Controlador de acceso por reconocimiento facial

Guía de inicio rápido

V1.0.0

Prefacio

General

Este manual presenta las funciones y operaciones del Controlador de acceso por reconocimiento facial (en adelante, el "Dispositivo"). 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
	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
	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.
	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
	Proporciona información adicional como complemento al texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	abril 2022

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otras personas, como su rostro, audio, 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 Dispositivo, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el Dispositivo y cumpla con las pautas al usarlo.

Requisito de transporte

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

Requisito de almacenamiento

Guarde el dispositivo en condiciones permitidas de humedad y temperatura.

requerimientos de instalación

- No conecte el adaptador de corriente al dispositivo 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 dispositivo.
- No conecte el Dispositivo a dos o más tipos de fuentes de alimentación para evitar daños al Dispositivo.
- El uso inadecuado de la batería podría provocar un incendio o una explosión.
- Siga los requisitos eléctricos para alimentar el dispositivo.
  - A continuación se detallan los requisitos para seleccionar un adaptador de corriente.
    - La fuente de alimentación debe cumplir con los requisitos de las normas IEC 60950-1 e IEC 62368-1.
    - El voltaje debe cumplir con los requisitos SELV (voltaje extra bajo de seguridad) y no exceder los estándares ES-1.
    - Cuando la potencia del dispositivo no supera los 100 W, la fuente de alimentación debe cumplir con los requisitos de LPS y no ser superior a PS2.
  - Recomendamos utilizar el adaptador de corriente proporcionado con el dispositivo.
  - Al seleccionar el adaptador de corriente, los requisitos de la fuente de alimentación (como el voltaje nominal) están sujetos a la etiqueta del dispositivo.

- 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 Dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- Instale el dispositivo sobre una superficie estable para evitar que se caiga.
- Instale el dispositivo 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.
- El Dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del Dispositivo esté conectada a una toma de corriente con conexión a tierra de protección.

Requisitos de operación

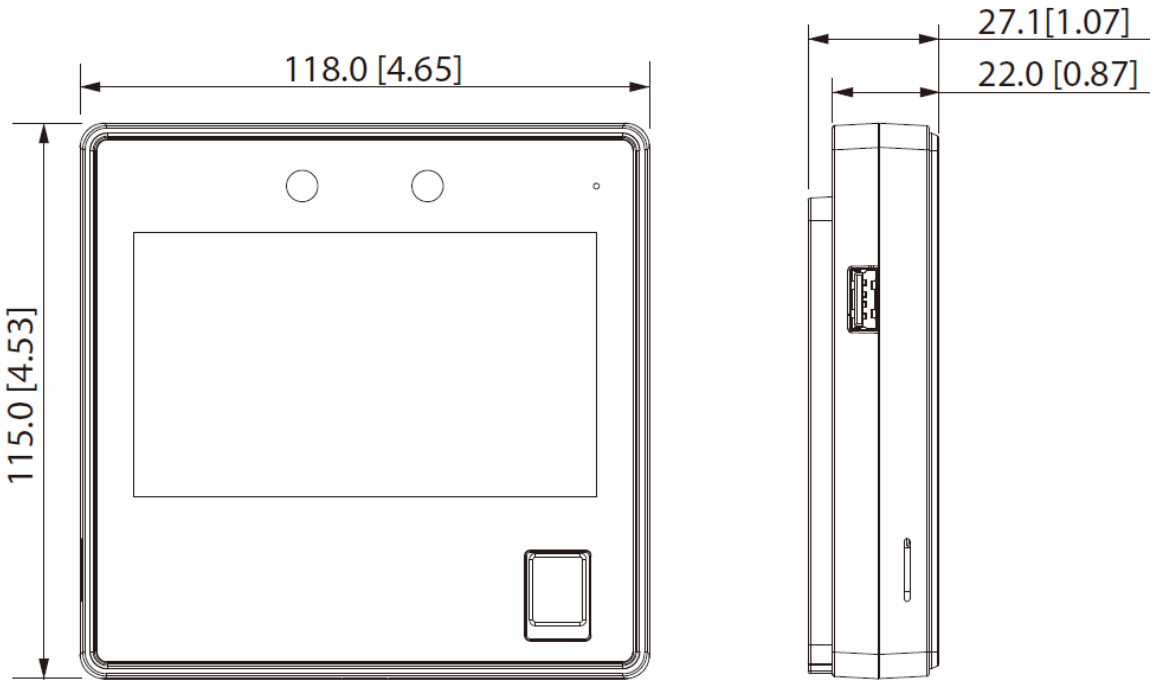
- Compruebe si la fuente de alimentación es correcta antes de su uso.
- Conecte el dispositivo a tierra protectora antes de encenderlo.
- No desenchufe el cable de alimentación en el costado del dispositivo mientras el adaptador esté encendido.
- Opere el dispositivo dentro del rango nominal de entrada y salida de energía.
- Utilice el dispositivo en condiciones permitidas de humedad y temperatura.
- No deje caer ni salpique líquido sobre el Dispositivo y asegúrese de que no haya ningún objeto lleno de líquido sobre el Dispositivo para evitar que el líquido fluya hacia él.
- No desmonte el dispositivo sin instrucción profesional.
- Este producto es un equipo profesional.
- El Dispositivo no es adecuado para su uso en lugares donde es probable que haya niños presentes.

Tabla de contenido

1 estructura

La apariencia frontal puede diferir según los diferentes modelos del Dispositivo. Aquí tomamos como ejemplo el modelo de huella digital.

Figura 1-1 Estructura (Unidad: mm [pulgadas])



