Lector de tarjetas de control de acceso

Manual de usuario

V1.0.1

Prefacio

General

Este manual presenta las funciones y operaciones del Lector de tarjetas de control de acceso (en lo sucesivo, "el Dispositivo").

Las instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Significado
 **PELIGRO**	Indica un peligro de alto potencial que, si no se evita, provocará la muerte o lesiones graves.
 **ADVERTENCIA**	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 **PRECAUCIÓN**	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, reducción del rendimiento o resultados impredecibles.
 CONSEJOS	Proporciona métodos para ayudarlo a resolver un problema o ahorrar tiempo.
 **NOTA**	Proporciona información adicional como suplemento al texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.1	Modelos de dispositivos actualizados y lector de tarjetas bluetooth agregado.	diciembre 2021
V1.0.0	Primer lanzamiento.	octubre 2020

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otros, 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 proporcione la información de contacto requerida.

Sobre el Manual

- El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas sufridas 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 reglamentos de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, use nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede haber 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 con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, póngase en contacto con el proveedor o con el servicio de atención al cliente si se produce algún problema durante el uso del Dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

Medidas de seguridad y advertencias importantes

Los siguientes contenidos tratan sobre las formas correctas de usar el Dispositivo, previniendo peligros y daños a la propiedad cuando está en uso. Lea atentamente el manual antes de utilizar el Dispositivo, siga estrictamente el manual y guárdelo adecuadamente para futuras consultas.

Requisito de transporte

Transporte el Dispositivo en condiciones de humedad y temperatura permitidas.

requisito de almacenamiento

Guarde el dispositivo en condiciones de humedad y temperatura permitidas.

Requerimientos de instalación

- Se recomienda una fuente de alimentación de CC lineal sin modo de conmutación para una mejor distancia de lectura. La
- distancia de la fuente de alimentación no debe exceder los 100 m; de lo contrario, se recomienda utilizar una fuente de alimentación dedicada.
- El voltaje de entrada debe estar dentro de los 12 V ± 10 % para asegurarse de que el dispositivo funcione
- correctamente. Conecte el dispositivo y el controlador de acceso con el cable blindado RVVP0.5 o superior.
- Cuando el Dispositivo se instale al aire libre o en lugares con alta humedad o infiltración de agua, le recomendamos que proteja el Dispositivo con una cubierta impermeable.
- Para reducir el ruido causado por la transmisión a larga distancia, la capa de blindaje del cable de transmisión debe conectarse junto con el cable de tierra del dispositivo y el cable de tierra del controlador de acceso.

Requisito de operación

Utilice el dispositivo en condiciones de humedad y temperatura permitidas.

Tabla de contenido

1. Introducción

El dispositivo puede leer huellas dactilares y varios tipos de tarjetas. Envía señales al controlador de acceso para la verificación de identidad. Es aplicable a zonas industriales, edificios de oficinas, escuelas, fábricas, estadios, CBD, áreas residenciales, propiedades gubernamentales y más.

1.1 Características

- Material PC y panel acrílico con un diseño delgado e impermeable.
- Soporta lectura de tarjetas sin contacto.
- Admite lectura de tarjeta IC (Mifare), lectura de tarjeta de identificación (solo para el dispositivo con función de lectura de tarjeta de identificación), lectura de tarjeta de identidad (solo para dispositivo con función de lectura de tarjeta IC y CPU); Lectura de código QR (solo para el Dispositivo con función de lectura de código QR); Lector de tarjetas Bluetooth (solo para el Dispositivo con función Bluetooth).
- Presenta la ranura para tarjetas PSAM y la tarjeta PSAM integradas, y admite la identificación de tarjetas de CPU con seguridad mejorada basada en el algoritmo criptográfico SM1 (aplicable al dispositivo con función de lectura de tarjetas de CPU).
- Admite comunicación a través de RS–485 y Wiegand (el lector de tarjetas de huellas dactilares y el lector de códigos QR solo admiten RS–485).
- Soporta actualización en línea.
- Admite alarma de manipulación.
- Zumbador incorporado y luz indicadora. Vigilancia integrada
- para garantizar la estabilidad del dispositivo.
- Seguro y estable con protección contra sobrecorriente y sobretensión.

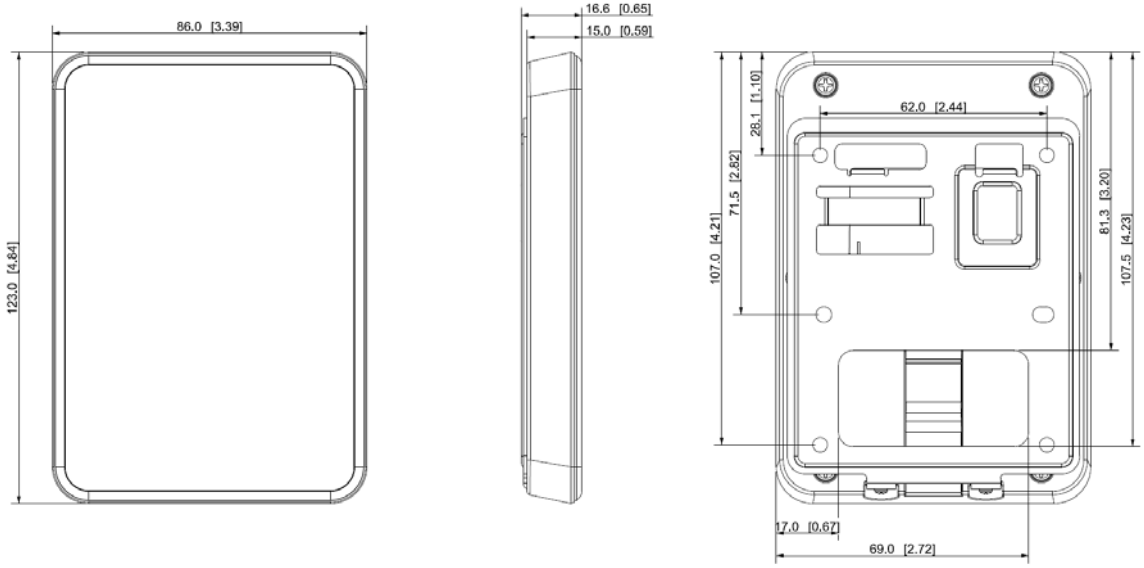
Las funciones pueden variar según los diferentes modelos.

