Terminal de reconocimiento facial

Guía de inicio rápido

V1.0.0

Prefacio

General

Este manual presenta la instalación y el funcionamiento básico del terminal de reconocimiento facial (en lo sucesivo, "terminal").

Las instrucciones de seguridad

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

Palabras de advertencia	Sentido
PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
NOTA	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento	agosto 2019

Sobre el Manual

- El manual es solo para 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 cumplen con el manual.
- El manual se actualizaría 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 de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Todavía puede haber desviación en los datos técnicos, descripción de funciones y operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final. Actualice el software del lector o
- pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).

- Todas las marcas comerciales, marcas comerciales registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio al cliente si ocurre algún problema al usar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

Medidas de seguridad y advertencias importantes

Este capítulo describe el contenido que cubre el manejo adecuado del terminal, la prevención de riesgos y la prevención de daños a la propiedad. Lea este contenido detenidamente antes de utilizar el terminal, respételo cuando lo utilice y guárdelo para futuras consultas.

Requisito 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 un 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 sobre 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.
- Transporte, utilice y almacene el terminal en las condiciones de humedad y temperatura permitidas.

Seguridad ELECTRICA

- El uso inadecuado de la batería puede provocar un incendio, una explosión o una
- inflamación. Cuando reemplace 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.
- Utilice el adaptador de corriente proporcionado con el terminal; de lo contrario, podría provocar lesiones personales y daños en el dispositivo.
- La fuente de alimentación debe cumplir con los requisitos del estándar de seguridad de voltaje extra bajo (SELV) y suministrar energía con un voltaje nominal que cumpla con el requisito de fuente de alimentación limitada de acuerdo con IEC60950-1. Tenga en cuenta que el requisito de fuente de alimentación está sujeto a la etiqueta del dispositivo.
- Conecte el dispositivo (estructura tipo I) a la toma de corriente con puesta a tierra de protección. El acoplador
- del aparato es un dispositivo de desconexión. Cuando use el acoplador, mantenga el ángulo para facilitar la operación.