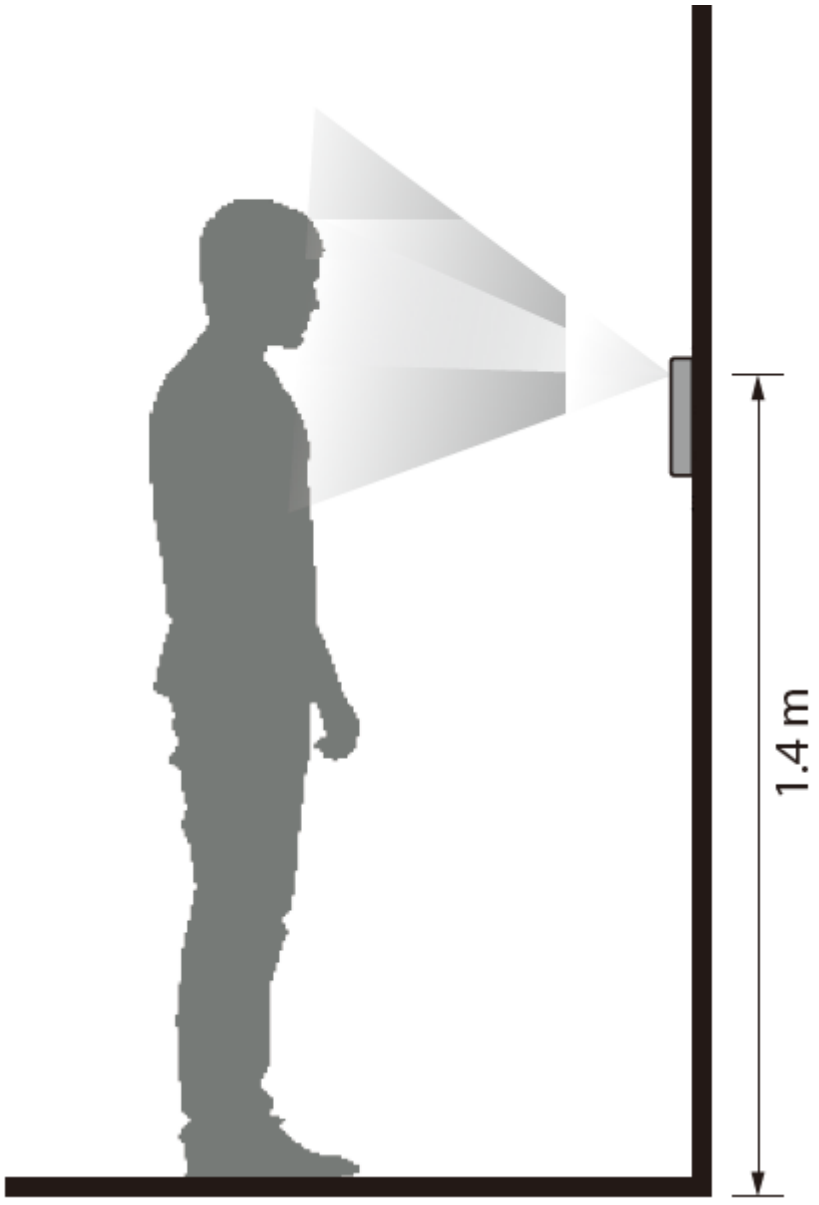
2 Conexión e instalación

2.1 Requisitos de instalación

- La altura de instalación es de 1,4 m (desde la lente hasta el suelo).
- La luz a 0,5 metros de distancia del dispositivo no debe ser inferior a 100 lux.
- Le recomendamos instalarlo en el interior, al menos a 3 metros de distancia de 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 2-1 Requisitos de altura de instalación