1.2 Apariencia del dispositivo

El dispositivo se puede dividir en modelo de caja 86, modelo delgado y modo de huella digital según su apariencia.

1.2.1 Modelo de caja 86

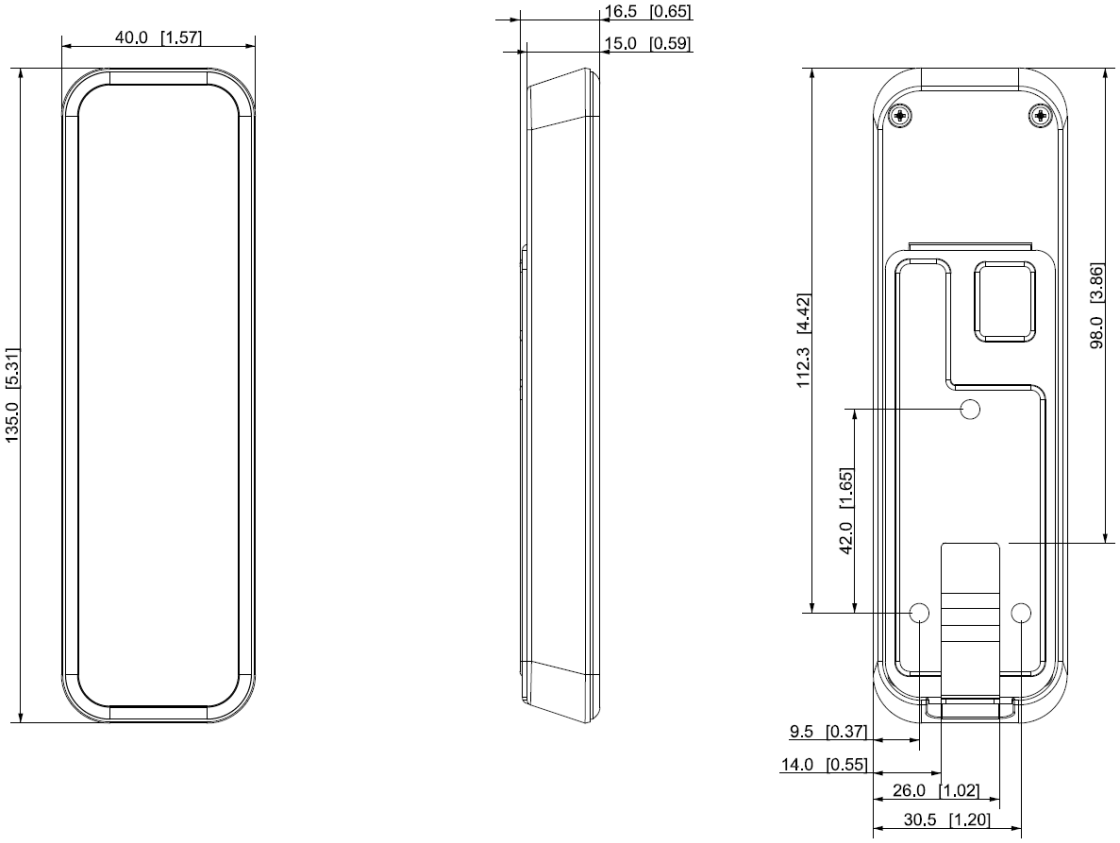
Figure 1-1 Dimensiones del modelo de caja 86 (mm [pulgadas])



El modelo de caja 86 se puede dividir en lector de tarjetas Bluetooth, lector de tarjetas de código QR y general lector de tarjetas según sus funciones.

1.2.2 Modelo delgado

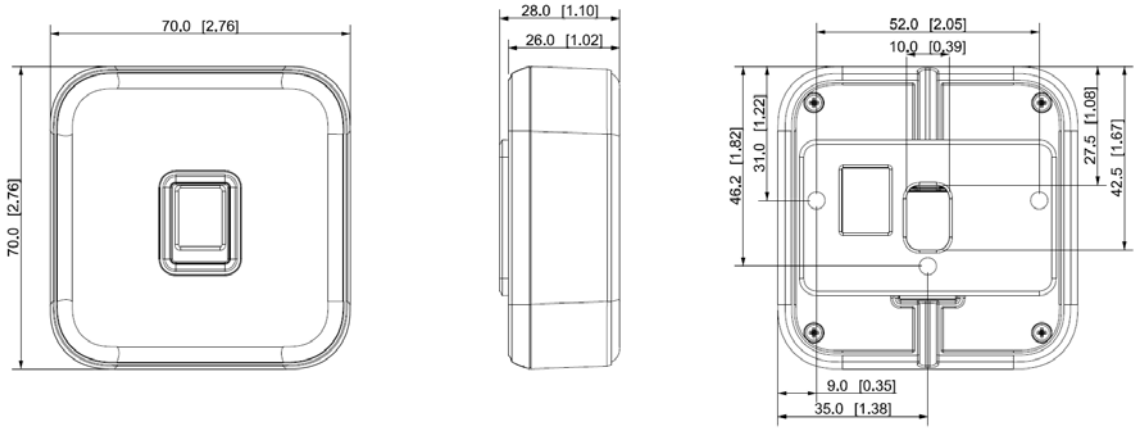
Figure 1-2 Dimensiones del modelo delgado (mm [pulgadas])



