Controlador de acceso de reconocimiento facial

Guía de inicio rápido

V1.0.0

Prefacio

General

Este manual presenta la instalación y las operaciones básicas del controlador de acceso de reconocimiento facial (en lo sucesivo, "controlador de acceso").

Las instrucciones de seguridad

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

Palabras de advertencia	Significado
PELIGRO	Indica un peligro de alto 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 provocar 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 revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	junio 2020

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 controlador de acceso, la prevención de riesgos y la prevención de daños a la propiedad. Lea este contenido detenidamente antes de utilizar el controlador de acceso, respételo cuando lo utilice y conserve el manual para futuras consultas.

Requisitos de operación

- No coloque ni instale el controlador de acceso en un lugar expuesto a la luz solar o cerca de una 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 un 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 sobre 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
- energía. No desmonte el controlador de acceso al azar.
- Para el controlador de acceso con una unidad de monitoreo de temperatura:
  - ◇ Instale la unidad de control de temperatura en un entorno interior sin viento y mantenga la temperatura ambiente interior entre 10 °C y 40 °C.
  - ◇ Caliente la unidad de control de temperatura durante más de una hora 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 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 controlador de acceso; 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

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

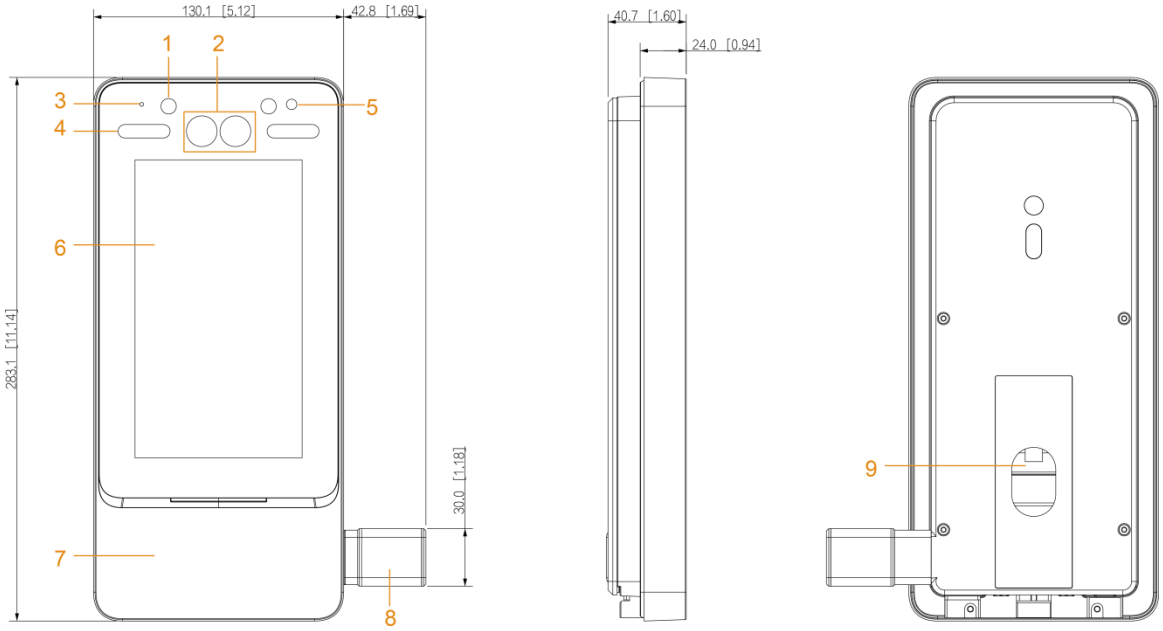


Tabla 1-1 Descripción del componente

No.	Nombre	No.	Nombre
1	luz infrarroja	5	fototransistor
2	Cámaras duales	6	Mostrar
3	Micrófono	7	Área de deslizamiento de tarjetas
4	Iluminador LED blanco	8	Unidad de control de temperatura
9	Entrada de cable	—	—

