Estuche para videoportero y control de acceso

Guía de inicio rápido

Versión 1.0.0

Prefacio

General

Este manual presenta el aspecto, las características y la conexión de cables de la carcasa para videoportero y control de acceso.

Instrucciones de seguridad

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

Palabras de advertencia	Significado
Nota	Proporciona información adicional como énfasis y complemento del texto.
PRECAUCIÓN	Indica un riesgo potencial que, de no evitarse, podría ocasionar daños materiales, pérdida de datos, menor rendimiento o resultados impredecibles.

Historial de revisiones

Versión	Contenido de la revisión	Fecha de lanzamiento
Versión 1.0.0	Primer lanzamiento.	Mayo de 2020

Acerca del manual

- Este manual es solo para referencia. En caso de discrepancia entre el manual y el producto real, prevalecerá el producto real.
- No nos hacemos responsables de las pérdidas ocasionadas por operaciones que no cumplan con el
- manual. El manual se actualizará conforme a las leyes y regulaciones vigentes en las jurisdicciones correspondientes. Para obtener información detallada, consulte el manual impreso, el CD-ROM, el código QR o nuestro sitio web oficial. En caso de discrepancia entre el manual impreso y la versión electrónica, prevalecerá esta última.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto podrían causar algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Podría haber variaciones en los datos técnicos, las funciones y la descripción de operaciones, o errores de impresión. En caso de duda o disputa, nos reservamos el derecho a la interpretación final. Actualice el software
- del lector o pruebe con otro software de lectura compatible si no puede abrir el manual (en formato PDF).

- Todas las marcas comerciales, marcas registradas y nombres de empresas que aparecen en este manual son propiedad de sus respectivos dueños.
- Por favor, visite nuestra página web, póngase en contacto con el proveedor o con el servicio de atención al cliente si surge algún problema al utilizar el dispositivo.
- En caso de duda o controversia, nos reservamos el derecho a la explicación final.

Medidas de seguridad y advertencias importantes

La siguiente descripción corresponde al método de aplicación correcto del dispositivo. Lea atentamente el manual antes de usarlo para evitar peligros y daños materiales. Siga estrictamente las instrucciones del manual durante su uso y consérvelo en buen estado después de leerlo.

Requisitos de funcionamiento

- No coloque ni instale el dispositivo en un área expuesta a la luz solar directa ni cerca de ningún dispositivo que genere calor.
- No instale el dispositivo en un área húmeda, polvorienta o fuliginosa.
- Manténgalo instalado en posición horizontal o en lugares estables y evite que se caiga. No derrame
- ni salpique líquidos sobre el dispositivo; no coloque sobre él objetos que contengan líquidos para evitar que estos penetren en su interior.
- Instale el dispositivo en lugares bien ventilados; no obstruya su abertura de ventilación. Utilice el
- dispositivo únicamente dentro del rango de entrada y salida nominal.
- No desmonte el dispositivo arbitrariamente.
- El dispositivo deberá utilizarse con cables de red apantallados.

Requisitos de energía

- ¡Utilice los cables eléctricos (cables de alimentación) recomendados para esta zona, que deberán utilizarse dentro de sus especificaciones nominales!
- Utilice una fuente de alimentación que cumpla con los requisitos SELV (tensión extra baja de seguridad) y suministre energía con una tensión nominal que cumpla con la norma Fuente de alimentación limitada IEC60950-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas del dispositivo.
- El acoplador del aparato es un dispositivo de desconexión. Durante su uso normal, manténgalo en un ángulo que facilite su funcionamiento.
- No desconecte la alimentación durante la actualización del dispositivo. La alimentación solo se puede desconectar una vez que el dispositivo haya completado la actualización y se haya reiniciado.

Tabla de contenido

1 Apariencia

Figure 1-1 Apariencia

2 Resumen

2.1 Introducción

El videoportero y los dispositivos de control de acceso se pueden alojar en el maletín y conectar a la corriente eléctrica. Puede transportar el maletín para promocionar productos a clientes en demostraciones de soluciones, ferias y otros eventos. Este maletín ofrece una gran comodidad a los comerciales.

2.2 Características

- Con forma de maleta, portátil.
- Fabricado en aleación de aluminio; marcos y esquinas resistentes.
- Ruedas multidireccionales y sistema de frenado.
- La superficie de acrílico negro le da un aspecto más brillante a la maleta.
- Asa telescópica.
- Dos asas.

