Controlador de acceso de huellas dactilares

Guía de inicio rápido

V1.0.0

Prefacio

General

Este manual presenta la instalación y el funcionamiento básico del controlador de acceso mediante huellas dactilares (en adelante denominado "controlador de acceso").

Las instrucciones de seguridad

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

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

Revisión histórica

Versión	Contenido de la revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento	Agosto de 2019

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. Aún 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 el servicio de atención al cliente si se produce algún problema al usar 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 del controlador de acceso, la prevención de peligros y la prevención de daños a la propiedad. Lea el contenido detenidamente antes de utilizar el controlador de acceso y guárdelo en un lugar seguro para futuras consultas.

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

Seguridad ELECTRICA

- El uso inadecuado de la batería puede provocar un incendio, una explosión o una inflamación. Cuando
- reemplace la batería, asegúrese de usar el mismo modelo.
- Utilice los cables de alimentación recomendados en la región y cumpla con la especificación de potencia nominal.
- Utilice el adaptador de corriente provisto con el controlador de acceso; 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 energía 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

1 General

El controlador de acceso de huellas dactilares de metal es un dispositivo de control de acceso que admite el desbloqueo de tarjetas y el desbloqueo de huellas dactilares.

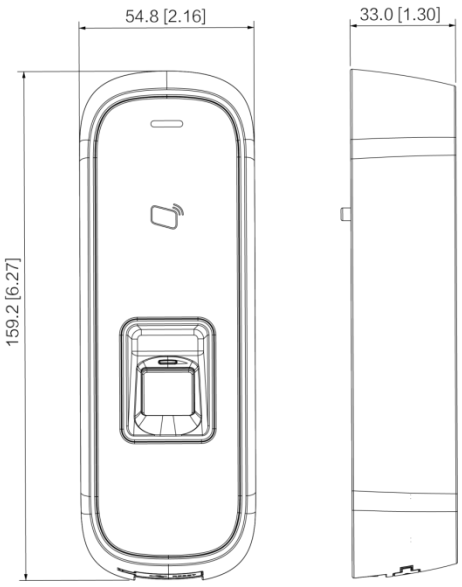
1.1 Características

- CPU de 32 bits del panel frontal de
- aleación de zinc
- Admite W26 \ W34 (sea compatible con productos de terceros) Admite RS-485 y
- protocolo Wiegand
- Frecuencia de lectura de la tarjeta: 13,56 MHZ; distancia de lectura de tarjetas: 1 cm – 3 cm; el tiempo de respuesta es inferior a 0,1 s

- Lectura de tarjetas sin contacto, puede leer la tarjeta Mifare, leer el número de tarjeta de la tarjeta IC de transporte público, la tarjeta IC bancaria y la tarjeta Mifare
- Soporte "perro guardián" (un dispositivo que protege un sistema de fallas de software o hardware) Soporte de actualización en línea; Si la
- actualización en línea falló, puede actualizar nuevamente Soporte de desbloqueo de tarjetas, desbloqueo de huellas digitales y desbloqueo de
- tarjetas y huellas digitales
- Zumbador y luces indicadoras Admite
- alarma de manipulación
- Función de protección contra truenos, antiestática y cortocircuito
- Todos los puertos con función de protección contra sobrecorriente y sobretensión Grado de
- protección: IP65 e IK10
- Temperatura de trabajo: -30 ℃ hasta +50 ℃
- Humedad de trabajo: ≤95%