2 Instalación

2.1 Notas de instalación

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

Requisito de iluminación ambiental

Figure 2-1 Requisito de iluminación ambiental

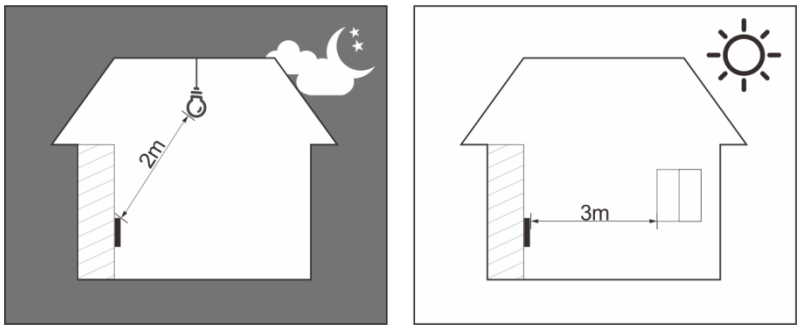
Requisito de monitoreo de temperatura

- Se recomienda instalar la unidad de monitoreo de temperatura en un ambiente interior sin viento (un área relativamente aislada del exterior) y mantener la temperatura ambiente entre 10 °C y 40 °C.
- Caliente la unidad de control de temperatura durante más de una hora después del encendido para permitir que la unidad de control de temperatura alcance el equilibrio térmico.
- Si no hay un ambiente interior adecuado (incluidas las áreas que dan directamente a las áreas interiores y exteriores, y las puertas exteriores), establezca un pasaje temporal con una temperatura ambiente estable para monitorear la temperatura.
- Los factores como la luz solar, el viento, el aire frío y el aire acondicionado 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 medida y la temperatura real. .
- Factores que influyen en el control de la temperatura
  - ◇ Viento: el viento quitará el calor corporal, lo que afectará la precisión del control de la temperatura.
  - ◇ Sudoración: la sudoración es una forma en que el cuerpo se enfría automáticamente y disipa el calor. 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 ambiente es demasiado alta, el cuerpo humano comenzará a sudar, lo que afectará la precisión del control de la temperatura.
  - ◇ La unidad de monitoreo de temperatura es sensible a las ondas de luz con una longitud de onda de 10um a 15um. Evite usarlo bajo el sol, fuentes de luz fluorescente, tomas de aire acondicionado,

calefacción, salidas de aire frío y superficies de vidrio.