Conexión de 3 cables

3.1 Cables

Figure 3-1 Cable de conexión

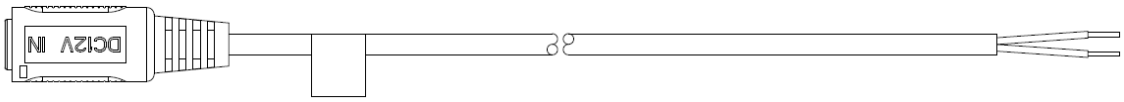
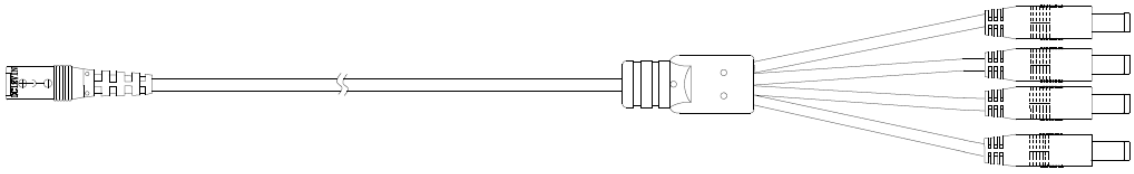


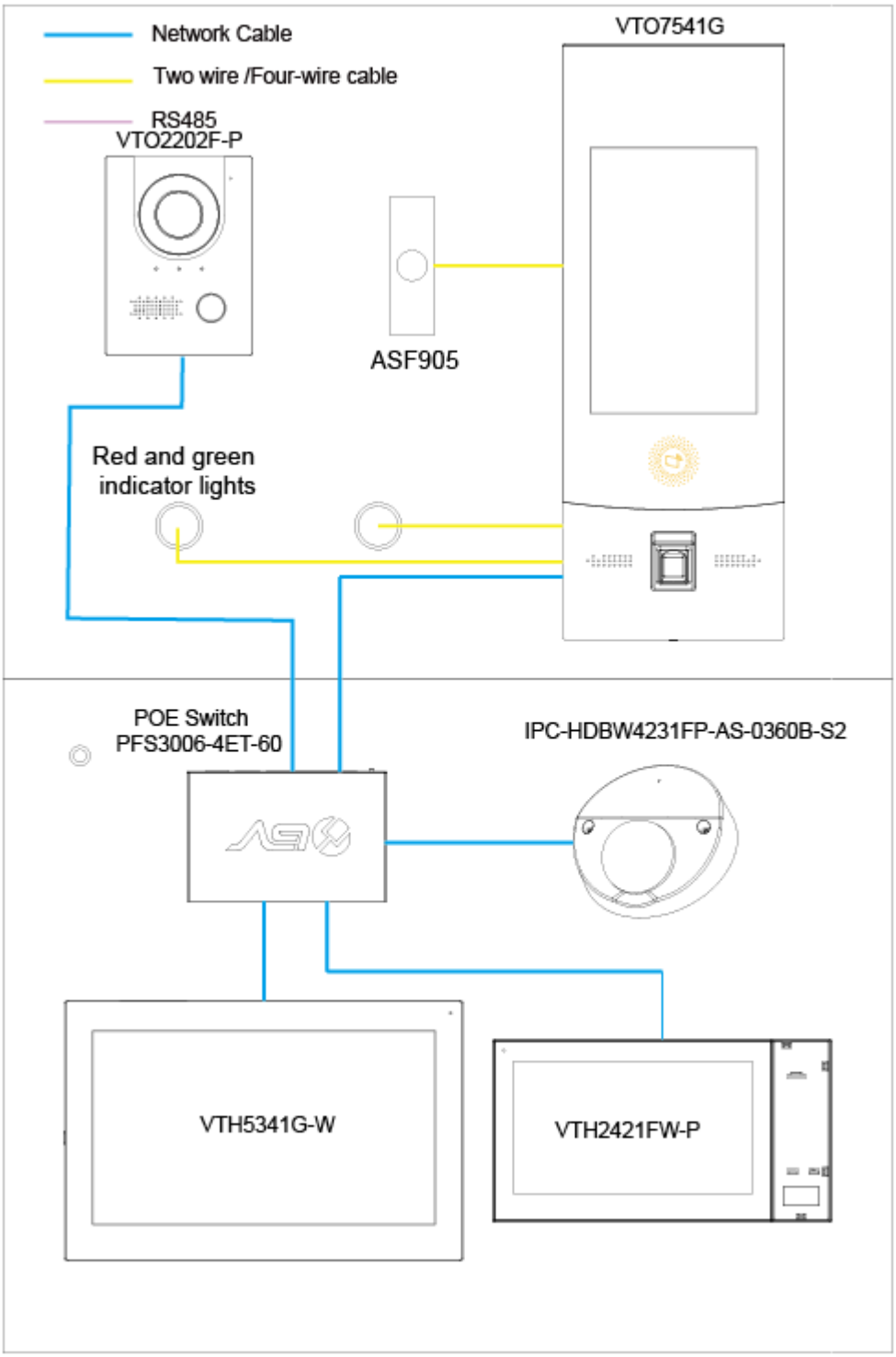
Figure 3-2 cable de alimentación de 4 puertos



