Conmutador Ethernet (conmutador PoE administrado en la nube)

Guía de inicio rápido

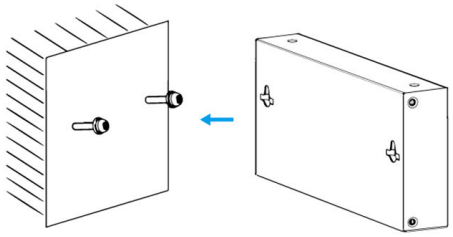
ZHEJIANG DAHUA VISIÓN TECNOLOGÍA CO., LTD. V1.0.0

[a] Los tornillos no vienen con el paquete. Cómprelos según sea necesario.

[a] Asegúrese de que la distancia entre los tornillos sea la distancia entre los orificios del montaje en pared (77,8 mm para un conmutador de 4 puertos y 128,4 mm para un conmutador de 8 puertos).

Paso 2 Alinee los orificios de montaje en pared en la cubierta posterior del Dispositivo con los tornillos y cuelgue el Dispositivo de los tornillos.

Figura 3-3 Montaje en pared



4 cableado

4.1 Conexión del cable GND

Información de contexto

La conexión GND normal del dispositivo es una garantía importante para la protección contra rayos y antiinterferencias del dispositivo.

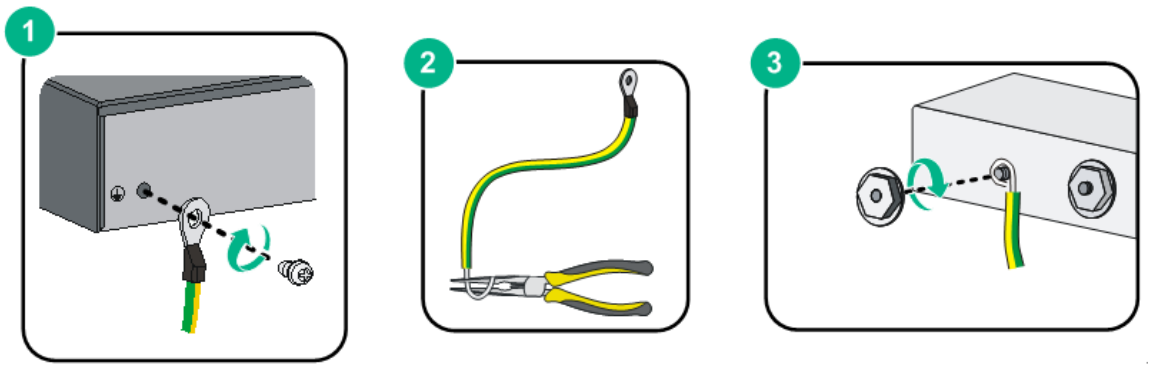
Procedimiento

Paso 1 Retire el tornillo de tierra del dispositivo y colóquelo correctamente. Pase el tornillo de tierra a través del orificio redondo del terminal OT del cable de tierra. Gire el tornillo de tierra en el sentido de las agujas del reloj con un destornillador de estrella para fijar el terminal OT del cable de tierra.

Paso 2 Enrolle el otro extremo del cable de tierra formando un círculo con unos alicates de punta fina.

Paso 3 Conecte el otro extremo del cable de tierra a la barra de tierra, gire la tuerca hexagonal en el sentido de las agujas del reloj con una llave para sujetar el otro extremo del cable de tierra al terminal de tierra.

Figura 4-1 Conexión GND



4.2 Conexión del cable de alimentación

Información de contexto

Antes de conectar el cable de alimentación, asegúrese de que el dispositivo esté conectado a tierra de manera confiable.

Procedimiento

Paso 1 Conecte con precisión un extremo del cable de alimentación al conector de alimentación del dispositivo.

Paso 2 Conecte el otro extremo del cable de alimentación a la toma de corriente externa.

4.3 Conexión del puerto Ethernet

El puerto Ethernet adopta el puerto RJ-45 estándar. Con función de autoadaptación, se puede configurar automáticamente en modo de operación full duplex/half-duplex. Admite el autorreconocimiento MDI/MDI-X del cable, por lo tanto, puede utilizar un cable cruzado o un cable directo para conectar el dispositivo terminal al dispositivo de red.