Tabla de contenido

1 Dimensiones y Componentes

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

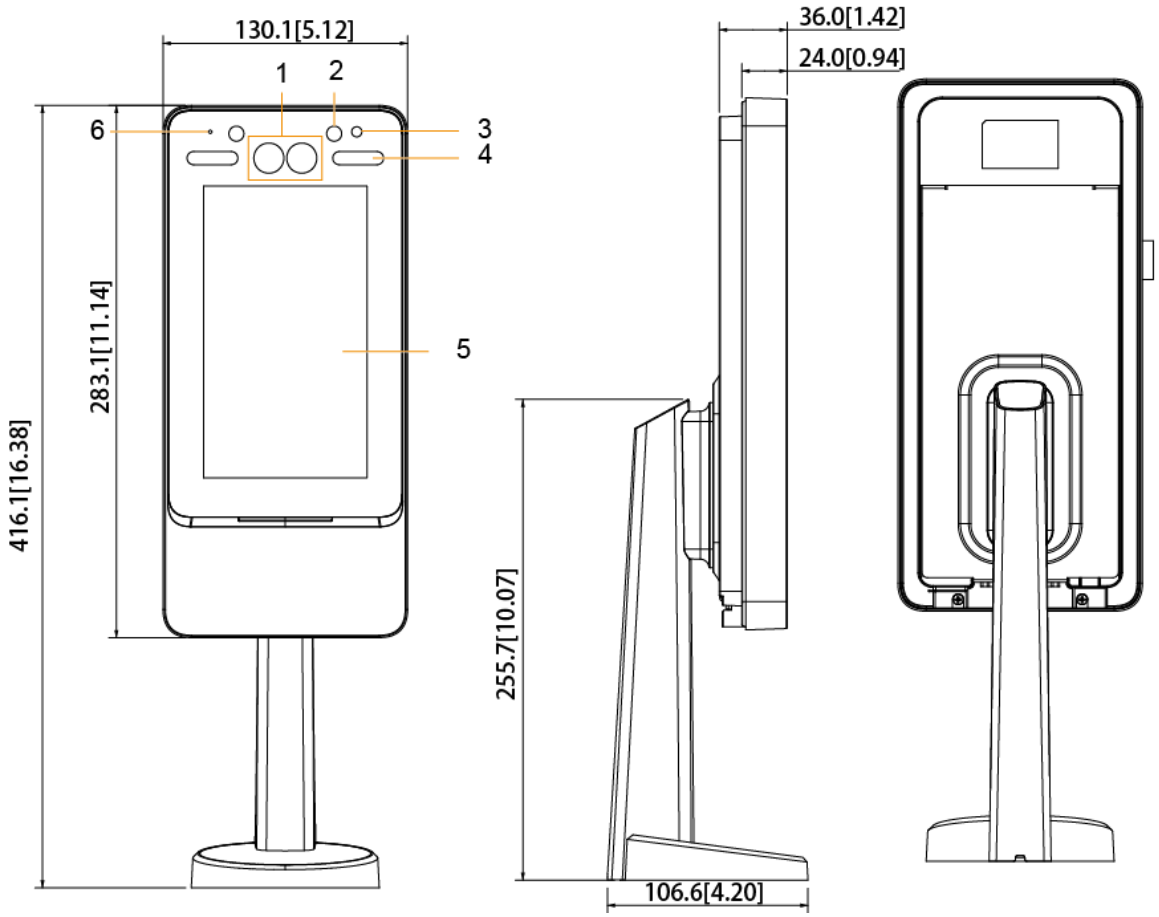


Tabla 1-1 Descripción del componente

No.	Nombre
1	Cámara doble
2	luz infrarroja
3	fototransistor
4	Luz de relleno blanca
5	Mostrar
6	MICRÓFONO

2 Instalación

2.1 Notas de instalación

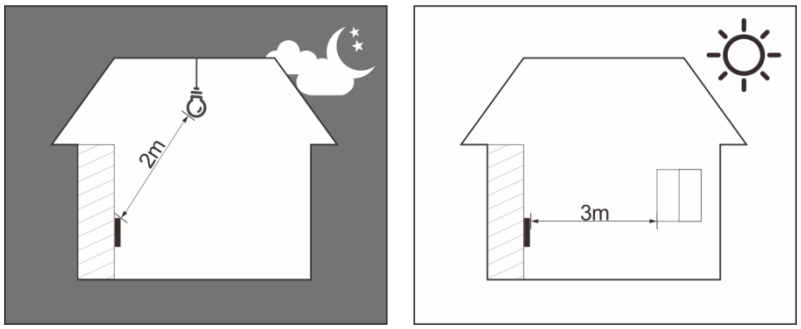
- Si hay una fuente de luz a 0,5 metros del dispositivo, la iluminación mínima debe ser no menos de 100Lux.
- Se recomienda instalar el dispositivo en interiores, a una distancia mínima de 3 metros de ventanas y puertas y a 2 metros de distancia de luces.
- Evite la luz de fondo y la luz solar directa.

