Terminal de reconocimiento facial

Guía de inicio rápido

V1.0.0

Prefacio

General

Este manual presenta la instalación y las operaciones básicas del terminal de reconocimiento facial (en adelante, "terminal").

Las instrucciones de seguridad

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

Palabras de advertencia	Sentido
PELIGRO	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
ADVERTENCIA	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría resultar en daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
CONSEJOS	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
NOTA	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de la revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	Septiembre de 2020

Acerca del manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No nos hacemos responsables de ninguna pérdida ocasionada por las operaciones que no cumplan con el
- manual. El manual se actualizaría de acuerdo con las leyes y regulaciones más recientes de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si existe inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden 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.
- Todavía puede haber desviaciones en los datos técnicos, las funciones y la descripción de las operaciones, o errores en la impresión. Si hay alguna duda o disputa, nos reservamos el derecho a una explicación final.

- Actualice el software del lector o pruebe con otro software de lectura convencional si no puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y los nombres de empresas que aparecen en el manual son propiedad de sus respectivos propietarios.
- Visite nuestro sitio web, póngase en contacto con el proveedor o el servicio de atención al cliente si surge algún problema al utilizar el dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho a una explicación final.

Advertencias y medidas de seguridad importantes

Este capítulo describe el contenido que cubre el manejo adecuado del terminal, la prevención de peligros y la prevención de daños a la propiedad. Lea atentamente estos contenidos antes de utilizar el terminal, cúmplalos al utilizarlos y guarde bien el manual para futuras consultas.

Requisitos de operación

- No coloque ni instale el terminal en un lugar expuesto a la luz solar o cerca de una fuente de calor. Mantenga
- el terminal alejado de la humedad, el polvo o el hollín.
- Mantenga el terminal instalado horizontalmente en el lugar estable para evitar que se caiga. No deje caer
- ni salpique líquido sobre el terminal, y asegúrese de que no haya ningún objeto lleno de líquido en el terminal para evitar que el líquido fluya hacia el terminal.
- Instale el terminal en un lugar bien ventilado y no bloquee la ventilación del terminal.

- Opere el terminal dentro del rango nominal de entrada y salida de
- energía. No desmonte el terminal al azar.
- Para el terminal con unidad de control de temperatura:
  - ◇ Instale la unidad de control de temperatura en un entorno interior sin viento y mantenga la temperatura ambiente interior entre 15 ° C y 32 ° C.
  - ◇ Caliente la unidad de control de temperatura durante más de 20 minutos después del encendido para permitir que la unidad de control de temperatura alcance el equilibrio térmico.

Seguridad ELECTRICA

- El uso inadecuado de la batería puede provocar un incendio, una explosión o una inflamación.
- Cuando reemplace la batería, asegúrese de que se use el mismo modelo.
- Utilice los cables de alimentación recomendados en la región y cumpla con la especificación de potencia nominal.
- Utilice el adaptador de corriente que se proporciona con el terminal; de lo contrario, podrían producirse lesiones personales y daños al dispositivo.
- La fuente de alimentación debe cumplir con el requisito de la norma de seguridad de voltaje muy bajo (SELV) y suministrar energía con un voltaje nominal que cumpla con el requisito de fuente de energía limitada de acuerdo con IEC60950-1. Tenga en cuenta que el requisito de suministro de energía está sujeto a la etiqueta del dispositivo.
- Conecte el dispositivo (estructura tipo I) a la toma de corriente con toma de tierra de protección. El acoplador del
- aparato es un dispositivo de desconexión. Cuando utilice el acoplador, mantenga el ángulo para facilitar la operación.

Tabla de contenido

1 Dimensiones y componentes

Figure 1-1 Dimensiones y componentes del modelo X (mm [pulgadas])

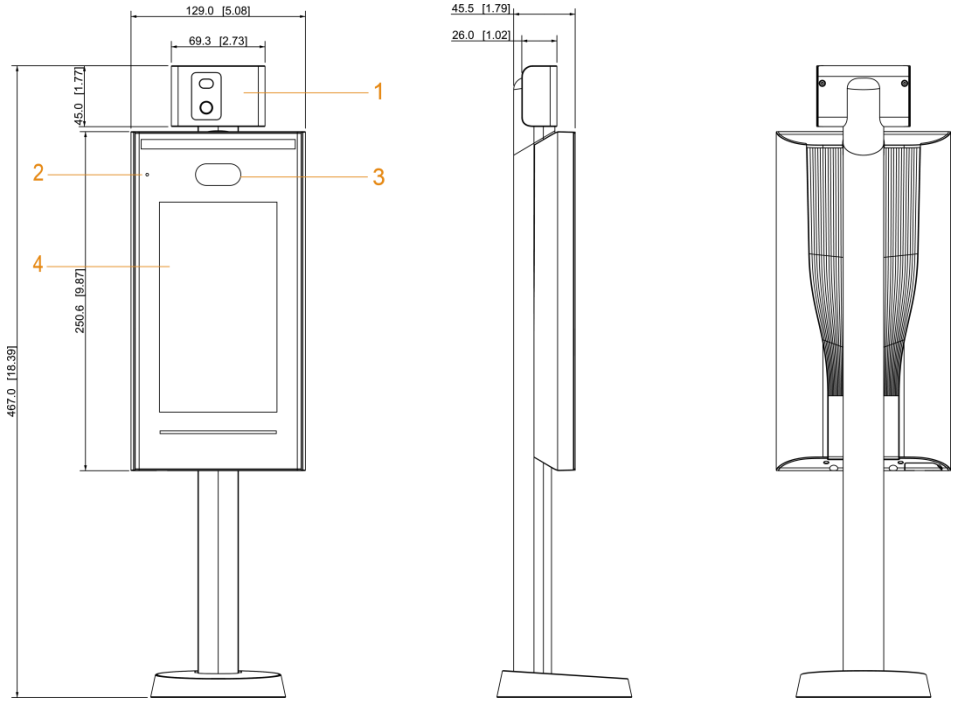


Tabla 1-1 Descripción de los componentes (1)

