Conmutador Ethernet (conmutador administrado en la nube de 16 y 24 puertos)

Guía de inicio rápido

ZHEJIANG DAHUA VISIÓN TECNOLOGÍA CO., LTD. V1.0.0

Prefacio

General

Este manual presenta la instalación, las funciones y las operaciones del conmutador administrado en la nube de 16 y 24 puertos (en adelante, "el conmutador"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para consultarlo en el futuro.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

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

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.1	Se agregó una descripción de PoE.	marzo 2023
V1.0.0	Primer lanzamiento.	marzo 2023

Aviso de protección de privacidad

Como usuario del dispositivo o controlador 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. Actualizaciones de Producto

Podría dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Comuníquese con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.

- Pueden existir errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en este manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de dar una explicación final.

Salvaguardias y advertencias importantes

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

Requisitos de transporte

Transporte el dispositivo en las condiciones permitidas de humedad y temperatura.

Requisitos de almacenamiento

Guarde el dispositivo en condiciones permitidas de humedad y temperatura.

requerimientos de instalación

WARNING

- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- Cumpla estrictamente con el código y las normas locales de seguridad eléctrica. Asegúrese de que el voltaje ambiental sea estable y cumpla con los requisitos de suministro de energía del dispositivo.
- El personal que trabaja en alturas debe tomar todas las medidas necesarias para garantizar la seguridad personal, incluido el uso de casco y cinturones de seguridad.

- No coloque el dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- Coloque el dispositivo en un lugar bien ventilado y no bloquee su ventilación.
- Utilice un adaptador o fuente de alimentación de gabinete proporcionado por el fabricante.
- 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.
- No conecte el dispositivo a dos o más tipos de fuentes de alimentación para evitar daños al dispositivo.
- El dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectada a una toma de corriente con conexión a tierra de protección.
- El dispositivo debe estar conectado a tierra mediante un cable de cobre con una sección transversal de 2,5 mm^2 y una resistencia de tierra no mayor a 4 Ω.
- El estabilizador de voltaje y el protector contra sobretensiones son opcionales según el suministro de energía real en el sitio y el entorno ambiental.
- Para garantizar la disipación del calor, el espacio entre el dispositivo y el área circundante no debe ser inferior a 10 cm en los lados y 10 cm en la parte superior del dispositivo.
- Al instalar el dispositivo, asegúrese de que se pueda acceder fácilmente al enchufe de alimentación y al acoplador del aparato para cortar la alimentación.

Requisitos de operación

WARNING

- No desmonte el dispositivo sin instrucción profesional.
- Opere el dispositivo dentro del rango nominal de entrada y salida de energía.
- Asegúrese de que la fuente de alimentación sea correcta antes de su uso.
- Asegúrese de que el dispositivo esté apagado antes de desmontar los cables para evitar lesiones personales.
- No desenchufe el cable de alimentación en el costado del dispositivo mientras el adaptador esté encendido.

- Utilice el dispositivo en las condiciones permitidas de humedad y temperatura.
- No deje caer ni salpique líquido sobre el dispositivo y asegúrese de que no haya ningún objeto lleno de líquido sobre el dispositivo para evitar que el líquido fluya hacia él.
- Temperatura de funcionamiento: –10 °C a +55 °C (+14 °F a +131 °F).
- Este es un producto de clase A. En un entorno doméstico, esto puede causar interferencias de radio, en cuyo caso es posible que deba tomar las medidas adecuadas.
- No bloquee el ventilador del dispositivo con objetos como periódicos, manteles o cortinas.
- No coloque una llama abierta sobre el dispositivo, como una vela encendida.

Requisitos de mantenimiento

WARNING

- Apague el dispositivo antes del mantenimiento.
- Marque los componentes clave en el diagrama del circuito de mantenimiento con señales de advertencia.

Tabla de contenido

1. Información general

1.1 Introducción

El conmutador gestionado en la nube es un conmutador comercial de capa 2. Con su función PoE de larga distancia, puede suministrar energía a dispositivos a una distancia de hasta 250 metros. El conmutador tiene funciones de puerto rojo PoE con una fuente de alimentación PoE de hasta 90 W. La potencia total PoE del conmutador de 16 puertos llega a 240 W y la del conmutador de 24 puertos llega a 360 W. Además , basado en el servidor en la nube de DoLynk Care, este conmutador se puede administrar a través de la aplicación DoLynk Care, la función de diagrama de topología de red se puede utilizar para localizar rápidamente el problema. El Switch es aplicable para usos en diferentes escenarios, incluidos hogares, fábricas y oficinas.