El modelo delgado se puede dividir en lector de tarjetas Bluetooth y lector de tarjetas general de acuerdo con sus funciones

1.2.3 Modelo de huellas dactilares

Figure 1-3 Dimensiones del modelo de huella digital (mm [pulgadas])



Conexión de 2 cables

Utilice RS–485 o Wiegand para conectar el dispositivo. El modelo de huella digital y el modelo de código QR solo son compatibles RS–485.

Cables de 8 núcleos para los modelos 86 Box y Slim

Tabla 2-1 Descripción de la conexión de cables (1)

Color	Puerto	Descripción
Rojo	RD+	ALIMENTACIÓN (12 VCC)
Negro	RD–	TIERRA
Azul	CASO	Señal de alarma de sabotaje
Blanco	D1	Señal de transmisión Wiegand (efectivo solo cuando se usa el protocolo Wiegand)
Verde	D0	Señal de transmisión Wiegand (efectivo solo cuando se usa el protocolo Wiegand)
Marrón	DIRIGIÓ	Señal de respuesta Wiegand (efectivo solo cuando se usa el protocolo Wiegand)
Amarillo	RS–485_B	RS–485_B
Púrpura	RS–485_A	RS–485_A

Cables de 5 núcleos para el modelo de huellas dactilares

Tabla 2-2 Descripción de la conexión de cables (2)

Color	Puerto	Descripción
Rojo	RD+	ALIMENTACIÓN (12 VCC)
Negro	RD–	TIERRA
Azul	CASO	Señal de alarma de sabotaje
Amarillo	RS–485_B	RS–485_B
Púrpura	RS–485_A	RS–485_A

Tabla 2-3 Especificación y longitud del cable

Tipo de dispositivo	Método de conexión	Largo
Lector de tarjetas RS485	Cada cable debe estar dentro de los 10 Ω.	100 m (328,08 pies)
Lector de tarjetas Wiegand	Cada cable debe estar dentro de los 2 Ω.	80 m (262,47 pies)

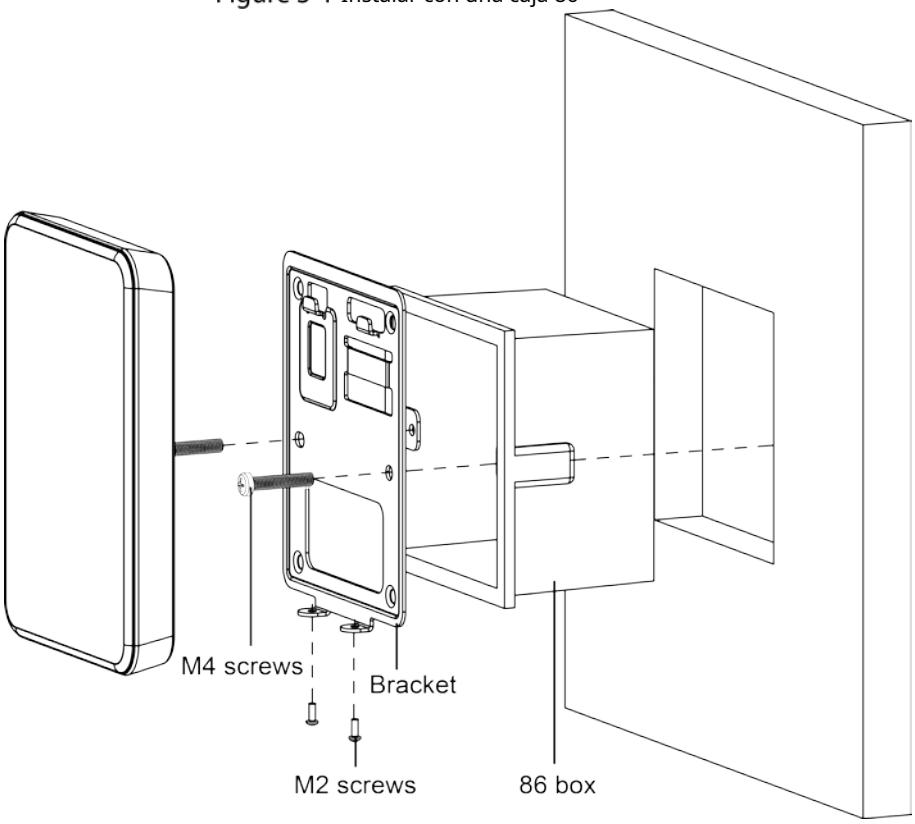
3 Instalación

La altura de instalación recomendada (desde el centro del dispositivo hasta el suelo) es de 130 cm a 150 cm (51,18" a 59,06") y no debe superar los 200 cm (78,74").