1.2 Dimensiones

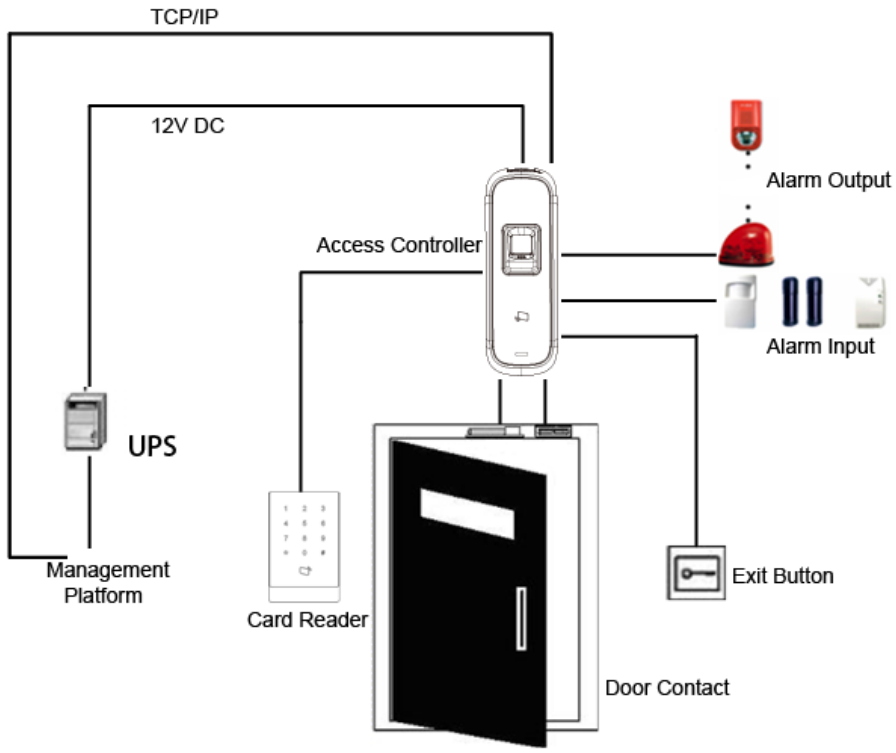
Figura 1-1 Dimensiones (mm [pulgadas])



2 Instalación

2.1 Diagrama de aplicación

Figura 2-1 Diagrama de aplicación



2.2 Componente

Figura 2-2 Panel frontal

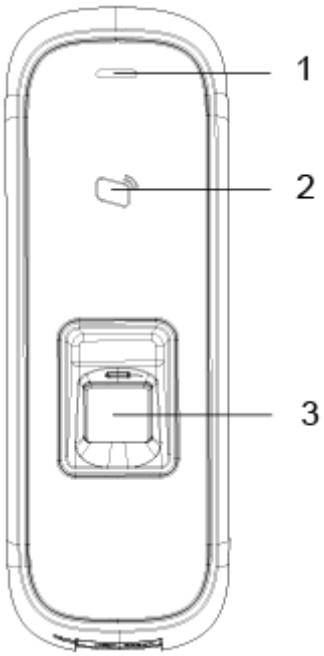


Figura 2-3 Puertos en la parte inferior

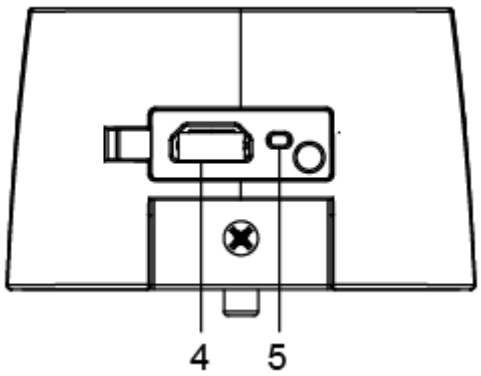


Tabla 2-1 Comp onent descripción (1)

Sin nombre		Sin nombre	
1	Luz indicadora	4	Puerto USB
2	Área de deslizamiento de tarjetas	5	REINICIAR
3	Sensor de huellas dactilares	-	-