3.2 Conexión de cable para videoportero

Cable de conexión para videoportero (1)

Figure 3-3 Conexión del cable del videoportero (1)



Si la luz indicadora está roja, significa que la puerta está cerrada; si la luz indicadora está verde, significa que la puerta está desbloqueada.

Step 1 Conecte el primer cable de alimentación de 4 puertos al puerto de alimentación situado en la placa acrílica de la parte inferior de la carcasa.

Step 2 Conecte un puerto del cable de alimentación de 4 puertos mencionado en el paso 1 al IPC-HDBW4231FP-AS-0360B-S2 y, a continuación, conecte otro puerto al segundo cable de alimentación de 4 puertos (incluido con la carcasa) para alimentar la estación de puerta VTO7541G. Conecte un

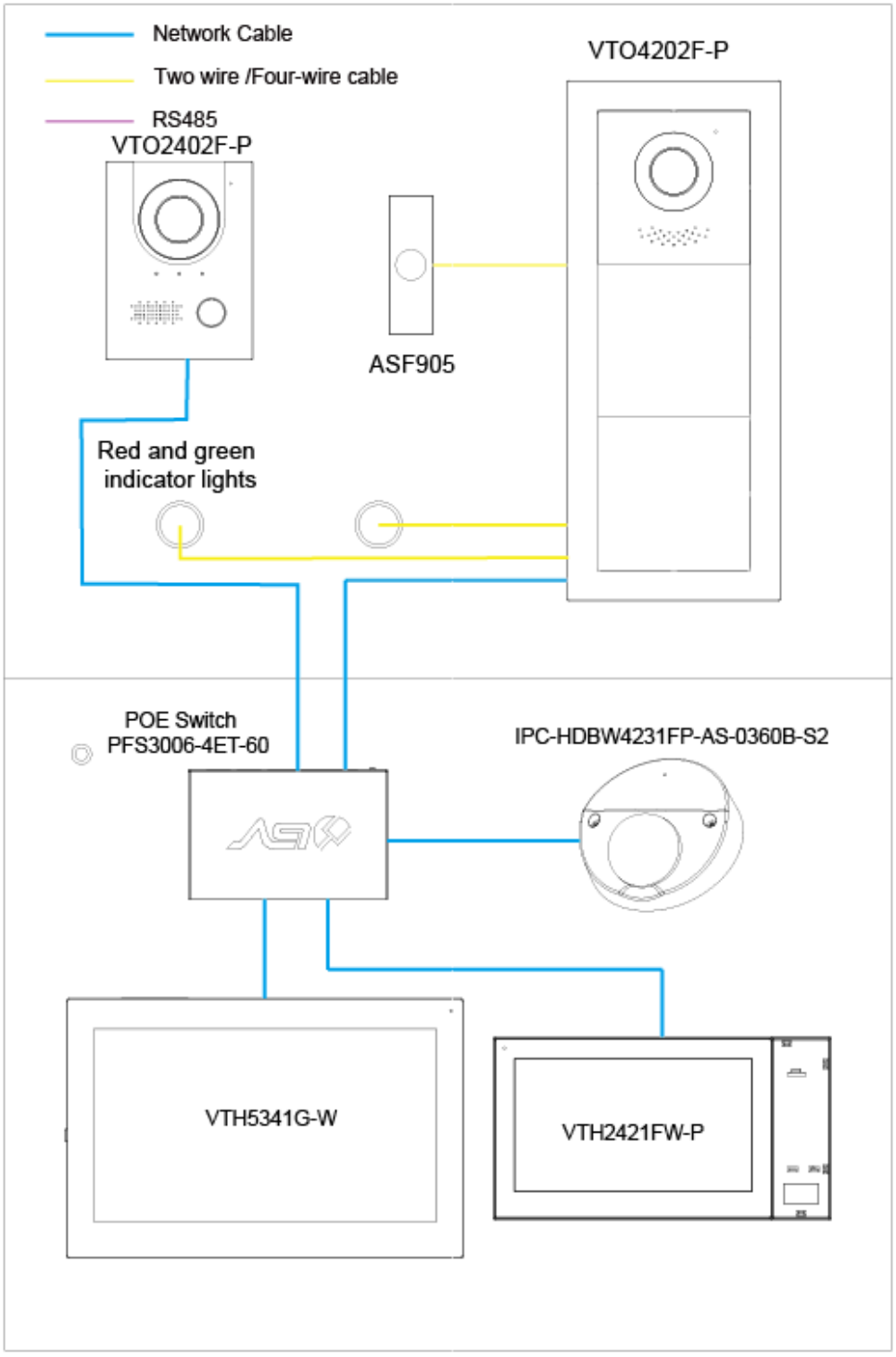
Step 3 puerto del segundo cable de alimentación de 4 puertos al cable de conexión, utilice los cables de alimentación negro y rojo para alimentar los indicadores LED rojo y verde, conecte ambos indicadores LED a la estación de puerta VTO7541G y, por último, conecte el botón de salida a la VTO7541G mediante los cables de alimentación negro y rojo.