3.1 Instalación del modelo de caja 86

Con una caja de 86

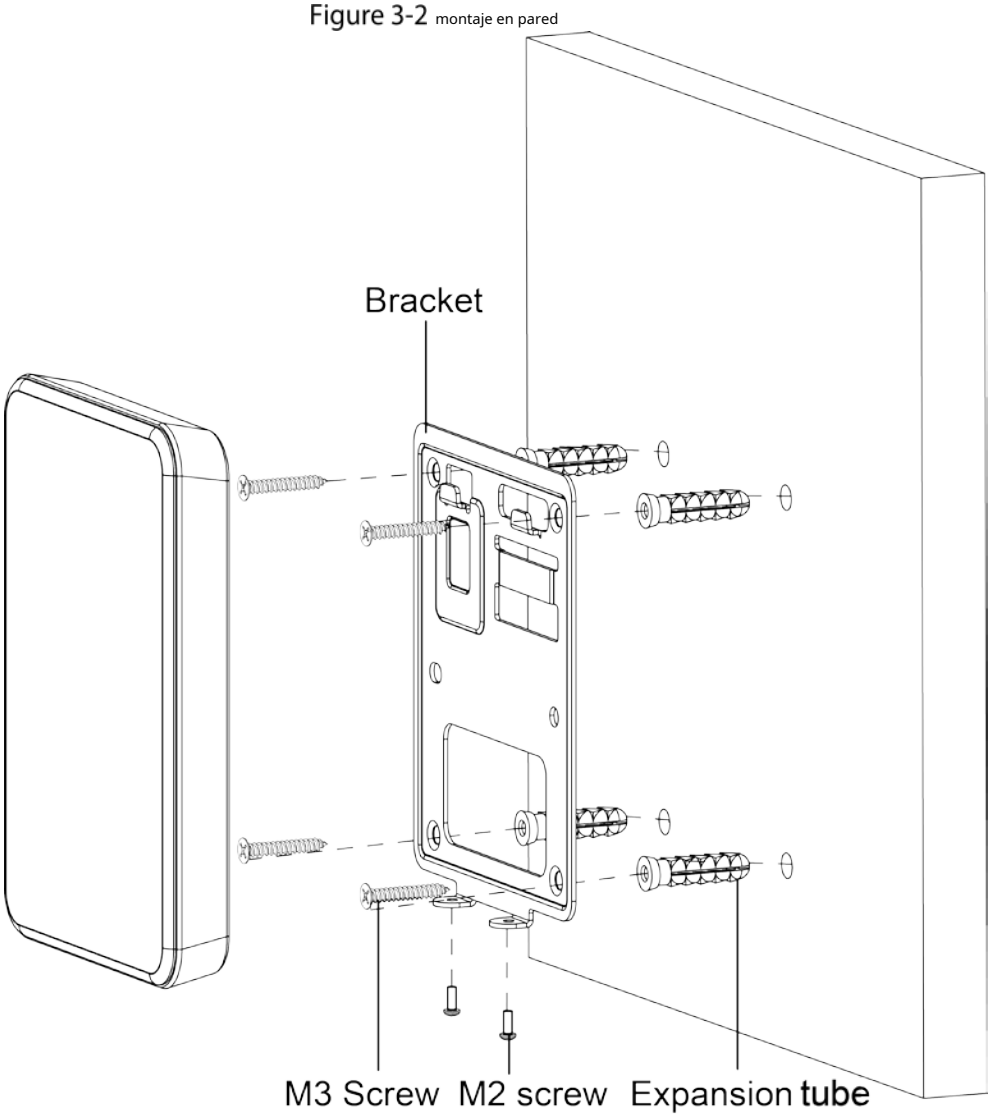
Figure 3-1 Instalar con una caja 86



Step 1 Coloque la caja 86 en la pared.
Step 2 Conecte los cables del Dispositivo y colóquelos dentro de la caja 86. Utilice
Step 3 dos tornillos M4 para fijar el soporte a la caja 86.
Step 4 Fije el dispositivo al soporte de arriba hacia abajo. Use dos
Step 5 tornillos M2 para asegurar el dispositivo en el soporte.

Montaje en pared

Figure 3-2 montaje en pared



Step 1 Haz agujeros en la pared.
Step 2 Coloque cuatro pernos de expansión en los agujeros.
Step 3 Conecte los cables del Dispositivo y póngalos dentro de la pared. Use
Step 4 dos tornillos M3 para fijar el soporte en la pared.
Step 5 Fije el dispositivo al soporte de arriba hacia abajo. Use dos
Step 6 tornillos M2 para asegurar el dispositivo en el soporte.