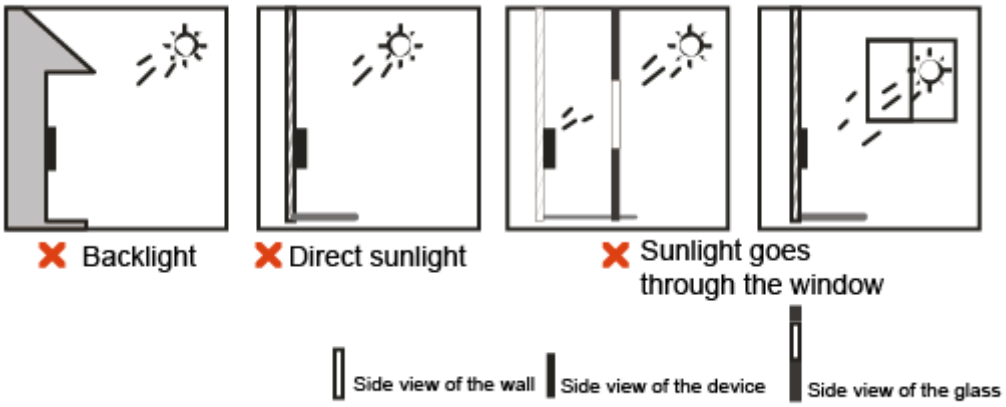
Lugares Recomendados

Figure 2-2 Lugares recomendados



Lugares No Recomendados

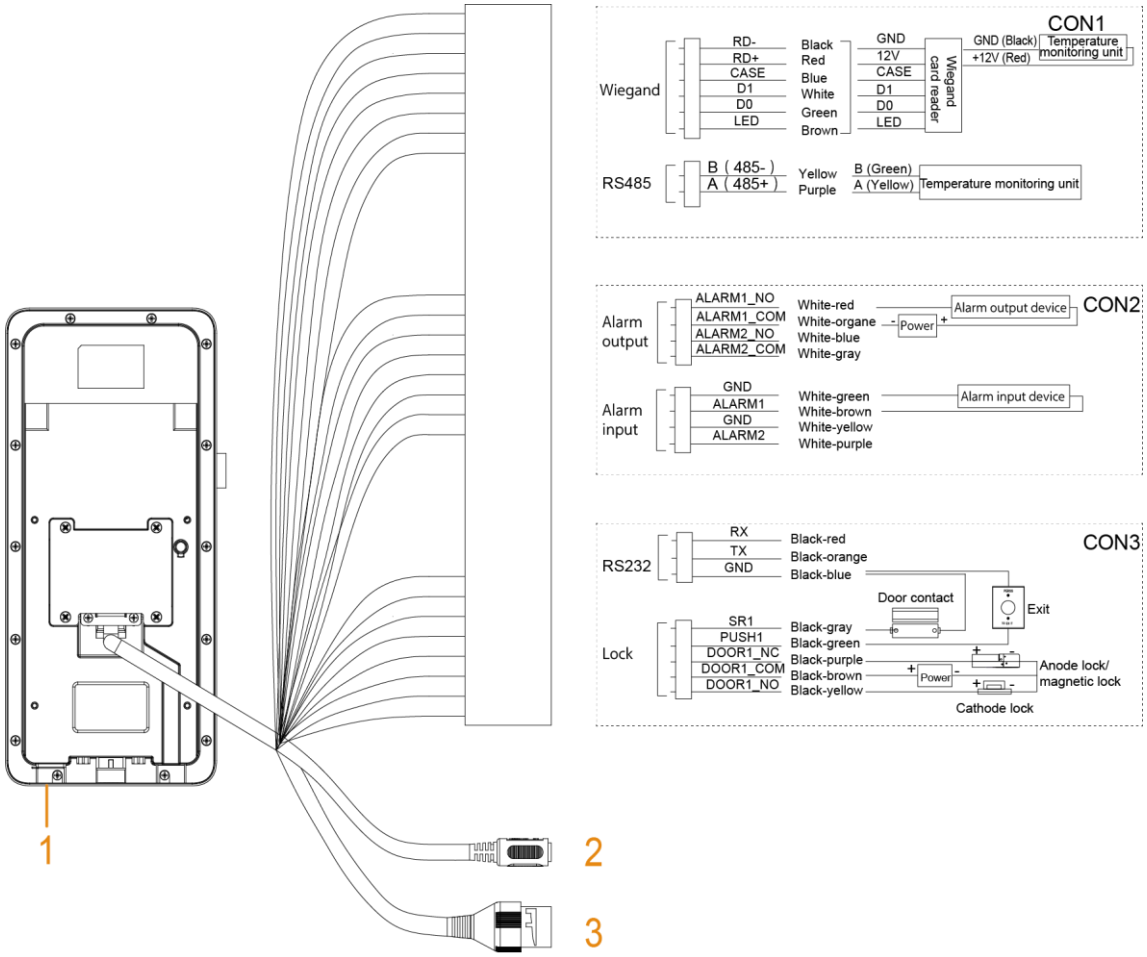
Figure 2-3 Lugares no recomendados



2.2 Conexiones de cables

- Compruebe si el módulo de seguridad de control de acceso está habilitado en**Función > Seguridad Módulo**. Si está habilitado, debe comprar el módulo de seguridad de control de acceso por separado. Él el módulo de seguridad necesita una fuente de alimentación independiente.
- Una vez habilitado el módulo de seguridad, el botón de salida, control de cerradura, enlace contra incendios y el monitor de temperatura no será válido.