Requisito de iluminación ambiental

Figura 2-1 Requisito de iluminación ambiental

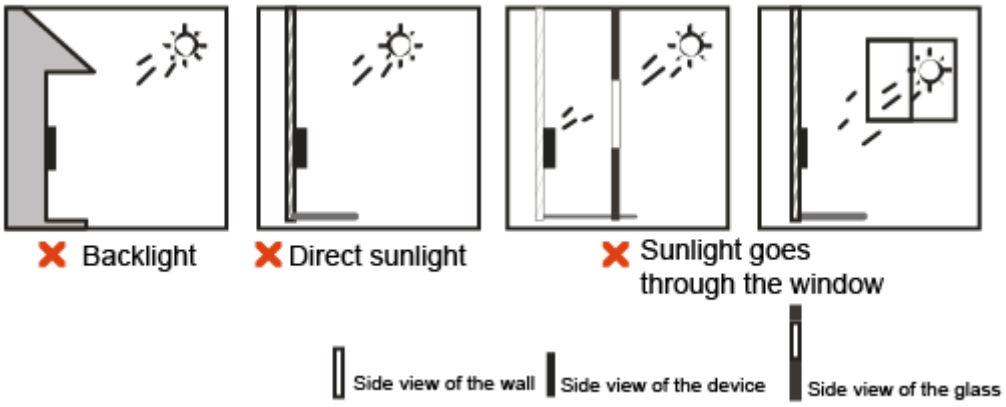
Lugares Recomendados

Figura 2-2 Lugares recomendados



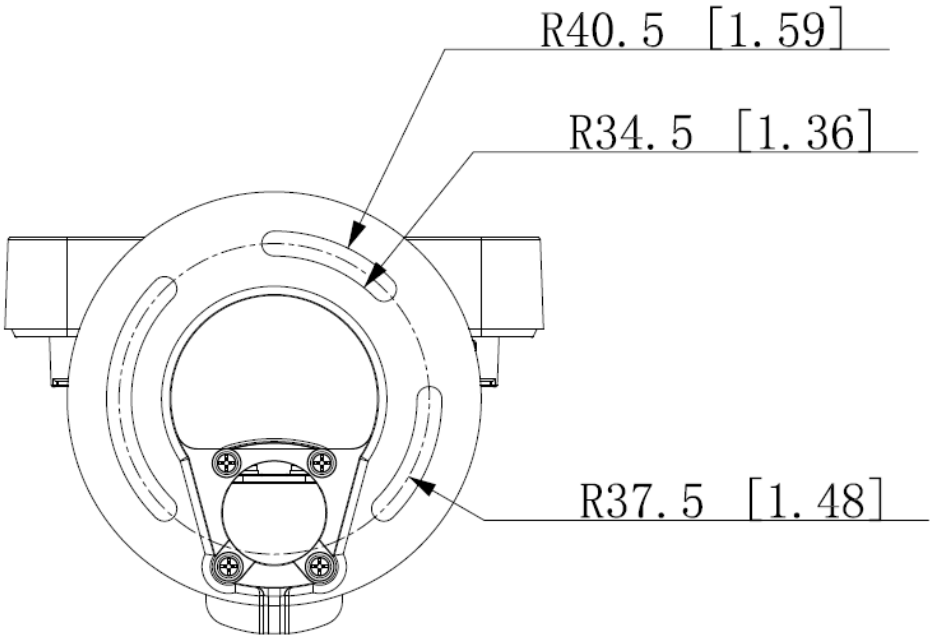
Lugares No Recomendados

Figura 2-3 Lugares no recomendados



2.2 Planos de instalación

Figura 2-4 Dibujos de instalación (mm [pulgadas])



2.3 Conexiones de cables

- 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 habilitado el módulo de seguridad, el botón de salida, control de torniquete y extinción de incendios la vinculación no será válida.