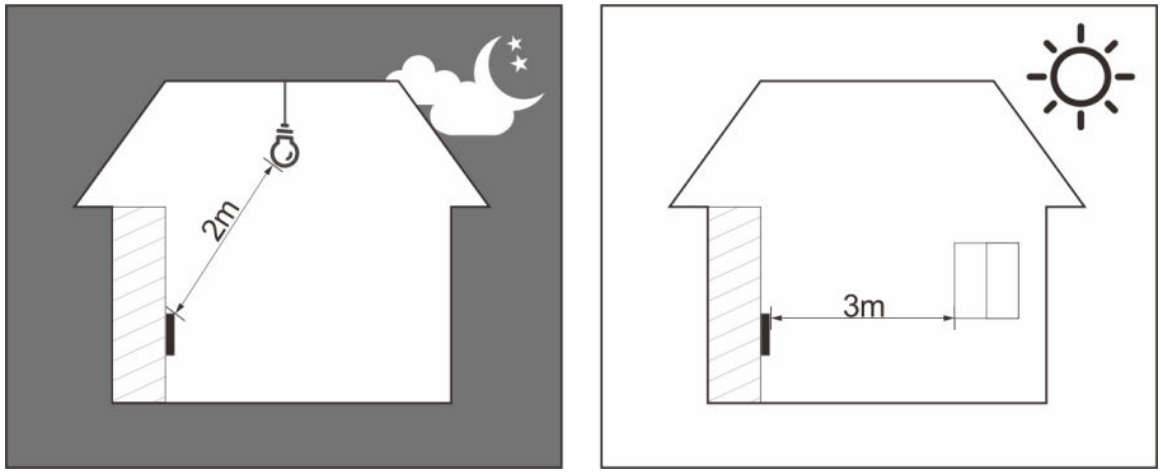


Requisitos de iluminación ambiental

Figura 2-2 Requisitos de iluminación ambiental

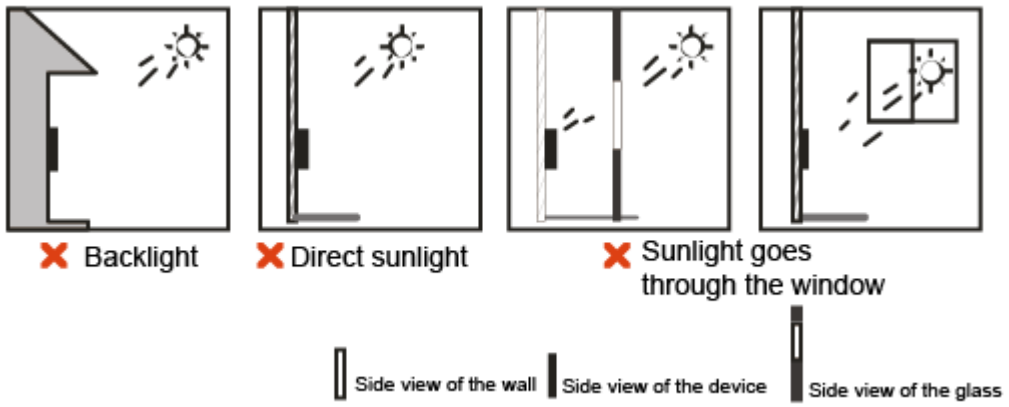
Ubicación de instalación recomendada

Figura 2-3 Ubicación de instalación recomendada



Ubicación de instalación no recomendada

Figura 2-4 Ubicación de instalación no recomendada

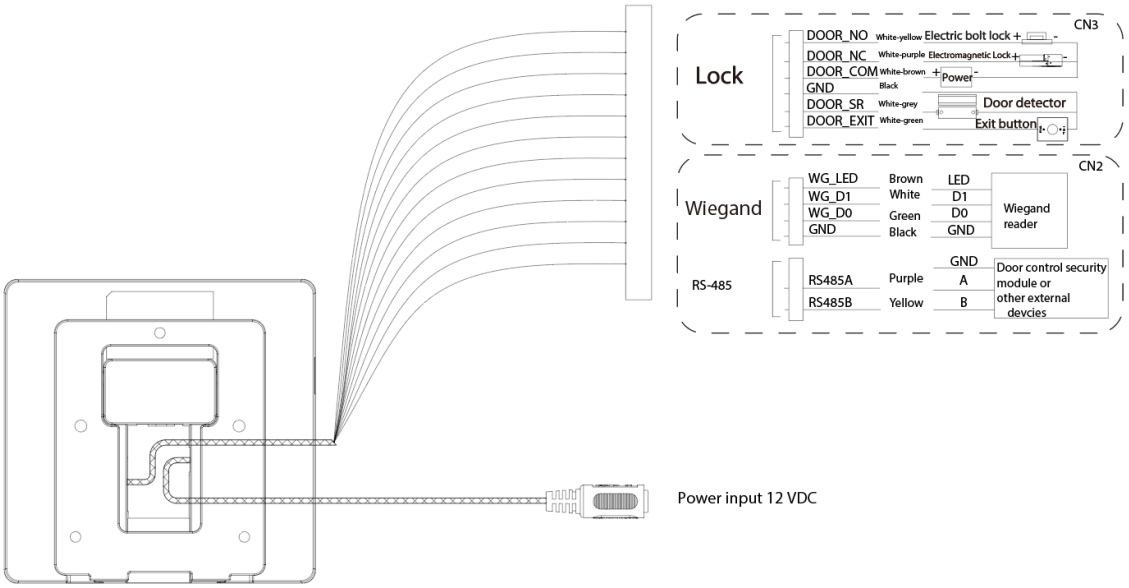


2.2 Cableado

Información de contexto

- Si desea conectar un módulo de seguridad externo, seleccione**Conexión**>**Puerto serial**>**Configuración RS-485**>**Módulo de seguridad**. Los clientes deben comprar el módulo de seguridad por separado.
- Cuando el módulo de seguridad esté encendido, el botón de salida y el control de bloqueo no serán efectivos.

Figura 2-5 Cableado



2.3 Proceso de instalación

Esta sección utiliza el modelo de huella digital del Dispositivo como ejemplo.

2.3.1 Montaje en pared

Procedimiento

Paso 1 Según la posición de los orificios en el soporte de instalación, taladre 3 orificios en la pared. Coloque pernos de expansión en los agujeros.

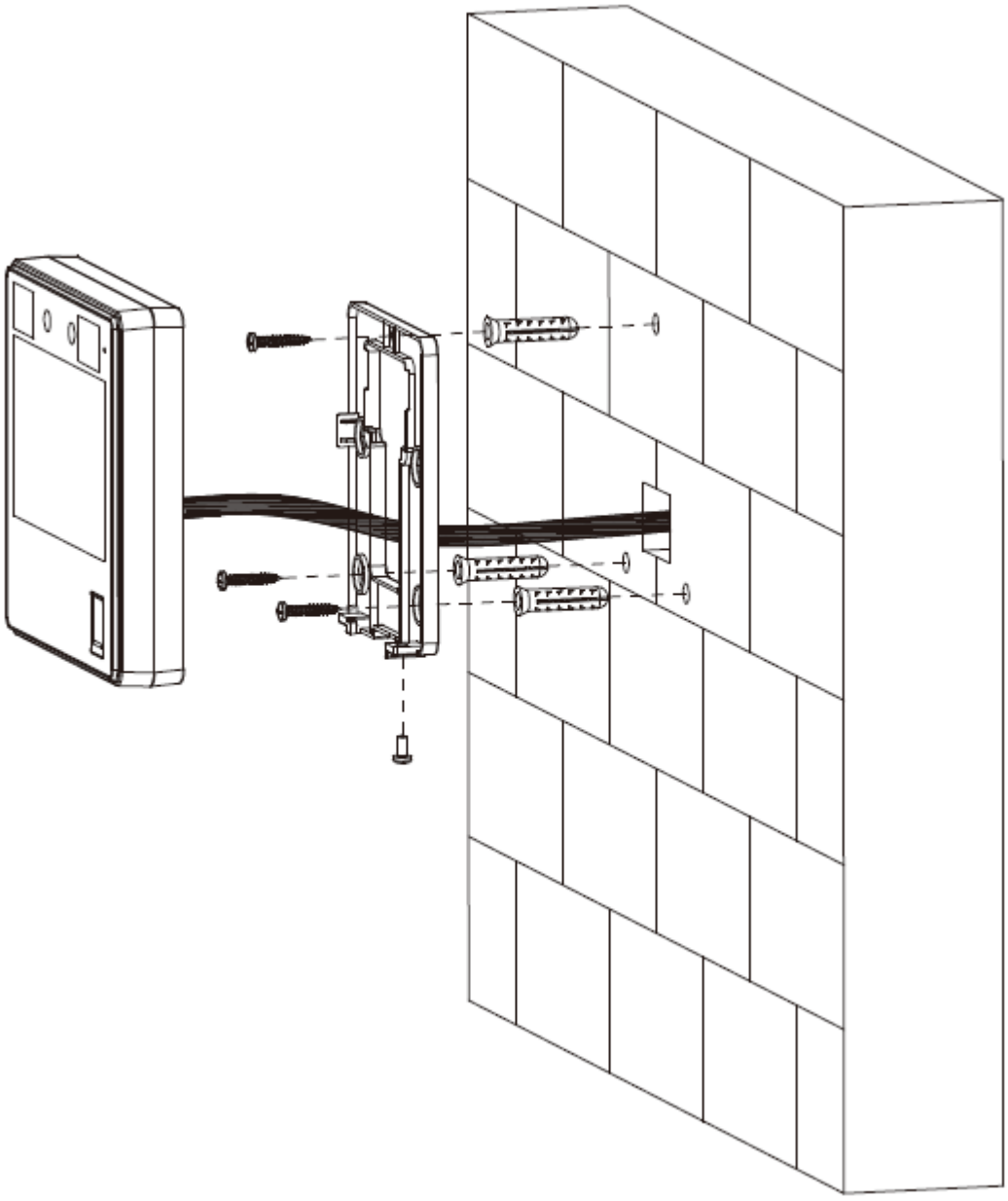
Paso 2 Utilice los 3 tornillos para fijar el soporte de instalación a la pared.

Paso 3 Conecte el dispositivo.

Etapa 4 Conecte el dispositivo al soporte.

Paso 5 Atornille 1 tornillo de forma segura en la parte inferior del dispositivo.