En modo extendido, la distancia de transmisión del puerto PoE es de hasta 250 metros, pero la transmisión La velocidad cae a 10 Mbps. La distancia de transmisión real puede variar debido al consumo de energía de dispositivos conectados o el tipo y estado del cable.

1.2 Características

- Puertos Ethernet PoE de 16/24 × 100/1000 Mbps, 2 puertos Ethernet de 100/1000 Mbps y 2 puertos ópticos de 1000 Mbps (Combo).
- Los puertos grises cumplen con los estándares IEEE802.3af e IEEE802.3at, los puertos naranjas cumplen con el estándar Hi-PoE y los puertos rojos cumplen con los estándares IEEE802.3bt.
- Admite visualización de topología de red.
- Admite fuente de alimentación de larga distancia de 250 m.

  En modo extendido, la distancia de transmisión del puerto PoE es de hasta 250 metros, pero el La velocidad de transmisión cae a 10 Mbps. La distancia de transmisión real puede variar debido a la potencia. consumo de dispositivos conectados o el tipo y estado del cable.
- Cuenta con gestión móvil por aplicación.
- Admite LLDP (Protocolo de descubrimiento de capa de enlace).
- Admite cliente DHCP (Protocolo de configuración dinámica de host).
- Montaje en escritorio y montaje en rack.

2 puertos e indicador

2.1 Panel frontal

La siguiente figura utiliza un conmutador administrado en la nube de 16 puertos y 100 Mbps como ejemplo y puede diferir del producto real.

Figura 2-1 Panel frontal

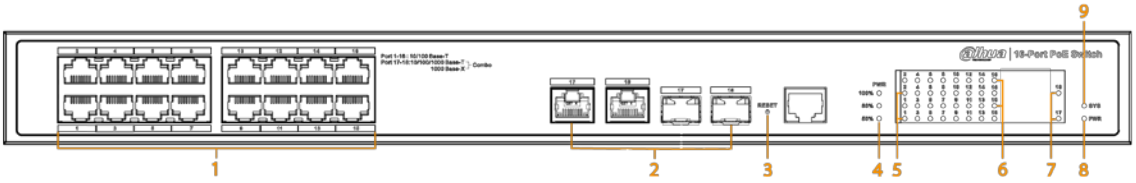


Tabla 2-1 Descripción del panel frontal

No.	Nombre	Descripción
1	Puertos PoE	Puertos Ethernet autoadaptativos de 16/24 × 10/100 Mbps o 10/100/1000 Mbps.
2	Puertos de enlace ascendente	Puertos Ethernet autoadaptativos de 10/100/1000 Mbps y puertos ópticos de 1000 Mbps.
3	Botón de reinicio	Manténgalo presionado durante más de 5 segundos y suéltelo después de que todos los indicadores de estado del panel se enciendan para restaurar el interruptor a la configuración predeterminada.
4	Potencia de salida PoE indicador	● Solo verde fijo: potencia de salida PoE ≤ 50 %. ● Verde y rojo fijos: 50 % < potencia de salida PoE ≤ 80 %. ● Verde, amarillo y rojo fijos: 80 % < potencia de salida PoE.
5	Indicador de enlace/actuación	● Encendido: conectado al dispositivo. ● Apagado: No conectado al dispositivo. ● Intermitente: Transmitiendo datos.
6	Estado del puerto PoE indicadores	● Encendido: alimentado por PoE. ● Apagado: No alimentado por PoE.
7	Estado del puerto de enlace ascendente (Enlace) indicadores	● Encendido: conectado al dispositivo. ● Apagado: No conectado al dispositivo.
8	Indicador de encendido	● Encendido: encendido. ● Apagado: apagado.
9	Estado del sistema indicador (SYS)	● El indicador parpadea rápidamente (intervalo de 1 segundo): Arranque. ● El indicador parpadea lentamente (intervalo de 2 segundos): funcionamiento normal.