Figura 2-5 Conexión de cables

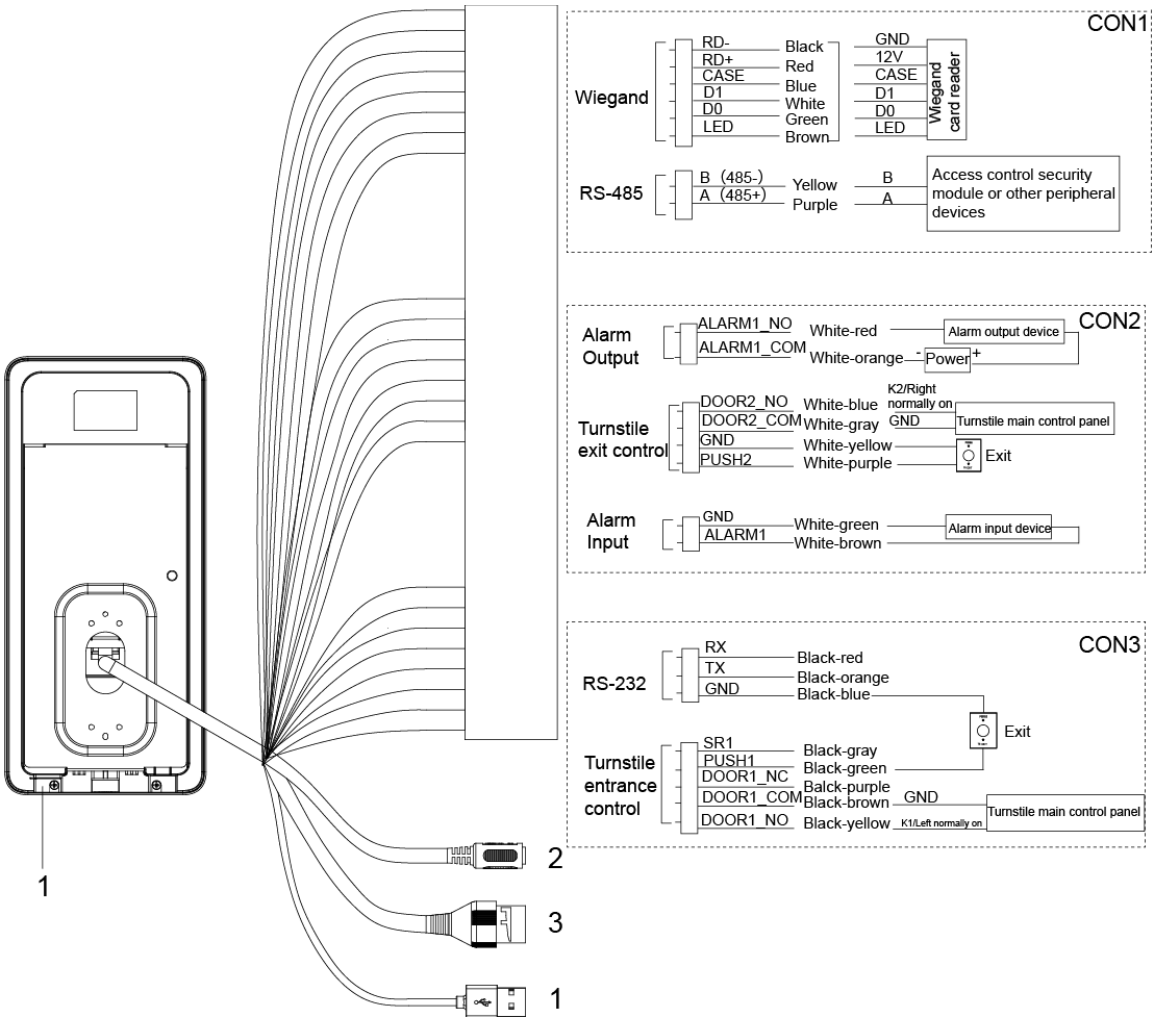


Tabla 2-1 Descripción del componente

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

2.4 Instalación

Figura 2-6 Instalado en la máquina de puerta

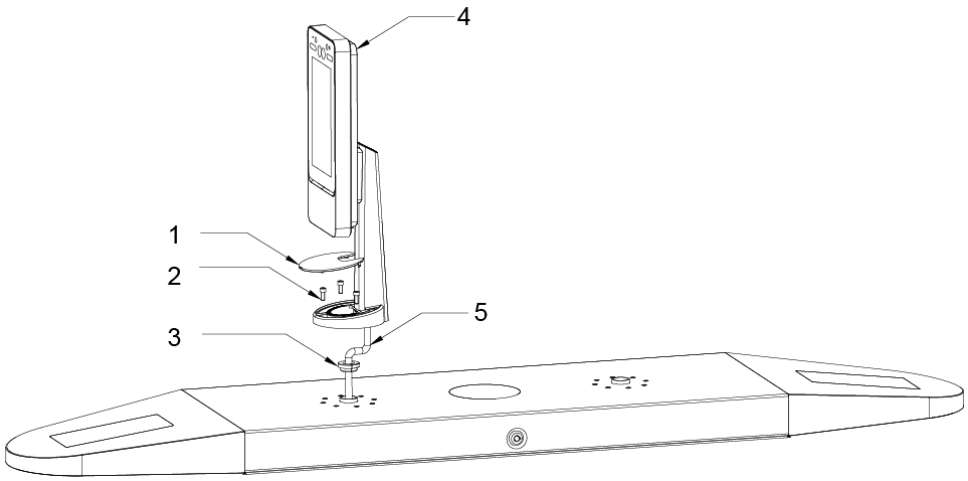


Tabla 2-2 Descripción de los componentes

No.	Nombre
1	cubierta ornamental
2	tornillo M5
3	Tapón de gel de sílice resistente al agua
4	Terminal
5	Cable

Procedimiento de instalación

Paso 1 Pase el cable a través del torniquete.

Paso 2 Coloque el enchufe de gel de sílice a prueba de agua en el cable. Fije el

Paso 3 terminal en el torniquete con tornillo M5. Conecte los cables para el terminal. Consulte "2.3 Conexiones de cables".

Etapa 4 Aplique sellador a los espacios entre el tapón impermeable de gel de sílice y el

Paso 5 torniquete. Instale la cubierta ornamental en la base del terminal.

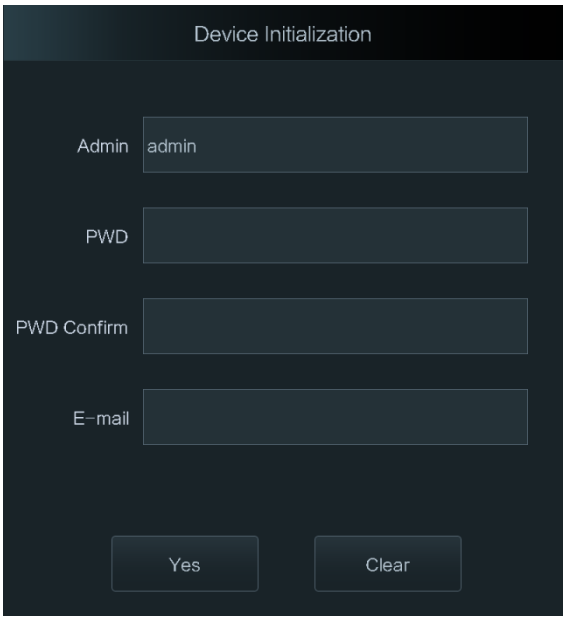
La instalación está terminada.