Figure 2-4 Conexión de cable



- Conecte el cable negro de la unidad de control de temperatura al cable negro correspondiente cable en CON1.
- Conecte el cable rojo de la unidad de control de temperatura al cable rojo correspondiente en CON1.
- Conecte el cable amarillo de la unidad de control de temperatura al cable violeta en CON1.
- Conecte el cable verde de la unidad de control de temperatura al cable amarillo en CON1.

Tabla 2-1 Descripción del componente

No.	Nombre
1	Puerto USB
2	Puerto de alimentación
3	puerto de red

2.3 Instalación

Asegúrese de que la distancia entre la lente y el suelo sea de 1,4 metros. Consulte la Figura 2-5.

Figure 2-5 Altura de instalación

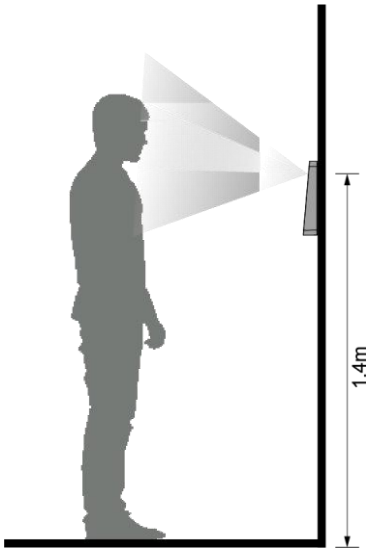


Figure 2-6 Instalación

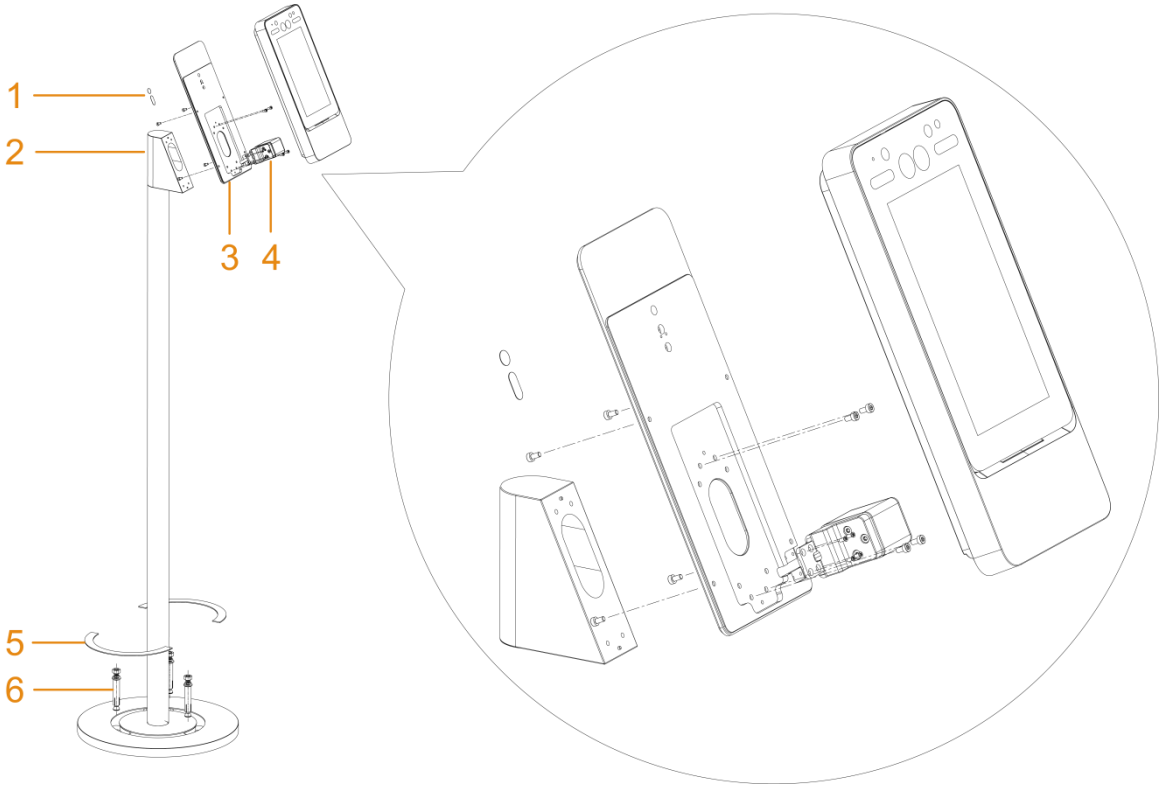


Tabla 2-2 Descripción de los componentes

No.	Nombre
1	Parche decorativo para los dos agujeros en el panel trasero de la placa de montaje.
2	Adaptador de tubo redondo de acero.
3	Placa de montaje.
4	La unidad de control de temperatura.
5	Parche decorativo para cubrir la base del bracket.
6	Perno de expansión.

Procedimiento de instalación

Step 1 Fije la placa de montaje al adaptador de tubo redondo de acero del soporte de piso con 4 tornillos.

Step 2 Fije la unidad de control de temperatura a la placa de montaje con 4 tornillos.

Step 3 Conecte los cables entre la unidad de control de temperatura y el controlador de acceso. Consulte "2.2 Conexiones de cables". Y luego aplique cinta impermeable a las uniones del cable.

Step 4 Fije el controlador de acceso en la placa de montaje con 4 tornillos.

Step 5 Pase los cables a través del soporte y luego conecte los cables para el controlador de acceso. Consulte "2.2 Conexiones de cables". Y luego aplique cinta impermeable a las uniones del cable.

Step 6 Fije el soporte al suelo con 4 tornillos de expansión.

Step 7 Cubra la base del soporte y los dos orificios en el panel posterior de la placa de montaje con los parches decorativos correspondientes.

3 Operaciones del sistema

3.1 Inicialización

La contraseña de administrador y un correo electrónico deben configurarse la primera vez que se enciende el controlador de acceso; de lo contrario, no se puede utilizar el controlador de acceso.

Figure 3-1 Inicialización

- La contraseña de administrador se puede restablecer a través de la dirección de correo electrónico que ingresó si el se olvida la contraseña.