2.2 Panel trasero

Figura 2-2 Panel trasero

Tabla 2-2 Descripción del panel trasero

No.	Nombre	Descripción
1	Dip switch	—
2	Puerto de alimentación	Soporta 53 VCC.
3	Suelo Terminal	Conexión a tierra. ● La conexión GND normal del interruptor garantiza protección contra rayos y antiinterferencias del dispositivo. Debe conectar el cable GND antes de encender el conmutador y apagar el conmutador antes de desconectar el cable GND. ● La sección del cable GND debe ser superior a 2,5 $mm.^2$, y la resistencia GND debe ser inferior a 4 Ω.

3 Instalación

3.1 Preparación

- Seleccione un método de instalación apropiado según sea necesario.
- Instale el interruptor sobre una superficie sólida y plana.
- Deje unos 10 cm de espacio abierto alrededor del Switch para disipar el calor y asegurar una buena ventilación.

3.2 Montaje en escritorio

El Switch admite montaje en escritorio. Puedes colocarlo directamente sobre un escritorio sólido y plano.

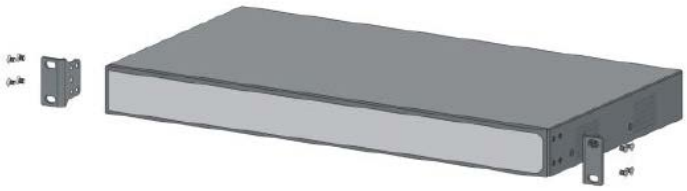
3.3 Montaje en bastidor

El conmutador admite montaje en bastidor.

Procedimiento

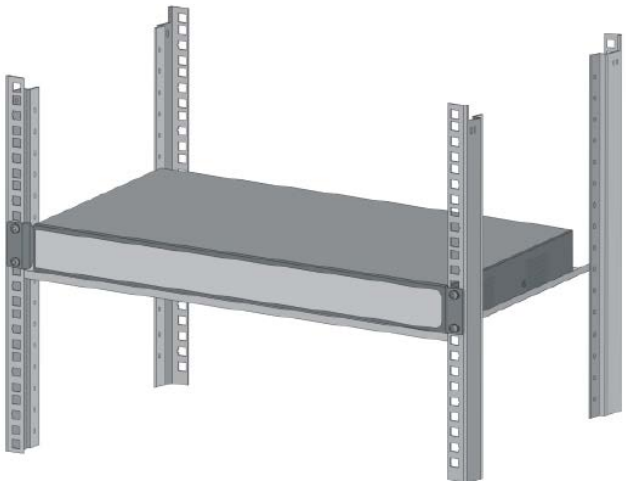
Paso 1 Conecte los soportes de montaje al Switch (uno a cada lado) y fíjelos con los tornillos proporcionados.

Figura 3-1 Coloque los soportes de montaje



Paso 2 Fije el interruptor en el estante.

Figura 3-2 Fije el interruptor en el bastidor



4 Inicialización y adición del conmutador

4.1 Inicializando el interruptor

Información de contexto

Puede inicializar dispositivos y modificar la dirección IP de los dispositivos utilizando ConfigTool.

- ConfigTool se puede descargar desde el sitio web oficial de Dahua y el enlace es https://support2.dahuasecurity.com/en.
- Se requiere la inicialización del dispositivo para el uso por primera vez o después de que se haya reiniciado el Switch.
- La inicialización del dispositivo está disponible solo cuando el Switch (la dirección IP es 192.168.1.110 de forma predeterminada) y la computadora está en el mismo segmento de red.
- Planifique el segmento de red correctamente para conectar el Switch a la red.