3 Operación del sistema

3.1 Inicialización

La contraseña de administrador y un correo electrónico deben configurarse la primera vez que se enciende el terminal; de lo contrario, no se puede utilizar el terminal. Consulte la 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 el 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 ' " ; : &).
- Para terminales sin pantalla táctil, la inicialización se puede completar a través de la web. Ver el manual de usuario para más detalles.

3.2 Adición de nuevos usuarios

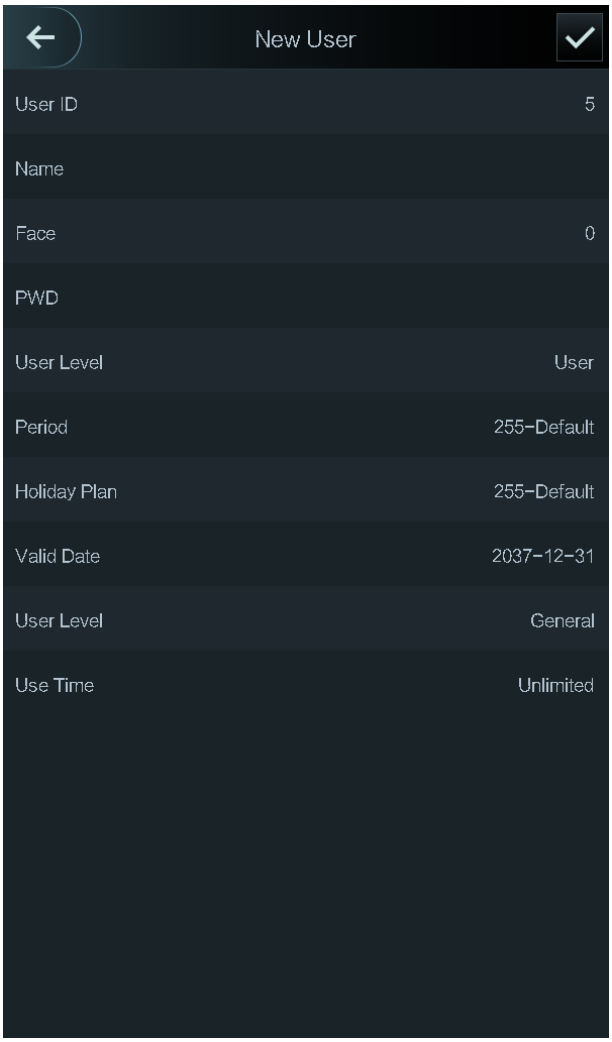
Puede agregar nuevos usuarios ingresando sus ID de usuario, nombres, importando imágenes de rostros, contraseñas, seleccionando sus niveles de usuario y más.

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

los**Nuevo Usuario**se muestra la interfaz. Consulte la Figura 3-2.

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

Figura 3-2 Nuevo usuario



Paso 2 Configure los parámetros en la interfaz. Consulte la Tabla 3-1.

Tabla 3-1 Descripción del nuevo parámetro de usuario

Parámetro	Descripción
ID de usuario	Puede introducir ID de usuario. Los ID constan de 32 caracteres (incluidos números y letras), y cada ID es único.
Nombre	Puede ingresar nombres con un máximo de 32 caracteres (incluidos números, símbolos y letras).
Rostro	Asegúrese de que su rostro esté centrado en el marco de captura de imágenes y luego se capturará automáticamente una imagen de su rostro. Para obtener más información sobre la grabación de imágenes de rostros, consulte el "Apéndice 1 Notas sobre la grabación de rostros".
Clave	La contraseña de desbloqueo de la puerta. La longitud máxima de los dígitos de identificación es 8. Si el terminal no tiene pantalla táctil, debe conectar el terminal a un lector de tarjetas periférico. Hay botones en el lector de tarjetas.

