Controlador de acceso por reconocimiento facial

Guía de inicio rápido

V1.0.2

Prefacio

General

Este manual presenta la instalación y las operaciones del Controlador de acceso con reconocimiento facial (en adelante, el "Controlador de acceso"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para consultarlo en el futuro.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Significado
DANGER	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
WARNING	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
CAUTION	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, reducciones en el rendimiento o resultados impredecibles.
TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
NOTE	Proporciona información adicional como complemento al texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.2	Actualizada la apariencia imagen del dispositivo.	abril 2023
V1.0.1	Se actualizó el apéndice.	febrero 2023
V1.0.0	Primer lanzamiento.	octubre 2022

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otras personas, como su rostro, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: Proporcionar una identificación clara y visible para informar a las personas sobre la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del Manual

- El manual es sólo para referencia. Pueden encontrarse ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas incurridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es sólo para referencia. Es posible que se encuentren ligeras diferencias entre la versión electrónica y la versión en papel.

- Todos los diseños y software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones de productos pueden provocar que aparezcan algunas diferencias entre el producto real y el manual. Comuníquese con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Pueden existir errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en este manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de dar una explicación final.

Salvaguardias y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del controlador de acceso, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el Controlador de acceso y cumpla con las pautas al usarlo.

Requisito de transporte

Transporte, utilice y almacene el controlador de acceso en condiciones permitidas de humedad y temperatura.

Requisito de almacenamiento

Guarde el controlador de acceso en condiciones permitidas de humedad y temperatura.

requerimientos de instalación

- No conecte el adaptador de corriente al controlador de acceso mientras el adaptador esté encendido.
- Cumpla estrictamente con el código y las normas locales de seguridad eléctrica. Asegúrese de que el voltaje ambiental sea estable y cumpla con los requisitos de suministro de energía del controlador de acceso.
- No conecte el Controlador de acceso a dos o más tipos de fuentes de alimentación para evitar daños al Controlador de acceso.
- El uso inadecuado de la batería podría provocar un incendio o una explosión.

- El personal que trabaja en alturas debe tomar todas las medidas necesarias para garantizar la seguridad personal, incluido el uso de casco y cinturones de seguridad.
- No coloque el controlador de acceso en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el Access Controller alejado de la humedad, el polvo y el hollín.
- Instale el controlador de acceso en una superficie estable para evitar que se caiga.
- Instale el controlador de acceso en un lugar bien ventilado y no bloquee su ventilación.
- Utilice un adaptador o fuente de alimentación de gabinete proporcionado por el fabricante.
- Utilice los cables de alimentación recomendados para la región y cumplan con las especificaciones de potencia nominal.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en el estándar IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de suministro de energía están sujetos a la etiqueta del Controlador de acceso.
- El Controlador de Acceso es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del controlador de acceso esté conectada a una toma de corriente con conexión a tierra protectora.

Requisitos de operación

- Compruebe si la fuente de alimentación es correcta antes de su uso.
- No desenchufe el cable de alimentación en el costado del controlador de acceso mientras el adaptador esté encendido.
- Opere el controlador de acceso dentro del rango nominal de entrada y salida de energía.

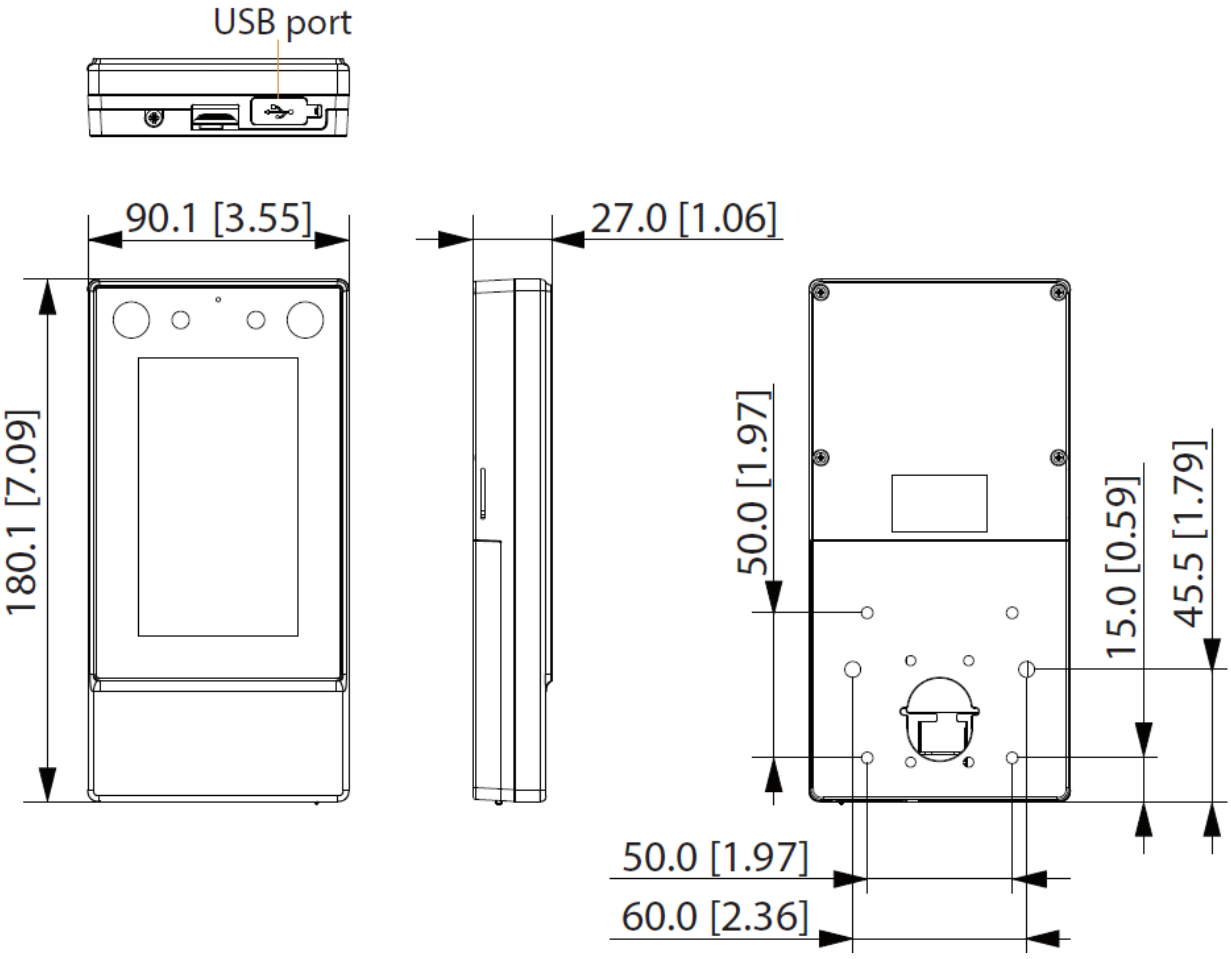
- Utilice el controlador de acceso en las condiciones permitidas de humedad y temperatura.
- No deje caer ni salpique líquido sobre el Controlador de acceso y asegúrese de que no haya ningún objeto lleno de líquido sobre el Controlador de acceso para evitar que el líquido fluya hacia él.
- No desmonte el controlador de acceso sin instrucción profesional.

