Tiempo y asistencia de reconocimiento facial

Guía de inicio rápido

V1.0.0

V1.0.0

Prefacio

General

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

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 riesgo 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 la revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	Junio 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 causada por las operaciones que no cumplan con el manual. El manual se
- actualizará de acuerdo con las últimas leyes y regulaciones 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 actualizado y la documentación complementaria. Todavía puede haber desviaciones en los datos técnicos, la
- 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 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 con el servicio de atención al cliente si se produce algún problema al utilizar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

Advertencias y medidas de seguridad importantes

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

Requisitos de operación

- No coloque ni instale la asistencia en un lugar expuesto a la luz solar o cerca de una fuente de calor.

- Mantenga la asistencia alejada de la humedad, el polvo o el hollín.
- Mantenga la asistencia instalada horizontalmente en el lugar estable para evitar que se caiga.
- No deje caer ni salpique líquido sobre la asistencia, y asegúrese de que no haya ningún objeto lleno de líquido sobre la asistencia para evitar que el líquido fluya hacia la asistencia.
- Instale la asistencia en un lugar bien ventilado y no bloquee la ventilación de la asistencia.

- Opere la asistencia dentro del rango nominal de entrada y salida de energía. No disimule la
- asistencia al azar.

Seguridad ELECTRICA

- El uso inadecuado de la batería puede provocar un incendio, una explosión o una inflamación. Al
- reemplazar la batería, asegúrese de utilizar 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 la asistencia; de lo contrario, podría provocar lesiones personales y daños al dispositivo.
- La fuente de alimentación debe cumplir con los requisitos 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 alimentación 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

Prólogo .... YO Advertencias y salvaguardias importantes .... III 1 Dimensiones y componentes 1

2 Conexión e instalación 2

2.1 Conexión de cable 2

2.2 Notas de instalación 3

2.3 Instalación 4

3 Operaciones del sistema 7

3.1 Inicialización 7

3.2 Agregar nuevos usuarios 7

4 Operaciones web 9

Apéndice 1 Notas de comparación / grabación facial 10

Apéndice 2 Recomendaciones de ciberseguridad 13

1 Dimensiones y componentes

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

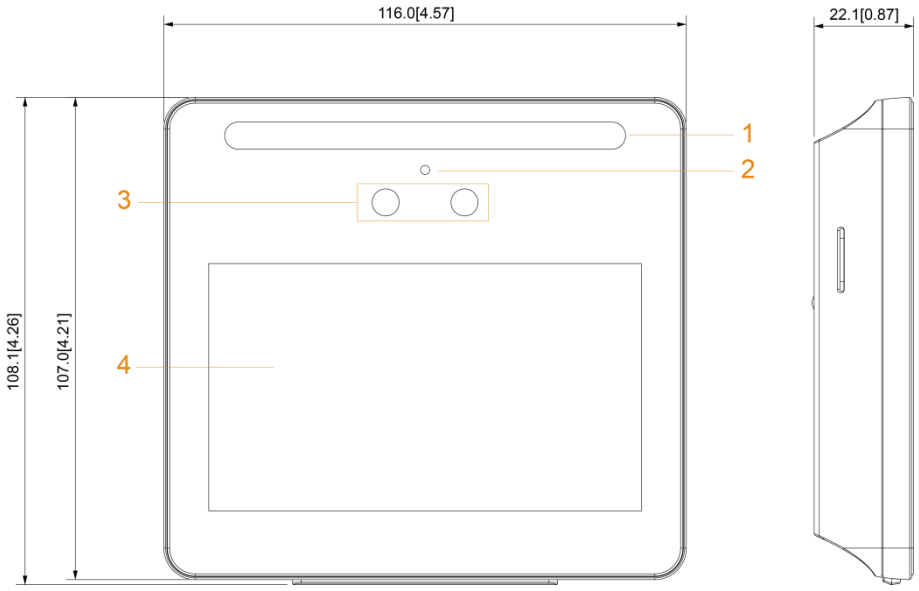


Tabla 1-1 Descripción de los componentes

No.	Nombre	No.	Nombre
1	Iluminador LED blanco	3	Cámaras duales
2	Micrófono	4	Monitor