3.2 Instalación del modelo delgado

Figure 3-3 Cableado de superficie

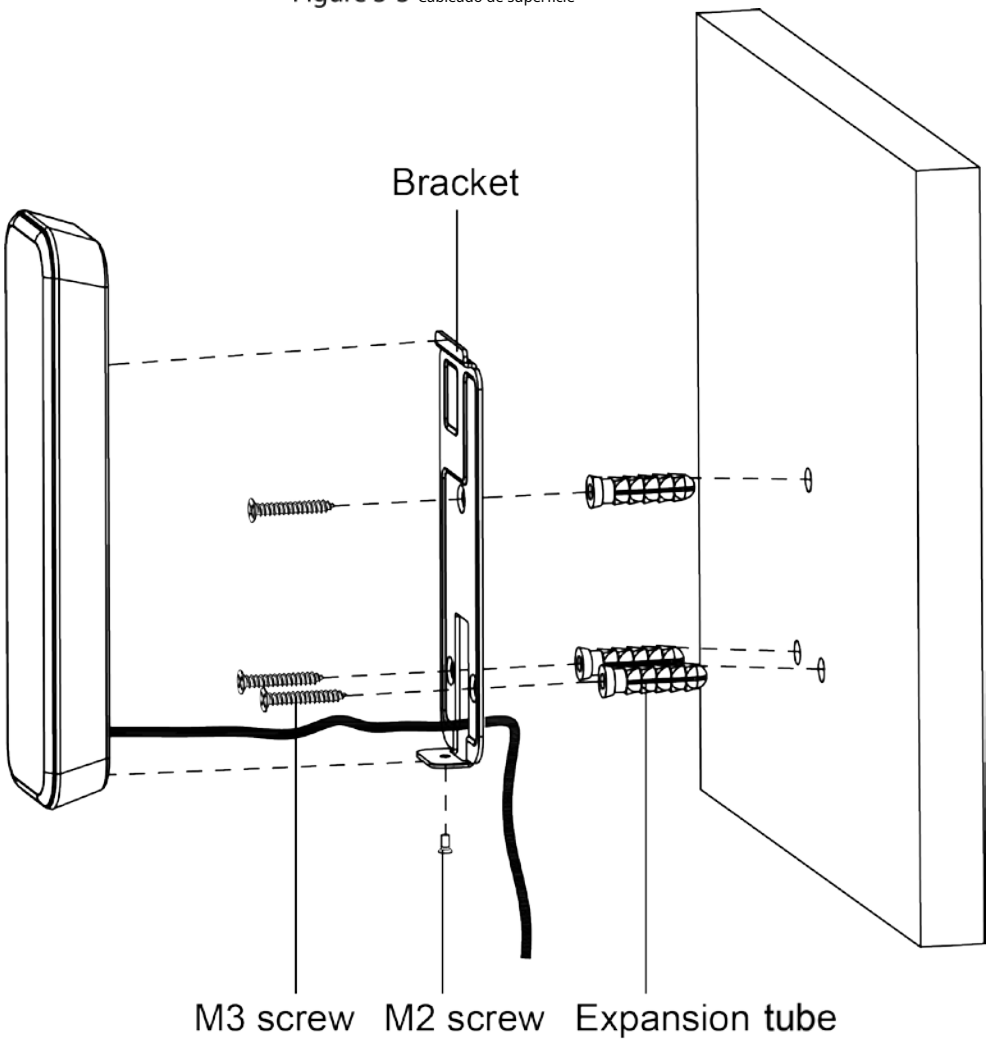
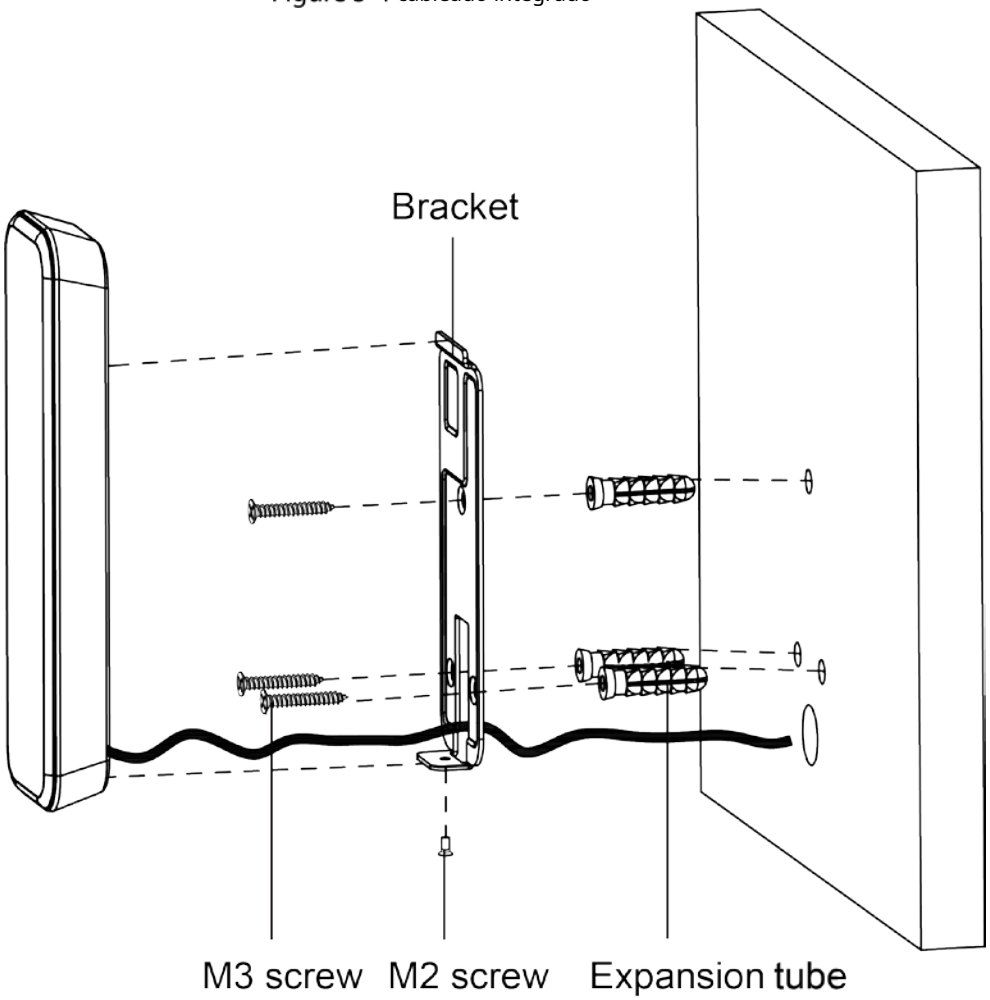


Figure 3-4 cableado integrado



Step 1 Haz agujeros en la pared.
Step 2 Coloque tres pernos de expansión en los agujeros.
Step 3 Conecte los cables del Dispositivo y páselos por la ranura del soporte. (Opcional)
Step 4 Coloque los cables dentro de la pared.
Step 5 Use tres tornillos M3 para fijar el soporte en la pared. Fije el
Step 6 dispositivo al soporte de arriba hacia abajo. Use un tornillo
Step 7 M2 para asegurar el dispositivo en el soporte.