- 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 el controlador de acceso sin pantalla táctil, inicialice a través de la interfaz web. Ver el manual de usuario para más detalles.

3.2 Adición de nuevos usuarios

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

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

Step 1 En la interfaz de espera, mantenga presionada la pantalla para ir a la**Inicio de sesión del administrador** interfaz.

Step 2 Tocar**Administración**para iniciar sesión en el**Menú principal**interfaz con una cuenta de administrador.

Step 3 Seleccione**Usuario > Nuevo usuario**.

Figure 3-2 Nuevo Usuario

Step 4 Configure los parámetros en la interfaz.

Tabla 3-1 Descripción del nuevo parámetro de usuario

Parámetro	Descripción
ID de usuario	Introduzca los ID de usuario. Los ID constan de 32 caracteres (incluidos números y letras), y cada ID es único.
Nombre	Introduzca 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 caras, consulte el "Apéndice 2 Notas sobre la grabación/comparación de caras".
Tarjeta	Puede registrar como máximo 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 de tarjeta de coacción en la interfaz de registro de tarjeta. Las alarmas se activarán si se utiliza una tarjeta de coacción para desbloquear la puerta. Si el controlador de acceso no tiene un módulo de lectura de tarjetas, debe conectar el dispositivo a los lectores de tarjetas periféricos.

PCD	La contraseña de desbloqueo de la puerta. La longitud máxima de la contraseña es de 8 dígitos. 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 los nuevos usuarios. Hay dos opciones. ● Usuario: los usuarios solo tienen permiso para abrir 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, es mejor que cree más de un administrador.
Período	El período en el que el usuario puede desbloquear la puerta. Para obtener información detallada sobre la configuración del período, consulte el manual del usuario.
Fiesta Plan	Puede establecer un plan de vacaciones en el que el usuario puede desbloquear la puerta. Para obtener información detallada sobre la configuración 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.
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 permiso de desbloqueo. ● VIP: cuando VIP abre la puerta, el personal de servicio recibirá un aviso. Especial: ● cuando personas especiales 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**Huésped**, puede establecer las veces máximas que el huésped puede desbloquear la puerta.

