Controlador de acceso de reconocimiento facial

Guía de inicio rápido

V1.0.0

Prefacio

General

Este manual presenta la instalación y el funcionamiento básico del reconocimiento facial.

Controlador de acceso (en adelante denominado "controlador de acceso").

Las instrucciones de seguridad

El siguiente gato Las palabras de señalización egorizadas con significado definido pueden aparecer en el manual.

Palabras de advertencia	Sentido
NOTA	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Revisión de contenido	Fecha de lanzamiento
V1.0.0	Primer lanzamiento	Agosto 2019

Sobre el manual

- El manual es solo de referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por las operaciones que no cumplan con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y reglamentos de las regiones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay 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 al cliente para obtener el último programa y la documentación complementaria.
- Todavía puede haber una desviación en los datos técnicos, la descripción de las funciones y operaciones, o errores en la impresión. Si hay alguna duda o disputa, consulte nuestra 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 compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, póngase en contacto con el proveedor o servicio al cliente si se produce algún problema al utilizar el dispositivo.
- Si existe alguna incertidumbre o controversia, consulte nuestra explicación final.

Importantes salvaguardas y advertencias

Este capítulo describe los contenidos que cubren el manejo adecuado del controlador de acceso, la prevención de riesgos y la prevención de daños a la propiedad. Lea este contenido detenidamente antes de usar el controlador de acceso, cumpla con ellos cuando lo use y guárdelo para futuras referencias.

Requisito de operación

- No coloque ni instale el controlador de acceso en un lugar expuesto a la luz solar o cerca de la fuente de calor.
- Mantenga el controlador de acceso alejado de la humedad, el polvo o el hollín.
- Mantenga el controlador de acceso instalado horizontalmente en el lugar estable para evitar que se caiga.
- No deje caer ni salpique líquido sobre el controlador de acceso, y asegúrese de que no haya ningún objeto lleno de líquido en el controlador de acceso para evitar que el líquido fluya hacia el controlador de acceso.
- Instale el controlador de acceso en un lugar bien ventilado y no bloquee la ventilación del controlador de acceso.
- Opere el controlador de acceso dentro del rango nominal de entrada y salida de potencia.
- No desmonte el controlador de acceso.
- Transporte, use y almacene el controlador de acceso bajo las condiciones de humedad y temperatura permitidas.

Seguridad ELECTRICA

- El uso incorrecto de la batería puede provocar incendios, explosiones o inflamaciones.
- Al reemplazar la batería, asegúrese de usar el mismo modelo.
- Utilice los cables de alimentación recomendados en la región y cumpla con la especificación de potencia nominal.
- Use el adaptador de corriente provisto con el controlador de acceso; de lo contrario, podría provocar lesiones personales y daños en el dispositivo.
- La fuente de alimentación debe cumplir con el requisito del estándar de seguridad de voltaje extra bajo (SELV) y suministrar energía con voltaje nominal que cumpla con el requisito de fuente de energía limitada de acuerdo con IEC60950-1. Tenga en cuenta que el requisito de la fuente de alimentación 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 use el acoplador, mantenga el ángulo para una fácil operación.

Tabla de contenido

1 Dimensiones y componentes

El controlador de acceso tiene dos tipos: controladores de acceso de 7 pulgadas y 10 pulgadas. Ver Figura 1-1 y Figura 1-2.

Controlador de acceso de 7 pulgadas

Dimensiones y componentes (1) (mm [pulgadas]) Figura 1-1

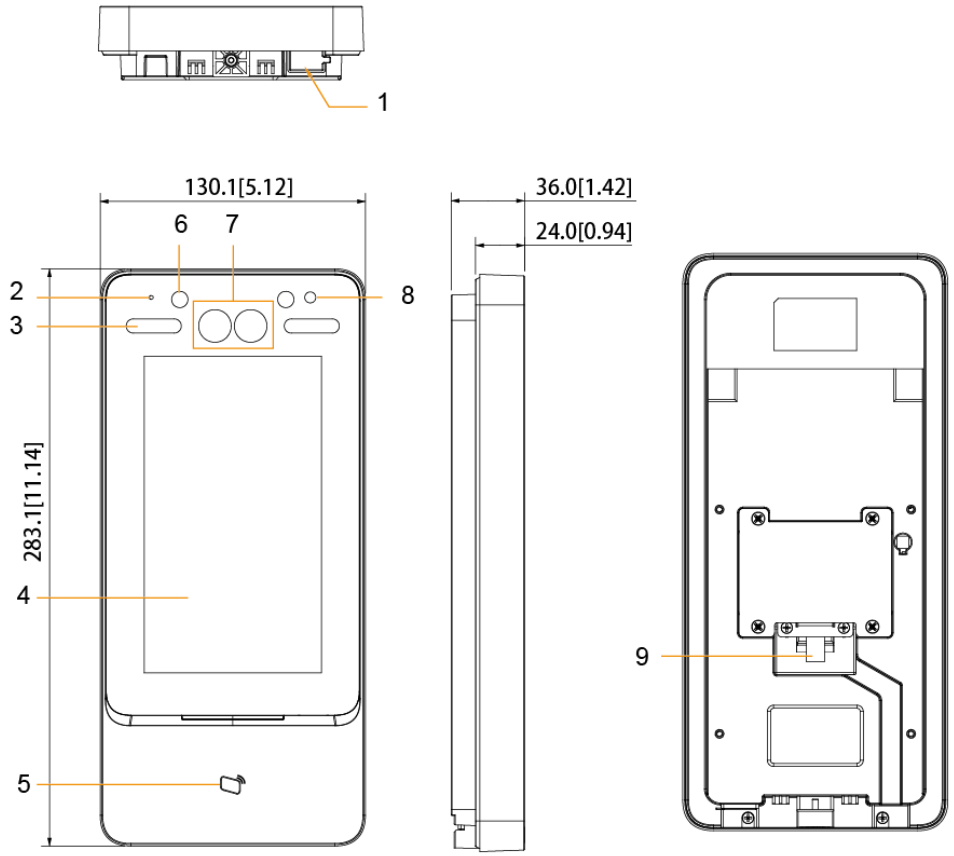


Table 1-1 Com ponent d escription (1)

No. Nombre		No.	Nombre
1	Puerto USB	6 6	Luz IR
2	MIC	7 7	Cámara doble
3	Luz de relleno blanco	8	Fototransistor
4 4	Monitor	9 9	Entrada de cable
5 5	Área de deslizamiento de tarjeta 10		-