Figura 4-2 Número de pin del puerto Ethernet

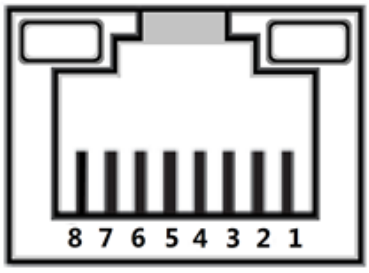
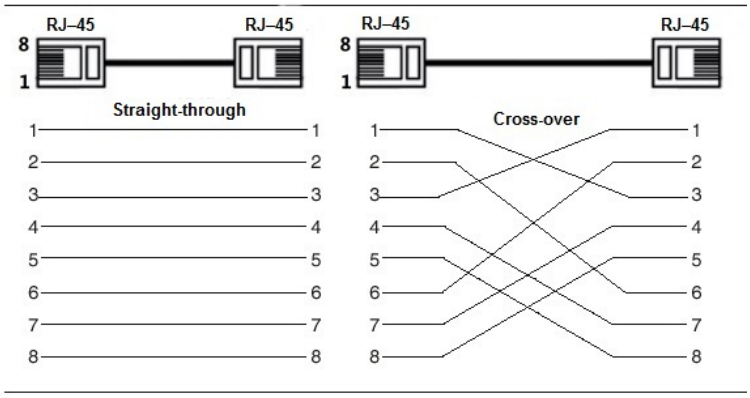


Figura 4-3 Descripción de pines



La conexión del cable del conector RJ-45 se ajusta al estándar 568B (1 naranja blanco, 2 naranja, 3 verde blanco, 4 azul, 5 azul blanco, 6 verde, 7 marrón blanco, 8 marrón) .

4.4 Conexión del puerto Ethernet SFP

- Al instalar el módulo óptico SFP, no toque el dedo dorado del módulo óptico SFP.
- No retire el tapón antipolvo del módulo óptico SFP antes de conectar la fibra óptica.
- No inserte directamente el módulo óptico SFP en la ranura mientras la fibra óptica esté insertada en ella. Desenchufe la fibra óptica antes de instalarla.

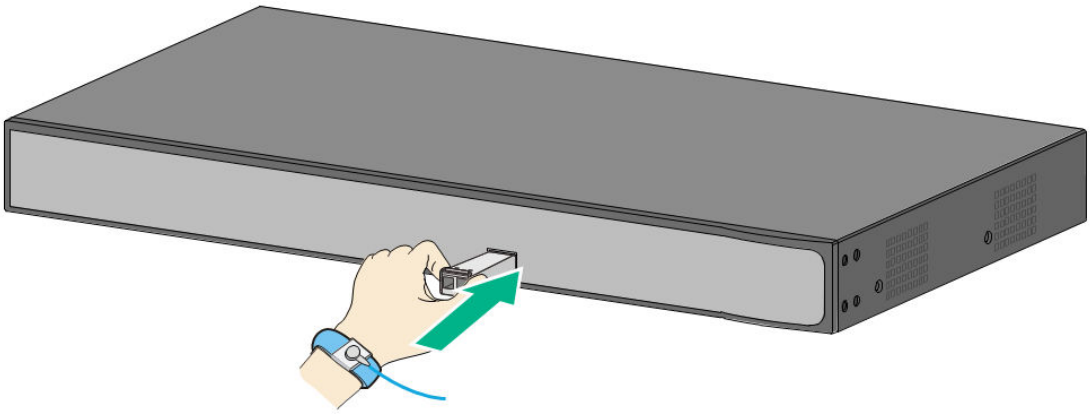
Procedimiento

Paso 1 Use la pulsera antiestática y confirme que esté en buen contacto con su piel y que el dispositivo esté conectado a tierra de manera confiable.

Paso 2 Levante verticalmente el asa del módulo óptico SFP y sujete el módulo óptico por ambos lados con las manos.

Paso 3 Empuje el módulo óptico suavemente dentro de la ranura en dirección horizontal hasta que el módulo óptico SFP esté firmemente conectado a la ranura.