2 Conexión e instalación

2.1 Conexión de cable

Figura 2-1 Conexión de cables

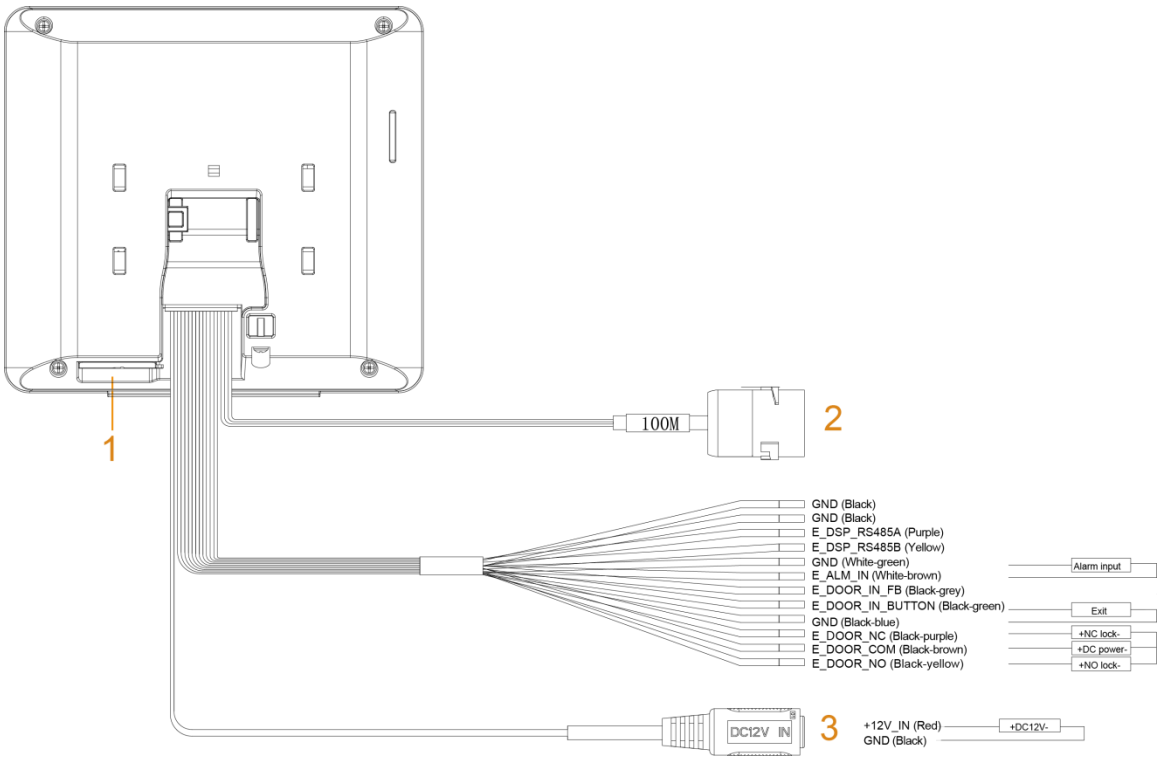
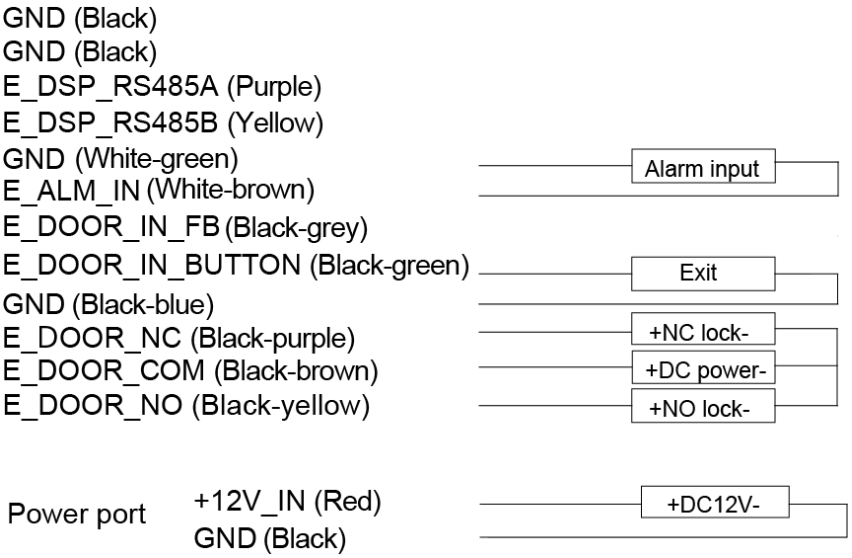