Dimensiones y componentes (2) (mm [pulgadas]) Figura 1-2

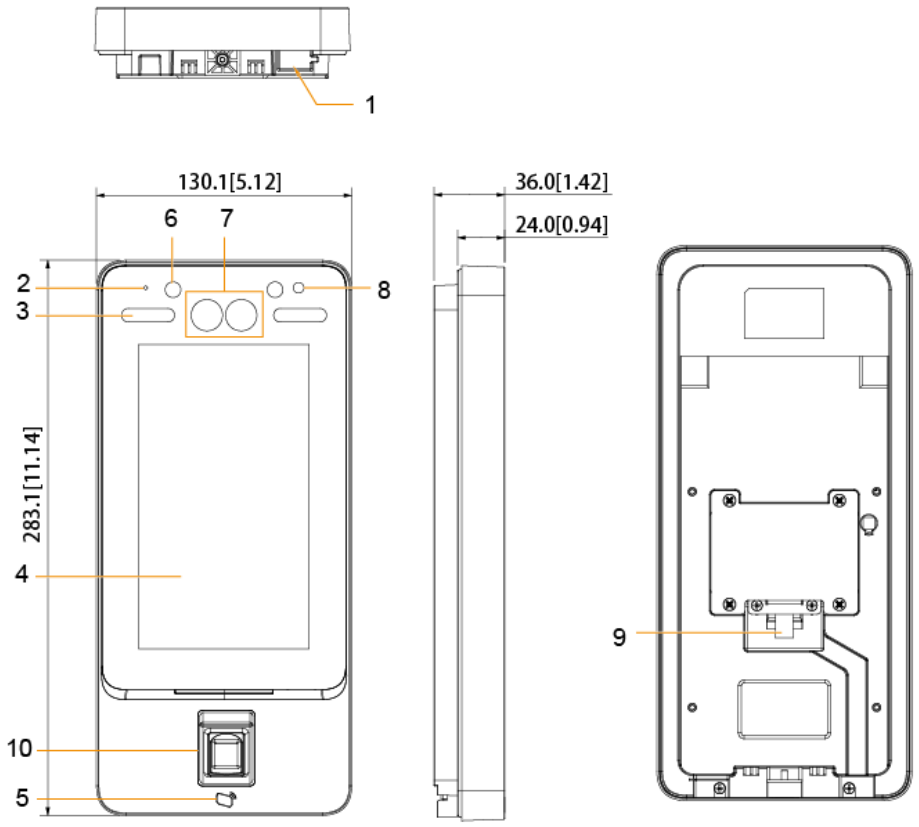


Table 1-2 Com pan de maíz nt descripción (2)

No.	Nombre	No.	Nombre
1	Puerto USB	6 6	Luz IR
2	MIC	7 7	Cámara doble
3	Luz de relleno blanco	8	Fototransistor
4 4	Monitor	9 9	Entrada de cable
5 5	Área de deslizamiento de tarjeta 10		Sensor de huellas digitales

Controlador de acceso de 10 pulgadas

Dimensiones y componentes (3) (mm [pulgadas]) Figura 1-3

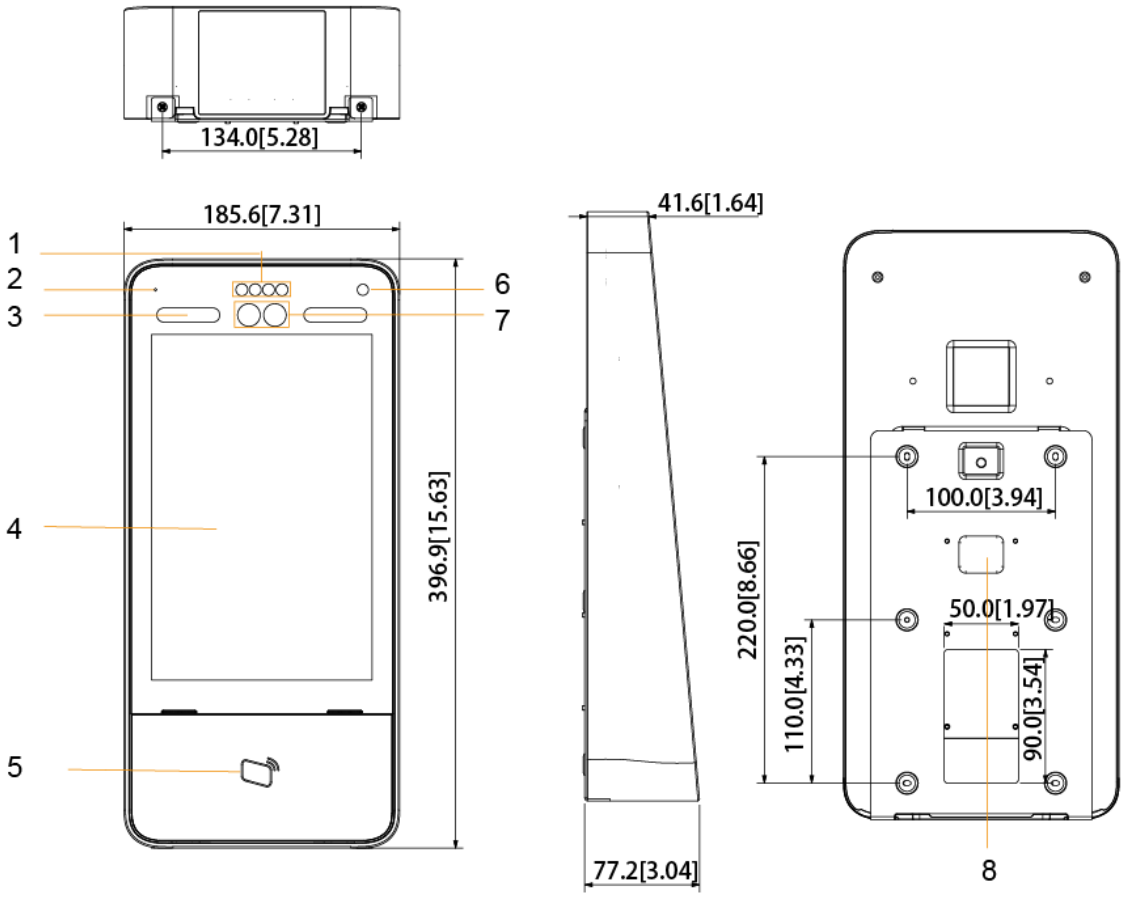


Table 1-3 Com pan de maíz nt descripción (3)