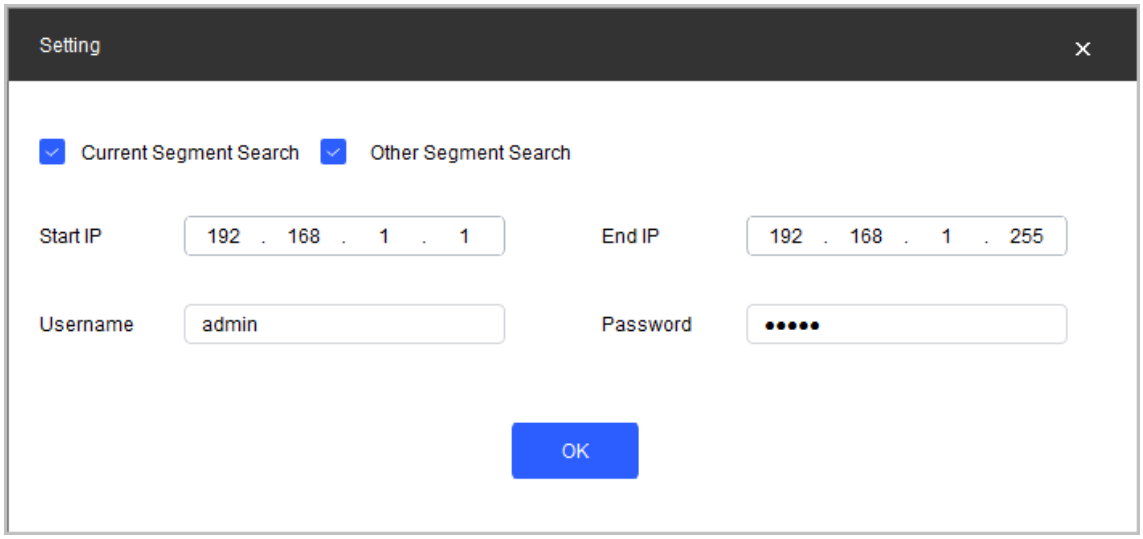
Procedimiento

Paso 1 Haga doble clic en "ConfigTool.exe" para abrir la herramienta. Grifo

Paso 2 **Configuración de búsqueda**.

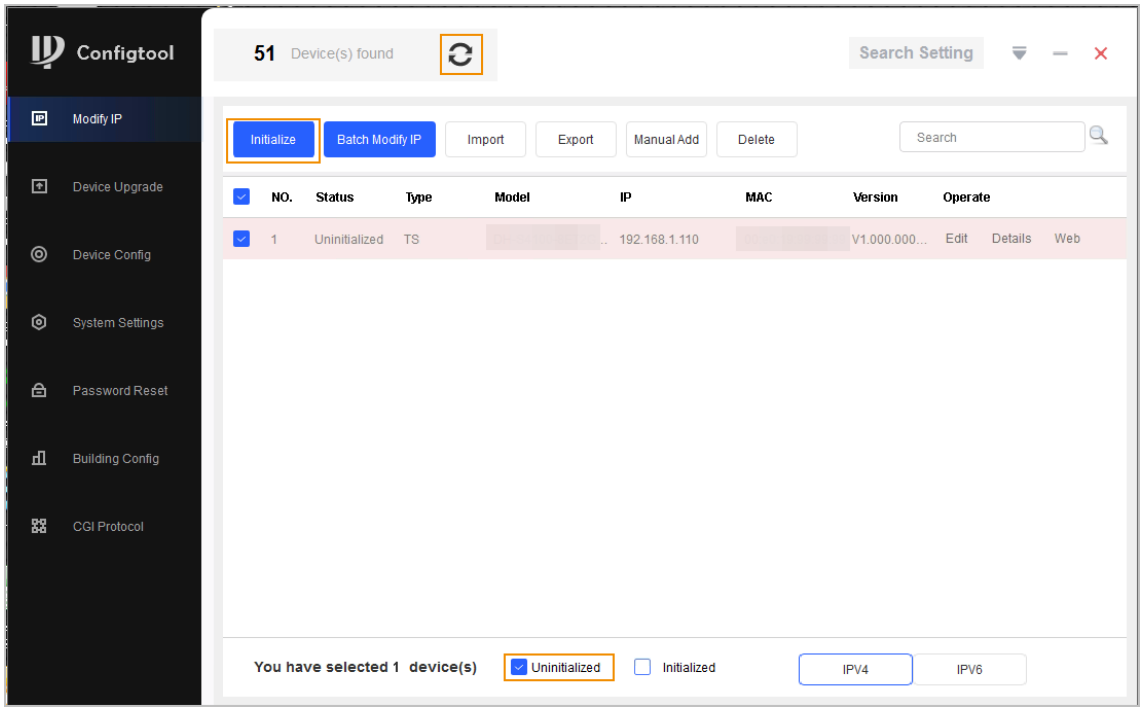
Paso 3 Ingrese la dirección IP inicial y la dirección IP final del segmento de red en el que desea buscar dispositivos y luego toque**DE ACUERDO**.