Step 5 Tocar  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 gestión. Ver detalles en el manual de usuario.

4 Operaciones Web

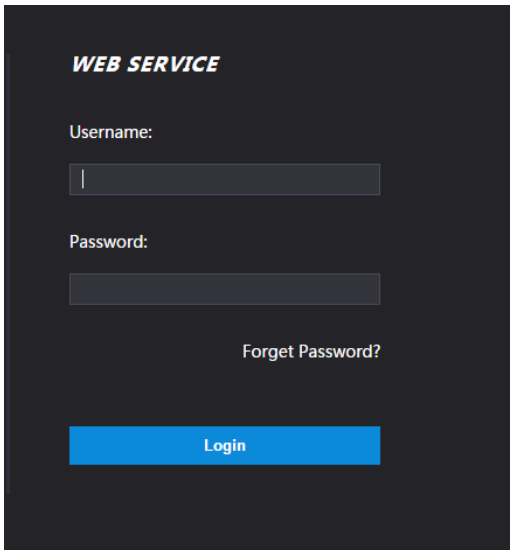
El controlador de acceso se puede configurar y operar en la interfaz web. A través de la interfaz web, puede establecer parámetros que incluyen parámetros de red, parámetros de video y parámetros del controlador de acceso; y también puede mantener y actualizar el sistema. Para obtener más información, consulte el manual del usuario. Aquí sólo 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 para el primera vez. La contraseña que establece se usa para iniciar sesión en la interfaz web y el correo electrónico se usa para restablecer contraseñas

Step 1 Abra el navegador web IE, ingrese la dirección IP del controlador de acceso en la barra de direcciones y luego presione la tecla Intro.

- Asegúrese de que la computadora utilizada para iniciar sesión en la interfaz web esté en el mismo LAN con el controlador de acceso .
- La dirección IP predeterminada es 192.168.1.108.

Figure 4-1 Acceso



Step 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 acceso controlador. Modificar el administrador contraseña regularmente y guárdela correctamente 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.

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 más de una hora 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 10 °C y 40 °C.
- Evite la luz solar directa sobre la unidad de control de temperatura.
- Evite instalar la unidad de monitoreo de temperatura mirando hacia la fuente de luz y el vidrio.
- Mantenga la unidad de monitoreo de temperatura alejada de fuentes de interferencia térmica.
- La distancia de control de temperatura es de 5 cm.
- 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 la temperatura entre la temperatura medida y la temperatura real.
- La sudoración también es una forma en que el cuerpo se enfría automáticamente y disipa el calor, lo que también causará la desviación de la temperatura entre la temperatura medida y la temperatura real.
- Mantenga la unidad de monitoreo de temperatura regularmente (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 cara Grabación/Comparación