2.3 Instalación

Figura 2-4 Instalación

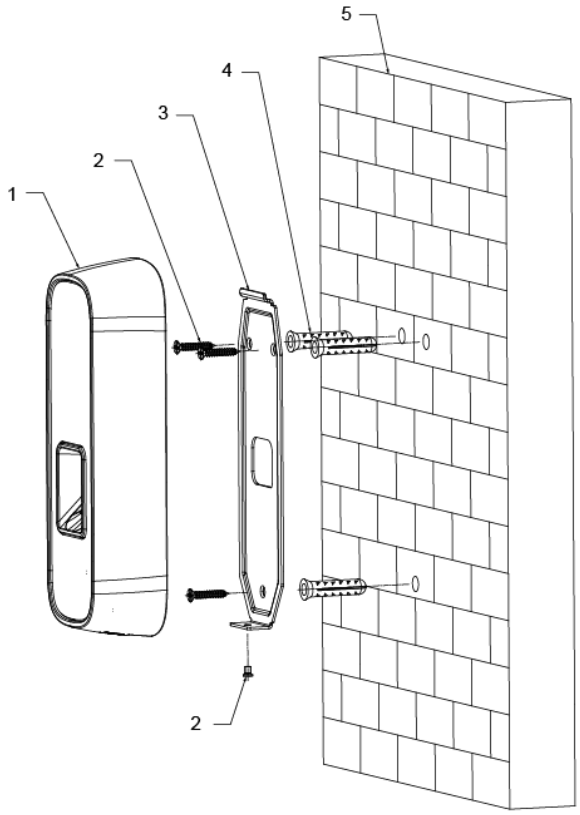


Tabla 2-2 Co mpon descripción ent (2)

No. Nombre		No. Nombre	
1	Controlador de acceso 4		Perno de ancla
2	Tornillo ST3 × 18	5	pared
3	Soporte	-	-

Procedimiento

Paso 1 Taladre tres orificios a la altura adecuada en la pared de acuerdo con las posiciones soporte.

Paso 2 Martille los pernos de anclaje en la pared.

Paso 3 Fije el soporte en la pared mediante los tres tornillos ST3 × 18.

Paso 4 Instale el controlador de acceso en el soporte a través del sujetador del soporte.

Paso 5 Compruebe si el controlador de acceso está firmemente fijado a la pared.

2.4 Conexión de cable

Figura 2-5 Conexión de cables

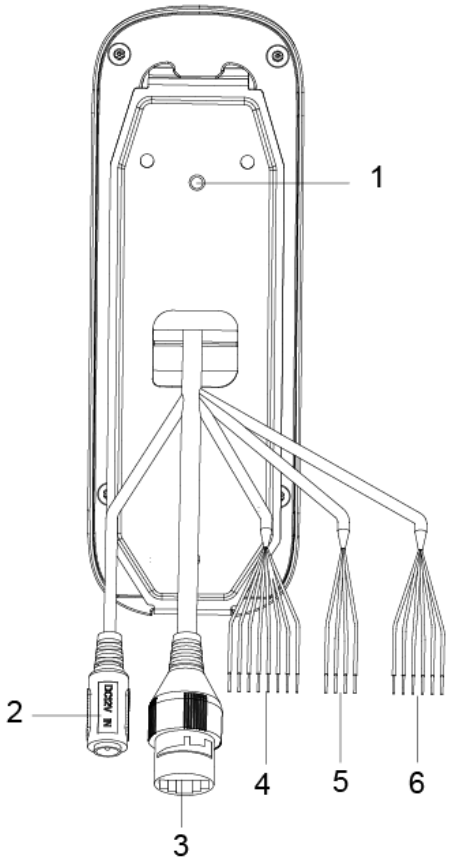


Tabla 2-3 Comp descripción onent (3)

No.	Nombre	No.	Nombre
1	Interruptor de sabotaje 4		CON4
2	Puerto de alimentación	5	CON5
3	Puerto Ethernet	6	CON6

2.4.1 Wiegand / RS-485

Tabla 2-4 Wiegand / RS -485 conexión de cable

Parámetro	Color del cable	Nombre del cable	Descripción
CON4 (Wiegand / RS-485)	Azul	CASO	Conectado al cable de señal CASE de los dispositivos periféricos; utilizado para detectar sabotaje.
	Blanco	D1	Entrada / salida Wiegand D1 (conectada a lectores de tarjetas periféricos) (conectado a controladores de acceso). Entrada
	Verde	D0	Wiegand D0 (conectada a lectores de tarjetas periféricos) / salida (conectado a controladores de acceso).