No.	Nombre	No.	Nombre
1	Unidad de control de temperatura	3	Cámaras duales
2	MIC	4	Monitor

Figure 1-2 Dimensiones y componentes del modelo Y (mm [pulgadas])

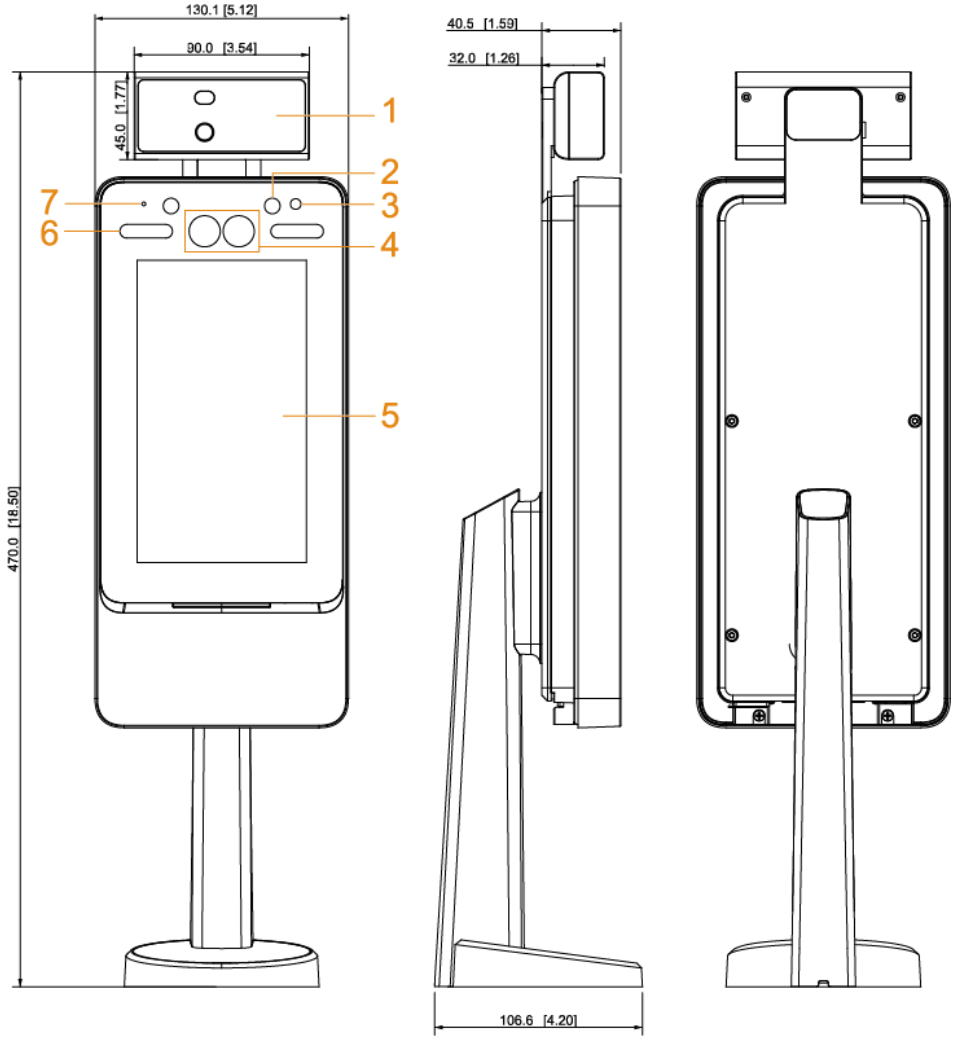


Tabla 1-2 Descripción de los componentes (2)

No.	Nombre	No.	Nombre
1	Unidad de control de temperatura	5	Monitor
2	Luz infrarroja	6	Iluminador LED blanco
3	Fototransistor	7	Micrófono
4	Cámaras duales	-	-

2 Conexión e instalación

2.1 Conexión de cable

La conexión del cable del modelo X y el modelo Y es la misma. Esta sección toma el modelo X como ejemplo.

- Compruebe si el módulo de seguridad de control de acceso está habilitado en **Función> Módulo de seguridad**. Si está habilitado, debe comprar el módulo de seguridad de control de acceso por separado. El módulo de seguridad necesita una fuente de alimentación independiente.
- Una vez que el módulo de seguridad está habilitado, el botón de salida, el control del torniquete y el enlace de extinción de incendios no serán válidos.