Tabla de contenido

1 apariencia

La apariencia frontal puede diferir según los diferentes modelos de Access Controller.

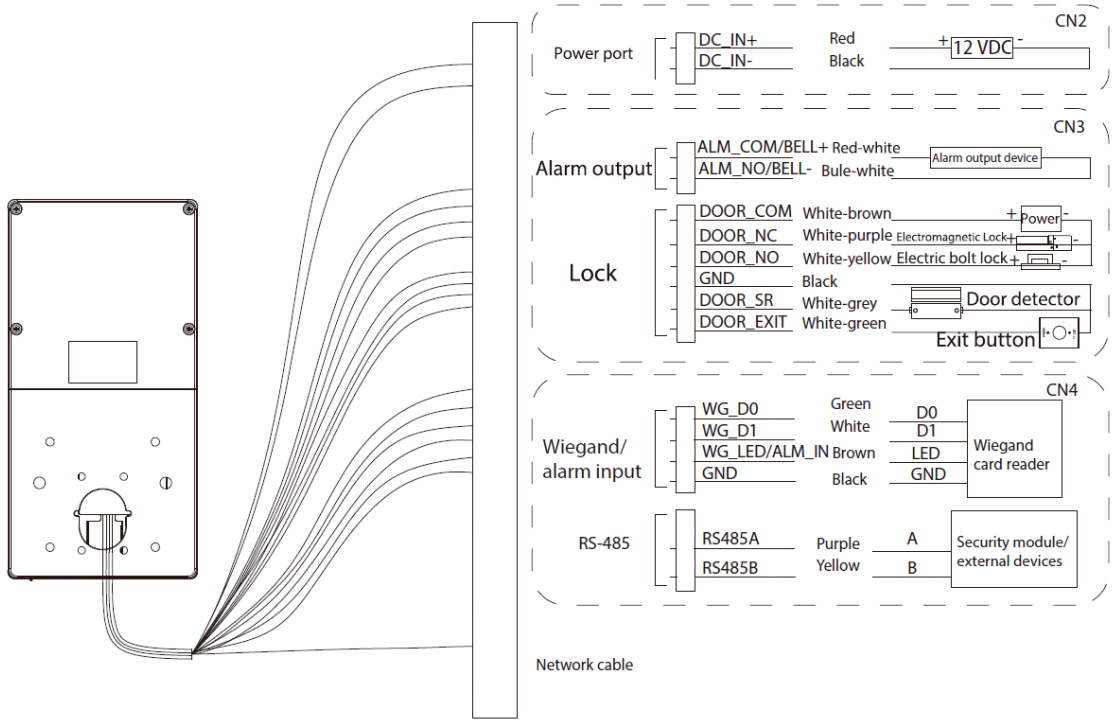
Figura 1-1 Apariencia del controlador de acceso (Unidad: mm [pulgadas])



2 Cableado e instalación

2.1 Cableado

Figura 2-1 Cableado del controlador de acceso



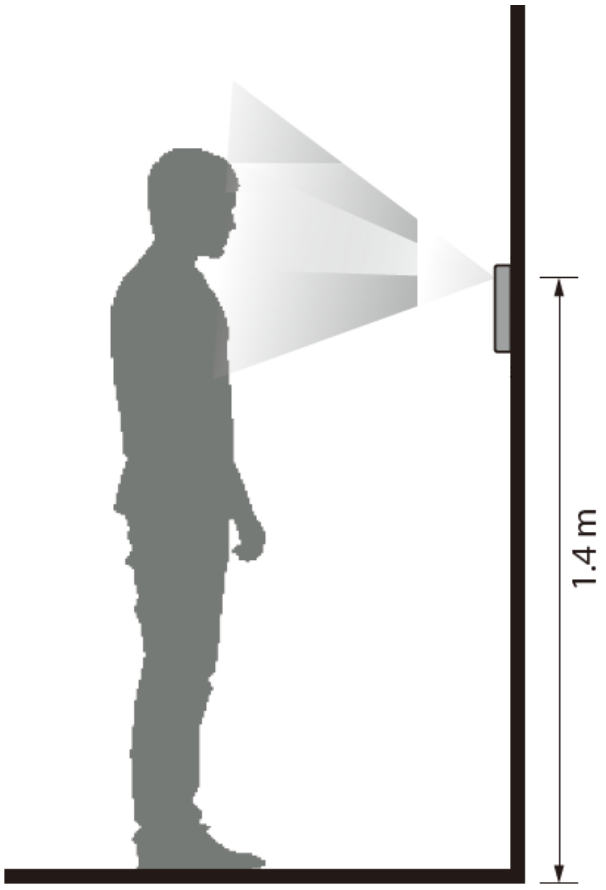
- El cable del LED y el cable de entrada de la alarma son iguales, y el cable de la campana y el cable de salida de la alarma son lo mismo.
- Si desea conectar un módulo de seguridad externo, seleccione**Conexión**>**Puerto serial**>**RS-485** **Ajustes**>**Módulo de seguridad**. El módulo de seguridad debe adquirirse por separado mediante clientes.
- Cuando el módulo de seguridad está encendido, el botón de salida y el control de bloqueo y la entrada de alarma se activarán. no ser efectivo.

2.2 Requisitos de instalación

- La luz a 0,5 metros de distancia del controlador de acceso no debe ser inferior a 100 Lux.
- Le recomendamos instalar el Controlador de Acceso en interiores, al menos a 3 metros de distancia de las ventanas.
  y puertas, y a 2 metros de la fuente de luz.
- Evite la luz de fondo, la luz solar directa, la luz cercana y la luz oblicua.