Parámetro	Color del cable	Nombre del cable	Descripción
	marrón	LED	Conectado a cables de señal LED periféricos para confirmar la validez de la transmisión de datos Wiegand D0 y D1. Entrada / salida negativa RS-485
	Amarillo	RS – 485_B	(conectada a lectores de tarjetas periféricos) (conectado a controladores de acceso). Entrada /
	Púrpura	RS – 485_A	salida positiva RS-485 (conectada a lectores de tarjetas periféricos) (conectado a controladores de acceso).
	rojo	12V_OUT	Potencia de salida positiva.
	Negro	GND	GND del puerto de alimentación.

Tabla 2-5 Especificación y longitud del cable

Parámetro	Descripción de la conexión del cable	Longitud
Entrada / Salida RS-485	Cable CAT5e, conexión RS-485	100 metros
Entrada / salida Wiegand	Cable CAT5e, conexión Wiegand	50 m

2.4.2 Bloqueo / Contacto de puerta / Botón de salida

Tabla 2-6 Conexión del cable de bloqueo / contacto de puerta / botón de salida

Parámetro	Color del cable	Nombre del cable	Descripción
CON6	Negro y verde	DOOR_BUTTON Botón de	salida
	Negro y azul	GND	Señal de bloqueo GND
	Negro y gris	DOOR_SR	Entrada de contacto de puerta
	Negro y marrón	DOOR_COM	Controlador de acceso común de salida de control de bloqueo
	Negro y amarillo	DOOR_NO	Salida de control de bloqueo normalmente abierta Salida de
	Negro y morado	DOOR_NC	control de bloqueo normalmente cerrada

Los métodos de conexión de cables pueden variar según los tipos de candados. Consulte la Figura 2-6, la Figura 2-7, la Figura 2-8 y la Figura 2-9.

Figura 2-6 Conexión del cable de bloqueo del motor

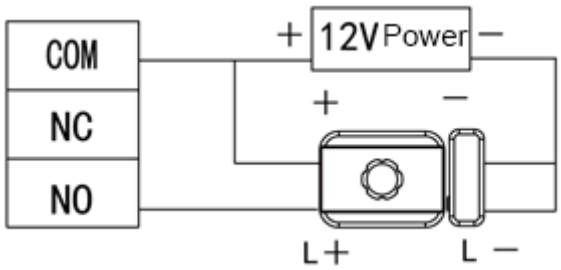


Figura 2-7 Conexión del cable de bloqueo magnético

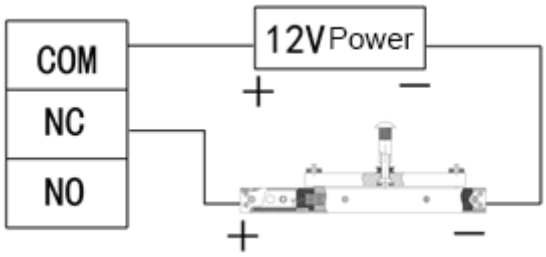


Figura 2-8 Conexión del cable de la cerradura eléctrica

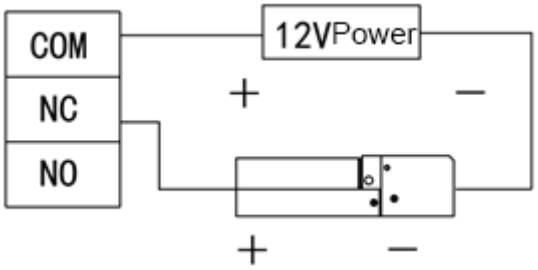
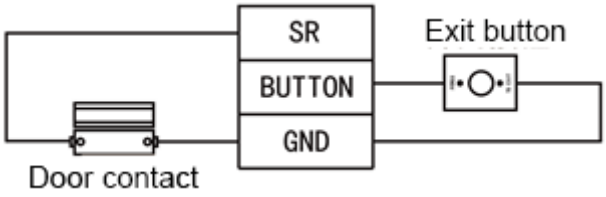