Figure 2-1 Conexión de cable

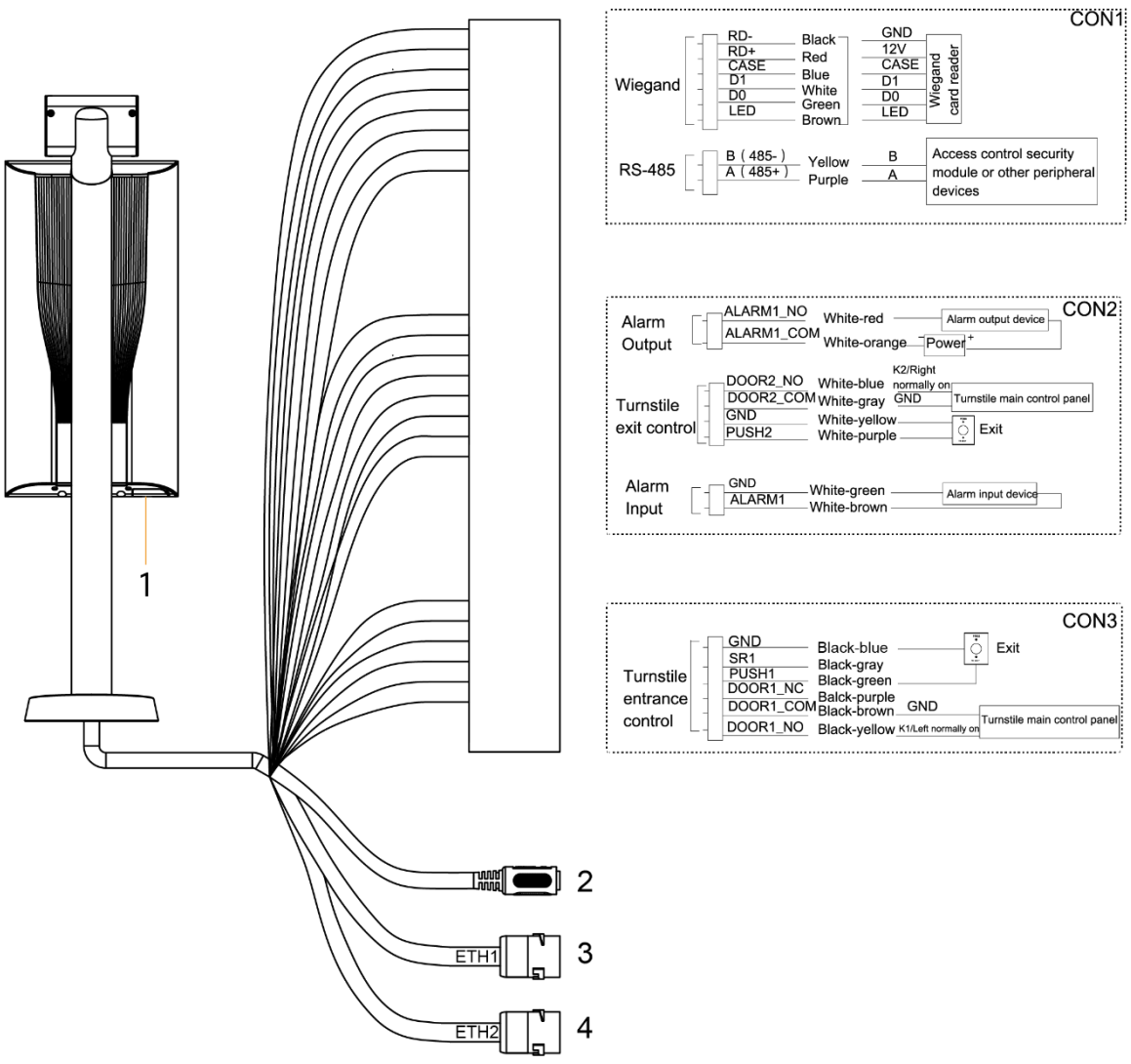


Tabla 2-1 Descripción de los componentes

No.	Nombre
1	Puerto USB
2	Puerto de alimentación

No.	Nombre
3	Puerto Ethernet
4	Puerto Ethernet (solo compatible con el terminal de 7 pulgadas del modelo X)

2.2 Dibujos de instalación

Figure 2-2 Dibujos de instalación del modelo X (mm [pulgadas])

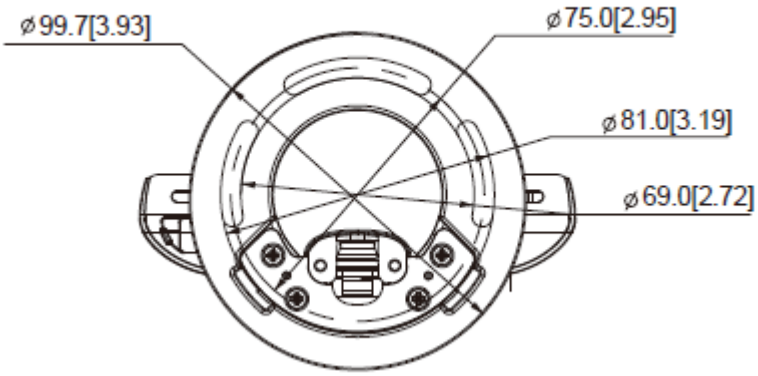
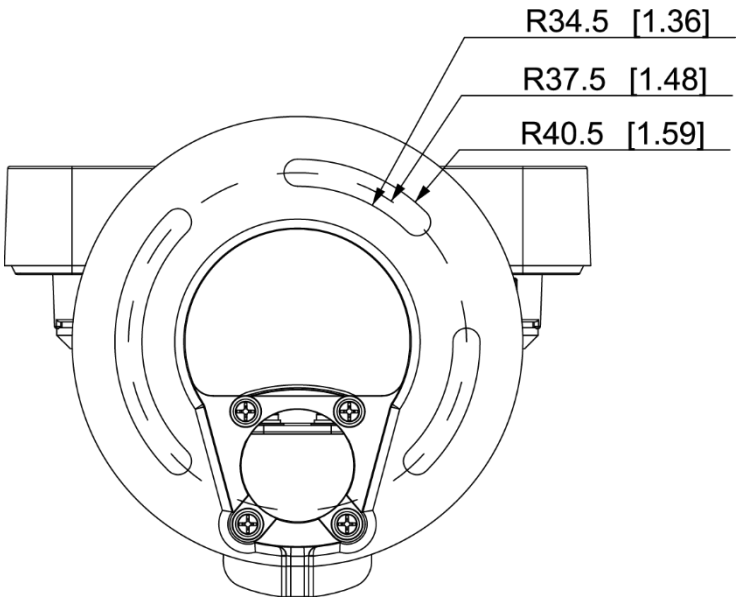


Figure 2-3 Dibujos de instalación del modelo Y (mm [pulgadas])



2.3 Notas de instalación

- Si hay una fuente de luz a 0,5 metros del terminal, la iluminación mínima no debe ser inferior a 100 Lux.
- Se recomienda que la terminal se instale en interiores, al menos a 3 metros de las ventanas y puertas y a 2 metros de las luces.
- Evite la luz de fondo y la luz solar directa.