Figura 4-1 Configuración de búsqueda



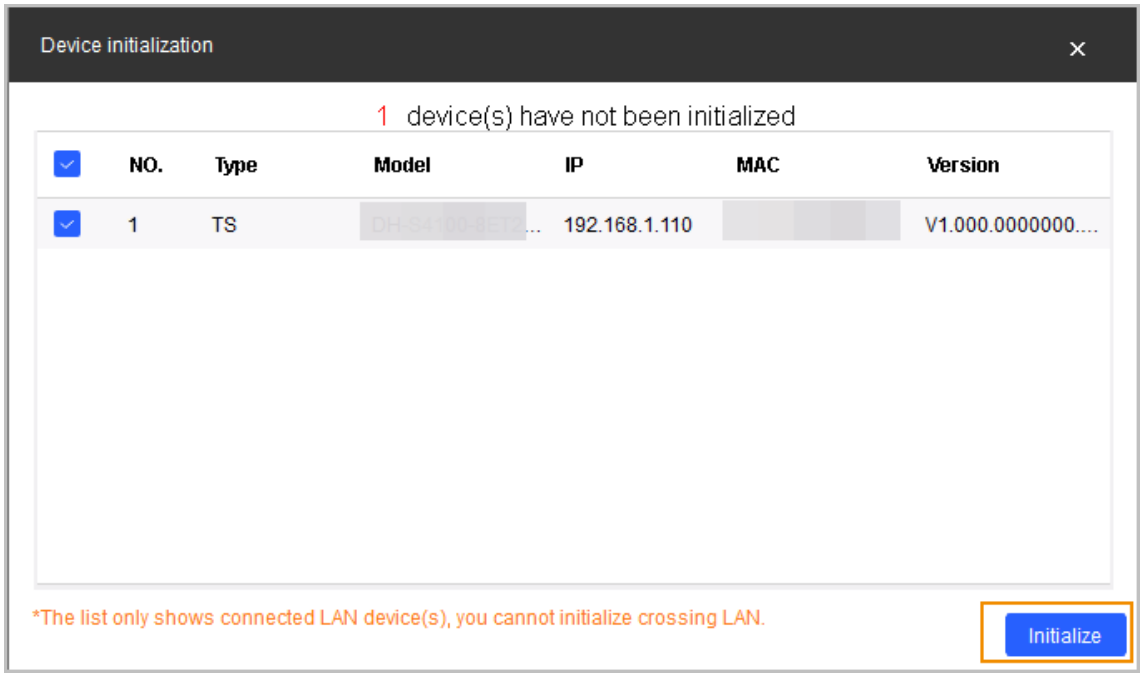
Etapa 4 Grifo sobre el**Modificar IP**pantalla y busque dispositivos en el segmento de red que han arreglado.