Parámetro	Descripción
Nivel	Puede seleccionar un nivel de usuario para los nuevos usuarios. Hay dos opciones. - Usuario: los usuarios solo tienen autoridad para desbloquear puertas. - Admin: los administradores no solo pueden desbloquear la puerta, sino que también tienen autoridad para configurar parámetros. En caso de que olvide la contraseña de administrador, es mejor que cree más de un administrador.
Período	Puede establecer un período en el que el usuario puede desbloquear la puerta. Para obtener información detallada sobre la configuración del período, consulte el manual de configuración.
Fiesta Plan	Puede establecer un plan de vacaciones en el que el usuario puede desbloquear la puerta. Para obtener información detallada sobre los ajustes 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 en la lista negra abren la puerta, el personal de servicio recibirá un aviso. - Invitado: los invitados pueden desbloquear la puerta en ciertos momentos en ciertos períodos. Una vez superados los tiempos y plazos máximos, no podrán volver a desbloquear la puerta. - Patrulla: los usuarios de Patrulla pueden hacer un seguimiento de su asistencia, pero no tienen autoridad de desbloqueo. - VIP: cuando VIP abre la puerta, el personal de servicio recibirá un aviso. Deshabilitar: - cuando las personas discapacitadas abren 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.

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

Para terminales sin pantalla táctil, la adición de nuevos usuarios se puede completar a través del web. Consulte el manual del usuario para obtener más información.

4 Operación web

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

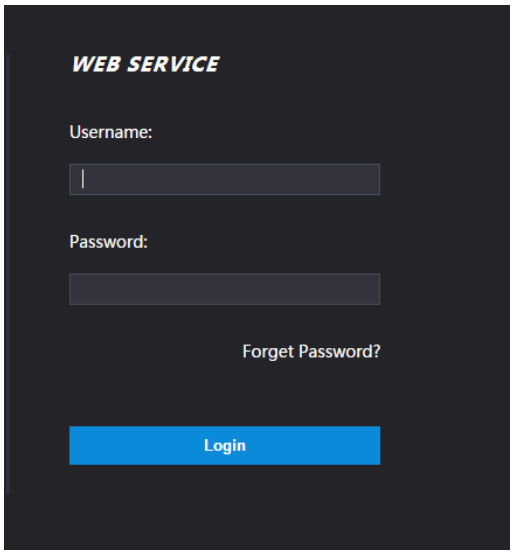
Acceso

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 terminal en la barra de direcciones y luego presione Enter.

Figura 4-1 Inicio de sesión



Paso 2 Introduzca el nombre de usuario y la contraseña.

- El nombre de usuario predeterminado del administrador es admin , y la contraseña es el inicio de sesión contraseña después de inicializar el Terminal . Modificar la contraseña de administrador regularmente y guárdelo adecuadamente por seguridad.
- Si olvida la contraseña de inicio de sesión del administrador, puede hacer clic en**¿Contraseña olvidada?**para reinicialo. Consulte el manual del usuario.

Paso 3 Hacer clic**Acceso**.

Se muestra la página de inicio de la web.

Apéndice 1 Notas sobre la grabación de rostros

Antes del registro

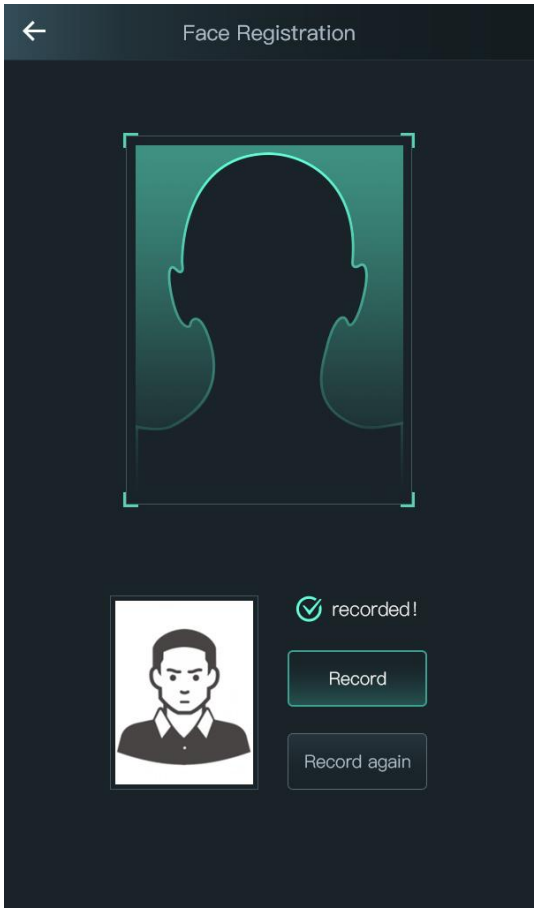
- Las gafas, los sombreros y la barba pueden influir en el rendimiento del
- reconocimiento facial. No cubra sus cejas cuando use sombreros.
- No cambie mucho su estilo de barba si va a usar el dispositivo; de lo contrario, el reconocimiento facial podría fallar.
- Mantén tu cara limpia.
- Mantenga el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