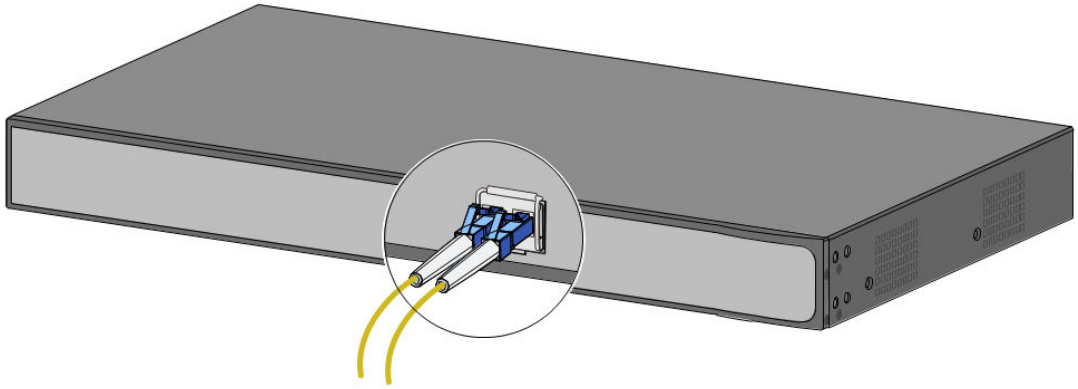
Figura 4-4 Instalar el módulo SFP



Etapa 4 Retire la tapa antipolvo del conector LC de la fibra óptica y el tapón antipolvo del módulo óptico SFP.

Paso 5 Conecte el conector LC de la fibra óptica al módulo óptico SFP.

Figura 4-5 Conexión de fibra óptica



4.5 Conexión del puerto Ethernet PoE

Puede conectar directamente el puerto Ethernet PoE del dispositivo al puerto Ethernet PoE del conmutador a través del cable de red para lograr una conexión de red y una fuente de alimentación sincronizadas. Con**Modo extendido** desactivado, la distancia máxima entre el interruptor y el Dispositivo es de unos 100 m.

Al conectarse a un dispositivo que no sea PoE, el dispositivo debe usarse con una fuente de alimentación aislada.

5 Inicialización y adición del dispositivo

5.1 Inicializando el dispositivo

- Puede utilizar la aplicación DoLynk Care para escanear el código QR del dispositivo y luego agregar e inicializar el dispositivo cuando esté conectado a Internet.
- Puede iniciar sesión en la página web para inicializar el Dispositivo y modificar la dirección IP cuando el Dispositivo no está conectado a Internet.

- La inicialización del dispositivo es necesaria para el uso por primera vez o después de que se haya reiniciado el dispositivo.
- El cliente DHCP está habilitado de forma predeterminada. Si no se asigna ninguna dirección IP, se puede utilizar la dirección IP predeterminada. (Consulte la etiqueta del dispositivo, generalmente 192.168.1.110).
- La inicialización del dispositivo está disponible solo cuando el dispositivo y la computadora están en el mismo segmento de red.
- Planifique el segmento de red correctamente para conectar el Dispositivo a la red.
- Diferentes modelos admiten diferentes métodos de inicialización local. Para más detalles, consulte las especificaciones técnicas.
- La inicialización de páginas web solo se admite en modelos parciales.

5.2 Inicialización de la página web

Puede iniciar sesión en el dispositivo a través de la página web para su administración y operación. Para obtener más información, consulte el manual de funcionamiento web.

El Dispositivo no tiene contraseña inicial. Puede configurar su contraseña de acuerdo con las indicaciones de la página web cuando inicia sesión por primera vez e inicializa el dispositivo.

5.3 Agregar el dispositivo

Agregue rápidamente el Dispositivo a DoLynk Care escaneando el código QR o ingresando manualmente el SN en el Dispositivo.

Procedimiento

Paso 1 Descargue y active DoLynk Care y luego toque**+Añadir dispositivo**.

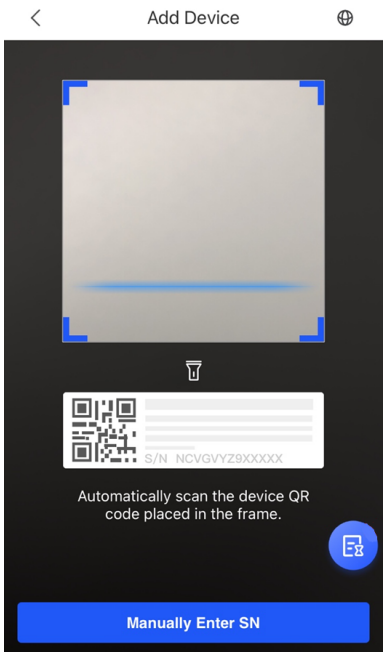
Figura 5-1 Aplicación DoLynk Care

Para más detalles, ver*Manual del usuario de DoLynk Care*.