Altura de instalación

Figura 2-2 Requisitos de altura de instalación

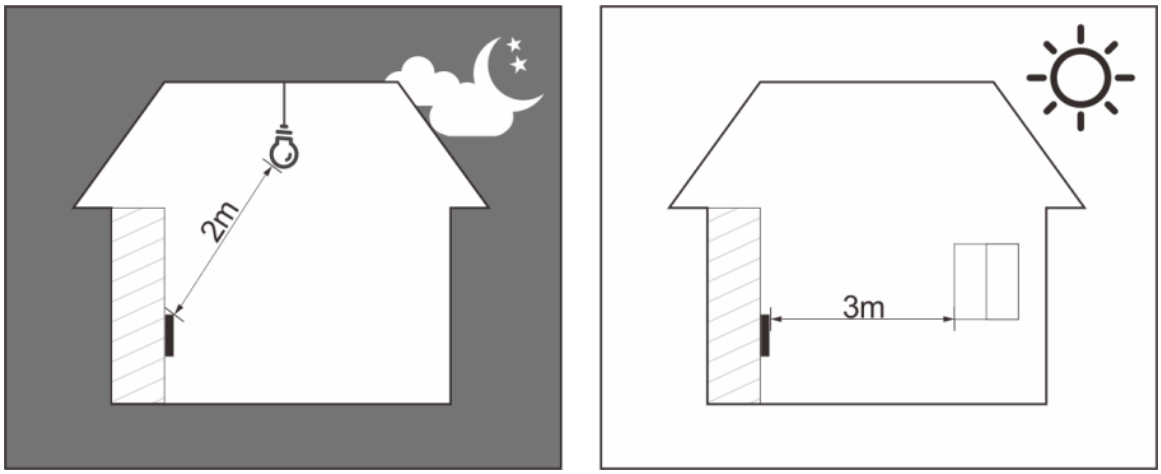


Requisitos de iluminación ambiental

Figura 2-3 Requisitos de iluminación ambiental

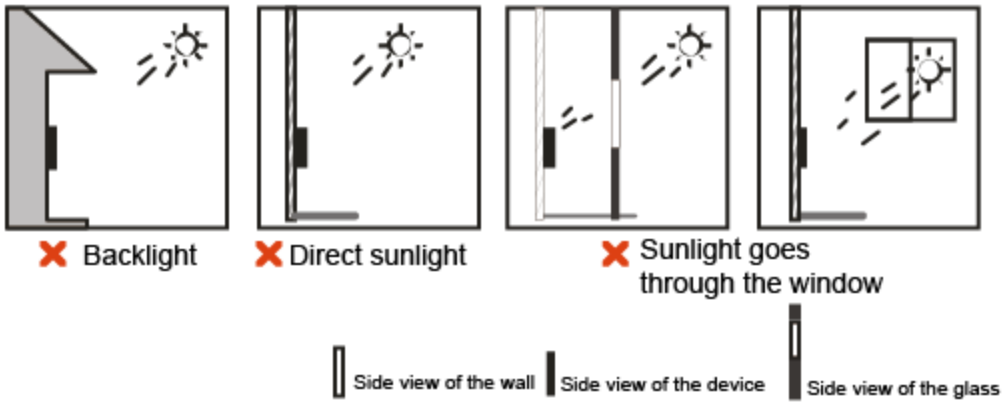
Ubicaciones de instalación recomendadas

Figura 2-4 Ubicaciones de instalación recomendadas



Ubicaciones de instalación no recomendadas

Figura 2-5 Ubicaciones de instalación no recomendadas



2.3 Proceso de instalación

El controlador de acceso tiene 4 métodos de instalación: montaje en pared, montaje en soporte de piso, montaje en torniquete y montaje en caja 86. Esta sección solo presenta el soporte de pared y el soporte de caja 86. Para obtener detalles sobre el soporte de piso y el soporte de torniquete, consulte el manual del usuario de los dispositivos correspondientes.

2.3.1 Montaje en pared

Procedimiento

Paso 1 Según la posición de los agujeros del soporte, taladre 4 agujeros y 1 salida de cable en la pared. Coloque pernos de expansión en los agujeros.

La salida de cable no es necesaria para el cableado de superficie.

Paso 2 Utilice los 4 tornillos para fijar el soporte a la pared. Conecte el controlador de

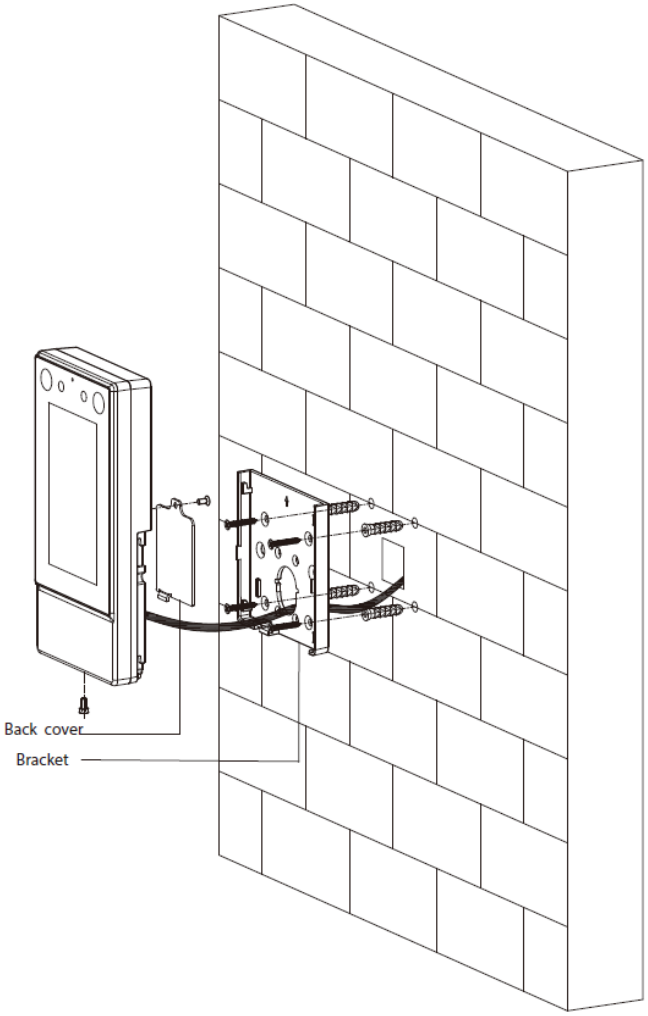
Paso 3 acceso. Para obtener más información, consulte "2.1 Cableado". Utilice 1 tornillo

Etapa 4 para fijar la cubierta posterior al controlador de acceso.