Para la conexión por cable de las luces indicadoras y los botones de salida, consulte la guía de inicio rápido de Estación de puerta VTO7541G.

Step 4 Conecte los cinco cables de red a los dos monitores interiores, una estación de puerta, una estación de villa y un IPC.

Cable de conexión para videoportero (2)

Figure 3-4 Conexión de cable para videoportero (2)



Si la luz indicadora está roja, significa que la puerta está cerrada; si la luz indicadora está verde, significa que la puerta está desbloqueada.

Step 1 Conecte el primer cable de alimentación de 4 puertos al puerto de alimentación situado en la placa acrílica de la parte inferior de la carcasa.

Step 2 Conecte un puerto del cable de alimentación de 4 puertos mencionado en el Paso 1 a IPC-HDBW4231FP-AS-0360B-S2.

Step 3 Conecte otro puerto del cable de alimentación de 4 puertos al cable de conexión, usando los cables negro y rojo.

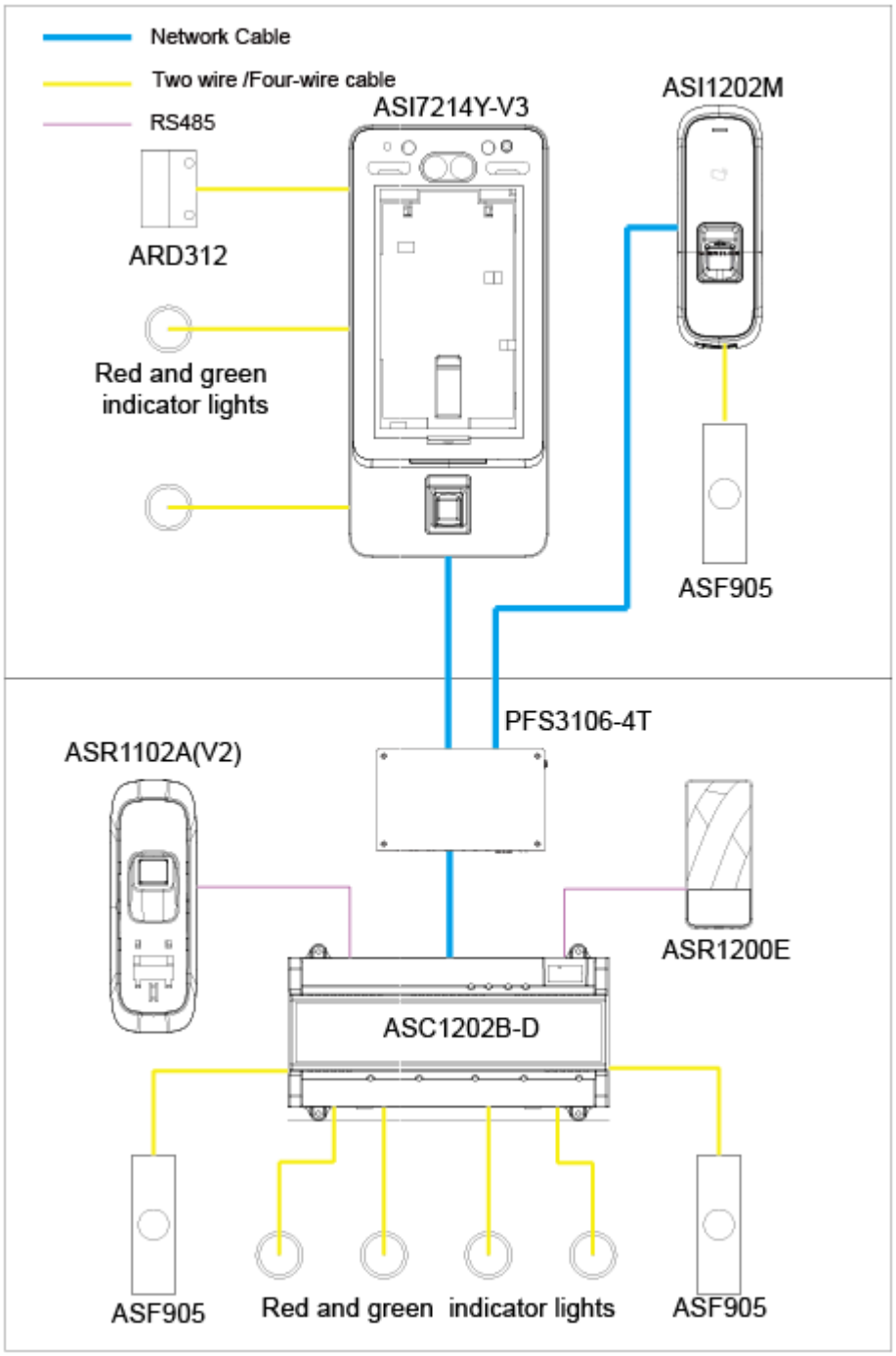
Conecte el cable de alimentación para alimentar las luces indicadoras roja y verde, conecte las dos luces indicadoras a la estación de puerta VTO4202F-P y, a continuación, conecte el botón de salida a la VTO4202F-P utilizando el cable de alimentación negro y rojo.