3.3 Instalación del modelo de huellas dactilares

Figure 3-5 Cableado de superficie

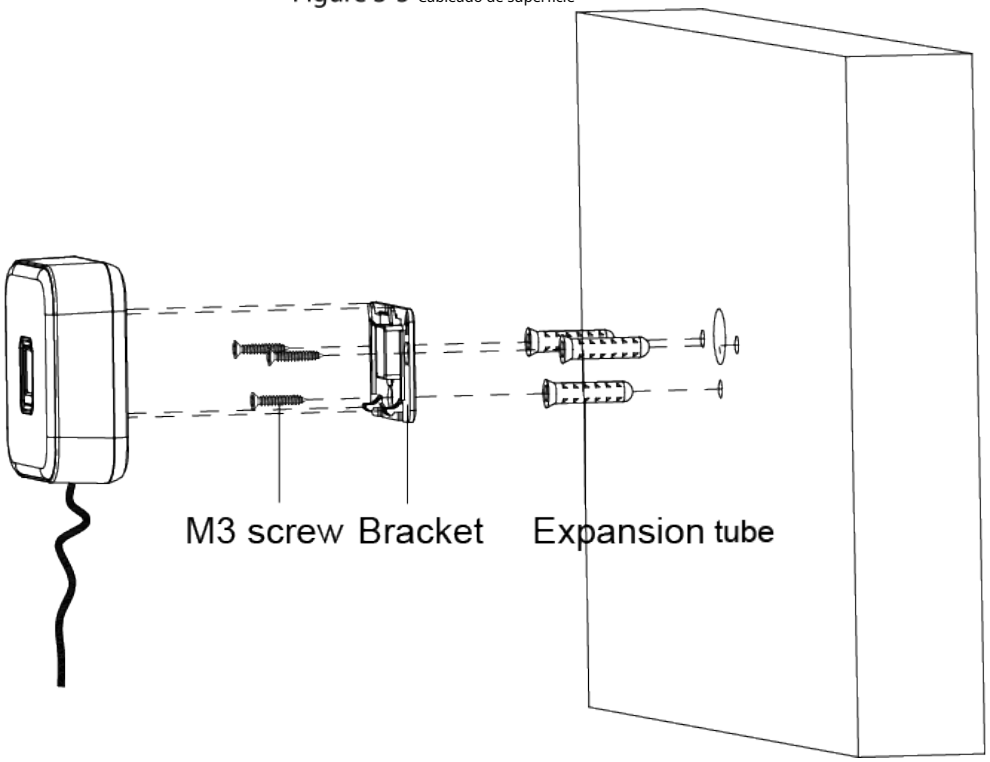
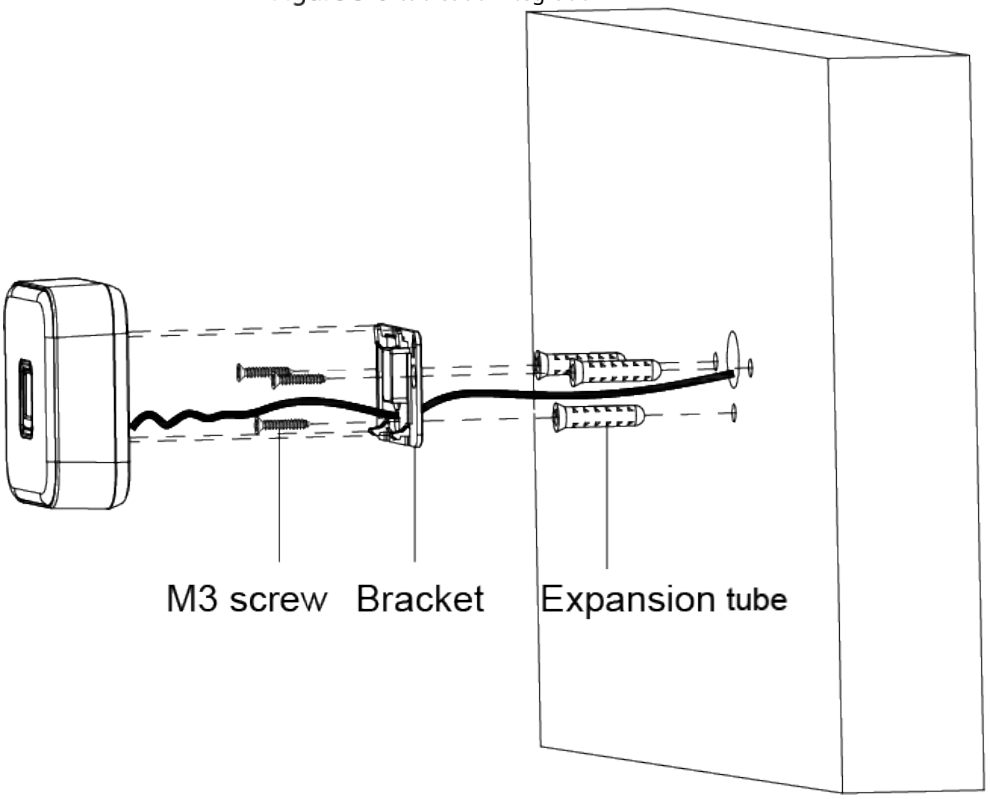