Paso 5 Fije el controlador de acceso en el soporte.

Paso 6 Atornille 1 tornillo de forma segura en la parte inferior del controlador de acceso.

Figura 2-6 Montaje en pared



2.3.2 Montaje en caja 86

Procedimiento

Paso 1 Coloque una caja de 86 en la pared a una altura adecuada. Fije el soporte a

Paso 2 la caja 86 con 2 tornillos. Conecte el controlador de acceso. Para obtener

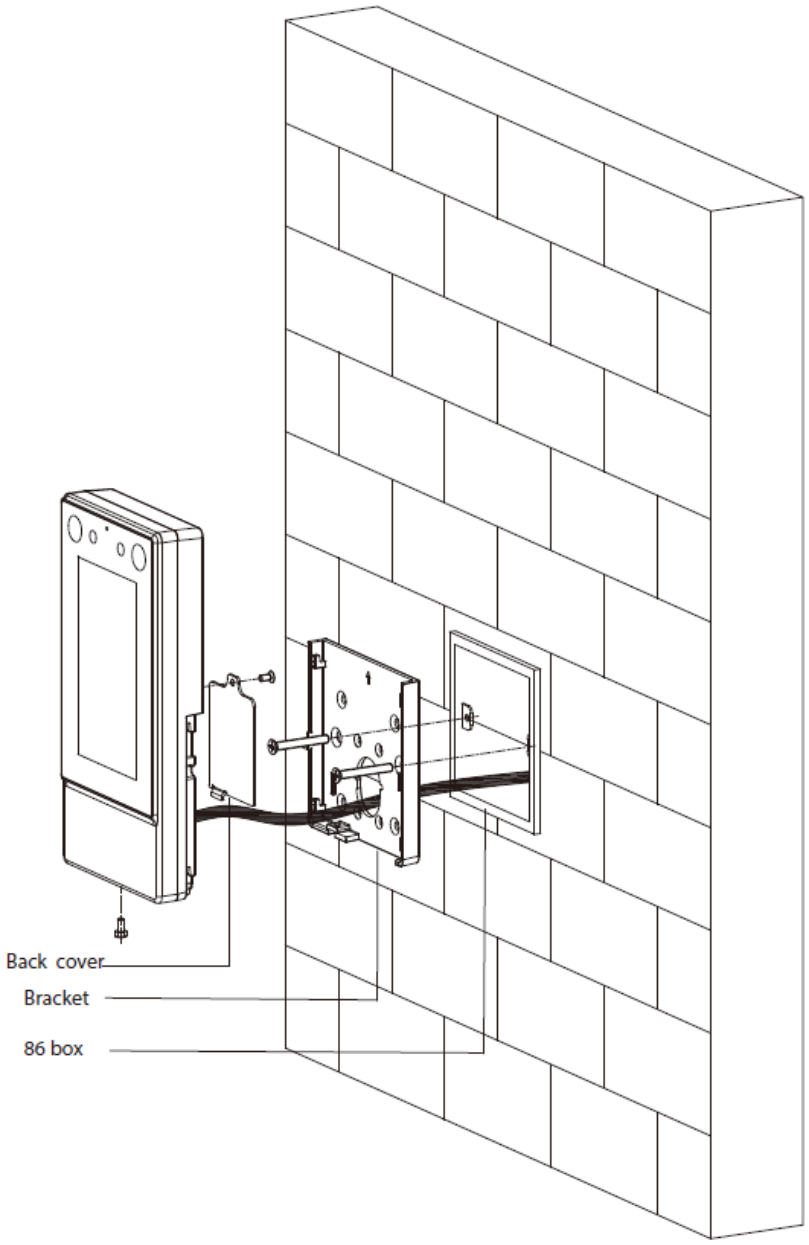
Paso 3 más información, consulte "2.1 Cableado". Utilice 1 tornillo para fijar la

Etapa 4 cubierta posterior al controlador de acceso. Fije el controlador de acceso en

Paso 5 el soporte.

Paso 6 Atornille 1 tornillo de forma segura en la parte inferior del controlador de acceso.

Figura 2-7 Montaje en caja 86



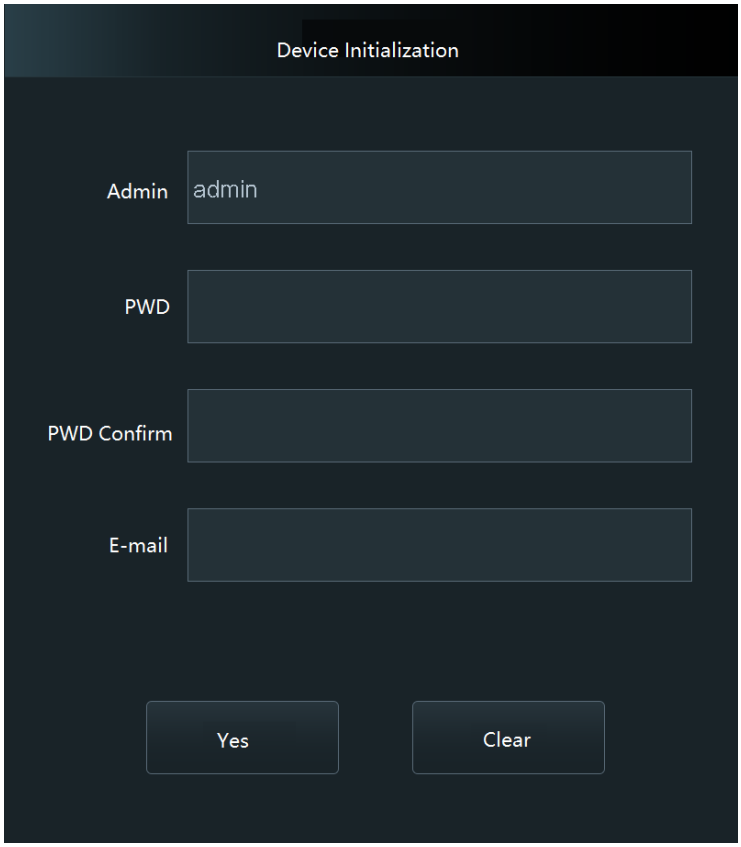
3 configuraciones locales

Las operaciones locales pueden diferir según los diferentes modelos de Access Controller.