Requisito de iluminación ambiental

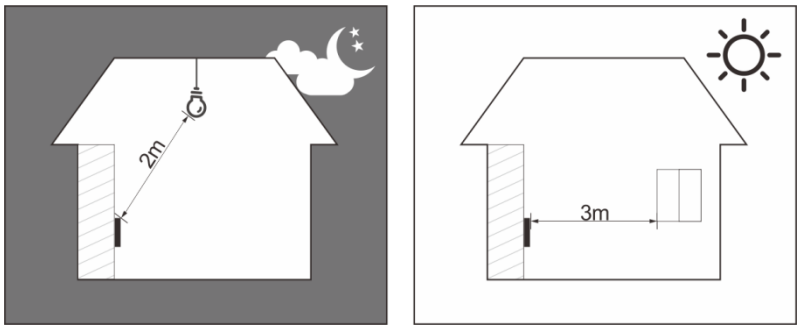
Figure 2-4 Requisito de iluminación ambiental

Requisito de monitoreo de temperatura

- Se recomienda instalar la unidad de control de temperatura en un entorno interior sin viento (un área relativamente aislada del exterior) y mantener la temperatura ambiente entre 15 ° C y 32 ° C.
- Caliente la unidad de control de temperatura durante más de 20 minutos después del encendido para permitir que la unidad de control de temperatura alcance el equilibrio térmico.
- Si no hay un entorno interior adecuado (incluidas las áreas que dan directamente a las áreas interiores y exteriores y las puertas exteriores), configure un pasaje temporal con temperatura ambiente estable para el control de la temperatura.
- Los factores como la luz solar, el viento, el aire frío y el aire acondicionado, el aire frío y caliente pueden afectar fácilmente la temperatura de la superficie del cuerpo humano y el estado de funcionamiento del controlador de acceso, lo que provocará la desviación de temperatura entre la temperatura monitoreada y la temperatura real. .
- Factores que influyen en el control de la temperatura
  - ◇ Viento: el viento quitará el calor de la frente, lo que afectará la precisión del control de la temperatura.
  - ◇ Sudoración: la sudoración es una forma en que el cuerpo se enfría y disipa el calor automáticamente. Cuando el cuerpo suda, la temperatura también disminuirá.
  - ◇ Temperatura ambiente: si la temperatura ambiente es baja, la temperatura de la superficie del cuerpo humano disminuirá. Si la temperatura de la habitación es demasiado alta, el cuerpo humano comenzará a sudar, lo que afectará la precisión del control de temperatura.
  - ◇ La unidad de control de temperatura es sensible a las ondas de luz con una longitud de onda de 10 um a 15 um. Evite usarlo al sol, fuentes de luz fluorescente, salidas de aire acondicionado, calefacción, salidas de aire frío y superficies de vidrio.

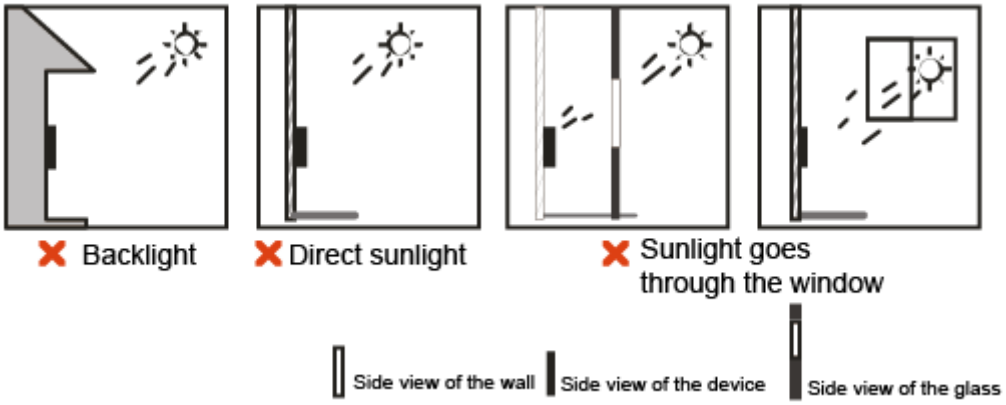
Lugares recomendados

Figure 2-5 Lugares recomendados



Lugares no recomendados

Figure 2-6 Lugares no recomendados



2.4 Instalación

La instalación del modelo X y del modelo Y es la misma. Esta sección toma el modelo X como ejemplo.