Figura 2-9 Conexión del cable de contacto de puerta y botón de salida



2.4.3 Entrada / Salida de alarma

Tabla 2-7 Conexión del cable de entrada / salida de alarma

Parámetro	Color del cable	Nombre del cable	Descripción
CON5 (Periférico entrada de alarma y salida)	blanco y rojo	ALM_NO	Un puerto de salida de alarma, que se utiliza para conectar el controlador de acceso a dispositivos de alarma de luz y sonido. Una vez que ocurren alarmas como el tiempo de espera del contacto de la puerta (entrada de alarma interna) y la intrusión (salida de alarma externa), el dispositivo de salida de alarma emitirá alarmas de luz y sonido durante 15 segundos.
	blanco y naranja	ALM_COM	
	blanco y marrón	ALM_IN	Un puerto de entrada de alarma, utilizado para conectar el controlador de acceso a dispositivos de entrada de alarma periféricos como detectores de infrarrojos y detectores de humo.
	blanco y verde	GND	Señal de entrada de alarma GND

- Hay dos métodos para conectar dispositivos de salida de alarma periféricos. Debe seleccionar según sea necesario.
- Cuando utiliza una cámara IP, puede seleccionar el método de conexión del cable del dispositivo de salida periférico en la Figura 2-10.

- Cuando usa sirena de luz y sonido, puede seleccionar el método de conexión del cable en la Figura 2-11.

Figura 2-10 Conexión del cable del dispositivo de salida de alarma periférica (1)

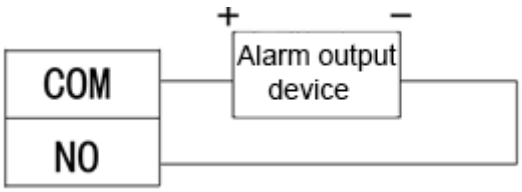
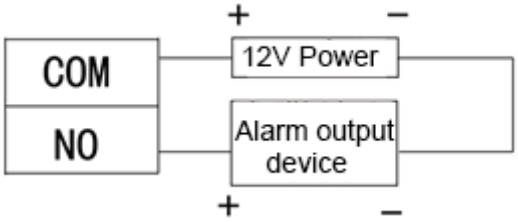
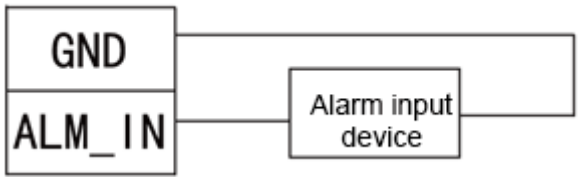


Figura 2-11 Conexión del cable del dispositivo de salida de alarma periférica (2)



- Para la conexión del cable del dispositivo de entrada de alarma periférica, consulte la Figura 2-12.

Figura 2-12 Conexión del cable del dispositivo de entrada de alarma periférica



2.4.4 Otros cables

Tabla 2-8 Otras descripciones de conexiones de cables

Parámetro	Descripción
Manibela de encendido	Cuando el controlador de acceso se separa de la pared a la fuerza, el controlador de acceso emitirá alarmas.
Puerto de alimentación	Conectado a una fuente de alimentación de 12 V CC.
Puerto Ethernet	Conectado al cable de red.

3 Operaciones

Después de que el controlador de acceso se enciende por primera vez, la primera tarjeta que se pasa es la tarjeta de administrador. Hay tres modos disponibles para el controlador de acceso: verificación en espera, administración de usuarios locales y administración de unidades flash USB. Puede agregar, eliminar y borrar usuarios; exportar e importar datos desde una unidad flash USB y actualizar el controlador de acceso con la unidad flash USB.