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

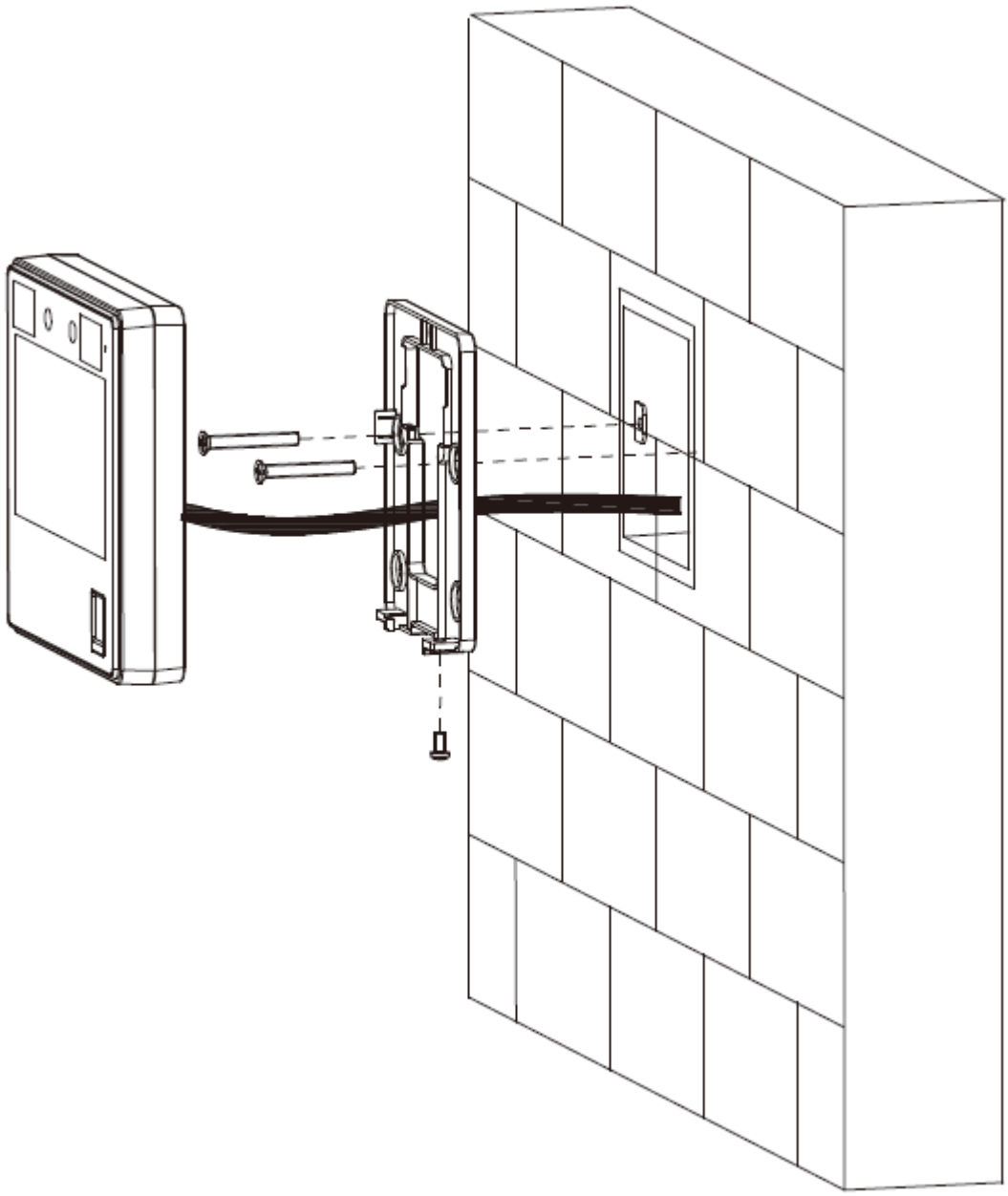
Paso 2 soporte de instalación a la caja 86 con 2 tornillos. Conecte el

Paso 3 dispositivo.

Etapa 4 Conecte el dispositivo al soporte.

Paso 5 Atornille 1 tornillo de forma segura en la parte inferior del dispositivo.

Figura 2-7 Montaje en caja 86



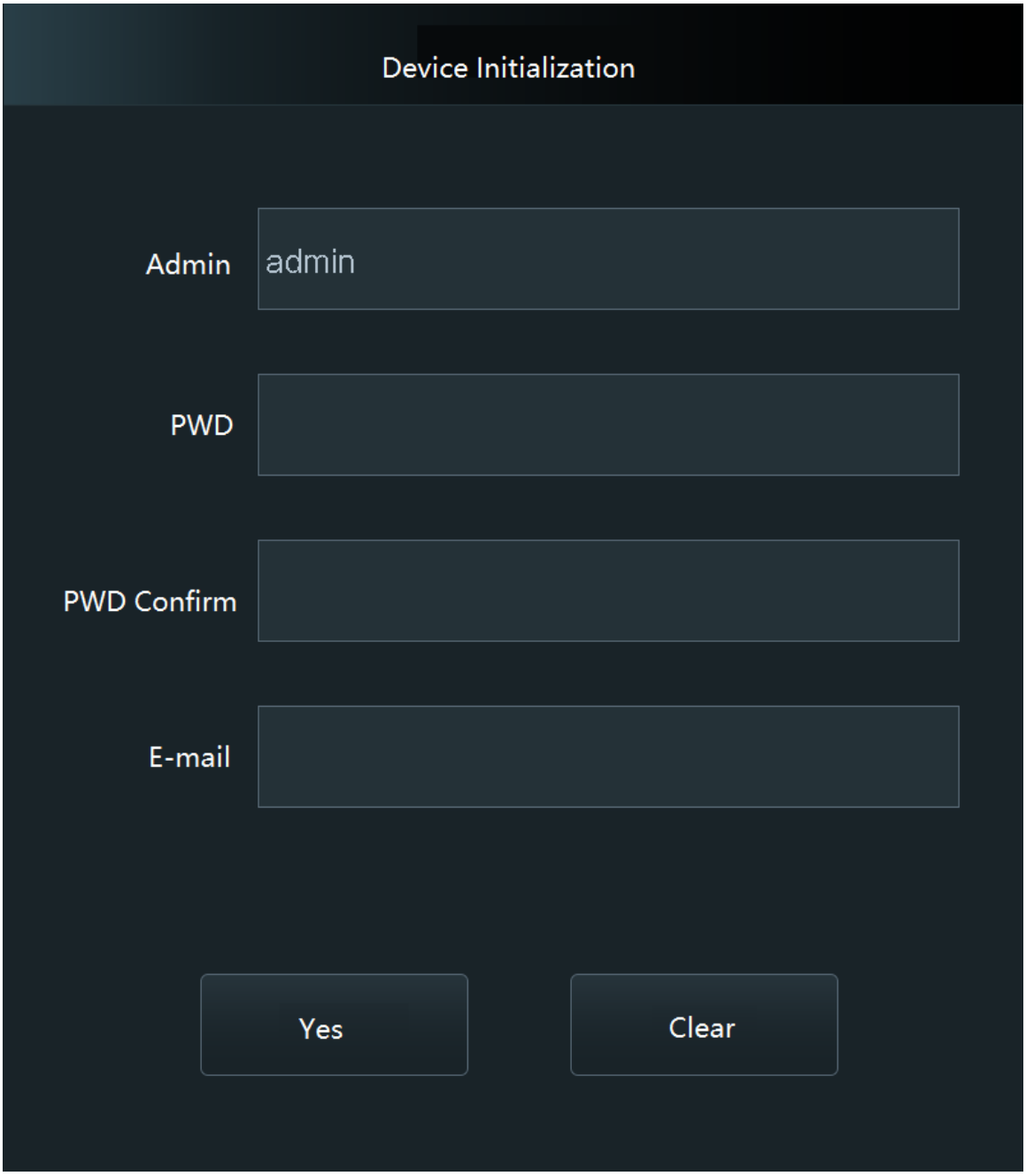
3 configuraciones locales

Las operaciones locales pueden diferir según los diferentes modelos.