No.	Nombre	No.	Nombre
1	Luz IR	6 6	Fototransistor
2	MIC	7 7	Cámara doble
3	Luz de relleno blanco	8	Entrada de cable
4 4	Monitor	9 9	-
5 5	Área de deslizamiento de tarjeta 10		-

Dimensiones y componentes (4) (mm [pulgadas]) Figura 1-4

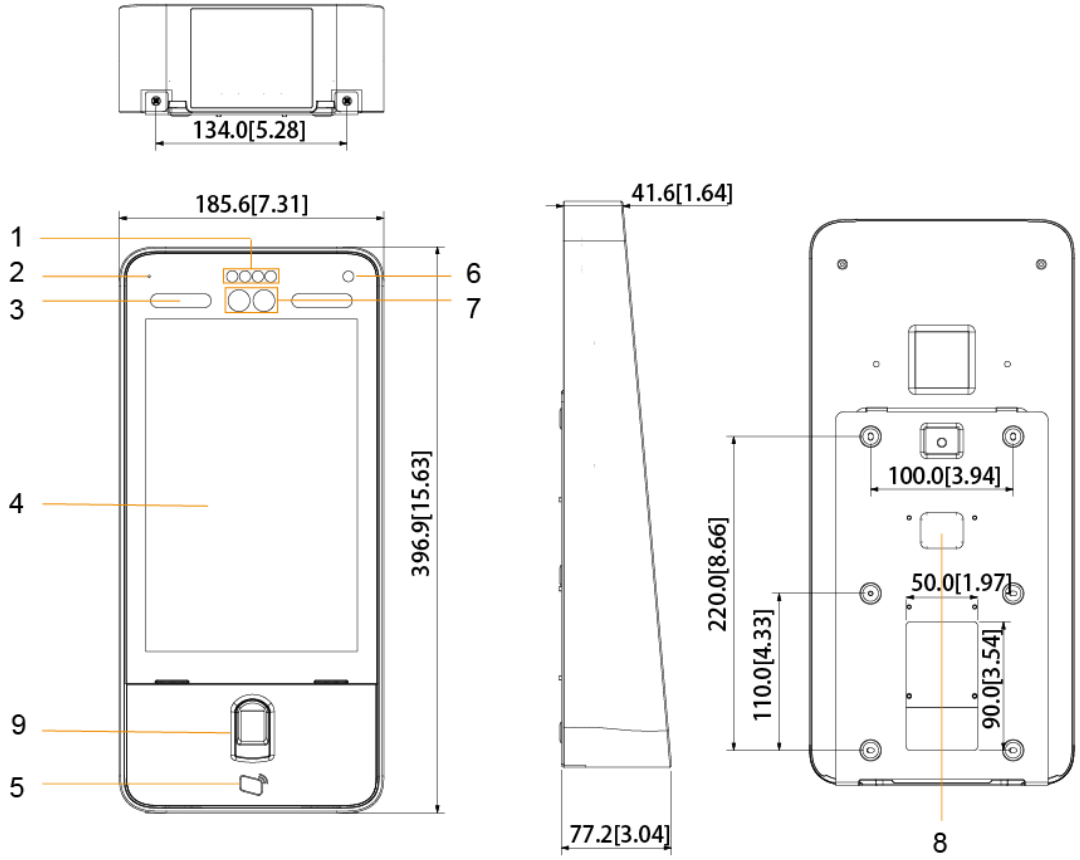


Tabla 1-4 Com pan de maíz nt descripción (4)

No.	Nombre	No.	Nombre
1	Luz IR	6 6	Fototransistor
2	MIC	7 7	Cámara doble
3	Luz de relleno blanco	8	Entrada de cable
4 4	Monitor	9 9	Sensor de huellas dactilares
5 5	Área de deslizamiento de tarjeta 10		-

2 Instalación

2.1 Notas de instalación

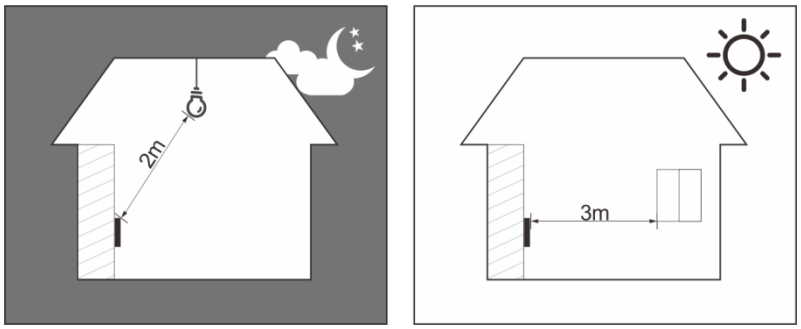
- Si hay una fuente de luz a 0,5 metros del dispositivo, la iluminación mínima no debe ser inferior a 100Lux.
- Se recomienda que el dispositivo se instale en interiores, al menos a 3 metros de las ventanas y puertas y a 2 metros de las luces.
- Evite la luz de fondo y la luz solar directa.