- El controlador de acceso puede funcionar como todo en uno o como lector de tarjetas. Esta sección solo presenta las operaciones del dispositivo como un todo en uno.
- Si se pierde la tarjeta de administrador, puede abrir la cubierta posterior del controlador de acceso y presionar el botón de reinicio en la placa base durante 5 segundos para reiniciar el dispositivo a la configuración de fábrica.

3.1 Verificación en espera

Encienda el controlador de acceso y luego deslice la tarjeta de administrador; la luz amarilla se ilumina, lo que significa que el dispositivo, como todo en uno, está en modo de verificación de espera.

Si la luz amarilla no se enciende, deslice continuamente la tarjeta de administrador 7 veces en 15 segundos para poner el dispositivo como todo en uno en modo de verificación en espera.

3.2 Gestión de usuarios

Puede agregar, eliminar y borrar usuarios en el controlador de acceso.

- Asegúrese de que el controlador de acceso como todo en uno esté en modo de verificación en espera y que no haya una unidad flash USB insertada.
- El intervalo de deslizamiento continuo de la tarjeta de administrador no puede ser superior a 5 segundos.
- Si no se realiza ninguna operación en 15 segundos, el sistema saldrá del modo de gestión de usuarios.

3.2.1 Agregar usuario

Puede agregar un usuario agregando una tarjeta o una huella digital.

Paso 1 Pase la tarjeta de administrador una vez.

La luz amarilla está encendida.

Paso 2 Vuelva a deslizar la tarjeta de administrador y, a continuación, podrá comenzar a agregar usuarios.

Espere 5 segundos, la luz cian está encendida y la luz del módulo de huellas digitales también parpadea.

Paso 3 Deslice la tarjeta o presione la huella digital que desea agregar.

Paso 4 Deslice la tarjeta de administrador una vez para guardar al usuario.

- Al agregar un usuario, deslice la tarjeta solo una vez. Se debe recopilar una huella digital tres veces y se pueden recopilar hasta tres huellas digitales.
- Solo puede agregar un usuario a la vez. Un usuario debe estar vinculado a al menos 1 tarjeta o 1 huella digital, o como máximo 1 tarjeta y 3 huellas digitales.

3.2.2 Eliminar usuarios

Puede eliminar un usuario eliminando la tarjeta o huella digital del usuario.

Paso 1 Pase la tarjeta de administrador una vez.

La luz amarilla está encendida.

Paso 2 Deslice la tarjeta de administrador 3 veces y luego podrá comenzar a eliminar usuarios.

Espere 5 segundos, la luz cian está encendida.

Paso 3 Pase la tarjeta o presione la huella digital que se agregó al controlador de acceso.

Puede eliminar hasta 10 usuarios a la vez.

Paso 4 Deslice la tarjeta de administrador una vez para eliminar al usuario.

3.2.3 Usuarios de compensación

Puede borrar usuarios deslizando la tarjeta de administrador.

Paso 1 Pase la tarjeta de administrador una vez.

La luz amarilla está encendida.

Paso 2 Pase la tarjeta de administrador 5 veces.

Espere 5 segundos, la luz cian está encendida.

Paso 3 Deslice la tarjeta de administrador una vez para borrar los usuarios.

3.2.4 Cambio de modo de trabajo

El controlador de acceso puede funcionar como todo en uno o como lector de tarjetas.

Paso 1 Pase la tarjeta de administrador una vez.

La luz amarilla está encendida.

Paso 2 Pase la tarjeta de administrador 7 veces.

Espere 5 segundos, la luz cian está encendida.

Paso 3 Pase la tarjeta de administrador una vez y el controlador de acceso cambiará a un lector de tarjetas.

Cuando el controlador de acceso funciona como un lector de tarjetas, deslice continuamente la tarjeta de administrador 7 veces en 15 segundos para cambiar el dispositivo a todo en uno en modo de verificación en espera.

3.3 Gestión de la unidad flash USB

Puede exportar datos de usuario o importarlos desde una unidad flash USB, exportar registros de deslizamiento de tarjetas y registros de alarma a la unidad flash o actualizar el controlador de acceso con la unidad flash.