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 Dispositivo 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 los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excluidos ' " ; : &). Establezca una contraseña de alta seguridad siguiendo la indicación de seguridad de la contraseña.

3.2 Agregar nuevos usuarios

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**>**Nuevo Usuario**.

Paso 2 Configurar parámetros de usuario.

Figura 3-2 Nuevo usuario(1)

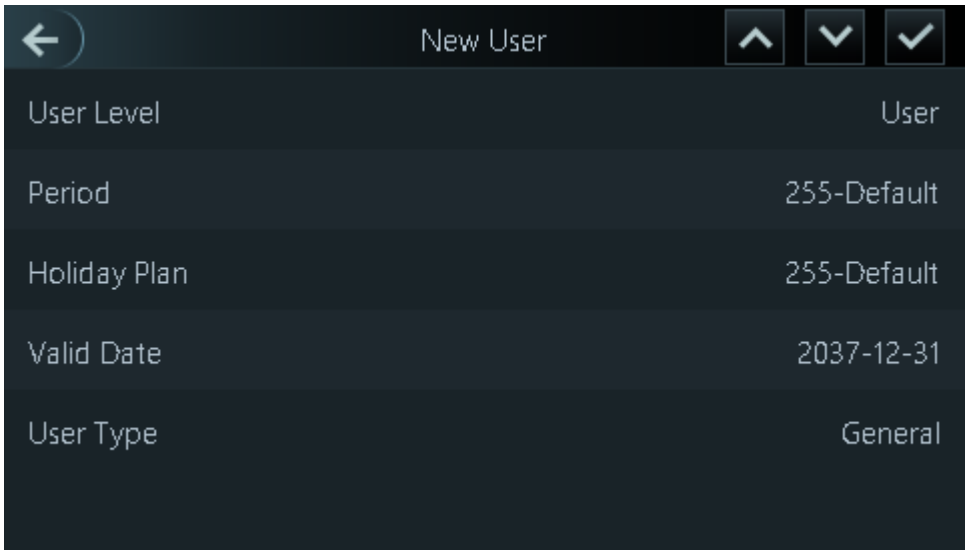


Figura 3-3 Nuevo usuario(2)

Tabla 3-1 Descripción de nuevo usuario

Parámetro	Descripción
ID de usuario	Ingrese la identificación de usuario. La identificación puede ser números, letras y sus combinaciones, y la longitud máxima de la identificación de usuario es de 32 caracteres. Cada identificación es única.
Nombre	Ingrese el nombre de usuario y la longitud máxima es de 32 caracteres, incluidos números, símbolos y letras.
FP	Cada usuario puede registrar hasta 3 huellas dactilares. Siga las instrucciones en pantalla para registrar huellas digitales. Puede configurar la huella digital registrada como huella digital de coacción y se activará una alarma si la puerta se desbloquea con la huella digital de coacción.  ● No recomendamos configurar la primera huella digital como huella digital de coacción. ● La función de huellas dactilares solo está disponible para el modelo de huellas dactilares del dispositivo.
Rostro	Asegúrese de que su rostro esté centrado en el marco de captura de imágenes y la imagen del rostro se capturará automáticamente. Puede registrarse nuevamente si encuentra que la imagen de la cara capturada no le satisface.
Tarjeta	Un usuario puede registrar hasta cinco tarjetas. Ingrese el número de su tarjeta o pase la tarjeta y luego el dispositivo leerá la información de la tarjeta. Puede configurar la tarjeta registrada como tarjeta de coacción y luego se activará una alarma cuando se utilice una tarjeta de coacción para desbloquear la puerta.  Sólo el modelo con tarjeta magnética admite esta función.
PCD	Ingrese la contraseña de usuario para desbloquear la puerta. La longitud máxima de la contraseña es de 8 dígitos.
Nivel de usuario	Establecer permisos de usuario para nuevos usuarios. ● **General**:Los usuarios solo tienen permiso de acceso a la puerta. ● **Administración**:Los administradores pueden desbloquear la puerta y configurar el dispositivo.
Período	Los usuarios pueden ingresar a un área controlada dentro del período definido. El valor predeterminado es 255, lo que significa que no se configura ningún período.
Plan de vacaciones	Los usuarios pueden ingresar a un área controlada dentro de los días festivos programados. El valor predeterminado es 255, lo que significa que no hay ningún plan de vacaciones configurado.
Fecha válida	Defina un período durante el cual se le otorga al usuario acceso a un área segura.

Parámetro	Descripción
Tipo de usuario	• **General**:Los usuarios generales pueden desbloquear la puerta normalmente. • **Lista de bloqueos**:Cuando los usuarios en la lista de bloqueo desbloquean la puerta, el personal de servicio recibe una notificación. • **Invitado**:Los huéspedes pueden desbloquear la puerta dentro de un período definido o durante un número determinado de veces. Una vez transcurrido el período definido o los tiempos de desbloqueo, no pueden desbloquear la puerta. • **Patrulla**:A los usuarios en libertad condicional se les puede realizar un seguimiento de su asistencia, pero no tienen permisos de desbloqueo. • **VIP**:Cuando VIP abra la puerta, el personal de servicio recibirá una notificación. • **Otros**:Cuando desbloqueen la puerta, la puerta permanecerá desbloqueada durante 5 segundos más. • **Usuario personalizado 1/2**:Igual que**General**.

Paso 3 Grif

4 Iniciar sesión en la página web

En la página web, también puede configurar y actualizar el Dispositivo.

Requisitos previos

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

Información de contexto

Las configuraciones de la página web difieren según los modelos del Dispositivo. Solo ciertos modelos del dispositivo admiten conexión de red.

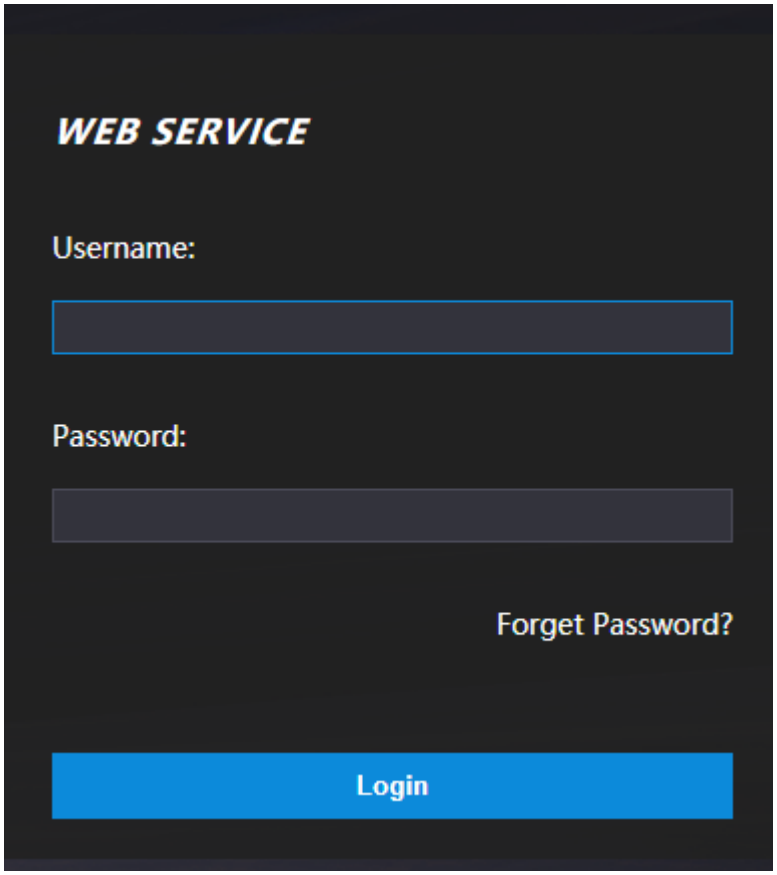
Procedimiento

Paso 1 Abra un navegador web, vaya a la dirección IP del Dispositivo.