Requisito de iluminación ambiental

2-1 Requisito de iluminación ambiental Figura

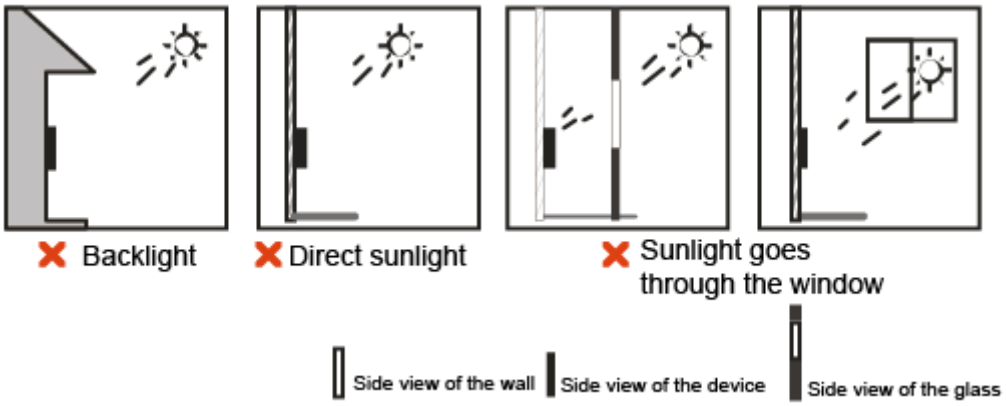
Lugares recomendados

Figura 2-2 Lugares recomendados



Lugares no recomendados

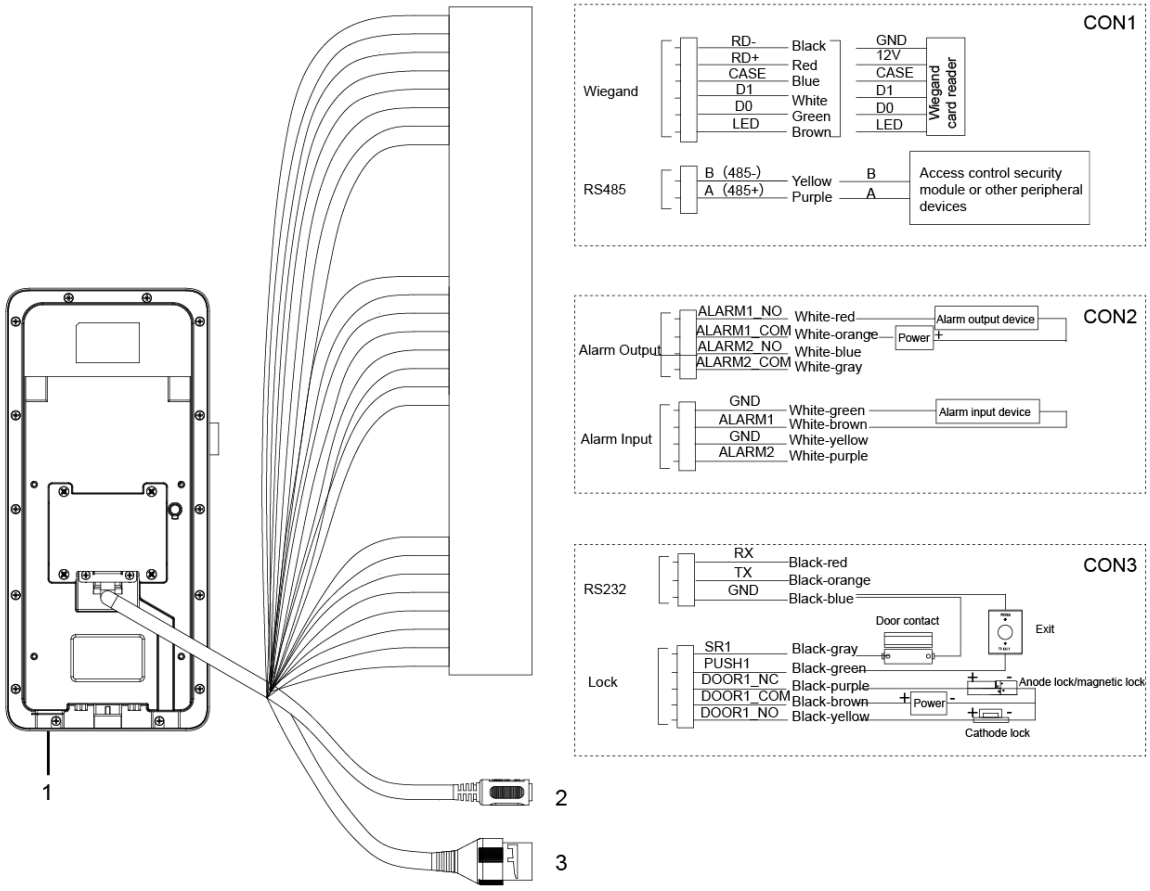
2-3 Lugares no recomendados Figura



2.2 Conexiones de cable

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

Figura 2-4 Conexión de cable



T capaz 2-1 Componente descriptivo ion

No.	Nombre
1	Puerto USB 2
	Puerto de
alimentación 3	Puerto Ethernet

2.3 Instalación

El método de instalación del modelo A y el modelo B es el mismo. Asegúrese de que la distancia entre la lente y el suelo sea de 1,4 metros. Ver Figura 2-5.

Figura 2-5 Altura de instalación

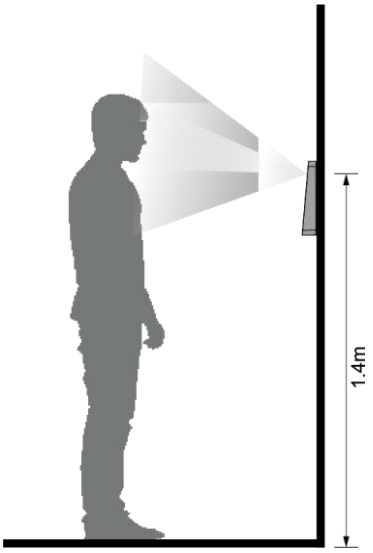
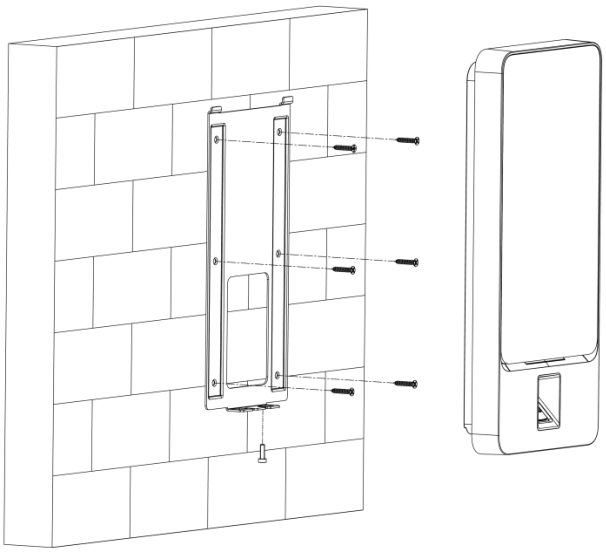


Figura 2-6 Diagrama de instalación



Procedimiento de instalación

Paso 1 Taladre siete agujeros (seis agujeros de instalación de soporte y una entrada de cable) en la pared según los agujeros en el soporte.