Figura 2-2 Puertos



El puerto RS485 y el puerto de retroalimentación de contacto de puerta (FB) están reservados. Actualmente, las funciones correspondientes no son compatibles.

Tabla 2-1 Descripción de los componentes

No.	Nombre
1	Puerto USB
2	Puerto de red 100M
3	Puerto de alimentación

2.2 Notas de instalación

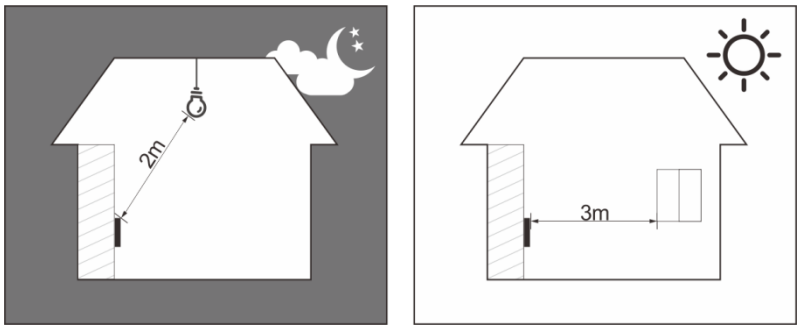
- Si hay una fuente de luz a 0,5 metros de la asistencia, la iluminación mínima no debe ser inferior a 100 Lux.
- Se recomienda que la asistencia se instale en interiores, al menos a 3 metros de ventanas y puertas ya 2 metros de luces.
- Evite la luz de fondo y la luz solar directa.

Requisito de iluminación ambiental

Figura 2-3 Requisito de iluminación ambiental

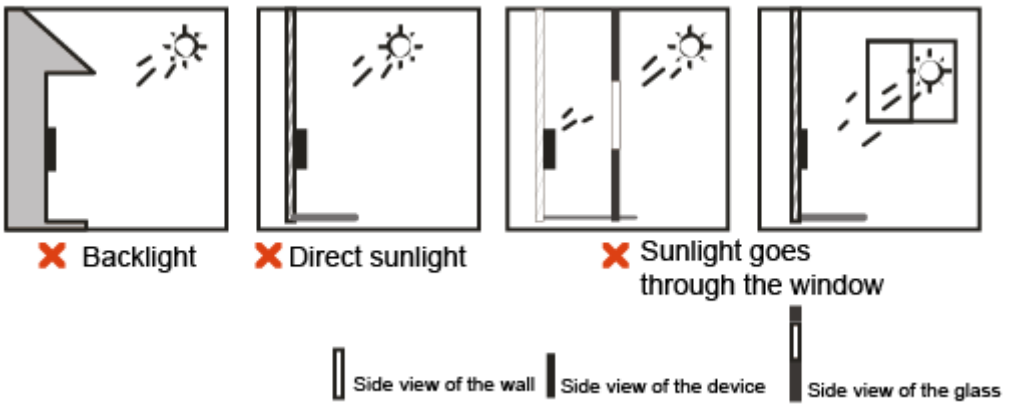
Lugares recomendados

Figura 2-4 Lugares recomendados



Lugares no recomendados

Figura 2-5 Lugares no recomendados



2.3 Instalación

Instalación de escritorio

Inserte la hebilla del soporte del escritorio en la ranura trasera de la asistencia y luego deslícela hacia abajo hasta el final.