Figure 2-7 Instalación de la terminal

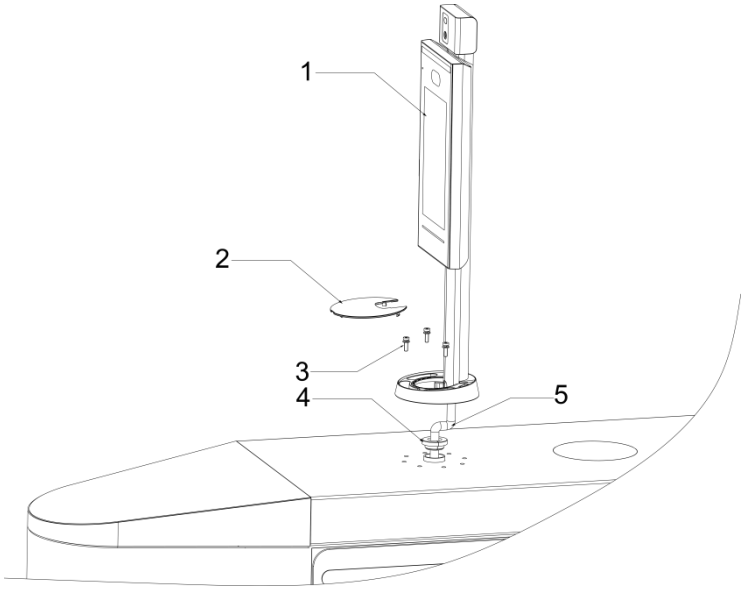


Figure 2-8 Aplicar sellador de silicona al terminal

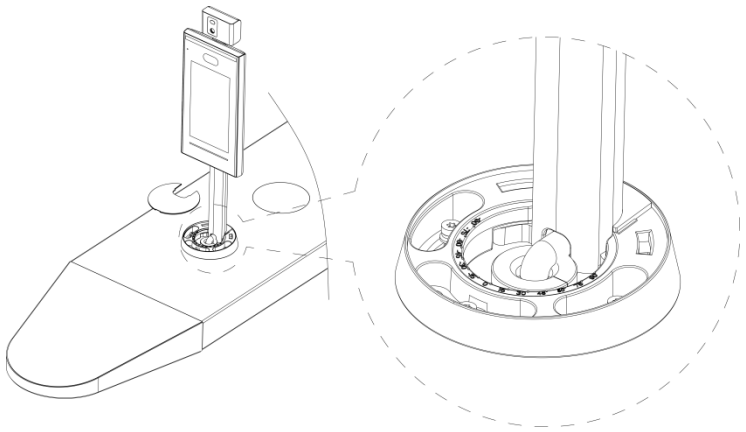


Tabla 2-2 Descripción de los componentes

No.	Nombre
1	Terminal
2	Cubierta ornamental
3	Tornillo M5
4	Tapón de gel de sílice impermeable
5	Cable

Procedimiento de instalación

Step 1 Pase el cable a través del torniquete.

Step 2 Coloque el enchufe de gel de sílice impermeable en el cable. Fije el

Step 3 terminal al torniquete con tornillos M5. Conecte los cables para el

Step 4 terminal. Consulte "2.1 Conexión de cables".

Step 5 Aplique sellador en los espacios entre el tapón de gel de sílice impermeable y el torniquete. Vea la Figura 2-8.

Step 6 Instale la cubierta ornamental en la base del terminal.

3 Operaciones del sistema

3.1 Inicialización

La contraseña de administrador y un correo electrónico deben establecerse la primera vez que se enciende el terminal; de lo contrario, no se podrá utilizar el terminal.

Figure 3-1 Inicialización

- La contraseña de administrador se puede restablecer a través de la dirección de correo electrónico que ingresó si el administrador olvida la contraseña de administrador.
- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo '";: &).

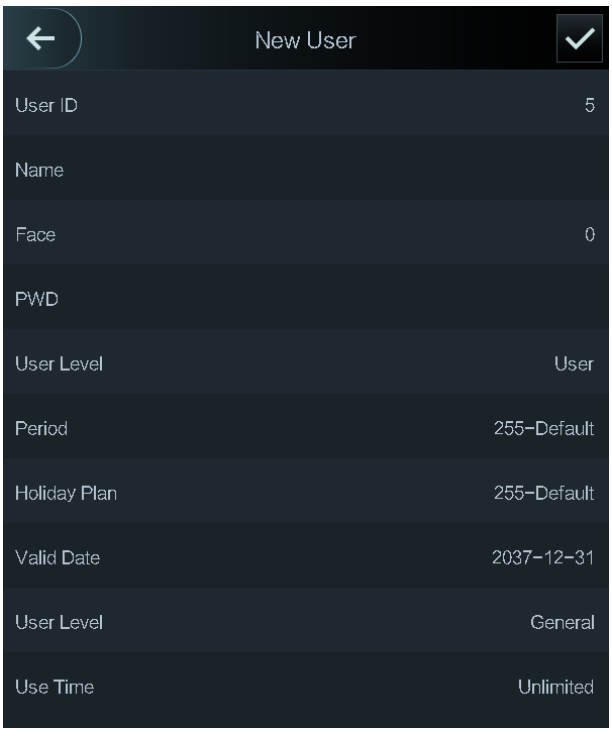
3.2 Agregar nuevos usuarios

Puede agregar nuevos usuarios ingresando ID de usuario, nombres, importando huellas digitales, imágenes de rostros, contraseñas y seleccionando niveles de usuario.

Las siguientes figuras son solo de referencia y prevalecerá la interfaz real.

Step 1 Seleccione **Usuario> Nuevo usuario**.

Figure 3-2 Nuevo Usuario



Step 2 Configure los parámetros en la interfaz.

Tabla 3-1 Descripción del nuevo parámetro de usuario

Parámetro	Descripción
ID de usuario	Ingrese los ID de usuario. Las identificaciones constan de 32 caracteres (incluidos números y letras) y cada identificación es única.
Nombre	Ingrese nombres con un máximo de 32 caracteres (incluidos números, símbolos y letras).
Cara	Asegúrese de que su rostro esté centrado en el marco de captura de la imagen, y luego se capturará automáticamente una imagen de su rostro. Para obtener más información sobre la grabación de imágenes de rostros, consulte el "Apéndice 2 Notas sobre la comparación / grabación de rostros".
Contraseña	La contraseña de desbloqueo de la puerta. La longitud máxima de la contraseña es de 8 dígitos.
Nivel	Puede seleccionar un nivel de usuario para nuevos usuarios. Hay dos opciones. ● Usuario: los usuarios solo tienen permiso de desbloqueo de puertas. ● Admin: los administradores pueden desbloquear la puerta y también tener permiso de configuración de parámetros. En caso de que olvide la contraseña de administrador, será mejor que cree más de un administrador.
Período	El período en el que el usuario puede desbloquear la puerta. Para conocer la configuración detallada del período, consulte el manual del usuario.
Fiesta Plan	Puede establecer un plan de vacaciones en el que el usuario puede abrir la puerta. Para conocer la configuración detallada del plan de vacaciones, consulte el manual del usuario.
Fecha válida	Puede establecer un período durante el cual la información de desbloqueo del usuario es válida.

Parámetro	Descripción
Nivel de usuario	Hay seis niveles: ● General: los usuarios generales pueden desbloquear la puerta normalmente. ● Lista negra: cuando los usuarios de la lista negra abren la puerta, el personal de servicio recibirá un aviso. ● Invitado: Los invitados pueden abrir la puerta en ciertos momentos o en ciertos períodos. Una vez que superan los tiempos o períodos máximos, no pueden desbloquear la puerta. ● Patrulla: los usuarios de patrulla pueden hacer un seguimiento de su asistencia, pero no tienen permiso de desbloqueo. ● VIP: cuando VIP abre la puerta, el personal de servicio recibirá un aviso. Especial: ● cuando personas especiales desbloquean la puerta, habrá un retraso de 5 segundos antes de que se cierre la puerta.
Tiempo de uso	Cuando el nivel de usuario es Invitado, puede establecer el número máximo de veces que el invitado puede desbloquear la puerta.