3.1 Inicialización

Para el uso por primera vez o después de restaurar los valores predeterminados de fábrica, debe seleccionar un idioma y luego establecer una contraseña y una dirección de correo electrónico para la cuenta de administrador. Después de eso, puede usar la cuenta de administrador para iniciar sesión en la pantalla del menú principal del Access Controller y su página web.

Figura 3-1 Inicialización



- Si olvida la contraseña de administrador, envíe una solicitud de restablecimiento a su dirección de correo electrónico vinculada.
- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excepto ' " ; : &). Establezca una contraseña de alta seguridad siguiendo las instrucciones de seguridad de la contraseña.

3.2 Agregar nuevos usuarios

Información de contexto

Agregue nuevos usuarios ingresando información del usuario como nombre, número de tarjeta, rostro y huella digital, y luego establezca los permisos de usuario.

Procedimiento

Paso 1 Sobre el**Menú principal**pantalla, seleccione**Usuario**y luego toque .

Paso 2 Configurar parámetros de usuario.

Figura 3-2 Nuevo usuario

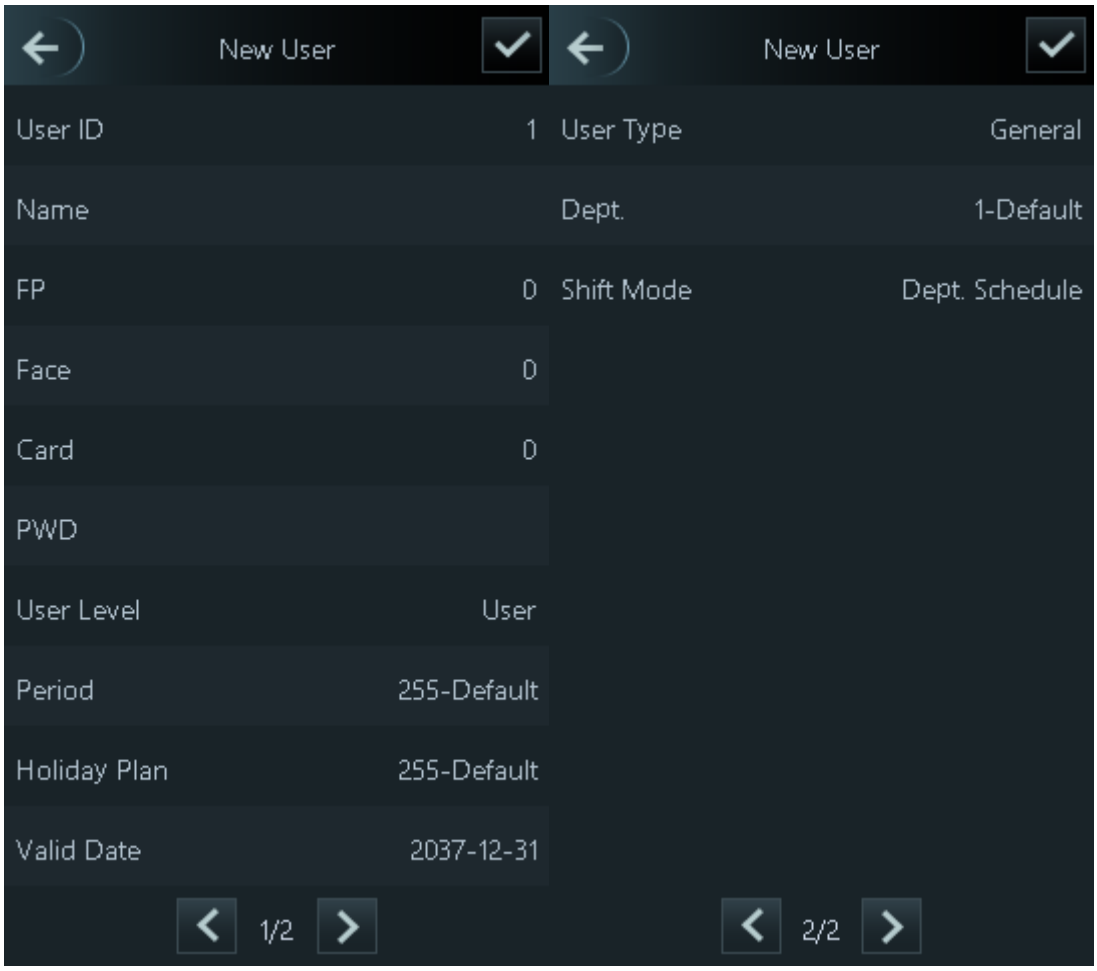


Tabla 3-1 Descripción de los parámetros para agregar un nuevo usuario

Parámetro	Descripción
ID de usuario	Ingrese el ID del usuario. Los ID pueden ser números, letras y sus combinaciones, y la longitud máxima del ID es de 32 caracteres. Cada identificación es única.
Nombre	Ingrese el nombre con un máximo de 32 caracteres (incluidos números, símbolos y letras).
FP	Registrar huellas dactilares. Un usuario puede registrar hasta 3 huellas digitales y usted puede configurar una huella digital para la huella digital de coacción. Se activará una alarma cuando se utilice la huella digital de coacción para desbloquear la puerta. Sólo ciertos modelos admiten el desbloqueo por huella digital.
Rostro	Asegúrese de que su rostro esté centrado en el marco de captura de imágenes, y se capturará y analizará automáticamente una imagen del rostro.
Tarjeta	Un usuario puede registrar cinco tarjetas como máximo. Ingrese su número de tarjeta o pase su tarjeta y luego el controlador de acceso leerá la información de la tarjeta. Puedes habilitar el**Tarjeta de coacción**función. Se activará una alarma si se utiliza una tarjeta de coacción para desbloquear la puerta.