Paso 2 Fije el soporte en la pared instalando los tornillos de expansión en los seis soportes agujeros de instalación

Paso 3 Conecte los cables para el controlador de acceso.

Consulte "2.2 Conexiones de cable".

Paso 4 Cuelgue el controlador de acceso en el gancho del soporte.

Paso 5 Apriete los tornillos en la parte inferior del controlador de acceso.

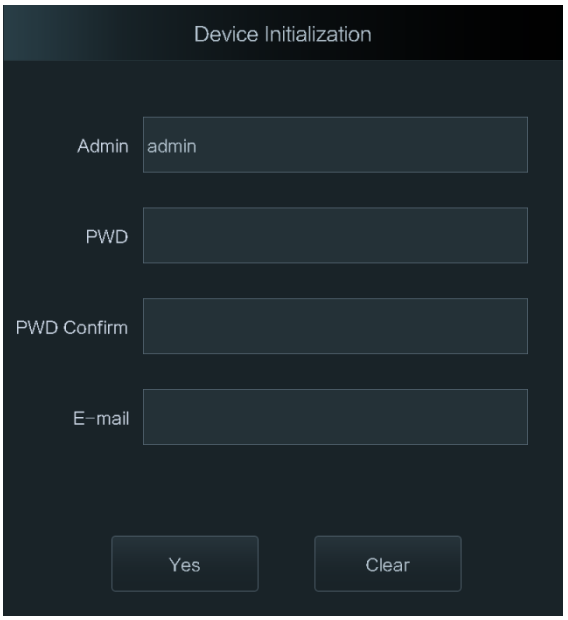
La instalación está completa.

3 Operación del sistema

3.1 Inicialización

La contraseña del administrador y un correo electrónico deben establecerse la primera vez que se enciende el controlador de acceso; de lo contrario, no se puede usar el controlador de acceso. Ver Figura 3-1.

Figura 3-1 Inicialización



- La contraseña de administrador se puede restablecer a través de la dirección de correo electrónico que ingresó si se olvida la contraseña.
- La contraseña debe constar de 8 a 32 caracteres no en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo '";: &).
- Para el controlador de acceso sin pantalla táctil, la inicialización se puede completar a través de la web. Consulte el manual del usuario para más detalles.

3.2 Agregar nuevos usuarios

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

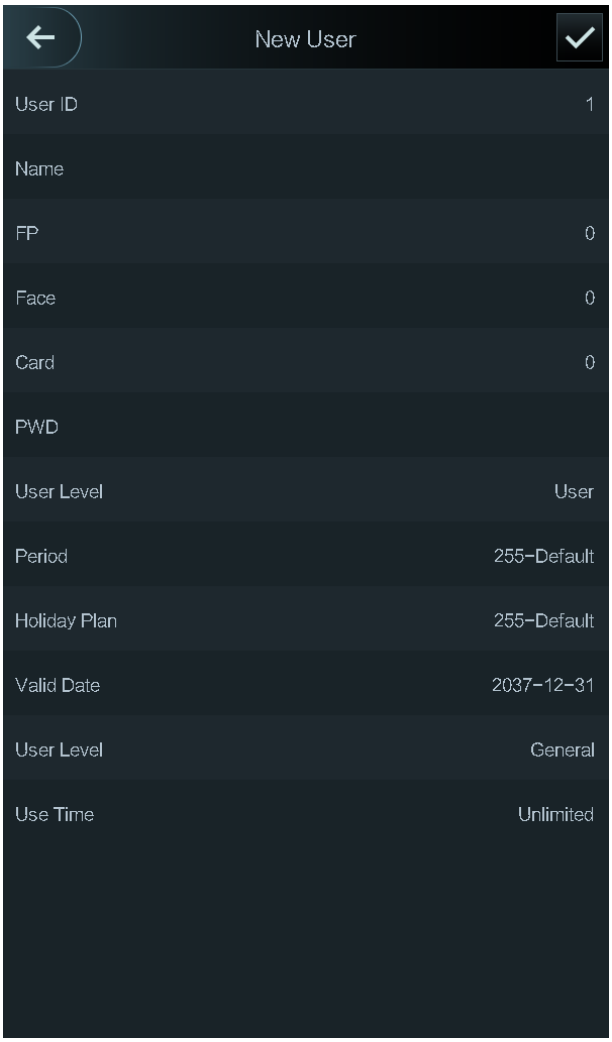
Las siguientes cifras son solo de referencia y prevalecerá la interfaz real.

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

los **Nuevo Usuario** Se muestra la interfaz. Ver Figura 3-2.

La siguiente figura es solo de referencia y prevalecerá la interfaz real.

Figura 3-2 Nuevo usuario



Paso 2 Configurar parámetros en la interfaz. Ver tabla 3-1.

Tabla 3-1 Descripción del nuevo parámetro de usuario

Parámetro	Descripción
ID de usuario	Puede ingresar ID de usuario. Las ID constan de 32 caracteres (incluidos números y letras), y cada ID es única.
Nombre	Puede ingresar nombres con un máximo de 32 caracteres (incluidos números, símbolos y letras).
FP	Como máximo se pueden registrar tres huellas digitales de un usuario, y una huella digital debe verificarse tres veces. Puede habilitar la función Duress FP debajo de cada huella digital, y solo una de las tres huellas digitales puede ser la huella digital de coacción. Las alarmas se activarán si se usa una huella dactilar forzada para desbloquear la puerta. • No se recomienda establecer la huella digital del pulgar como huella digital de coacción. • El desbloqueo de huellas digitales está disponible en modelos seleccionados.
Cara	Asegúrese de que su rostro esté centrado en el marco de captura de imagen, y luego se capturará automáticamente una imagen de su rostro. Para obtener detalles sobre la grabación de imágenes faciales, consulte el "Apéndice 1 Notas sobre la grabación de rostros".