Figura 2-6 Instalación de escritorio (1)

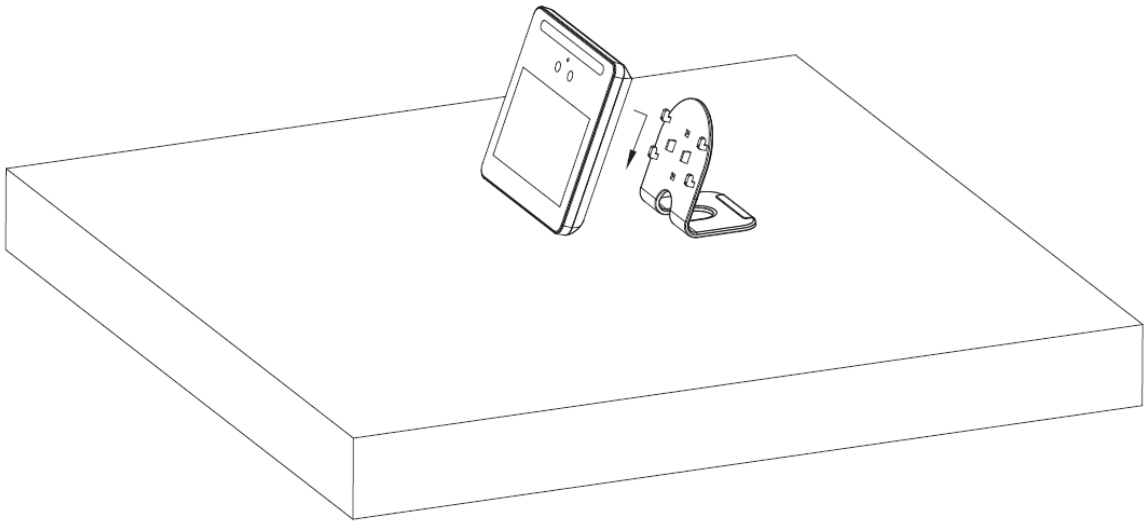
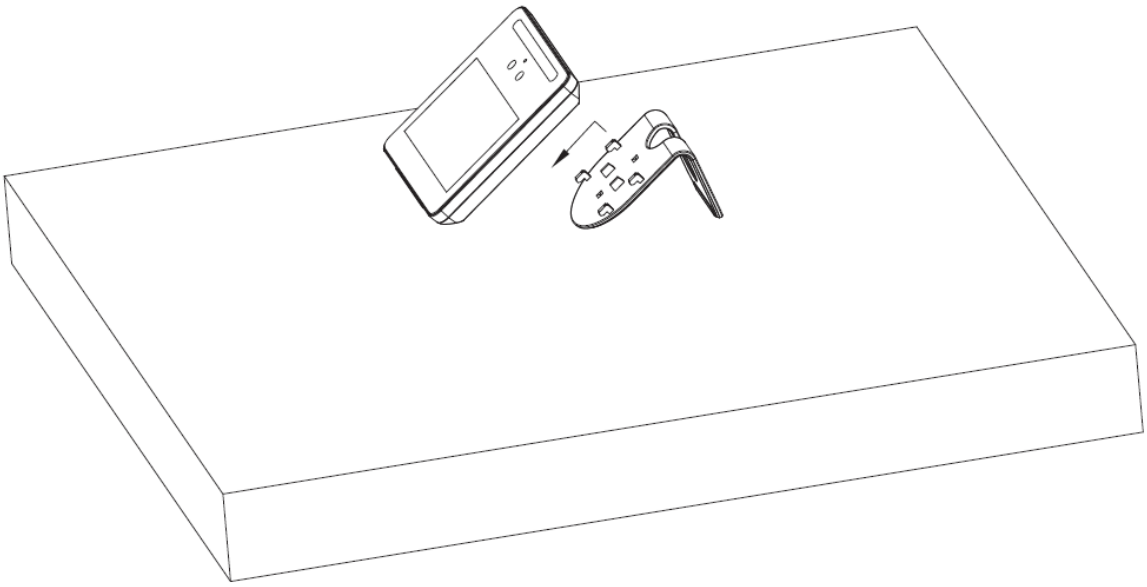