Parámetro	Descripción
PCD	Ingrese 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. ● **Usuario**: Los usuarios solo tienen permiso de acceso a la puerta. ● **Administración**: Los administradores pueden desbloquear la puerta y configurar el controlador de acceso.
Período	Los usuarios pueden desbloquear la puerta solo durante el período definido.
Plan de vacaciones	Los usuarios pueden desbloquear la puerta sólo durante el plan de vacaciones definido.
Fecha válida	Establezca una fecha en la que expirarán los permisos de acceso de la persona.
Tipo de usuario	● **General**: Los usuarios generales pueden desbloquear la puerta. ● **Lista de bloqueos**: Cuando los usuarios en la lista de bloqueo desbloquean la puerta, el personal de servicio recibirá una notificación. ● **Invitado**: Los huéspedes pueden desbloquear la puerta dentro de un período definido o durante una determinada cantidad de veces. Una vez transcurrido el período definido o los tiempos de desbloqueo, no pueden desbloquear la puerta. ● **Patrulla**: Se realizará un seguimiento de la asistencia de los usuarios de Patrol, pero no tendrán permisos de desbloqueo. ● **VIP**: Cuando VIP abra la puerta, el personal de servicio recibirá un aviso. ● **Otros**: Cuando desbloqueen la puerta, la puerta permanecerá desbloqueada durante 5 segundos más. ● Usuario personalizado 1/Usuario personalizado 2: Lo mismo con los usuarios generales.
Departamento	Establecer departamentos.
Modo de cambio	Seleccione los modos de cambio.

Paso 3 Grifo**Ahorrar**.

4 configuraciones web

En la página web, también puede configurar y actualizar el controlador de acceso.

Las configuraciones web difieren según los modelos de Access Controller.

4.1 Inicialización

Inicialice el Controlador de acceso cuando inicie sesión en la página web por primera vez o después de que el Controlador de acceso se restablezca a los valores predeterminados de fábrica.

Requisitos previos

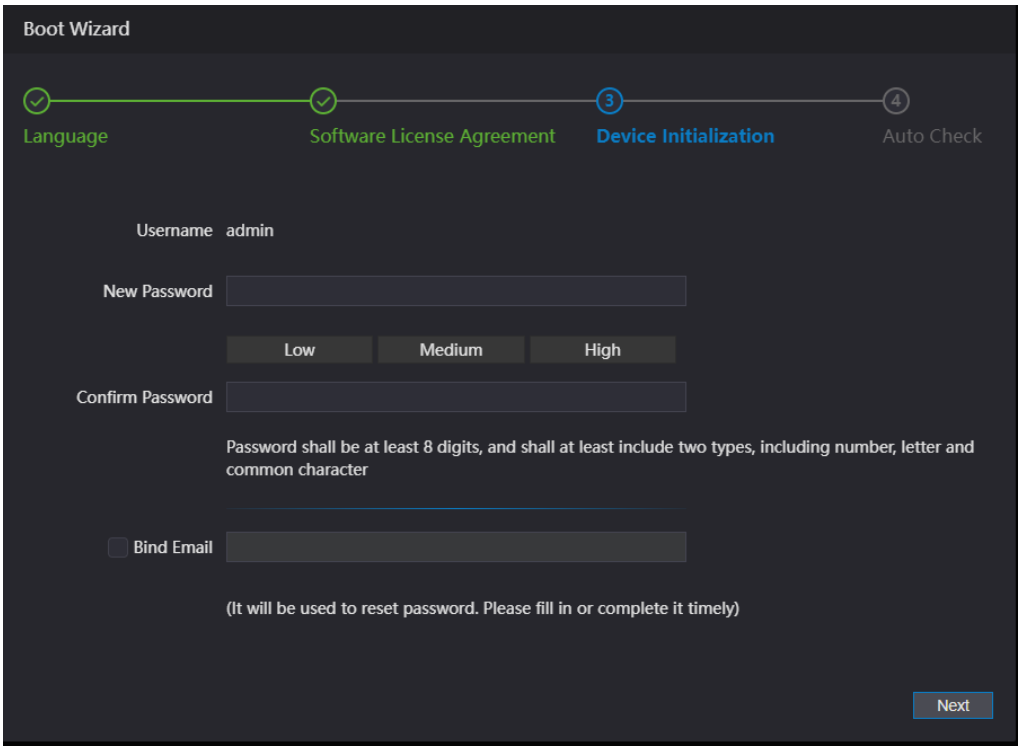
Asegúrese de que la computadora utilizada para iniciar sesión en la página web esté en la misma LAN que el controlador de acceso.

Procedimiento

Paso 1 Abra un navegador web y vaya a la dirección IP (la dirección predeterminada es 192.168.1.108) del Controlador de acceso.

Puede iniciar sesión en la web con Chrome o Firefox.

Figura 4-1 Yo



Paso 2 Ingrese y confirme la contraseña, ingrese una dirección de correo electrónico y luego haga clic en**Terminado**.

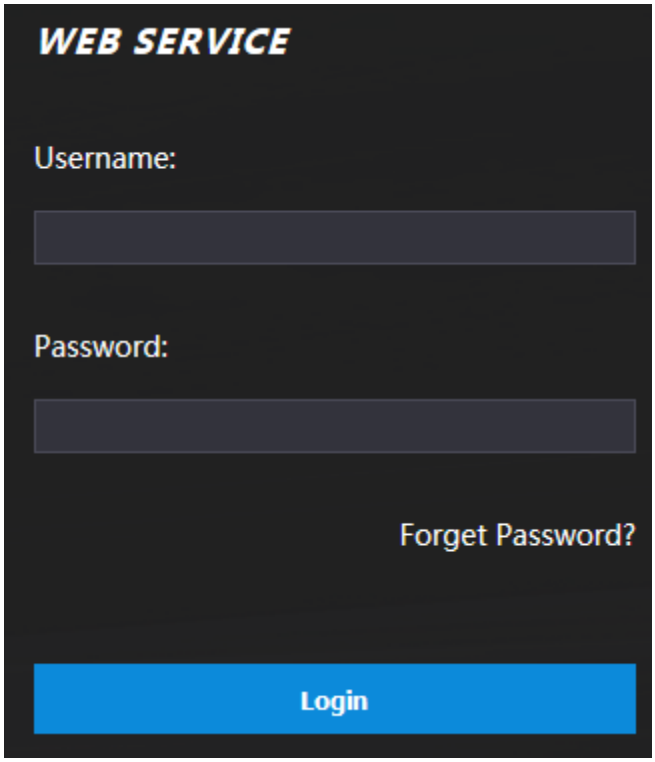
- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y especiales caracteres (excepto ' " ; : &). Establezca una contraseña de alta seguridad siguiendo la contraseña indicación de fuerza.
- Mantenga la contraseña segura después de la inicialización y cámbiela periódicamente para mejorar la seguridad.
- Si desea restablecer la contraseña de administrador escaneando el código QR, necesita el dirección de correo electrónico vinculada para recibir el código de seguridad.