Figure 3-6 cableado integrado



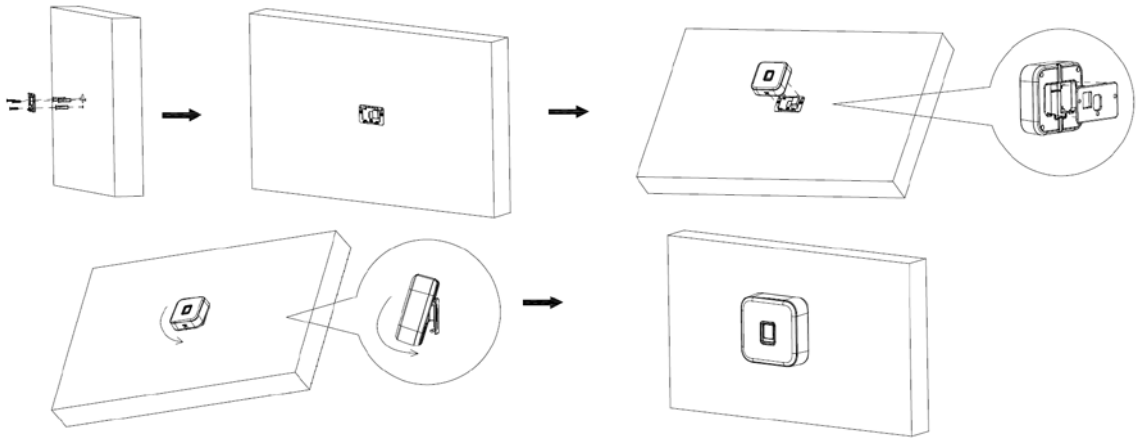
Procedimiento

Step 1 En la pared, perfore tres orificios para los pernos de expansión y un orificio para los cables.
Step 2 Coloque tres pernos de expansión en los agujeros.
Step 3 Use tres tornillos M3 para fijar el soporte en la pared.
Step 4 Conecte los cables del Dispositivo.
Step 5 (Opcional) Coloque los cables dentro de la pared.

Step 6 Fije el dispositivo en el soporte de arriba hacia abajo.

Step 7 Presione el dispositivo con fuerza hacia la dirección de la flecha hasta que escuche un "clic" y la instalación finalice.

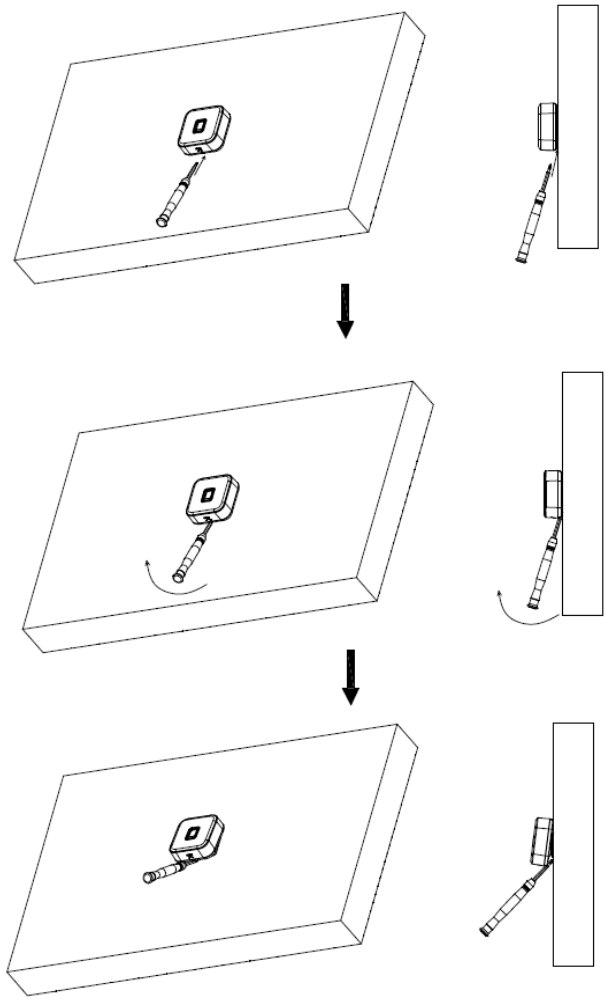
Figure 3-7 Presione el dispositivo con fuerza hasta que escuche un "clic"



Operación relacionada

Para desabrochar el dispositivo de la pared, inserte el destornillador provisto en la ranura en la parte inferior, haga palanca para abrir el dispositivo de acuerdo con la dirección de la flecha a continuación hasta que escuche un "clic".

Figure 3-8 Desabroche el dispositivo



4 Configuración del lector de tarjetas Bluetooth

El lector de tarjetas Bluetooth se utiliza junto con la aplicación Easy4Key para abrir la puerta de forma remota.

requisitos previos

- La última versión de SmartPSS AC está instalada en la computadora.
- Los permisos para pasar la tarjeta se han asignado correctamente a los usuarios. Para obtener más información, consulte el manual de usuario de SmartPSS AC.
- La aplicación Easy4Key está instalada en el teléfono.

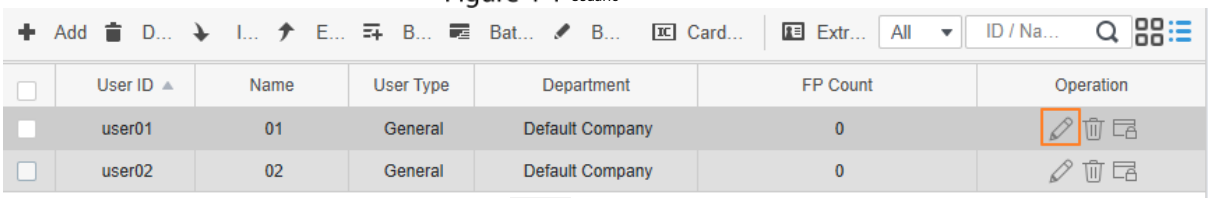
Procedimiento

Step 1 Inicie sesión en SmartPSS AC.