Para la conexión por cable de las luces indicadoras y los botones de salida, consulte la guía de inicio rápido de Estación de puerta VTO4202F-P.

Step 4 Conecte los cinco cables de red a los dos monitores interiores, una estación de puerta, una estación de villa y un IPC.

3.3 Conexión de cable del dispositivo de control de acceso

Figure 3-5 Conexión de cable de control de acceso



Si la luz indicadora está roja, significa que la puerta está cerrada; si la luz indicadora está verde, significa que la puerta está desbloqueada.

Step 1 Conecte el primer cable de alimentación de 4 puertos al puerto de alimentación situado en la placa acrílica de la parte inferior de la carcasa.

Step 2 Conecte un puerto del cable de alimentación de 4 puertos mencionado en el Paso 1 al segundo cable de alimentación de 4 puertos y luego conecte el segundo cable de alimentación de 4 puertos al controlador de acceso ASI7214Y-V3.

Step 3 Conecte los otros tres puertos del cable de alimentación de 4 puertos al cable de conexión, utilice el cable de alimentación negro y rojo para proporcionar energía al controlador de acceso ASI1202M y a las luces indicadoras roja y verde, y luego conecte las dos luces indicadoras al controlador de acceso ASI7214Y-V3.

Para la conexión del cable de la luz indicadora, consulte la guía de inicio rápido del acceso ASI7214Y-V. controlador.

Step 4 Conecte el controlador de acceso modelo ASI7214Y-V3, ASI1202M y ASC1202B-D al switch PFS3005-5ET-L con los tres cables de red.

Step 5 Conecte los dos cables de alimentación de 4 puertos al puerto de alimentación en la placa acrílica de la parte inferior de la carcasa y luego utilice dos de los puertos para conectar el controlador de acceso ASR1200E y ASR1102A(V2) al cable de conexión.

Step 6 Utilice los otros puertos, cables de alimentación y el cable de alimentación negro y rojo para proporcionar energía al controlador de acceso ASC1202B-D y a las cuatro luces indicadoras rojas y verdes, y luego conecte las cuatro luces indicadoras al controlador de acceso ASC1202B-D.

Para la conexión del cable de la luz indicadora, consulte la guía de inicio rápido del acceso al ASC1202B-D. controlador.

Step 7 Conecte los puertos RS-485 de los controladores de acceso del modelo ASR1200E y ASR1102A(V2) al puerto RS-485 del controlador de acceso del modelo ASC1202B-D.

Para la conexión del cable RS-485, consulte la guía de inicio rápido del acceso ASC1202B-D. controlador.