Figura 4-2 Buscar dispositivos



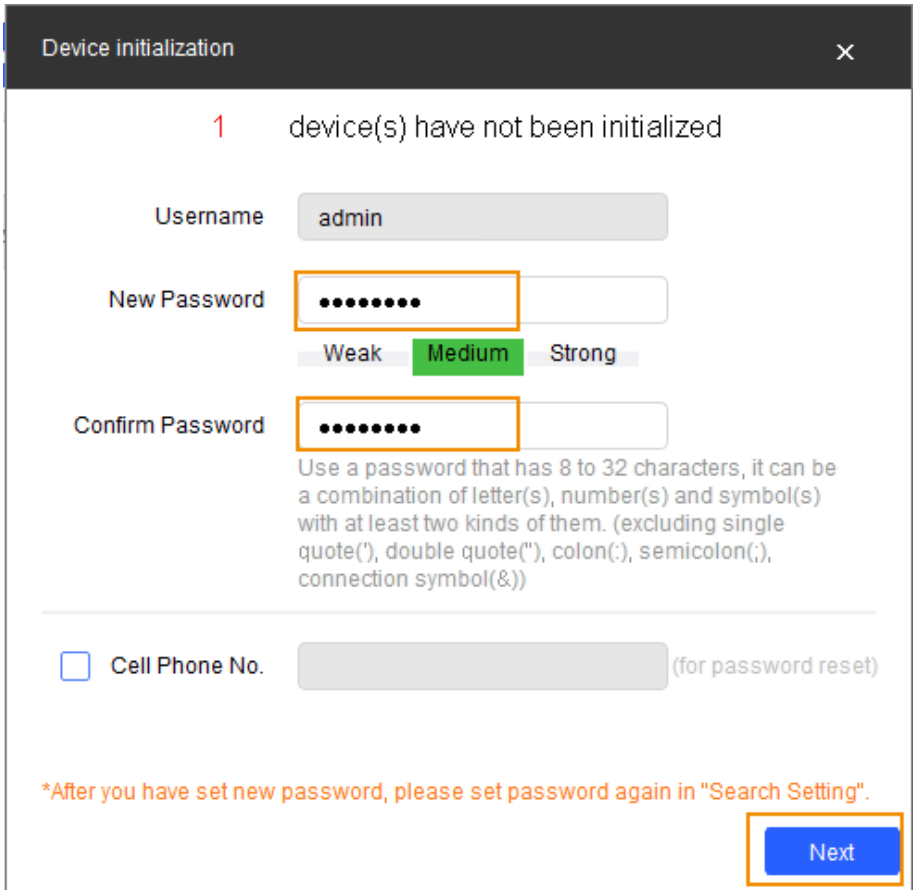
Paso 5 Seleccione los dispositivos que necesitan inicialización y luego toque**Inicializar**.

Figura 4-3 Inicialización



Paso 6 Configure y confirme la contraseña de los dispositivos, luego ingrese un número de teléfono celular válido y luego toque**Próximo**.

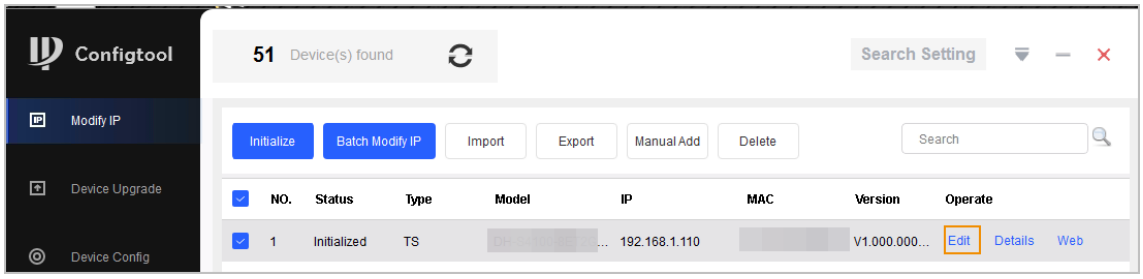
Figura 4-4 Establecer contraseña



Paso 7 Seleccione los dispositivos cuyas direcciones IP deben modificarse y luego toque**Modificar IP**. Grifo

Paso 8 **Editar**sobre el**Modificar IP**pantalla.