Puede utilizar IE11, Firefox o Chrome.

Paso 2 Ingrese el nombre de usuario y la contraseña.

Figura 4-1 Inicialización



- El nombre de usuario predeterminado del administrador es admin y la contraseña es la que estableció durante la inicialización. Le recomendamos que cambie la contraseña del 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 de las huellas dactilares

Instrucciones de registro

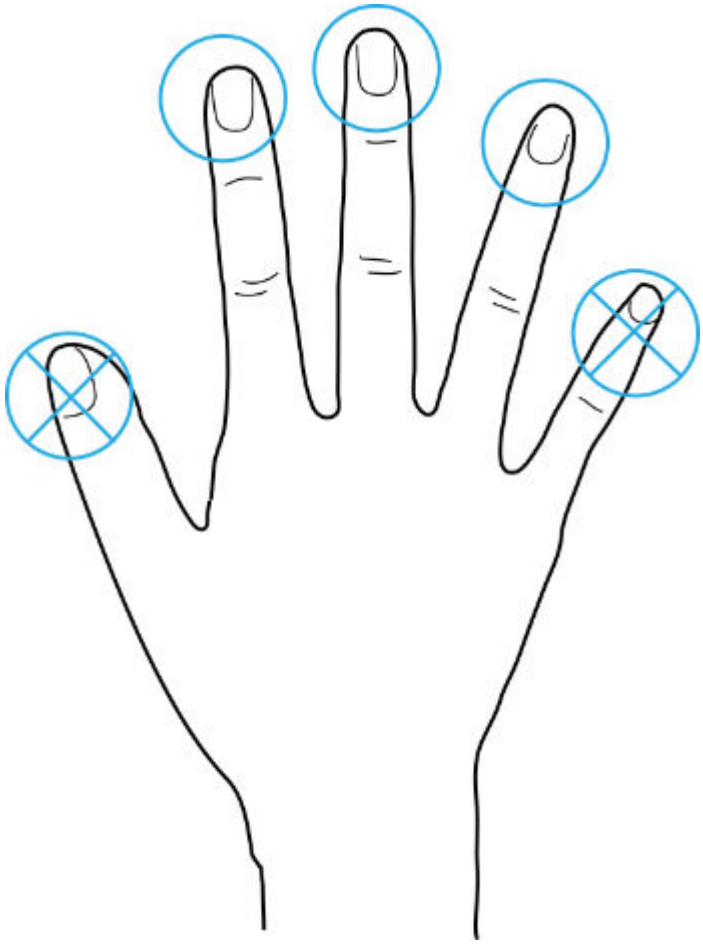
Al registrar la huella digital, preste atención a los siguientes puntos:

- Asegúrese de que sus dedos y la superficie del escáner estén limpios y secos.
- Presione su dedo en el centro del escáner de huellas digitales.
- No coloque el sensor de huellas dactilares en un lugar con luz intensa, alta temperatura y alta humedad.
- Si sus huellas digitales no están claras, utilice otros métodos de desbloqueo.

Dedos recomendados

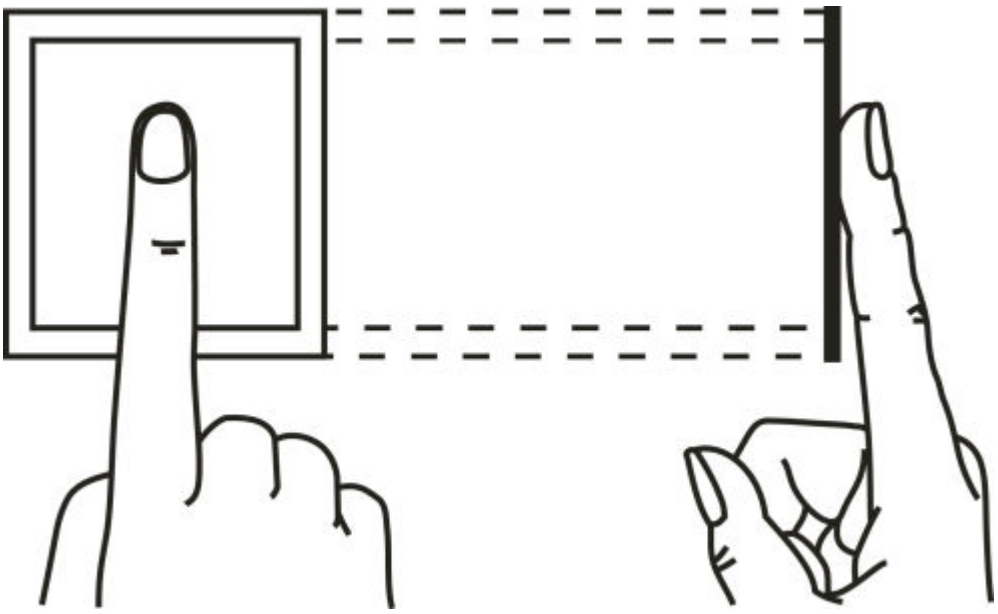
Se recomiendan los dedos índice, medio y anular. Los pulgares y los meñiques no se pueden colocar fácilmente en el centro de grabación.