- Asegúrese de que el controlador de acceso como todo en uno esté en modo de verificación de espera y que la unidad flash USB esté insertada.

- No extraiga la unidad flash USB ni realice otras operaciones durante la importación, exportación o actualización. De lo contrario, la importación, exportación o actualización podría fallar.
- El intervalo de deslizamiento continuo de la tarjeta de administrador no puede ser superior a 5 segundos.

3.3.1 Exportación de datos

Exporte los datos del controlador de acceso a la unidad flash USB.

Paso 1 Pase la tarjeta de administrador una vez.

La luz amarilla está encendida.

Paso 2 Deslice la tarjeta de administrador 2 veces.

Paso 3 Después de 5 segundos, deslice la tarjeta de administrador una vez y los datos se exportarán al Memoria USB.

Durante la exportación, la luz violeta está encendida.

3.3.2 Importación de datos

Después de exportar los datos del usuario desde un controlador de acceso mediante una unidad flash USB, puede importar dichos datos a otro controlador de acceso.

Paso 1 Inserte la unidad flash USB con datos de usuario en el controlador de acceso de destino. Desliza el tarjeta de administrador una vez.

La luz amarilla está encendida.

Paso 2 Deslice la tarjeta de administrador 4 veces.

Paso 3 Después de 5 segundos, deslice la tarjeta de administrador y los datos se importarán al destino. controlador de acceso.

Durante la importación, la luz violeta está encendida.

3.3.3 Actualización de Access Controller

Puede actualizar su controlador de acceso con una unidad flash USB.

Paso 1 Nombra el archivo de actualización en la PC como "update.bin" y guarda el archivo de actualización en la raíz. directorio de la unidad flash USB. Pase la tarjeta de

Paso 2 administrador una vez. La luz amarilla está encendida.

Paso 3 Pase la tarjeta de administrador 6 veces.

Paso 4 Después de 5 segundos, deslice la tarjeta de administrador una vez y comenzará la actualización. El controlador de acceso se reiniciará después de que finalice la actualización.

Durante la actualización, la luz violeta está encendida.

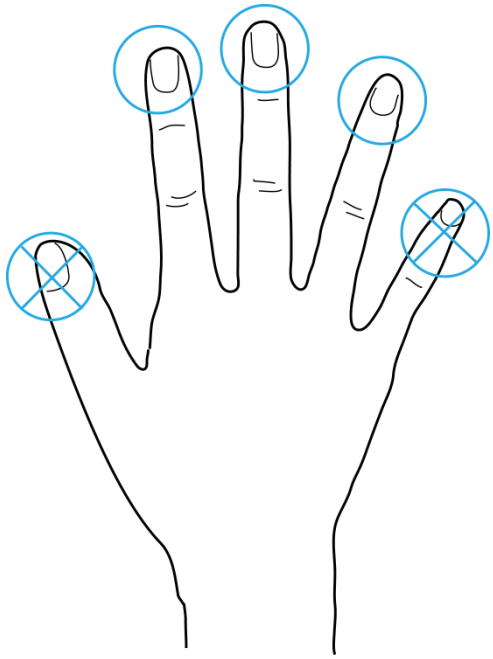
darse cuenta

- Asegúrese de que sus dedos estén limpios y secos antes de registrar sus huellas digitales.
- Presione con el dedo el área de grabación de huellas digitales y haga que su huella digital esté centrada en el área de grabación.
- No coloque el sensor de huellas dactilares en lugares con mucha luz, alta temperatura y mucha humedad.
- Para aquellos cuyas huellas digitales están gastadas o no están claras, pruebe con otros métodos de desbloqueo.