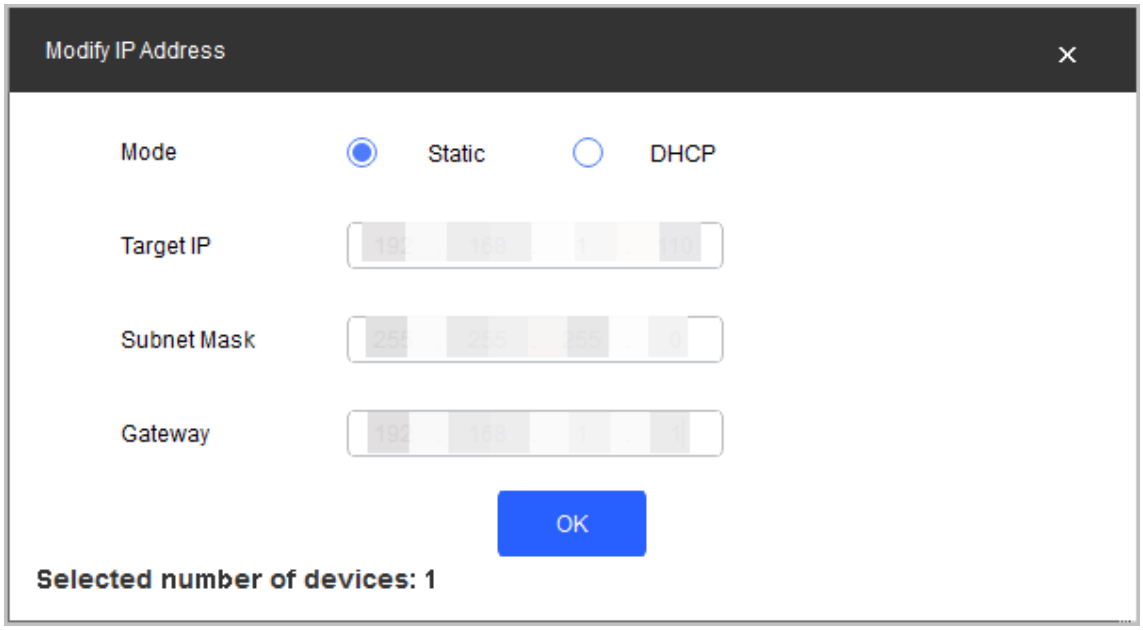
Figura 4-5 Modificar la dirección IP del dispositivo (1)



Paso 9 Grifo**Estático**modo y luego ingrese la IP de destino, la máscara de subred y la puerta de enlace.

La dirección IP de destino del Switch debe estar en el mismo segmento de red que la computadora.

Figura 4-6 Modificar la dirección IP del dispositivo (2)



Paso 10 Grifo**DE ACUERDO**.

4.2 Agregar el interruptor

Escanee el código QR y agregue el Switch a la aplicación DoLynk Care.

Procedimiento

Paso 1 Abra la aplicación DoLynk Care.

Paso 2 Grifo**+**en la esquina superior derecha del**Hogar**pantalla y escanee el código QR del Switch.

Figura 4-7 Escanee el código QR

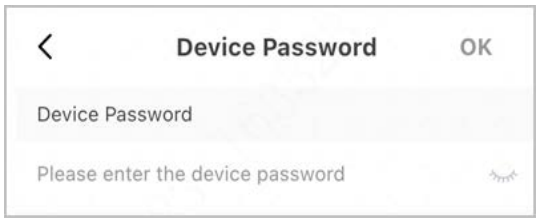
Paso 3 Si el Switch no se ha inicializado, debe ingresar la contraseña SC en la etiqueta y luego tocar**DE ACUERDO**.

Ingrese la contraseña del dispositivo y luego toque**DE ACUERDO**.

Si el Switch se ha inicializado, no necesita ingresar la contraseña SC. Introducir el

contraseña del dispositivo y luego toque**DE ACUERDO**.

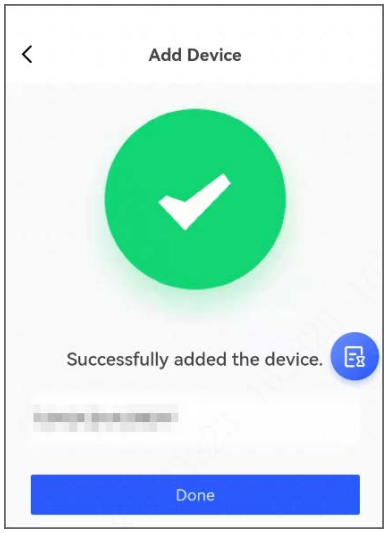
Figura 4-8 Ingrese la contraseña del dispositivo



Etapa 4 Grifo**Hecho**.

Seleccionar**A mí**>**AYUDA**>**Manual de usuario**en DoLynk Care para más detalles.

Figura 4-9 Complete la suma



5 Información relacionada

Escanee el código QR a continuación para obtener la aplicación DoLynk Care.

Figura 5-1 Aplicación DoLynk Care

Apéndice 1 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

1024–65535, 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 a la

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