciones de armado y desarmado ni por derivación. Cuando se detecta un evento de alarma, la zona activa mensajes de alarma de luz y sonido en el teclado y activa la sirena si la conexión de sirena está habilitada. Mientras tanto, genera un informe de evento y lo envía a la central receptora de alarmas. Puede ver el estado de la alarma de la zona en el cliente.
Zona silenciosa las 24 horas	Se aplica con frecuencia al botón de emergencia de bancos, mostradores de joyería y otros escenarios. Puede activar y reportar alarmas a la estación central, sin mostrar el número de zona en el teclado. Sin tono de alarma, sólo informes de comunicación de programación de línea telefónica y puerto serie. No se ve afectado por las operaciones de armado y desarmado.
Zona retrasada	Se utiliza en entradas y salidas principales (como puertas de entrada). Entra en vigor cuando finaliza el retardo de ausencia después del armado. Cuando se activa la zona, se habilita el retardo de entrada. Debe desarmar el sistema antes de que finalice el retraso para evitar activar una alarma. El panel de control emitirá un zumbido durante el período de retardo de entrada como recordatorio para desarmar el sistema.

Término	Descripción
Zona Instantánea	Aplicable para su uso en escenarios donde los informes inmediatos van seguidos de cerca por una alarma activada. No se admiten retrasos de entrada y salida. Los detectores que trabajan en esta zona están armados las 24 horas del día y pueden verse afectados por operaciones de armado y desarmado y anulación permitida. Cuando se detecta un evento de alarma, la zona activa mensajes de alarma de luz y sonido en el teclado y activa la sirena si la conexión de sirena está habilitada. Mientras tanto, genera un informe de evento y lo envía a la central receptora de alarmas (el código de informe cargado difiere del de la zona audible de 24 horas). Puede ver el estado de la alarma de la zona en el cliente. Generalmente se usa con detectores de humo.
Zona de fuego	Se utiliza en áreas con detectores de humo y calor y está armado las 24 horas del día. Cuando se activa la zona, genera una señal de alarma de incendio, el teclado muestra el número de zona, activa la sirena externa e informa a la estación central. No se ve afectado por las operaciones de armado y desarmado.
Zona de ladrones	Se utiliza en áreas de defensa, como en lugares donde las puertas o ventanas exteriores normalmente están cerradas, en perímetros de vallas y en pasajes prohibidos. Se activa una alarma inmediata cuando se produce una intrusión. No se ve afectado por las operaciones de armado y desarmado.
Zona Perimetral	Se utiliza principalmente en puertas o ventanas exteriores. Cuando el sistema está armado, los detectores de la zona están armados. Una alarma se activa y se informa inmediatamente después de que se detecta un evento de alarma. Cuando una zona está desarmada pero permanece en estado armado, el sistema envía un registro de operación a la central receptora de alarmas automáticamente. Luego, el estado de la zona cambia a falla.
Zona de entrada sin alarma	La central no genera alarmas cuando se activa esta zona. Únicamente recoge, como entrada de estado, indicar el estado de funcionamiento del panel de control. También se puede utilizar para ejecutar acciones vinculadas, mostrar el estado de apertura de puertas, encender luces a través de la programación del módulo de salida correspondiente y más.
Zona clave fija	Especialmente diseñado para cambiar el estado de armado/desarmado del sistema. Cuando la zona es normal, el sistema está en estado desarmado y, cuando se activa, el estado del sistema cambia a armado.
Zona de clave variable	Especialmente diseñado para cambiar el estado de armado/desarmado del sistema. Cada vez que se activa la zona, el estado del sistema cambia.
Armamento	Encienda el sistema. El sistema de seguridad se puede activar (armar) de muchas maneras diferentes, dependiendo del comando de armado utilizado.
Armado en casa	Un modo de armado que permite al usuario armar el sistema cuando se encuentra dentro del área del sistema de alarma. En este modo, todas las zonas perimetrales (como los detectores perimetrales exteriores) del sistema están en estado armado, pero el sistema anula las zonas internas (como el detector IR interior), por lo que las alarmas no se activarán cuando las personas se muevan libremente. en la zona porque las zonas internas del subsistema están desarmadas.
Armado Ausente	Armar el sistema cuando todos los usuarios abandonen la zona del sistema de alarma. En este modo, todas las zonas del sistema están en estado de funcionamiento, lo que significa que todas las zonas del subsistema están armadas.

Término	Descripción
Encantador	Apague el sistema de seguridad. Lo contrario de armarse.
Cancelar alarma	Cancelar alarmas vinculadas de subsistemas o zonas.
Cancelación global	Cancele todas las alarmas vinculadas a subsistemas o zonas, incluidas las alarmas vinculadas a fallas del panel de control.
Derivación	Cuando todo el sistema no puede armarse debido a fallas en los detectores o actividades humanas en algunas zonas, los usuarios pueden evitar estas zonas eliminando selectivamente los detectores del sistema de seguridad. Por ejemplo, se puede pasar por alto un detector para armar el perímetro con una ventana abierta.
Aislar	Si una o más zonas están aisladas, quedan deshabilitadas hasta que se desanulan.
desviar	Restaura manualmente una zona al funcionamiento normal eliminando una condición de anulación.
Retardo de salida	Un retraso programado en la respuesta de alarma del sistema que permite que una persona salga después de armar un área. Si no se sale antes de que expire el tiempo de retraso, comenzará el retraso de entrada. Luego se debe desarmar el sistema. Si no se desarma antes de que expire el tiempo de demora, el sistema producirá una respuesta de alarma que podría incluir el envío de informes a la estación central.
Retraso de entrada	Un retraso programado en la respuesta de alarma del sistema que permite a una persona ingresar a un área armada a través del detector correcto y desarmar el área. Si el sistema no se desarma antes de que expire el tiempo de demora, el sistema iniciará una respuesta de alarma que puede incluir el envío de informes a la estación central.
0 o 1 fin de vida	El tipo de detector puede ser NA o NC, y devuelve dos estados: Normal y alarma (cortocircuito y circuito roto se consideran estados de alarma).
2 fin de vida	El tipo de detector puede ser NO o NC y devuelve cuatro estados: Normal, alarma, manipulación y alarma de cortocircuito.
3 fin de vida	El tipo de detector puede ser NO o NC y devuelve cinco estados: Normal, alarma, manipulación, máscara y alarma de cortocircuito.
Manipulación de caja	La alarma se activa cuando se abre el estuche.
manipulación de pared	La alarma se activa cuando la caja se separa de la pared.

Apéndice 2 Recomendaciones de ciberseguridad

La ciberseguridad es más que una simple palabra de moda: es algo que pertenece a todos los dispositivos 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 conectados los hará menos susceptibles a los ataques. A continuación se presentan algunos consejos y recomendaciones de Dahua sobre cómo crear un sistema de seguridad más seguro.

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.

Más información

Visite el centro de respuesta a emergencias de seguridad del sitio web oficial de Dahua para obtener anuncios de seguridad y las últimas recomendaciones de seguridad.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188