Dedos recomendados

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

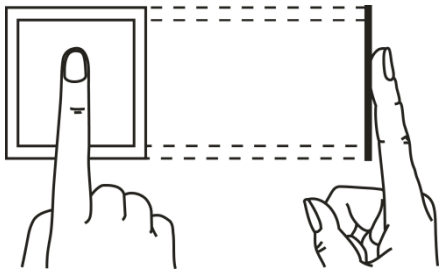
Apéndice figura 1-1 Dedos recomendados



Método de presión con los dedos

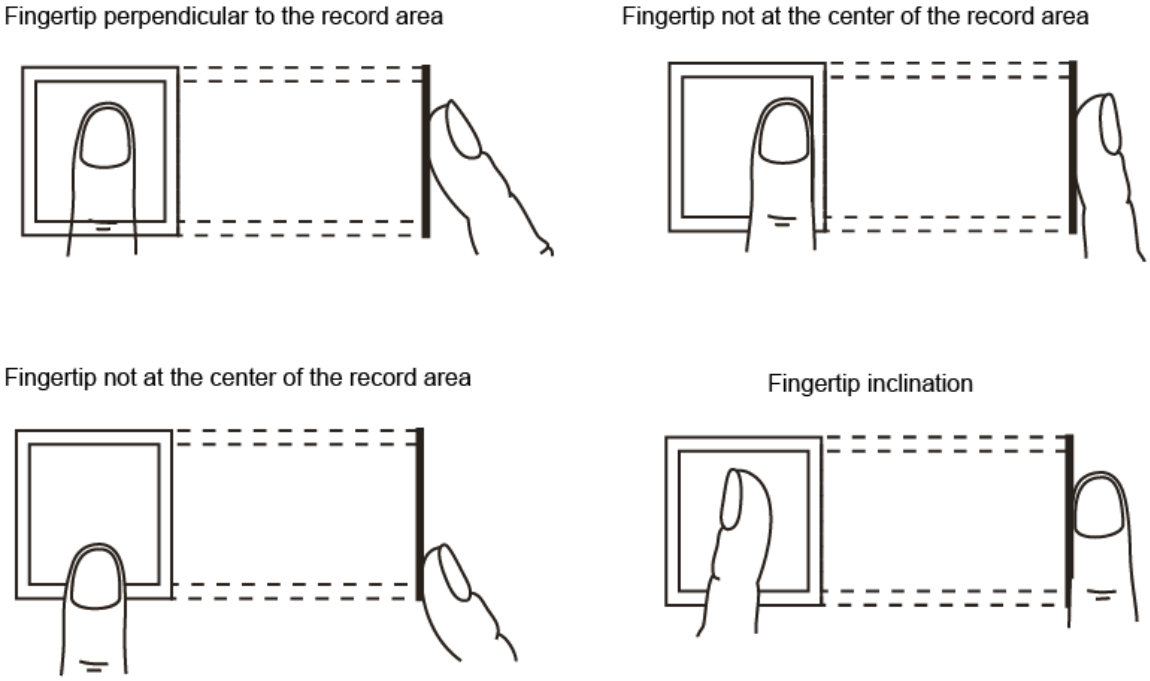
- Método correcto

Apéndice figura 1-2 Presión correcta con los dedos



- Método incorrecto

Apéndice figura 1-3 Presión incorrecta con los dedos



Apéndice 2 Lista de empaque

Después de desempacar el paquete, verifique si los elementos están completos con la lista de empaque y guarde esta guía correctamente para referencia futura.

Apéndice tabla 2-1 Lista de empaque

Nombre	Cantidad
Controlador de acceso	1
Guía de inicio rápido	1
Bolsa de tornillo	1
Cable de conexión USB	1

Apéndice 3 Recomendaciones de ciberseguridad

La ciberseguridad es más que una simple 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 "comprobación 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 ajenas puedan adivinar qué puertos está utilizando.

6. **Habilitar HTTPS**

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

7. **Habilitar lista blanca**

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

8. **Enlace de dirección MAC**

   Le recomendamos que vincule la dirección IP y MAC del gateway 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 servicios innecesarios y elija modos seguros**

    Si no es necesario, se recomienda apagar 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 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 cifrada provocará alguna 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, se sugiere usar 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.