Apéndice Figura 1-1 Dedos recomendados

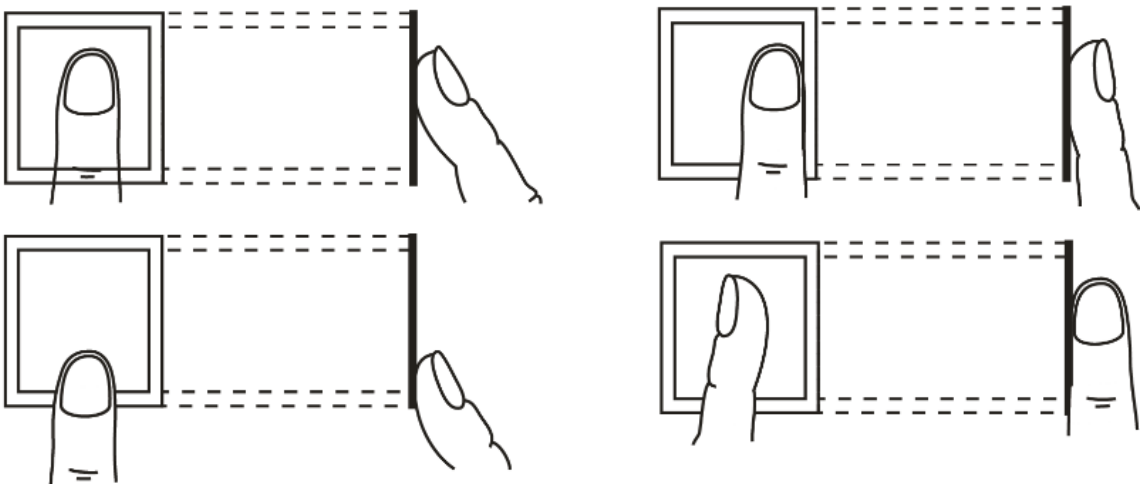


Cómo presionar su huella digital en el escáner

Apéndice Figura 1-2 Colocación correcta



Apéndice Figura 1-3 Ubicación incorrecta



Apéndice 2 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 cambie mucho el estilo de su barba si usa el Dispositivo; de lo contrario, el reconocimiento facial podría fallar.
- Mantén tu cara limpia.
- Mantenga el Dispositivo al menos a 2 metros de distancia de fuentes de luz y al menos a 3 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

- Puede registrar rostros a través del Dispositivo 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.

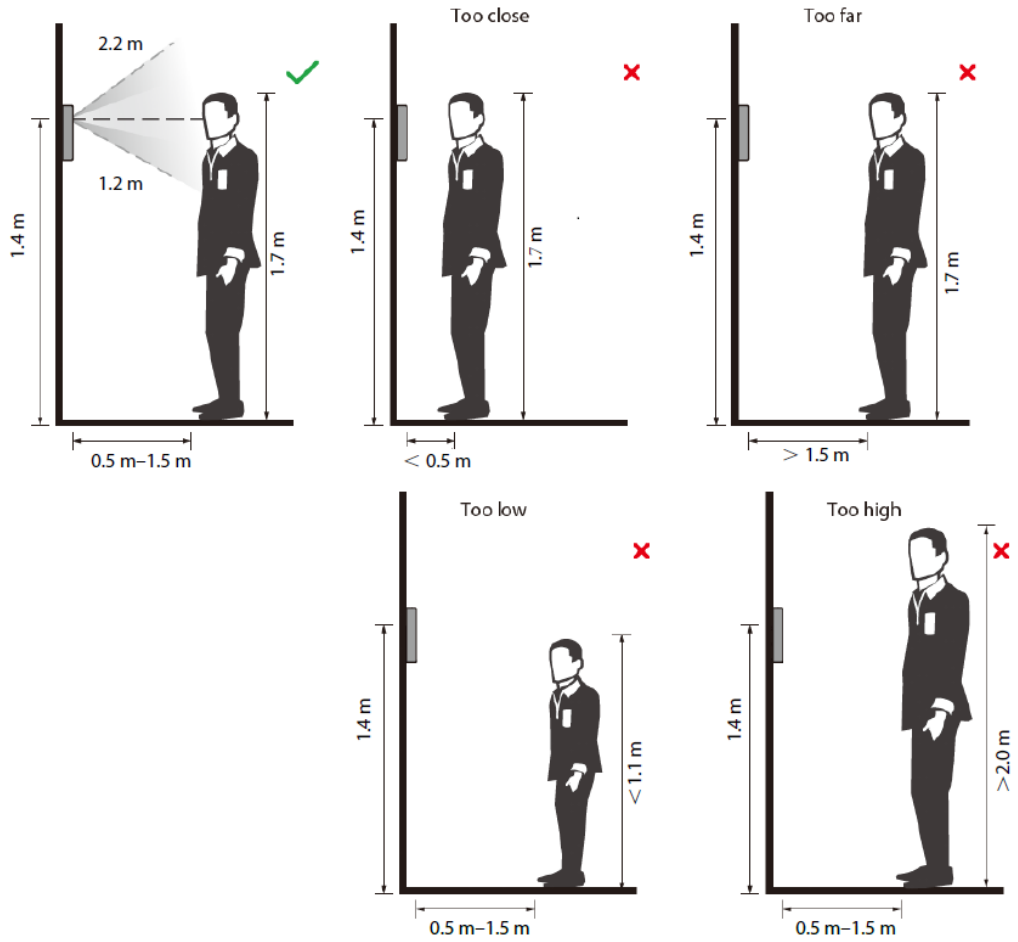
- No sacuda la cabeza ni el cuerpo, de lo contrario el registro podría fallar.
- Evite que aparezcan 2 caras en el marco de captura al mismo tiempo.

Posición de la cara

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

La posición de la cara a continuación es solo como referencia y puede diferir de la situación real.

Apéndice Figura 2-1 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 2-2 Posición de la cabeza

Apéndice Figura 2-3 Distancia de la cara

- 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 píxeles a 600 × 1200 píxeles. Se recomienda que la resolución sea superior a 500 × 500 píxeles, que el tamaño de la imagen sea inferior a 100 KB y que el nombre de la imagen y el ID de la persona sean 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 que la relación de aspecto no exceda 1:2.