Parámetro	Descripción
Tarjeta	Puede registrar cinco tarjetas para cada usuario. En la interfaz de registro de la tarjeta, ingrese su número de tarjeta o deslice su tarjeta, y luego el controlador de acceso leerá la información de la tarjeta. Puede habilitar la función Duress Card en la interfaz de registro de la tarjeta. Las alarmas se activarán si se utiliza una tarjeta de coacción para desbloquear la puerta. Si el dispositivo no tiene un módulo de lectura de tarjetas, debe conectar el dispositivo a lectores de tarjetas periféricos.
Contraseña	La contraseña de desbloqueo de la puerta. La longitud máxima de los dígitos de ID es 8. Si el controlador de acceso no tiene pantalla táctil, debe conectar el controlador de acceso a un lector de tarjetas periférico. Hay botones en el lector de tarjetas.
Nivel	Puede seleccionar un nivel de usuario para nuevos usuarios. Hay dos opciones • Usuario: los usuarios solo tienen autorización para desbloquear la puerta. • Administrador: los administradores no solo pueden desbloquear la puerta sino que también tienen autoridad de configuración de parámetros. En caso de que olvide la contraseña de administrador, será mejor que cree más de un administrador.
Período	Puede establecer un período en el que el usuario pueda desbloquear la puerta. Para conocer la configuración detallada del período, consulte el manual de configuración.
Plan de vacaciones	Puede establecer un plan de vacaciones en el que el usuario pueda desbloquear la puerta. Para conocer la configuración detallada del plan de vacaciones, consulte el manual de configuración.
Fecha válida	Puede establecer un período durante el cual la información de desbloqueo del usuario es válida.
Nivel de usuario	Hay seis niveles: • General: los usuarios generales pueden desbloquear la puerta normalmente. • Lista negra: cuando los usuarios de la lista negra desbloquean la puerta, el personal de servicio obtener un aviso • Invitado: los invitados pueden desbloquear la puerta ciertas veces en ciertos períodos. Una vez que exceden los tiempos y períodos máximos, no pueden volver a abrir la puerta. • Patrulla: los usuarios de patrulla pueden hacer un seguimiento de su asistencia, pero no tienen desbloquear autoridad. • VIP: cuando VIP abre la puerta, el personal de servicio recibirá un aviso. • Deshabilitar: cuando los deshabilitados desbloquean la puerta, habrá un retraso de 5 segundos antes de que se cierre la puerta.
Use Time	Cuando el nivel de usuario es **Invitado,** puede establecer los tiempos máximos que el invitado Puede abrir la puerta.

Paso 3 Después de haber configurado todos los parámetros, toque para guardar la configuración.

Se crea un nuevo usuario.

Para los controladores de acceso sin pantalla táctil, debe crear usuarios a través de plataformas de administración. Ver detalles en el manual del usuario.

4 4 Operación web

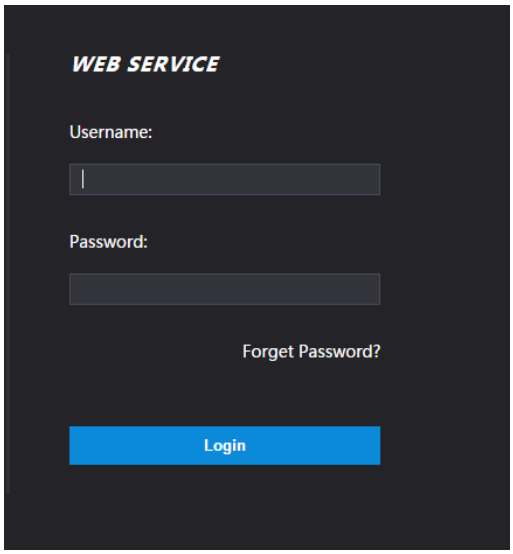
El controlador de acceso se puede configurar y operar en la web. A través de la web puede establecer parámetros que incluyen parámetros de red, parámetros de video y parámetros del controlador de acceso; y también puede mantener y actualizar el sistema.

Iniciar sesión

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

Paso 1 Abra el navegador web IE, ingrese la dirección IP (192.168.1.108 por defecto) del acceso controlador en la barra de direcciones, y luego presione Entrar.

sesión Figura 4-1



Paso 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 controlador de acceso. Modifique la contraseña de administrador con regularidad y guárdela adecuadamente por seguridad.
- Si olvida la contraseña de inicio de sesión del administrador, puede hacer clic en **¿Contraseña olvidada?** para reiniciarlo. Ver el manual del usuario. Hacer clic **Iniciar sesión.**

Paso 3

Se muestra la página de inicio de la web.

Apéndice 1 Notas de grabación de rostros

Antes del registro

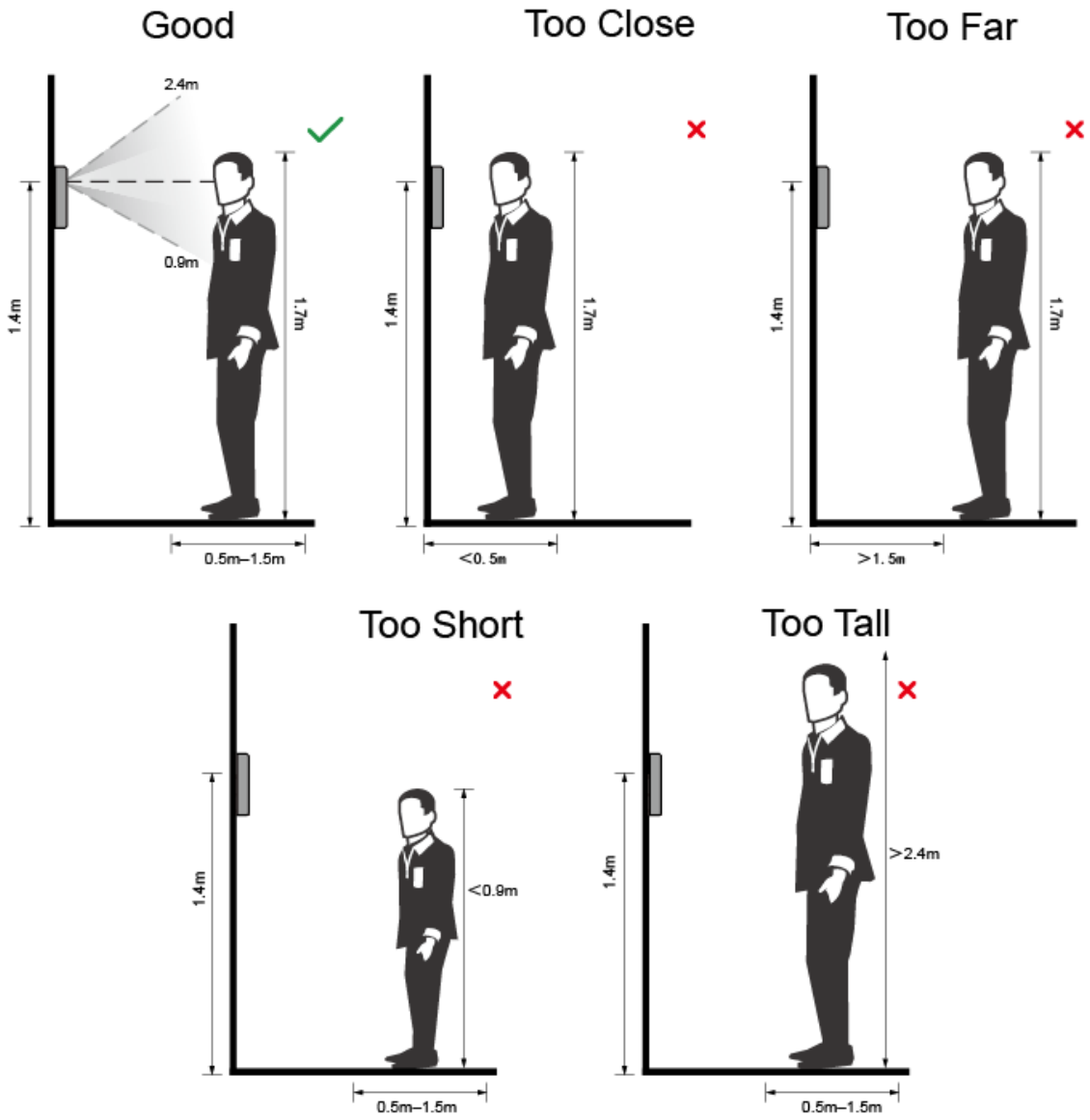
- Las gafas, sombreros y barbas pueden influir en el rendimiento del reconocimiento facial.
- No cubra las cejas cuando use sombreros.
- No cambie mucho el estilo de su barba si va a usar el dispositivo; de lo contrario, el reconocimiento facial podría fallar.