Figura 2-7 Instalación de escritorio (2)



Instalación en la pared

La distancia recomendada entre el objetivo y el suelo es de 1,4 a 1,6 metros.

Figura 2-1 Altura de instalación

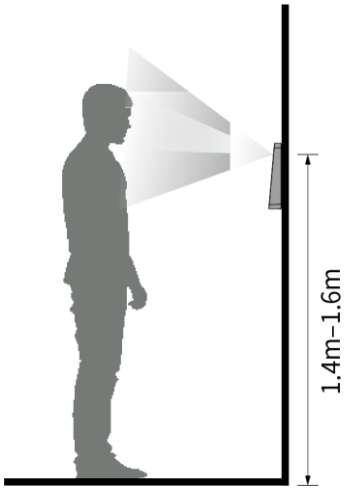
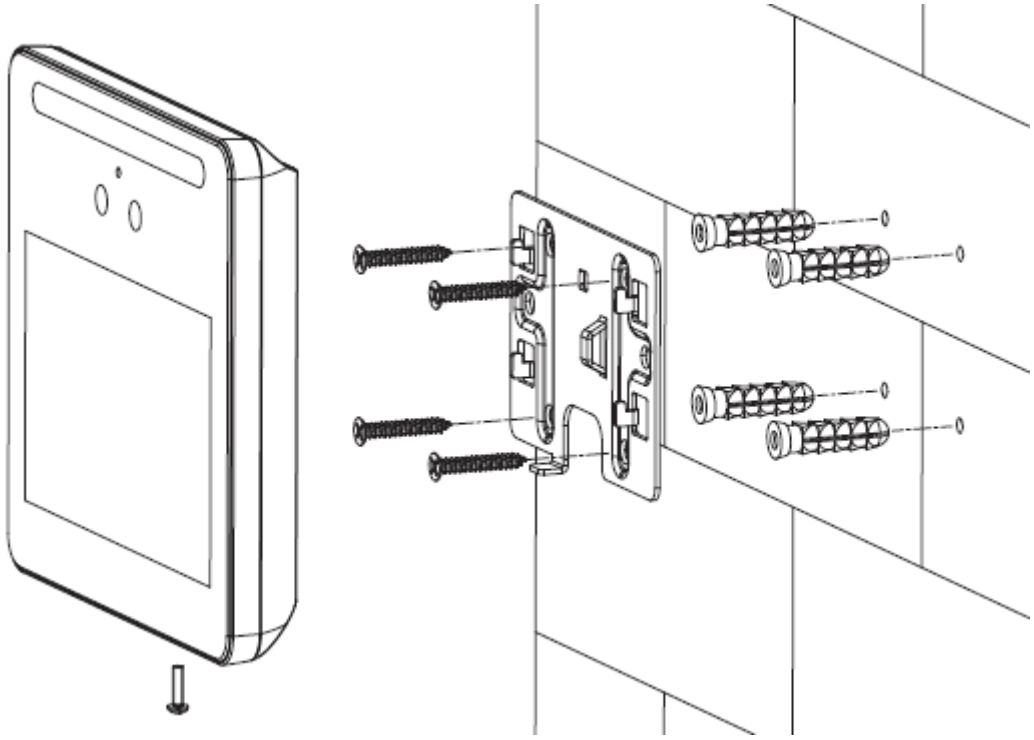


Figura 2-2 Instalación en la pared



Paso 1 Taladre cuatro orificios en la pared de acuerdo con los orificios del soporte.