Antes del registro

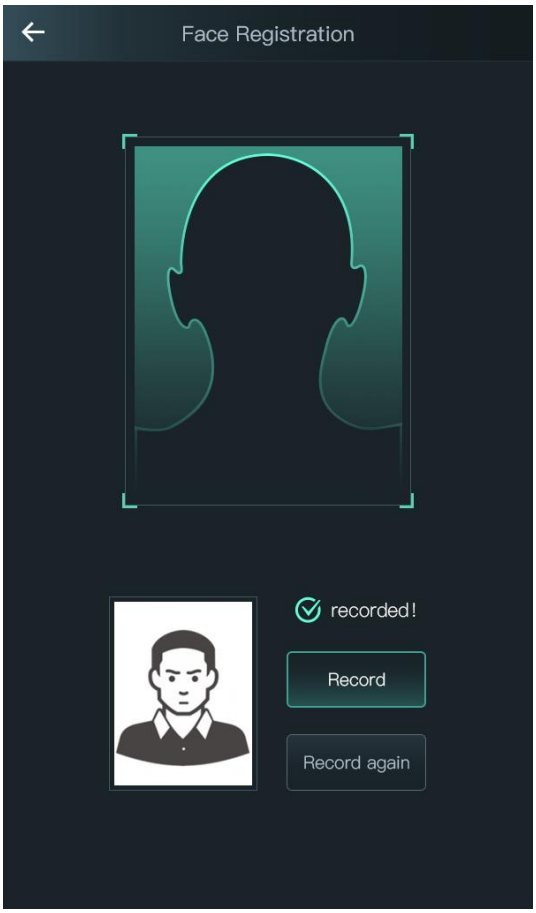
- Las gafas, los sombreros y la barba pueden influir en el rendimiento del
- reconocimiento facial. No cubra sus cejas cuando use sombreros.
- No cambie mucho su estilo de barba si va a usar el dispositivo; de lo contrario, el reconocimiento facial podría fallar.
- Mantén tu cara limpia.
- Mantenga el 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 podrían influir en el rendimiento del reconocimiento facial del dispositivo.

Durante el registro

Puedes registrar rostros a través del controlador de acceso 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 2-1 Registro