- 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 solar directa podría influir en el rendimiento del reconocimiento facial del dispositivo.

Posición de la cara

Si su cara no está en la posición adecuada, el efecto de reconocimiento facial puede verse influenciado.

Apéndice figura 1-1 Posición de la cara adecuada

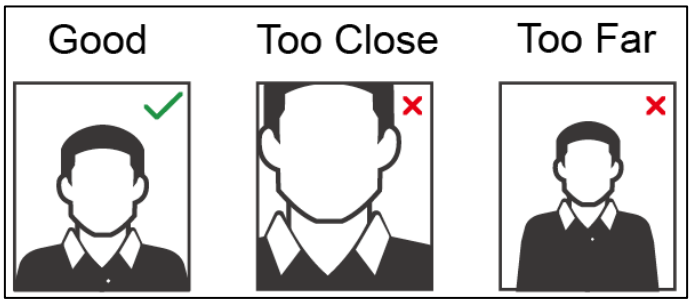


Requisitos de caras

- Asegúrese de que la cara esté limpia y que la frente no esté cubierta por pelo.
- No use anteojos, sombreros, barbas gruesas u otros adornos faciales que influyan en la grabación de imágenes faciales.
- Con los ojos abiertos, sin expresiones faciales, y haz que tu cara esté 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 1-2 Posición de la cabeza

Apéndice figura 1-3 Distancia de la cara



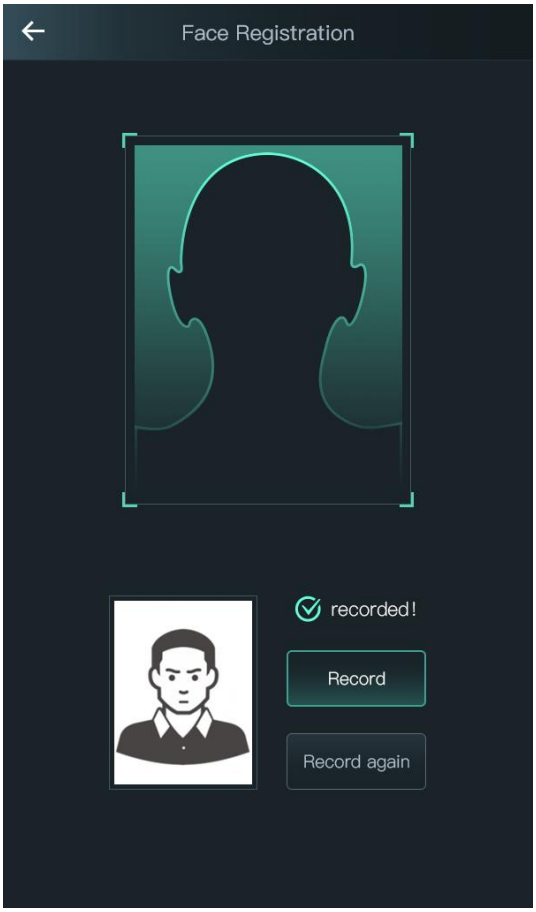
- Al importar imágenes faciales a través de la plataforma de administración, asegúrese de que la resolución de la imagen esté dentro del rango de 150 × 300–600 × 1200; los píxeles de la imagen son más de 500 × 500; el tamaño de la imagen es inferior a 75 KB, y el nombre de la imagen y la identificación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

Durante el registro

Puede registrar caras a través del controlador de acceso o la plataforma. Para registrarse a través de la plataforma, consulte el manual del usuario de la plataforma.

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

Apéndice figura 1-4 Registro



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

Apéndice 2 Instrucción de registro de huellas digitales

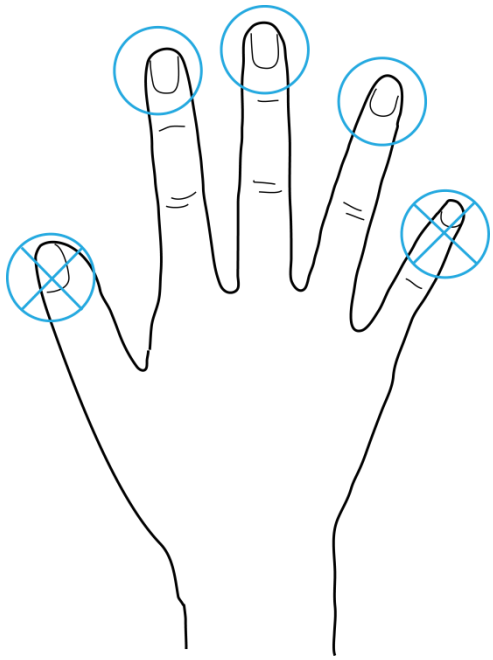
aviso

- Asegúrese de que sus dedos estén limpios y secos antes de registrar sus huellas digitales.
- Presione su dedo hacia el área de grabación de huellas digitales y haga que su huella digital se centre en el área de grabación.
- No coloque el sensor de huellas digitales en lugares con luz intensa, alta temperatura y alta humedad.
- Para aquellos cuyas huellas digitales están desgastadas o no están claras, pruebe otros métodos de desbloqueo.