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

Paso 3 Conecte los cables de asistencia. Consulte "2.1 Conexión de cables".

Paso 4 Cuelgue la asistencia en el gancho del soporte.

Paso 5 Apriete los tornillos en la parte inferior de la asistencia.

3 Operaciones del sistema

3.1 Inicialización

Se debe establecer una contraseña de administrador y un correo electrónico la primera vez que se activa la asistencia; de lo contrario, no se podrá utilizar la asistencia.

Figura 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, imágenes de caras, tarjetas, contraseñas y seleccionando niveles de usuario.

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

Paso 1 En la interfaz de espera, mantenga pulsado 3 s para ir al **Acceso de administrador** interfaz.

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

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

Figura 3-2 Nuevo usuario

Paso 4 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 faciales, consulte el "Apéndice 1 Notas sobre la comparación / grabación facial".
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 los asistentes leerán la información de la tarjeta.
PWD	La contraseña de usuario. La longitud máxima de la contraseña es de 8 dígitos.
Nivel de usuario	Puede seleccionar un nivel de usuario para nuevos usuarios. Hay dos opciones: Usuario y Administrador. En caso de que olvide la contraseña de administrador, será mejor que cree más de un administrador.
Dpto.	Seleccione un departamento al que pertenece el usuario. Seleccione un
Modo de cambio	modo de cambio para el usuario. • Horario del Departamento: Verifique la asistencia según el horario del departamento al que pertenece el usuario. • Horario personal: Verifique la asistencia de acuerdo con el horario personal.

Paso 5 Toque  para guardar la configuración.

4 Operaciones web

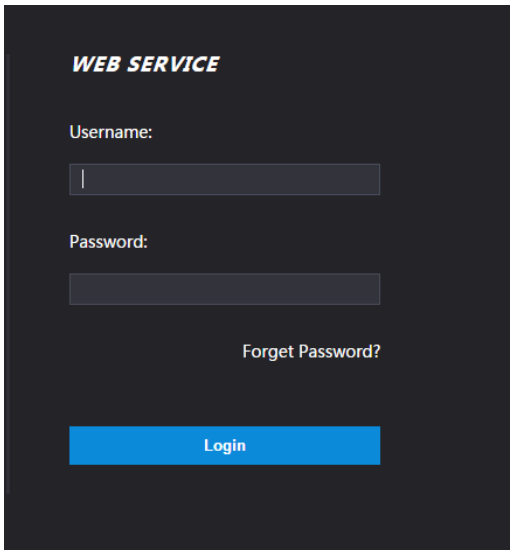
La asistencia se puede configurar y operar en la interfaz web. A través de la interfaz web, puede configurar parámetros, como parámetros de red, parámetros de video y parámetros de detección de rostros; y también puede mantener y actualizar el sistema. Para obtener más información, consulte el manual del usuario. Aquí solo 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.

Paso 1 Abra el navegador web IE, ingrese la dirección IP de la asistencia 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 con la asistencia.
- La dirección IP predeterminada de la asistencia es 192.168.1.108.

Figura 4-1 Inicio de sesión



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 la asistencia. Modifique la contraseña de administrador con regularidad y consérvela correctamente por seguridad.
- Si olvida la contraseña de inicio de sesión de administrador, puede hacer clic en **¿Contraseña olvidada?** para restablecerlo. Consulte el manual de usuario.

Paso 3 Haga clic en **Iniciar sesión.**

Se muestra la página de inicio de la interfaz web.

Apéndice 1 Notas de comparación / grabación facial

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.