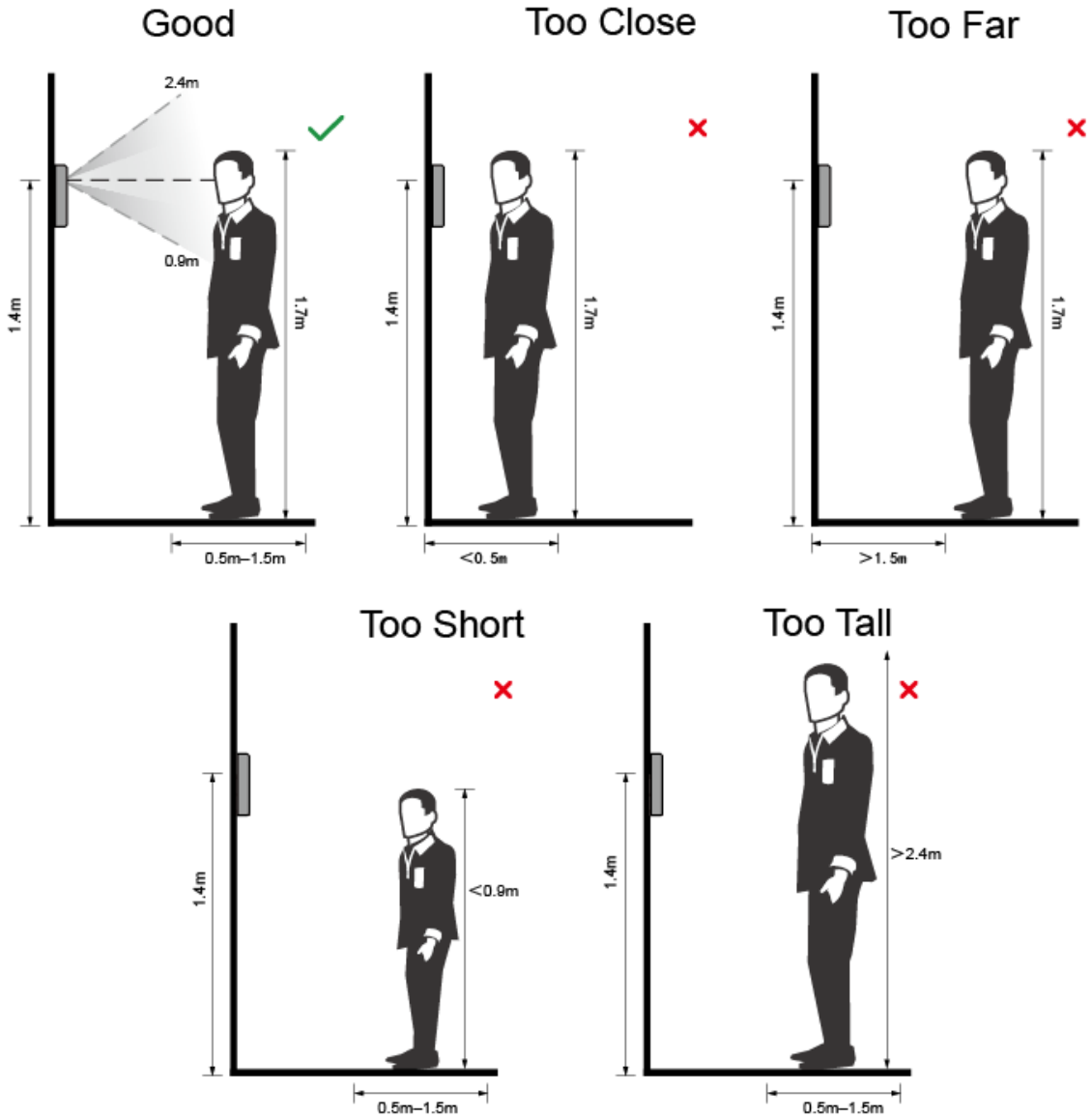


- No sacuda la cabeza o el cuerpo, de lo contrario, el registro podría fallar.
- Evite que aparezcan dos rostros en el cuadro de captura al mismo tiempo.

Posición de la cara

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

Apéndice Figura 2-2 Posición adecuada de la cara

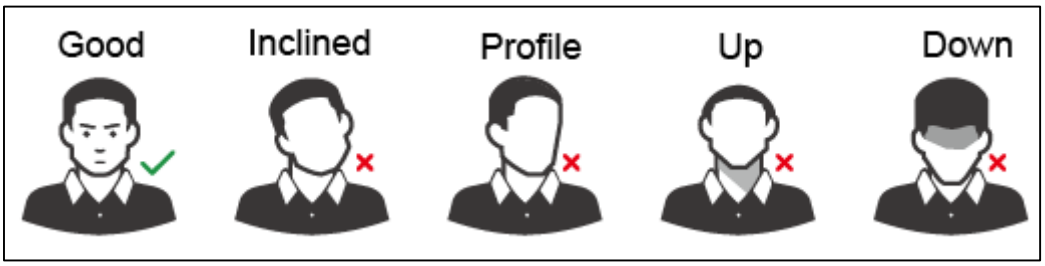


Requisitos de las caras

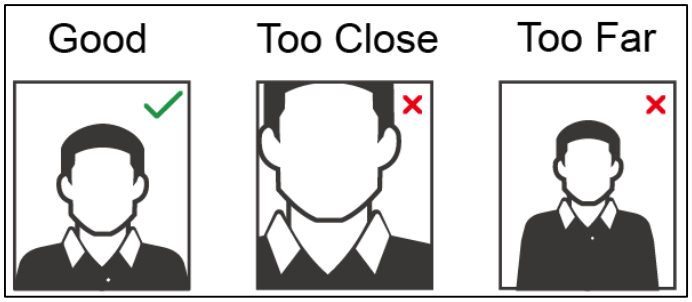
- Asegúrese de que la cara esté limpia y que la frente no esté cubierta por pelo.
- No use anteojos, sombreros, barbas pobladas u otros adornos faciales que influyan en la grabación de imágenes faciales.
- Con los ojos abiertos, sin expresiones faciales, y coloca tu rostro hacia el centro de la cámara.

- 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 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.

Appendix 3 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 presentan 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. 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 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 "verificación automática 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 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 y gabinete de computadoras especiales, e implemente un permiso de control de acceso y una administración de claves bien hechos para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de un dispositivo extraíble (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 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 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. Enlace de dirección MAC

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

8. 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.

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

10. 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.

11. 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 dispositivo: al ver los registros, puede conocer las direcciones IP que se usaron 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 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.

13. Construya un entorno de red seguro

Para garantizar mejor la seguridad del dispositivo 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.

- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts que pueden acceder al dispositivo.