Paso 2 Grifo**+**en la esquina superior derecha del**Hogar**pantalla, seleccione**Escanee el código para agregar**,y luego toque**Próximo**.

Puede escanear el código QR para obtener el SN o ingresar el SN manualmente.

Figura 5-2 Escanee el código QR



Paso 3 Seleccionar**Cambiar**y seleccione un sitio, y luego toque**DE ACUERDO**.

Si no hay ningún sitio, toque y luego seleccione un sitio.

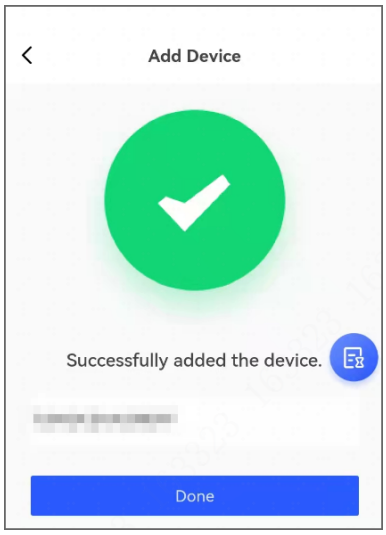
Etapa 4 Si el Dispositivo no ha sido inicializado, podrá modificar el Código SC como contraseña inicial en la etiqueta. Ingrese la contraseña del dispositivo y luego toque**Ahorrar**.

Si el dispositivo se ha inicializado, ingrese la contraseña del dispositivo y luego toque**Ahorrar**.

Figura 5-3 Ingrese la contraseña del dispositivo

Paso 5 Grifo**Hecho**.

Figura 5-4 Agregar dispositivo



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

Apéndice 1 Compromiso de seguridad y Recomendación

Dahua Vision Technology Co., Ltd. (en lo sucesivo, "Dahua") concede gran importancia a la ciberseguridad y la protección de la privacidad, y continúa invirtiendo fondos especiales para mejorar integralmente la conciencia y las capacidades de seguridad de los empleados de Dahua y proporcionar una seguridad adecuada para los productos. Dahua ha establecido un equipo de seguridad profesional para brindar potenciación y control de seguridad del ciclo de vida completo para el diseño, desarrollo, prueba, producción, entrega y mantenimiento de productos. Si bien se adhieren al principio de minimizar la recopilación de datos, minimizar los servicios, prohibir la implantación de puertas traseras y eliminar servicios innecesarios e inseguros (como Telnet), los productos Dahua continúan introduciendo tecnologías de seguridad innovadoras y se esfuerzan por mejorar las capacidades de garantía de seguridad del producto, brindando servicios globales. usuarios con alarma de seguridad y servicios de respuesta a incidentes de seguridad 24 horas al día, 7 días a la semana para proteger mejor los derechos e intereses de seguridad de los usuarios. Al mismo tiempo, Dahua alienta a los usuarios, socios, proveedores, agencias gubernamentales, organizaciones industriales e investigadores independientes a informar cualquier riesgo o vulnerabilidad potencial descubierto en los dispositivos Dahua a Dahua PSIRT. Para conocer métodos de informes específicos, consulte la sección de seguridad cibernética de Dahua. página web oficial.

La seguridad del producto requiere no sólo la atención y los esfuerzos continuos de los fabricantes en I+D, producción y entrega, sino también la participación activa de los usuarios que pueden ayudar a mejorar el entorno y los métodos de uso del producto, a fin de garantizar mejor la seguridad de los productos después de su fabricación. se ponen en uso. Por este motivo, recomendamos que los usuarios utilicen el dispositivo de forma segura, lo que incluye, entre otros:

Administración de cuentas

1.**Utilice contraseñas complejas**

Consulte las siguientes sugerencias para establecer contraseñas:

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

2.**Cambiar contraseñas periódicamente**

Se recomienda cambiar periódicamente la contraseña del dispositivo para reducir el riesgo de que la adivinen o la descifren.