Durante el registro

Puedes registrar rostros a través de la terminal o a través de la plataforma. Para el registro 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. Una imagen de su cara será capturada automáticamente.

Apéndice figura 1-1 Registro

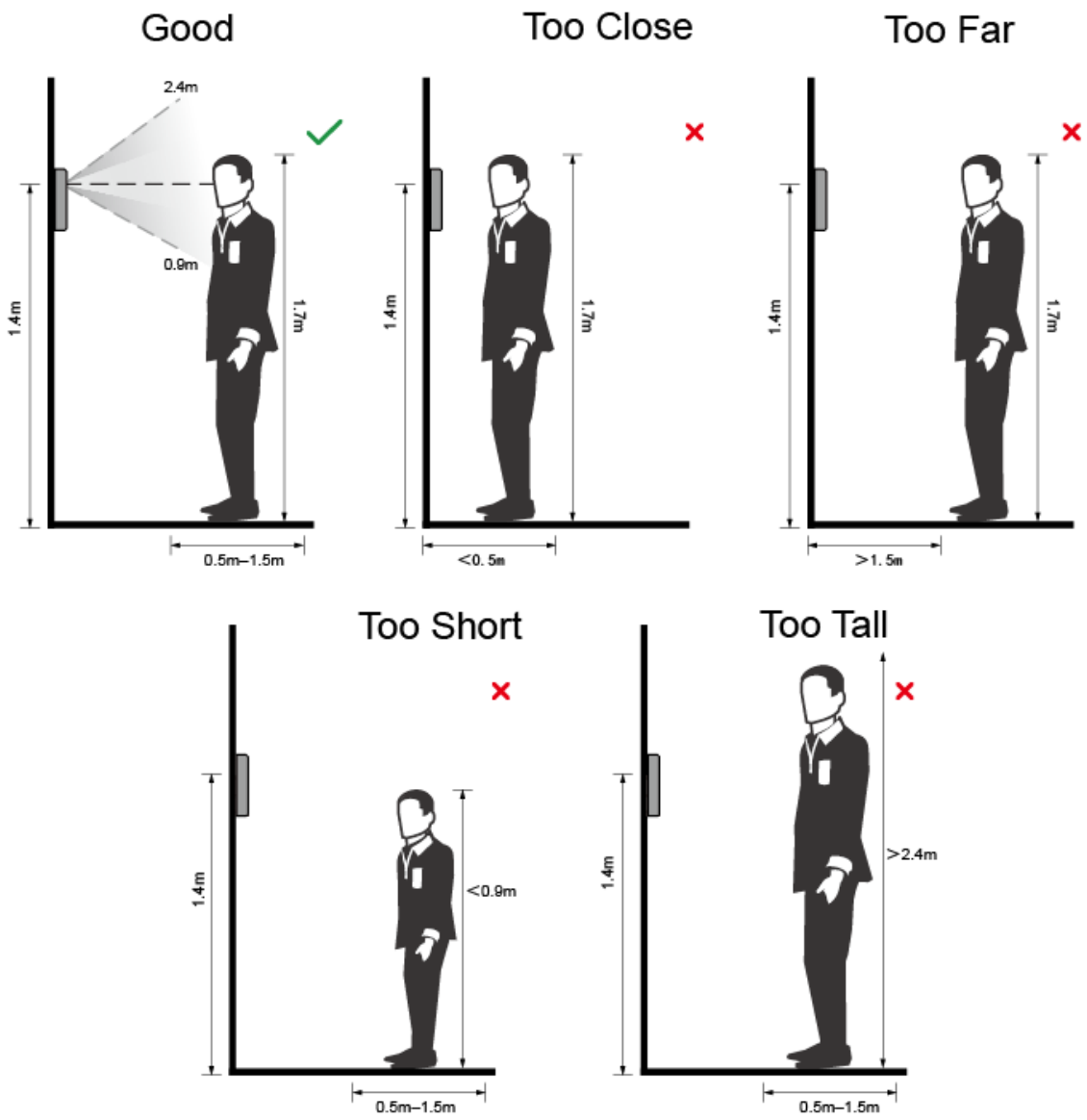


- No sacuda la cabeza o el cuerpo, o el registro podría fallar.
- Evita que aparezcan dos caras en el cuadro al mismo tiempo.