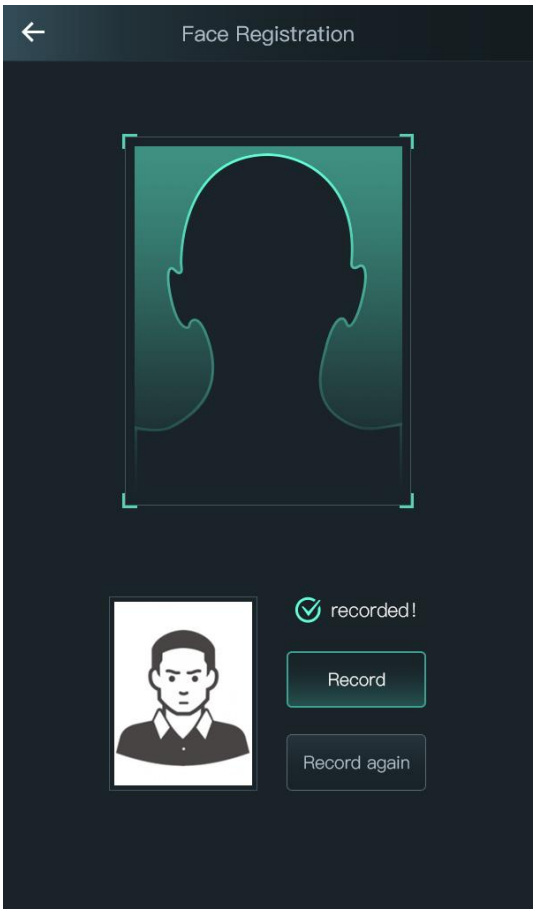
- Mantén tu cara limpia.
- Mantenga el dispositivo al menos a dos metros de la fuente de luz y al menos a tres metros de ventanas o puertas; de lo contrario, la luz de fondo y la luz solar directa podrían influir en el rendimiento del reconocimiento facial del dispositivo.

Durante el registro

Puedes registrar rostros a través de la asistencia o mediante 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 1-1 Registro