Step 3 Grifo  para guardar la configuración.

4 Operaciones web

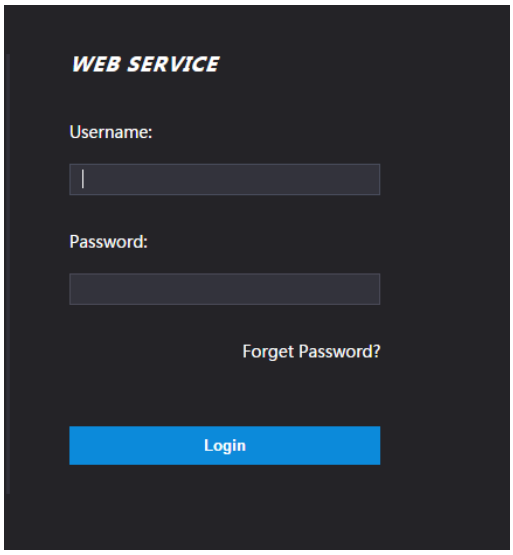
El terminal se puede configurar y operar en la interfaz web. A través de la interfaz web, puede establecer parámetros, incluidos los parámetros de red, los parámetros de video y los parámetros del terminal; y también puede mantener y actualizar el sistema. Para obtener más información, consulte el manual del usuario. Aquí solo se describe la operación de inicio de sesión.

Debe establecer una contraseña y una dirección de correo electrónico antes de iniciar sesión en la interfaz web por primera vez. La contraseña que establezca se usa para iniciar sesión en la web y el correo electrónico se usa para restablecer las contraseñas.

Step 1 Abra el navegador web IE, ingrese la dirección IP (192.168.1.108 por defecto) del terminal en la barra de direcciones, y luego presione la tecla Enter.

- Asegúrese de que la dirección IP de la computadora utilizada para iniciar sesión en la web esté en la misma LAN que el terminal.
- El terminal de 7 pulgadas del modelo X tiene dos NIC. La dirección IP predeterminada para el puerto de red ETH1 es 192.168.1.108 y para ETH2 es 192.168.2.108.

Figure 4-1 Acceso



Step 2 Ingrese el nombre de usuario y la contraseña.

- El nombre de usuario predeterminado del administrador es admin y la contraseña es la contraseña de inicio de sesión después de inicializar el terminal. Modifique la contraseña de administrador con regularidad y consérvela correctamente por motivos de seguridad.
- Si olvida la contraseña de inicio de sesión de administrador, puede hacer clic en **¿Contraseña olvidada?** para restablecerlo. Consulte el manual de usuario.

Step 3 Hacer clic **Acceso**.

Se muestra la página de inicio de la interfaz web.

Appendix 1 Notas de monitoreo de temperatura

- Caliente la unidad de control de temperatura durante 20 minutos después del encendido para permitir que la unidad de control de temperatura alcance el equilibrio térmico.
- Instale la unidad de control de temperatura en un entorno interior sin viento y mantenga la temperatura ambiente interior entre 15 ° C y 32 ° C.
- Evite la luz solar directa sobre la unidad de control de temperatura.
- Evite instalar la unidad de control de temperatura orientada hacia la fuente de luz y el vidrio.
- Mantenga la unidad de control de temperatura alejada de fuentes de interferencia térmica.
- Los factores como la luz solar, el viento, el aire frío y el aire acondicionado frío y caliente afectarán la temperatura de la superficie del cuerpo humano, lo que provocará la desviación de temperatura entre la temperatura monitoreada y la temperatura real.
- La sudoración también es una forma en que el cuerpo se enfría y disipa el calor automáticamente, lo que también provocará la desviación de temperatura entre la temperatura monitoreada y la temperatura real.
- Mantenga la unidad de control de temperatura con regularidad (cada 2 semanas). Utilice un paño suave sin polvo para limpiar suavemente el polvo de la superficie del sensor de temperatura y el sensor de distancia para mantenerlo limpio.

Appendix 2 Notas de la cara Grabación / comparación

Antes del registro

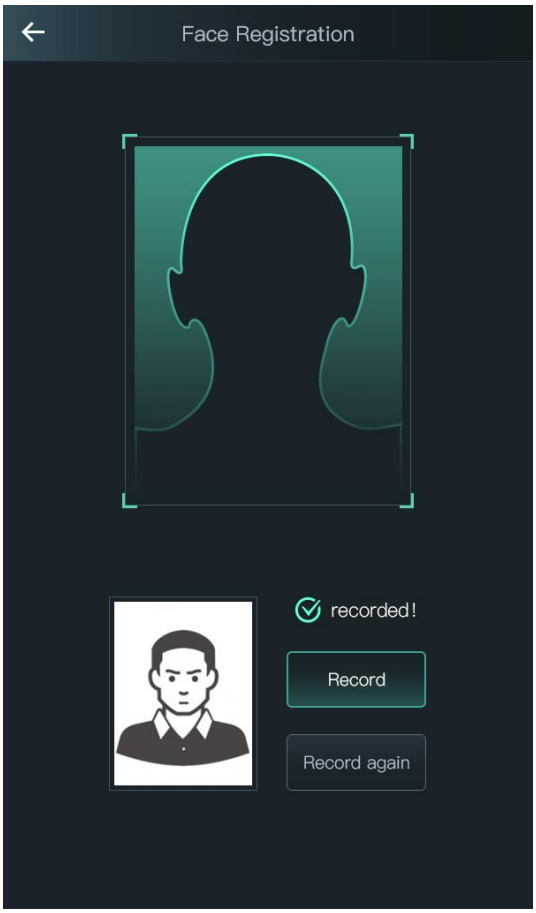
- Los anteojos, los sombreros y la barba pueden influir en el rendimiento del
- reconocimiento facial. No cubra sus cejas cuando use sombreros.
- No cambie mucho el estilo de su barba si va a utilizar el dispositivo; de lo contrario, el reconocimiento facial podría fallar.
- Mantén tu cara limpia.
- Mantenga el dispositivo al menos a dos metros de la fuente de luz y al menos a tres metros de las ventanas o puertas; de lo contrario, la luz de fondo y la luz solar directa podrían influir en el rendimiento del reconocimiento facial del dispositivo.