Step 8 Conecte los dos botones de salida del modelo ASF905 al controlador de acceso del modelo ASC1202B-D con el cable de alimentación negro y rojo, y luego conecte un botón de salida del modelo ASF905 a ASI1202M con el cable de alimentación negro y rojo.

Para la conexión del cable del botón de salida del modelo ASF905, consulte la guía de inicio rápido de ASC1202B-D y ASI1202M.

Appendix 1 Recomendaciones de ciberseguridad

La ciberseguridad es más que una simple tendencia: afecta 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 vulnerables a los ataques. A continuación, encontrará algunos consejos y recomendaciones para crear un sistema de seguridad más seguro.

Medidas obligatorias para la seguridad de la red de equipos básicos: 1.

Utilizar contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de caracteres; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;
- No contenga el nombre de la cuenta ni el nombre de la cuenta en orden
- inverso; No utilice caracteres consecutivos, 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 sus equipos (como NVR, DVR, cámaras IP, etc.) para garantizar que el sistema cuente con los últimos parches y correcciones de seguridad. Cuando el equipo esté conectado a la red pública, se recomienda habilitar la función de "búsqueda automática de actualizaciones" para obtener información oportuna sobre las actualizaciones de firmware publicadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software cliente.

Recomendaciones útiles para mejorar la seguridad de su red de equipos: 1.

Protección física

Le sugerimos que proteja físicamente los equipos, especialmente los dispositivos de almacenamiento. Por ejemplo, coloque los equipos en una sala de servidores y un armario específicos, e implemente un control de acceso y una gestión de claves adecuados para evitar que personal no autorizado realice manipulaciones físicas que puedan dañar el hardware o conectar dispositivos extraíbles (como memorias USB o puertos serie).

2. Cambia tus contraseñas regularmente.

Le sugerimos que cambie sus contraseñas regularmente para reducir el riesgo de que las adivinen o las descifren.

3. Establezca y actualice la información de restablecimiento de contraseñas oportunamente.

El equipo admite la función de restablecimiento de contraseña. Configure a tiempo la información necesaria para el restablecimiento de contraseña, incluyendo el correo electrónico del usuario y las preguntas de seguridad. Si esta información cambia, modifíquela de inmediato. Al configurar las preguntas de seguridad, se recomienda no utilizar preguntas fáciles de adivinar.

4. Habilitar el bloqueo de cuenta

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

5. Cambiar los puertos HTTP y de otros servicios predeterminados

Le sugerimos que cambie los puertos HTTP y de otros servicios predeterminados por cualquier conjunto de números.

entre 1024~65535, reduciendo el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.

6. Habilitar HTTPS

Le sugerimos que habilite HTTPS para que pueda acceder al servicio web a través de un canal de comunicación seguro.

7. Habilitar la lista blanca

Le sugerimos que active la función de lista blanca para impedir el acceso al sistema a todos los usuarios, excepto a aquellos con direcciones IP específicas. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la del equipo conectado a la lista blanca.

8. Vinculación de direcciones MAC

Le recomendamos que vincule la dirección IP y la dirección MAC de la puerta de enlace al equipo, reduciendo así el riesgo de suplantación de ARP.

9. Asignar cuentas y privilegios de manera razonable

De acuerdo con los requisitos empresariales y de gestión, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

10. Desactive los servicios innecesarios y elija modos seguros.

Si no son necesarios, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir riesgos.

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

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

11. Transmisión encriptada de audio y vídeo

Si el contenido de sus datos de audio y vídeo 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 vídeo sean robados durante la transmisión.

Recordatorio: la transmisión cifrada provocará cierta pérdida de eficiencia en la transmisión.

12. Auditoría segura

- Comprueba los usuarios conectados: te sugerimos que compruebes periódicamente los usuarios conectados para ver si el dispositivo ha iniciado sesión sin autorización.
- Revisa el registro del equipo: Al consultar los registros, puedes conocer las direcciones IP que se utilizaron para iniciar sesión en tus dispositivos y sus operaciones clave.

13. Registro de red

Debido a la capacidad limitada de almacenamiento del equipo, 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 se sincronicen con el servidor de registro de red para su seguimiento.

14. Construir un entorno de red seguro

Para garantizar mejor la seguridad de los equipos y reducir los posibles riesgos cibernéticos, recomendamos:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa.
- La red debe particionarse y aislarse según las necesidades reales de la red. Si no existen requisitos de comunicación entre dos subredes, se sugiere utilizar VLAN, Network GAP y otras tecnologías para particionar la red.

para 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.