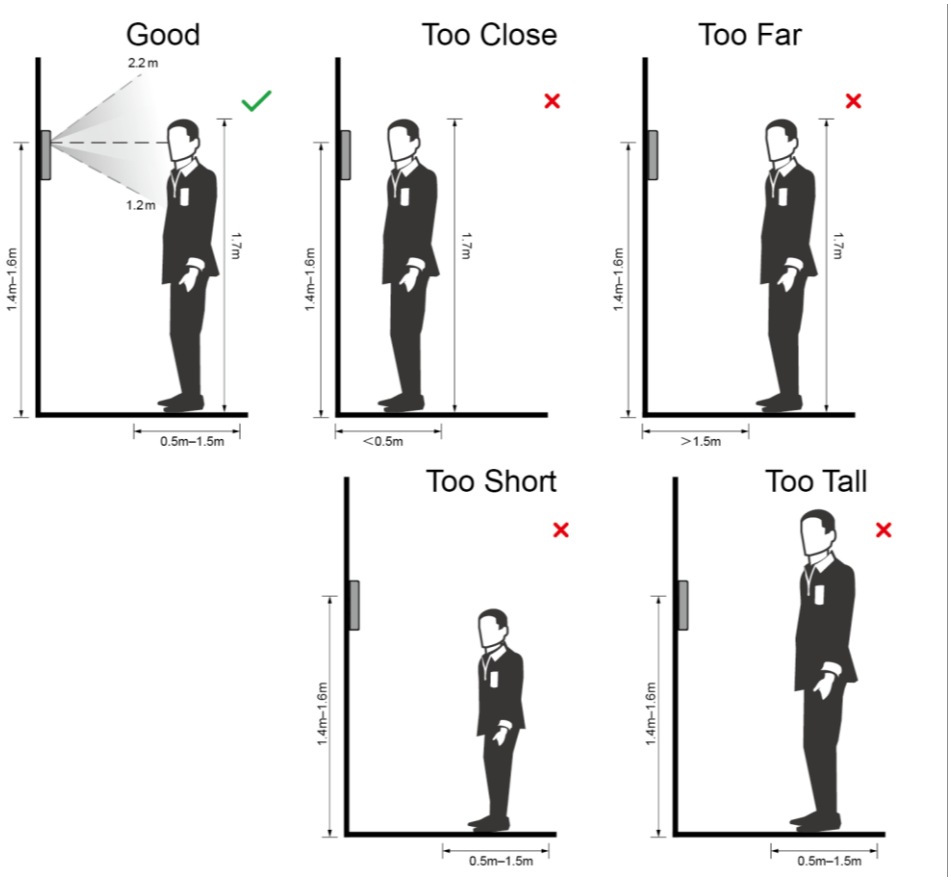


- No sacuda la cabeza o el cuerpo, de lo contrario, el registro podría fallar. Evite que aparezcan
- dos caras en el cuadro de captura al mismo tiempo.

Posición de la cara

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

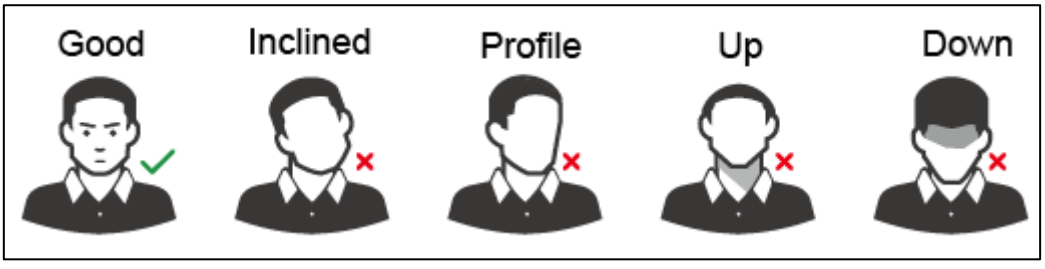
Apéndice Figura 1-2 Posición adecuada de la cara



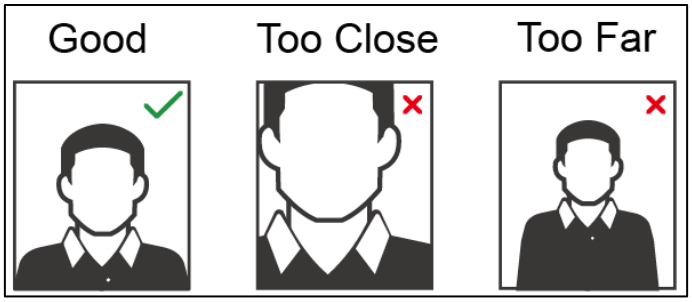
Requisitos de caras

- 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.
- Al grabar 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 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 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 supere 1: 2.

Apéndice 2 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 deben tomarse para la seguridad de la red de equipos básicos:

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 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 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 "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 equipo:

1. Protección física

Le sugerimos que realice protección física a los equipos, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el equipo 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 equipos 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 contraseñas Restablecer información 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 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. 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 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 externas 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 que vincule la dirección IP y MAC de la puerta de enlace al equipo, reduciendo así el riesgo de suplantación de ARP.

9. 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.

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 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 autenticación y de cifrado 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.

11. 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 encriptada provocará cierta pérdida en la eficiencia de transmisión.

12. 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.
- 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 limitada capacidad de almacenamiento 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 su seguimiento.

14. Construya un entorno de red seguro

Para garantizar mejor la seguridad de los equipos 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, es

sugirió utilizar VLAN, red GAP 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.
- Se recomienda que habilite el firewall de su dispositivo o la función de lista negra y lista blanca para reducir el riesgo de que su dispositivo sea atacado.