3.Asigne cuentas y permisos adecuadamente

Agregue usuarios adecuadamente según los requisitos de servicio y administración y asigne conjuntos de permisos mínimos a los usuarios.

4.**Habilitar la función de bloqueo de cuenta**

La función de bloqueo de cuenta está habilitada de forma predeterminada. Se recomienda mantenerlo habilitado para proteger la seguridad de la cuenta. Después de varios intentos fallidos de contraseña, la cuenta correspondiente y la dirección IP de origen se bloquearán.

5.**Establecer y actualizar la información de restablecimiento de contraseña de manera oportuna**

El dispositivo Dahua admite la función de restablecimiento de contraseña. Para reducir el riesgo de que esta función sea utilizada por actores de amenazas, si hay algún cambio en la información, modifíquelo a tiempo. Al establecer preguntas de seguridad, se recomienda no utilizar respuestas fáciles de adivinar.

Configuración del servicio

1.**Habilitar HTTPS**

Se recomienda habilitar HTTPS para acceder a servicios web a través de canales seguros.

2.**Transmisión cifrada de audio y vídeo.**

Si el contenido de sus datos de audio y video es muy importante o confidencial, le recomendamos utilizar la función de transmisión cifrada para reducir el riesgo de que sus datos de audio y video sean interceptados durante la transmisión.

3.**Apague los servicios no esenciales y use el modo seguro**

Si no es necesario, se recomienda desactivar algunos servicios como SSH, SNMP, SMTP, UPnP, punto de acceso AP, etc., para reducir las superficies de ataque.

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

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

4.**Cambiar HTTP y otros puertos de servicio predeterminados**

Se recomienda cambiar el puerto predeterminado de HTTP y otros servicios a cualquier puerto entre 1024 y 65535 para reducir el riesgo de que los actores de amenazas lo adivinen.

configuración de la red

1.**Habilitar lista de permitidos**

Se recomienda activar la función de lista de permitidos y solo permitir que IP en la lista de permitidos acceda al dispositivo. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del dispositivo compatible a la lista de permitidos.

2.**Enlace de dirección MAC**

Se recomienda vincular la dirección IP de la puerta de enlace a la dirección MAC del dispositivo para reducir el riesgo de suplantación de ARP.

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

Para garantizar mejor la seguridad de los dispositivos y reducir los posibles riesgos cibernéticos, se recomienda lo siguiente:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa;
- Particione la red de acuerdo con las necesidades reales de la red: si no hay demanda de comunicación entre las dos subredes, se recomienda utilizar VLAN, puerta de enlace y otros métodos para particionar la red y lograr el aislamiento de la red;
- Establecer un sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso ilegal de terminales a la red privada.

Auditoría de seguridad

1.**Verificar usuarios en línea**

Se recomienda comprobar periódicamente a los usuarios en línea para identificar a los usuarios ilegales.

2.**Verificar el registro del dispositivo**

Al ver los registros, puede obtener información sobre las direcciones IP que intentan iniciar sesión en el dispositivo y las operaciones clave de los usuarios registrados.

3.**Configurar el registro de red**

Debido a la capacidad de almacenamiento limitada de los dispositivos, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, 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.

Seguridad del software

1.**Actualice el firmware a tiempo**

De acuerdo con las especificaciones operativas estándar de la industria, el firmware de los dispositivos debe actualizarse a la última versión a tiempo para garantizar que el dispositivo tenga las últimas funciones y seguridad. Si el dispositivo está conectado a la red pública, se recomienda habilitar la función de detección automática de actualización en línea, para obtener la información de actualización del firmware publicada por el fabricante de manera oportuna.

2.**5.2 Actualizar el software del cliente a tiempo**

Le recomendamos descargar y utilizar el software de cliente más reciente.

Protección física

Se recomienda llevar a cabo protección física para los dispositivos (especialmente los dispositivos de almacenamiento), como colocar el dispositivo en una sala de máquinas y un gabinete dedicados, y tener control de acceso y administración de claves para evitar que personal no autorizado dañe el hardware y otros equipos periféricos. (por ejemplo, disco flash USB, puerto serie).