4.2 Iniciar sesión

Procedimiento

Paso 1 Abra un navegador web, vaya a la dirección IP del Controlador de acceso.

Figura 4-2 Iniciar sesión



Paso 2 Ingrese el nombre de usuario y la contraseña.

- Asegúrese de que la computadora esté en la misma LAN que el controlador de acceso.
- El nombre de usuario predeterminado del administrador es admin y la contraseña es la que usted establece durante la inicialización. Le recomendamos cambiar la contraseña de administrador periódicamente para aumentar la seguridad de la cuenta.
- Si olvida la contraseña de administrador, puede hacer clic**¿Contraseña olvidada?**para restablecer la contraseña.

Paso 3 Hacer clic**Acceso**.

Apéndice 1 Puntos importantes del intercomunicador

Operación

El controlador de acceso puede funcionar como VTO para realizar la función de intercomunicación.

Requisitos previos

La función de intercomunicación se configura en el controlador de acceso y en el VTO.

Procedimiento

Paso 1 En la pantalla de espera, toque Ingresar.

Paso 2 número de habitación y luego toque .

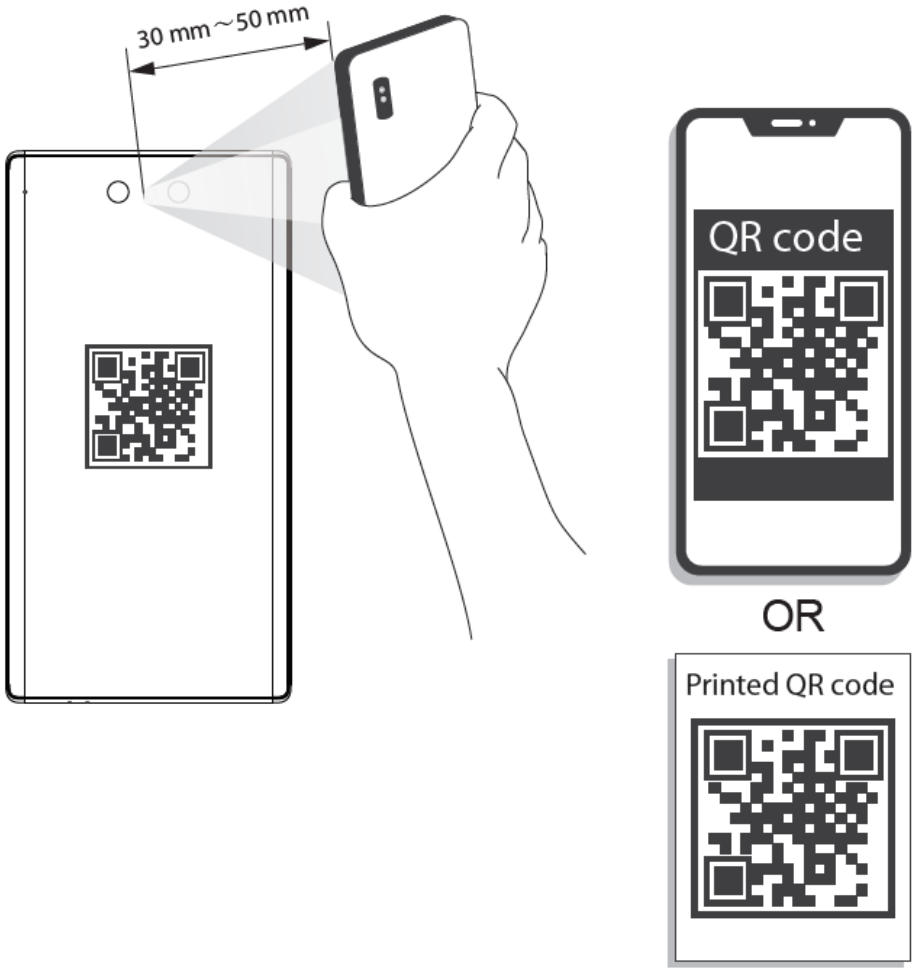
Apéndice 2 Puntos importantes del código QR

Exploración

Coloque el código QR en su teléfono a una distancia de 3 cm a 5 cm de la lente de escaneo del código QR. Admite códigos QR de más de 30 mm × 30 mm – 5 cm × 5 cm y menos de 128 bytes de tamaño.

La distancia de detección del código QR varía según los bytes y el tamaño del código QR. El código O a continuación es solo como referencia y escanee el código QR real.

Apéndice Figura 2-1 Escaneo de código QR



Apéndice 3 Puntos importantes de cara Registro

Antes del registro

- Las gafas, los sombreros y la barba pueden influir en el rendimiento del reconocimiento facial.
- No te cubras las cejas cuando uses sombreros.
- No cambies mucho el estilo de tu barba si utilizas el controlador de acceso; de lo contrario, el reconocimiento facial podría fallar.
- Mantén tu cara limpia.
- Mantenga el controlador de acceso al menos a dos metros de distancia de fuentes 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 afectar el rendimiento del reconocimiento facial del controlador de acceso.