Dedos recomendados

Se recomiendan los dedos índice, medio y anular. Los pulgares y los meñiques no pueden colocarse fácilmente en el centro de grabación.

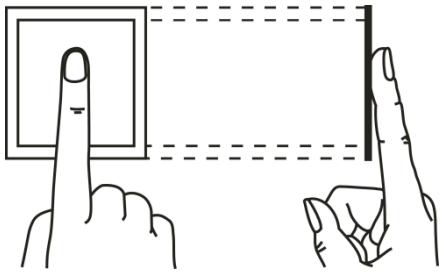
Apéndice figura 2-1 Dedos recomendados



Método de prensado de dedos

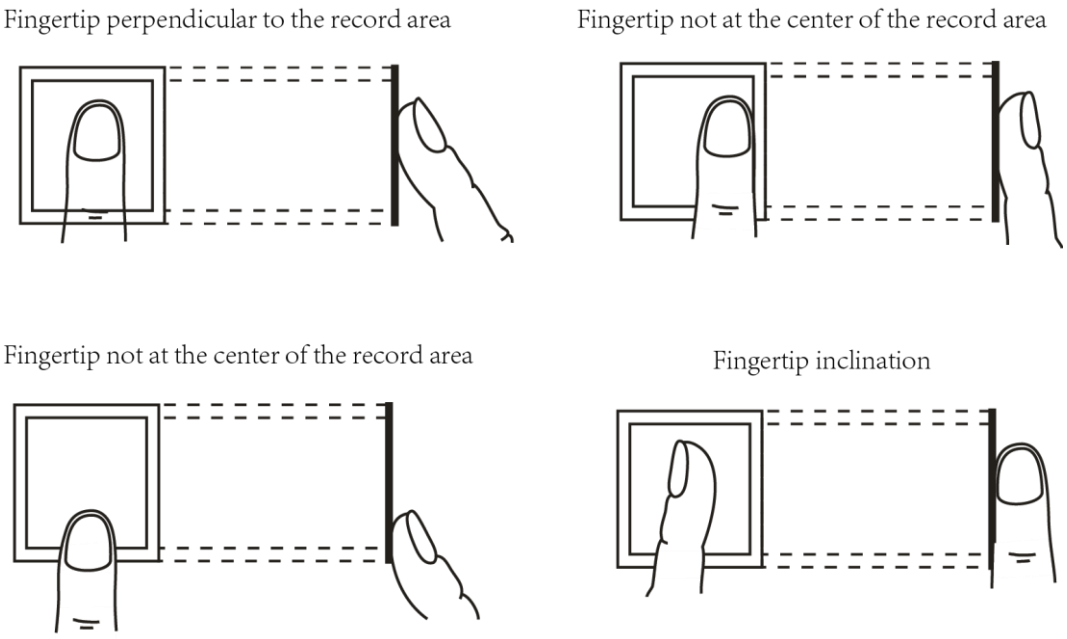
- Método correcto

Figura 2-2 del apéndice Al presionar correctamente el dedo



- Método incorrecto

Apéndice figura 2-3 Al presionar con el dedo incorrectamente



Apéndice 3 Recomendaciones de ciberseguridad

La ciberseguridad es más que una simple 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 presentan algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias a tomar para la seguridad de la red del equipo básico:

1. Use 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 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 del cliente a tiempo

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

- Sugerimos que descargue y use la última versión del software del cliente.

Recomendaciones "agradables de tener" para mejorar la seguridad de la red de su equipo:

1. Protección física

Sugerimos que realice protección física a los equipos, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en una sala y gabinete de computadoras especiales e implemente un permiso de control de acceso bien hecho y una administración de claves para evitar que personal no autorizado realice contactos físicos como daños en el hardware, conexión no autorizada de equipos extraíbles (como un disco flash USB). , puerto serie), etc.

2. Cambie las contraseñas regularmente

Sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinado o descifrado.

3. Establecer y actualizar las contraseñas Restablecer la información a tiempo

El equipo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluidas las preguntas de protección del buzón y la contraseña del usuario final. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección con contraseña, se sugiere no utilizar las que se puedan adivinar fácilmente.

4. Habilitar 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 los puertos HTTP y otros servicios predeterminados

Le sugerimos que cambie los puertos HTTP y otros puertos de servicio predeterminados en cualquier conjunto de números entre 1024 ~ 65535, lo que reduce el riesgo de que personas externas 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. Habilite la lista blanca

Le sugerimos que habilite la función de lista blanca para evitar que todos, excepto aquellos con direcciones IP especificadas, accedan al sistema. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del equipo que lo acompaña a la lista blanca.

8. Enlace de dirección MAC

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

9. Asignar cuentas y privilegios razonablemente

De acuerdo con los requisitos comerciales y de gestión, agregue razonablemente usuarios y asígneles un conjunto mínimo de permisos.

10. Desactiva los servicios innecesarios y elige 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 seguras y contraseñas de autenticación.
- 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.

11. Transmisión cifrada de audio y video

Si el contenido de sus 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 encriptada causará alguna pérdida en la eficiencia de la transmisión.

12. Auditoría segura

- Verificar usuarios en línea: le sugerimos que revise los usuarios en línea regularmente para ver si el dispositivo está conectado sin autorización.
- Verifique el registro del equipo: al ver los registros, puede conocer las direcciones IP que se utilizaron para iniciar sesión en sus dispositivos y sus operaciones clave.

13. Registro de red

Debido a la capacidad de almacenamiento limitada del equipo, 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 el 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 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 utilizar VLAN, GAP de red y otras tecnologías para particionar 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.