Durante el registro

Puedes registrar rostros a través del terminal o a través de la plataforma. Para registrarse a través de la plataforma, consulte el manual de usuario de la plataforma.

Haga que su cabeza se centre en el marco de captura de fotos. Se capturará automáticamente una imagen de su rostro.

Apéndice Figura 2-1 Registro

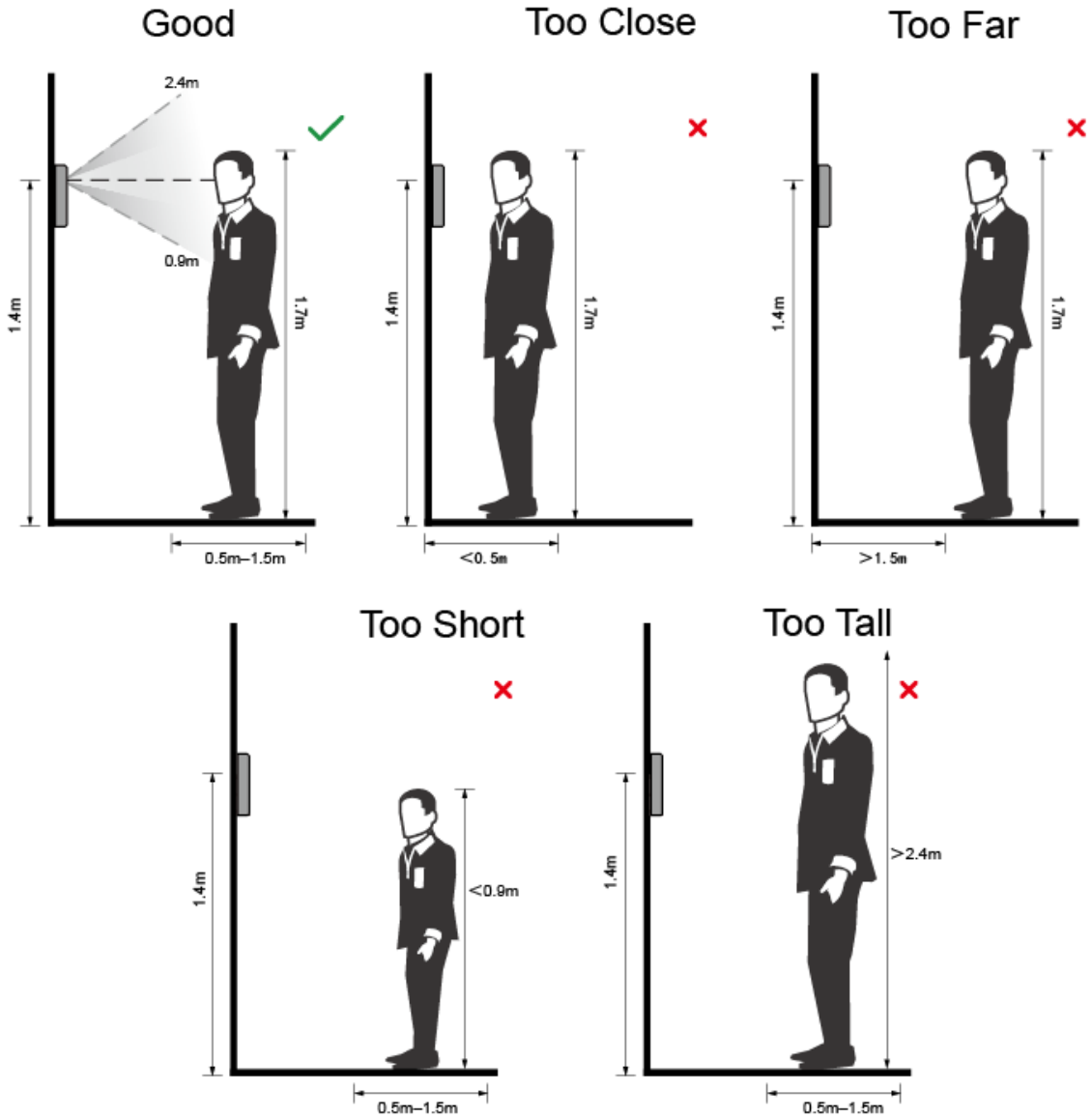


- No sacuda la cabeza o el cuerpo, de lo contrario, el registro podría fallar. Evite
- que aparezcan dos caras en el cuadro de captura al mismo tiempo.

Posición de la cara

Si su rostro no está en la posición adecuada, el efecto de reconocimiento facial podría verse afectado.