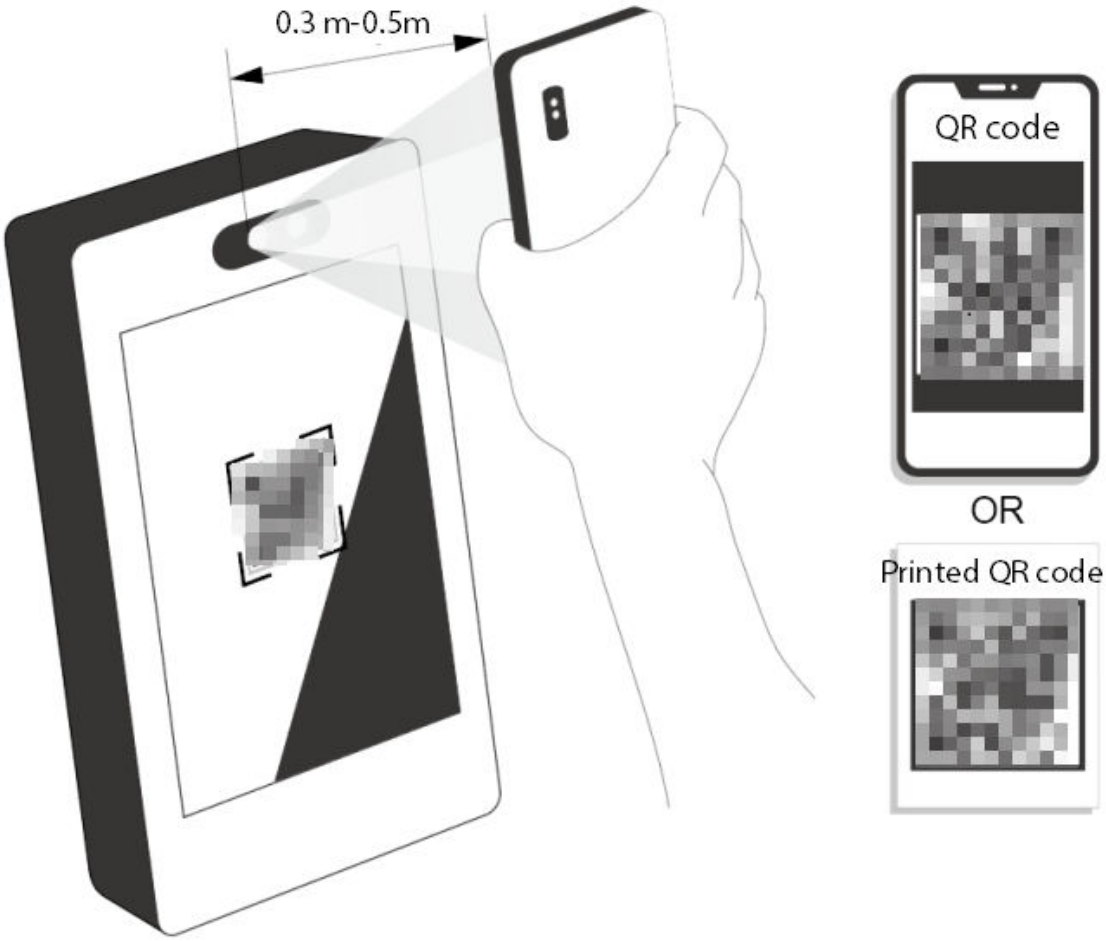
Apéndice 3 Puntos importantes del código QR

Exploración

Coloque el código QR a una distancia de 30 cm-50 cm de la lente del Controlador de acceso o de la lente del módulo de extensión del código QR. Admite códigos QR de más de 30 cm × 30 cm y menos de 100 bytes de tamaño.

La distancia de detección del código QR varía según los bytes y el tamaño del código QR.

Apéndice Figura 3-1 Escaneo de código QR



Apéndice 4 Recomendación de seguridad

Administración de cuentas

1.**Utilice contraseñas complejas**

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluir al menos dos tipos de caracteres: letras mayúsculas y minúsculas, números y símbolos;
- No contener 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 repetidos, como 111, aaa, etc.

2.**Cambiar contraseñas periódicamente**

Se recomienda cambiar periódicamente la contraseña del dispositivo para reducir el riesgo de que la adivinen o la descifren.

3.**Asigne cuentas y permisos adecuadamente**

Agregue usuarios adecuadamente según los requisitos de servicio y administración y asigne conjuntos de permisos mínimos a los usuarios.

4.**Habilitar la función de bloqueo de cuenta**

La función de bloqueo de cuenta está habilitada de forma predeterminada. Se recomienda mantenerlo habilitado para proteger la seguridad de la cuenta. Después de varios intentos fallidos de contraseña, la cuenta correspondiente y la dirección IP de origen se bloquearán.

5.**Establecer y actualizar la información de restablecimiento de contraseña de manera oportuna**

El dispositivo admite la función de restablecimiento de contraseña. Para reducir el riesgo de que esta función sea utilizada por actores de amenazas, si hay algún cambio en la información, modifíquelo a tiempo. Al establecer preguntas de seguridad, se recomienda no utilizar respuestas fáciles de adivinar.

Configuración del servicio

1.**Habilitar HTTPS**

Se recomienda habilitar HTTPS para acceder a servicios web a través de canales seguros.

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

Si el contenido de sus datos de audio y video es muy importante o confidencial, se recomienda utilizar la función de transmisión cifrada para reducir el riesgo de que sus datos de audio y video sean interceptados durante la transmisión.

3.**Apague los servicios no esenciales y use el modo seguro**

Si no es necesario, se recomienda desactivar algunos servicios como SSH, SNMP, SMTP, UPnP, punto de acceso AP, etc., para reducir las superficies de ataque.

Si es necesario, se recomienda encarecidamente elegir modos seguros, incluidos, entre otros, los siguientes servicios:

- SNMP: elija SNMP v3 y configure contraseñas de autenticación y cifrado seguras.
- SMTP: elija TLS para acceder al servidor de buzones.
- FTP: elija SFTP y configure contraseñas complejas.
- Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas complejas.

4.**Cambiar HTTP y otros puertos de servicio predeterminados**

Se recomienda cambiar el puerto predeterminado de HTTP y otros servicios a cualquier puerto entre 1024 y 65535 para reducir el riesgo de que los actores de amenazas lo adivinen.

configuración de la red

1.**Habilitar lista de permitidos**

Se recomienda activar la función de lista de permitidos y solo permitir que IP en la lista de permitidos acceda al dispositivo. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del dispositivo compatible a la lista de permitidos.

2.**Enlace de dirección MAC**

Se recomienda vincular la dirección IP de la puerta de enlace a la dirección MAC del dispositivo para reducir el riesgo de suplantación de ARP.

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

Para garantizar mejor la seguridad de los dispositivos y reducir los posibles riesgos cibernéticos, se recomienda lo siguiente:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa;
- Particione la red de acuerdo con las necesidades reales de la red: si no hay demanda de comunicación entre las dos subredes, se recomienda utilizar VLAN, puerta de enlace y otros métodos para particionar la red y lograr el aislamiento de la red;
- Establecer un sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso ilegal de terminales a la red privada.

Auditoría de seguridad

1.**Verificar usuarios en línea**

Se recomienda comprobar periódicamente a los usuarios en línea para identificar a los usuarios ilegales.

2.**Verificar el registro del dispositivo**

Al ver los registros, puede obtener información sobre las direcciones IP que intentan iniciar sesión en el dispositivo y las operaciones clave de los usuarios registrados.

3.**Configurar el registro de red**

Debido a la capacidad de almacenamiento limitada de los dispositivos, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, 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.

Seguridad del software

1.**Actualice el firmware a tiempo**

De acuerdo con las especificaciones operativas estándar de la industria, el firmware de los dispositivos debe actualizarse a la última versión a tiempo para garantizar que el dispositivo tenga las últimas funciones y seguridad. Si el dispositivo está conectado a la red pública, se recomienda habilitar la función de detección automática de actualización en línea, para obtener la información de actualización del firmware publicada por el fabricante de manera oportuna.

2.**Actualice el software del cliente a tiempo**

Se recomienda descargar y utilizar el software de cliente más reciente.

Protección física

Se recomienda llevar a cabo protección física para los dispositivos (especialmente los dispositivos de almacenamiento), como colocar el dispositivo en una sala de máquinas y un gabinete exclusivos, y tener control de acceso.

y gestión de claves implementada para evitar que personal no autorizado dañe el hardware y otros equipos periféricos (por ejemplo, disco flash USB, puerto serie).