Posición de la cara

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

Apéndice figura 1-2 Posición adecuada de la cara

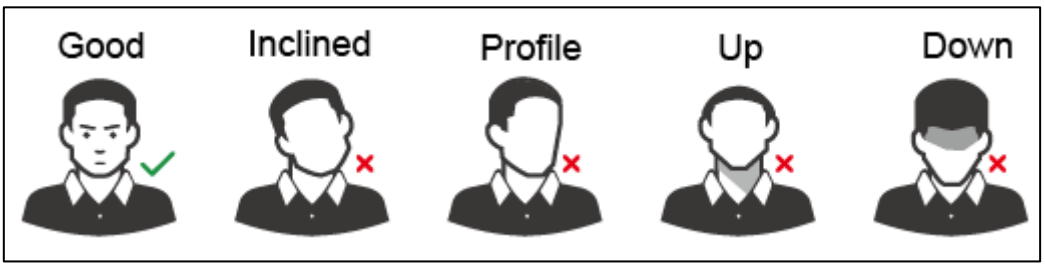


Requisitos de las caras

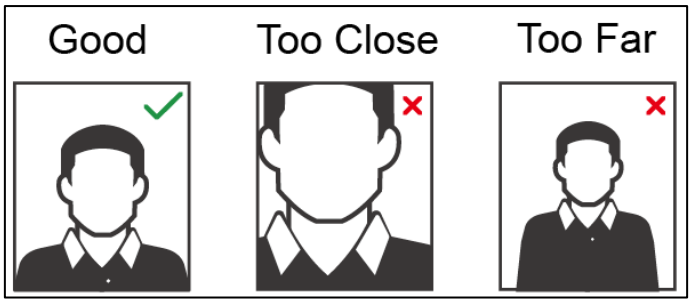
- Asegúrese de que la cara esté limpia y que la frente no esté cubierta por pelo.
- No use anteojos, sombreros, barbas pobladas u otros adornos faciales que influyan en la grabación de imágenes faciales.
- Con los ojos abiertos, sin expresiones faciales, y haz que tu cara esté hacia el centro de la cámara.
- Cuando grabe su rostro o durante el reconocimiento facial, no mantenga su rostro demasiado cerca o

demasiado lejos de la cámara.

Apéndice figura 1-3 Posición de la cabeza



Apéndice figura 1-4 Distancia entre caras



- Al importar imágenes de rostros a través de la plataforma de administración, asegúrese de que la imagen la resolución está 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 el ID de la persona son los mismos.
- Asegúrese de que la cara no ocupe 2/3 del área total de la imagen y que la relación de aspecto no no exceda de 1:2.

Apéndice 2 Recomendaciones sobre 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 presentan algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias a tomar para la seguridad de la red de equipos básicos: 1.

Usar 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 tecnológica, 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 "autoverificación de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones "agradables de tener" para mejorar la seguridad de su red de equipos: 1. Protección física

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

2. Cambie las contraseñas regularmente

Le sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinadas o descifradas.

3. Establezca y actualice la información de restablecimiento de contraseñas a tiempo

El equipo 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 de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección de contraseña, se sugiere no utilizar aquellas que se pueden 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 varias veces con la contraseña incorrecta, 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 a cualquier conjunto de números entre 1024 y 65535, lo que reduce el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.

6. Habilitar HTTPS

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

7. Habilitar lista blanca

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

8. Enlace de dirección MAC

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

9. Asigne cuentas y privilegios de manera razonable

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

10. 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.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de encriptación WPA2-PSK y configure contraseñas seguras.

11. Transmisión encriptada de audio y video

Si el contenido de sus datos de audio y video es muy importante o confidencial, 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 cierta pérdida en la eficiencia de la transmisión.

12. Auditoría segura

- Verifique a los usuarios en línea: le sugerimos que verifique a 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 usaron para iniciar sesión en sus dispositivos y sus operaciones clave.

13. Registro de red

Debido a la limitada capacidad de almacenamiento del equipo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, se recomienda habilitar la función de registro de red para asegurarse de que los registros críticos se sincronizan con el servidor de registro de red para su seguimiento.

14. Construya 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 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, GAP de red 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.