Durante el registro

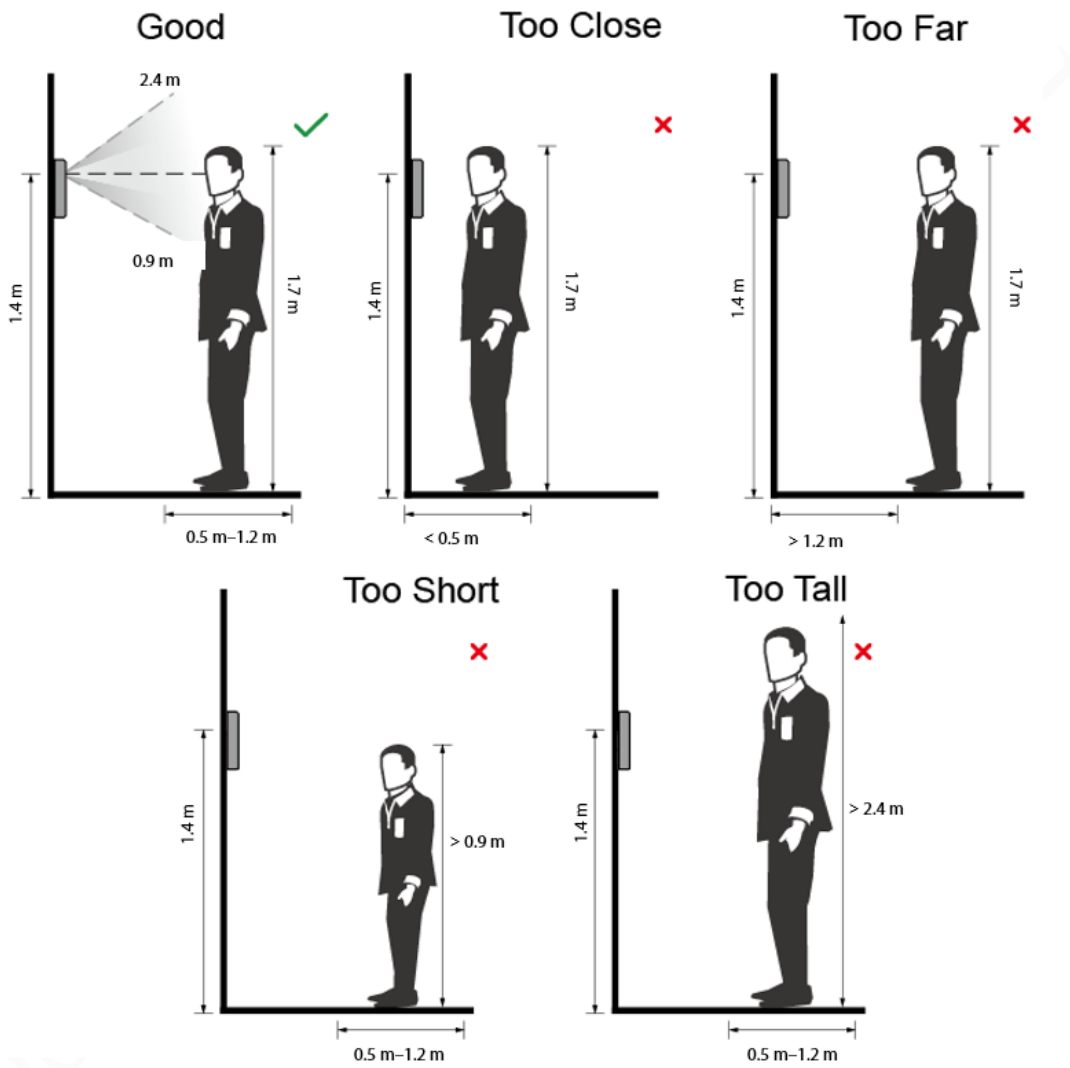
- Puedes registrar rostros a través del Controlador de Acceso o a través de la plataforma. Para el registro a través de la plataforma, consultar el manual de usuario de la plataforma.
- Coloque su cabeza en el centro del marco de captura de fotografías. La imagen de la cara se capturará automáticamente.

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

Posición de la cara

Si su rostro no está en la posición adecuada, la precisión del reconocimiento facial podría verse afectada.

Apéndice Figura 3-1 Posición adecuada de la cara



Requisitos de caras

- Asegúrese de que la cara esté limpia y que la frente no esté cubierta de pelo.
- No use gafas, sombreros, barbas espesas ni otros adornos faciales que influyan en la grabación de imágenes faciales.
- Con los ojos abiertos, sin expresiones faciales, y dirige tu 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 3-2 Posición de la cabeza

Apéndice Figura 3-3 Distancia de la cara

- 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 píxeles a 600 × 1200 píxeles; Los píxeles de la imagen son más de 500. × 500 píxeles; El tamaño de la imagen es inferior a 100 KB y el nombre de la imagen y el ID de la persona son los mismos.
- Asegúrese de que la cara ocupe más de 1/3 pero no más de 2/3 del área total de la imagen. y la relación de aspecto no supera 1:2.

Apéndice 4 Recomendaciones de ciberseguridad

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

1.**Utilice contraseñas seguras**

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres.
- Incluya al menos dos tipos de personajes; Los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos.
- No incluya el nombre de la cuenta ni 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 "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 "es bueno tener" para mejorar la seguridad de la red de su dispositivo:

1.**Protección física**

Le sugerimos que realice protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras y un gabinete especiales, e implemente permisos de control de acceso y administración de claves bien hechos para evitar que personal no autorizado lleve a cabo contactos físicos, como daños en el hardware, conexión no autorizada de un dispositivo extraíble (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 que las adivinen o las descifren.

3.**Establecer y actualizar contraseñas Restablecer información oportunamente**

El dispositivo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluido el buzón del usuario final y las preguntas sobre protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar preguntas de protección con contraseña, se sugiere no utilizar aquellas que puedan adivinarse fácilmente.

4.**Habilitar bloqueo de cuenta**

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

5.**Cambiar HTTP predeterminado y otros puertos de servicio**

Le sugerimos que cambie 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 habilitar 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 ARP.

8.**Asignar cuentas y privilegios de forma razonable**

De acuerdo con los requisitos comerciales y de administración, agregue usuarios de manera razonable y asigne un

conjunto mínimo de permisos para ellos.

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 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 cifrado WPA2-PSK y configure contraseñas seguras.

10.**Transmisión cifrada de audio y vídeo**

Si el contenido de sus datos de audio y video es muy importante o confidencial, le recomendamos que utilice la función de transmisión cifrada para reducir el riesgo de que los datos de audio y video sean robados durante la transmisión.

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

11.**Auditoría segura**

- Verifique los usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo inició sesión sin autorización.
- Verifique el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se utilizaron para iniciar sesión en sus dispositivos y sus operaciones clave.

12.**Registro de red**

Debido a la capacidad de almacenamiento limitada del dispositivo, el registro almacenado es limitado. Si necesita guardar el registro durante un período prolongado, se recomienda habilitar la función de registro de red para garantizar que los registros críticos estén sincronizados con el servidor de registro de red para su seguimiento.

13.**Construya un entorno de red seguro**

Para garantizar mejor la seguridad del dispositivo y reducir los posibles riesgos cibernéticos, recomendamos:

- Deshabilite la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa.
- La red debe dividirse y aislarse según las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere utilizar VLAN, red GAP y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts permitidos para acceder al dispositivo.