Apéndice Figura 2-2 Posición adecuada de la cara

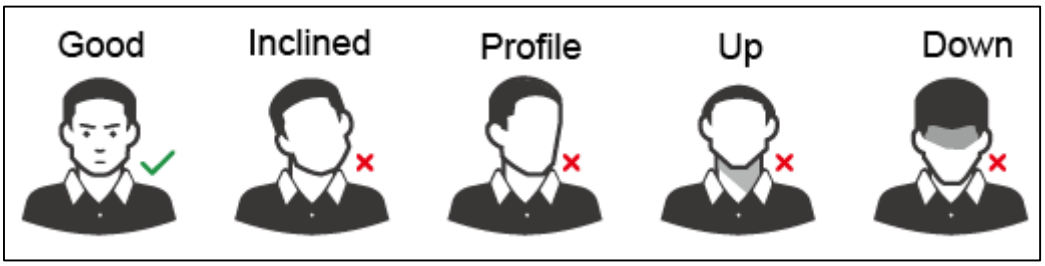


Requisitos de caras

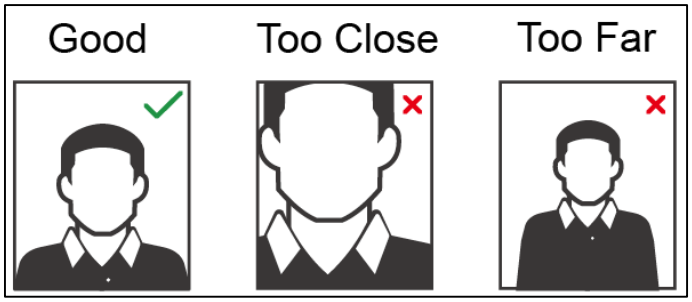
- Asegúrese de que la cara esté limpia y la frente no esté cubierta de pelo.
- No use anteojos, sombreros, barbas espesas u otros adornos faciales que influyan en la grabación de imágenes faciales.
- Con los ojos abiertos, sin expresiones faciales, y dirija su rostro hacia el centro de la cámara.

- Cuando grabe su rostro o durante el reconocimiento facial, no mantenga su rostro demasiado cerca o demasiado lejos de la cámara.

Apéndice Figura 2-3 Posición de la cabeza



Apéndice Figura 2-4 Distancia entre caras



- Al importar imágenes de rostros a través de la plataforma de administración, asegúrese de que la resolución de la imagen esté dentro del rango de 150 × 300–600 × 1200; los píxeles de la imagen son más de 500 × 500; el tamaño de la imagen es inferior a 75 KB y el nombre de la imagen y la identificación de la persona son iguales.
- Asegúrese de que la cara ocupe más de 1/3 pero no más de 2/3 de toda el área de la imagen y que la relación de aspecto no exceda 1: 2.

Appendix 3 Operación de llamada

El controlador de acceso puede funcionar como un VTO y llamar a otros dispositivos.

Requisito previo

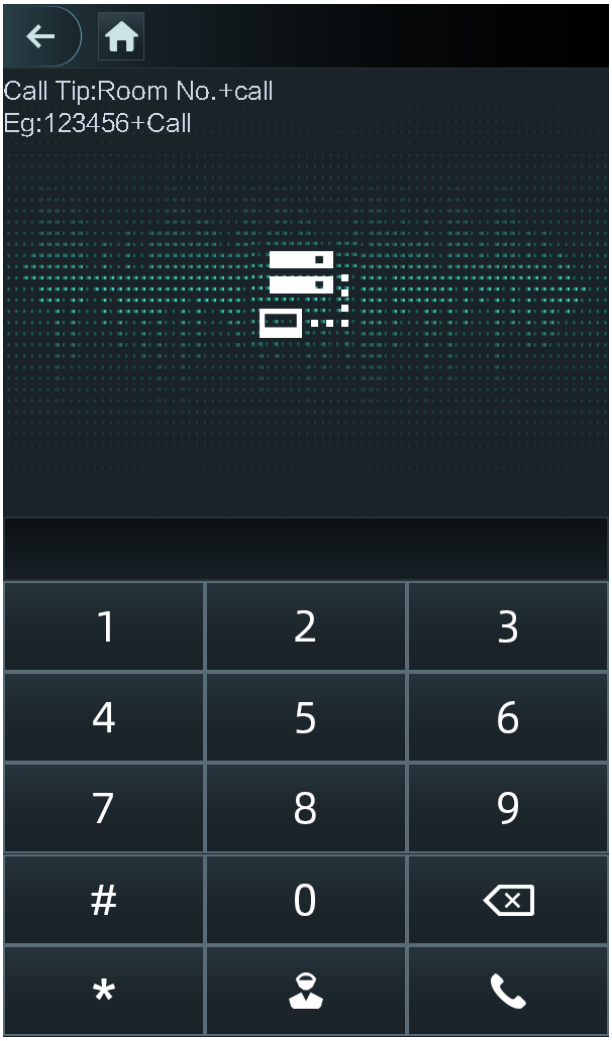
Configure los parámetros relevantes en el controlador de acceso, VTH y la estación maestra, para que puedan llamarse entre sí. Consulte "Configuración de llamadas" en el manual del usuario.

Procedimientos

Step 1 En la interfaz de espera, toque  .

Step 2 Ingrese el número de VTH y luego toque  .

Apéndice Figura 3-1 Interfaz de llamada



Appendix 4 Recomendaciones de ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que pertenece a todos los dispositivos que están 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 en red los hará menos susceptibles a los ataques. A continuación, se muestran algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

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

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Actualice el firmware y el software cliente a tiempo

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su dispositivo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el dispositivo está conectado a la red pública, se recomienda habilitar la función de "búsqueda automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware publicadas por el fabricante.

- Le sugerimos que descargue y utilice la última versión del software cliente.

Recomendaciones "Es bueno tener" para mejorar la seguridad de la red de su dispositivo: 1. Protección física

Le sugerimos que realice una protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras especial y gabinete, e implemente permisos de control de acceso bien hechos y administración de claves para evitar que el 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 ser adivinado o descifrado.

3. Establecer y actualizar la información de restablecimiento de contraseñas 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 las preguntas de protección por contraseña, se sugiere no utilizar aquellas que se puedan adivinar fácilmente.

4. Habilite el bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilite HTTPS

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

7. Enlace de dirección MAC

Le recomendamos que vincule 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 los riesgos.

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

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

10. Transmisión encriptada de audio y video

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

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

11. Auditoría segura

- Verificar usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo está conectado sin autorización.
- Verificar 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 mucho tiempo, se recomienda que habilite la función de registro de red para asegurarse de 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:

- Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde una red externa.
- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere usar VLAN, 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.