Step 2 Seleccione "Solución de acceso > Administrador de personal".

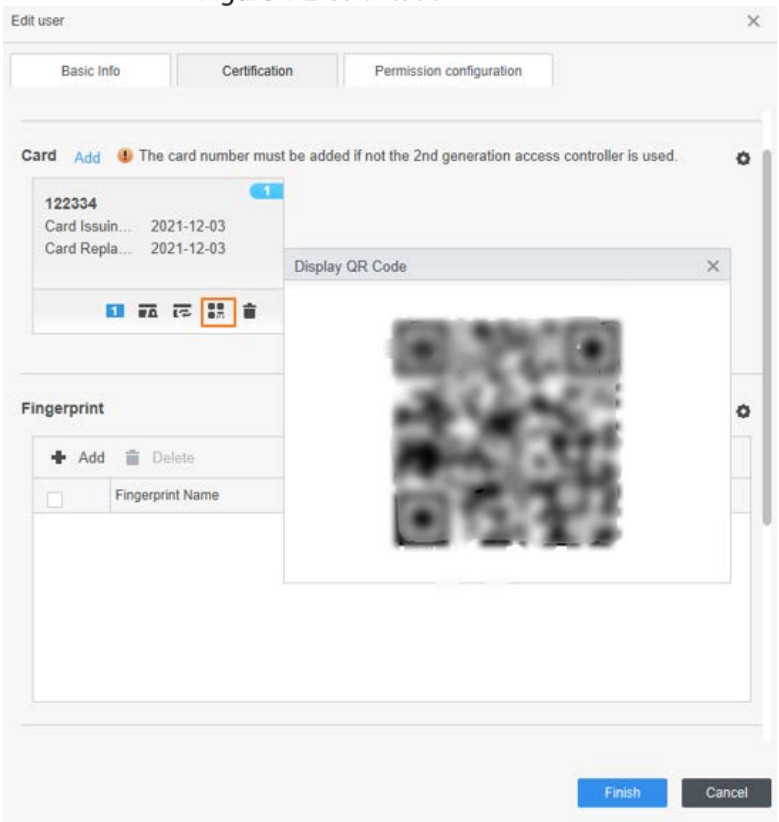
Step 3 Seleccione el usuario agregado y haga clic en .

Figure 4-1 Usuario



Step 4 Haga clic en "Certificación", y luego haga clic en

Figure 4-2 Certificación



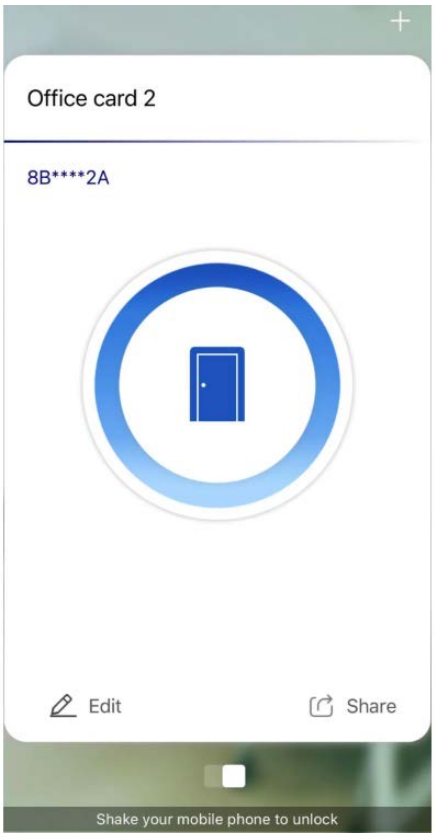
Step 5 Abra Easy4Key en el teléfono y haga clic en

Step 6 Escanee el código QR en el SmartPSS AC para agregar la tarjeta.

Después de agregar la tarjeta con éxito, el usuario puede abrir la puerta a través de Easy4Key en el teléfono.

La distancia entre el teléfono y el lector de tarjetas debe ser inferior a 10 m.

Figure 4-3 Easy4Key



5 Aviso de luz y sonido

Después de encender el dispositivo, emitirá un zumbido una vez y el indicador se iluminará en azul fijo, lo que significa que el dispositivo funciona correctamente.

El dispositivo solo puede leer una tarjeta a la vez. Cuando varias tarjetas se apilan juntas, no puede funcionar adecuadamente.

5.1 Modelos 86 Box y Slim

El indicador de sonido y luz de la caja 86 y los modelos delgados son los mismos.

Figure 5-1 Descripción del mensaje de luz y sonido

Situación	Aviso de luz y sonido
Encendido.	Buzz una vez. El indicador es azul fijo.
Extracción del dispositivo.	Zumbido largo durante 15 segundos.
Pulsando botones.	Zumbido corto una vez.
Alarma activada por el controlador.	Zumbido largo durante 15 segundos.
Comunicación RS–485 y deslizamiento de una tarjeta autorizada.	Buzz una vez. El indicador parpadea en verde una vez y luego se vuelve azul fijo como modo de espera.
Comunicación RS–485 y deslizamiento de una tarjeta no autorizada.	Buzz cuatro veces. El indicador parpadea en rojo una vez y luego se vuelve azul fijo como modo de espera.
Comunicación 485 anormal y deslizamiento de una tarjeta autorizada/no autorizada.	Zumbido tres veces. El indicador parpadea en rojo una vez y luego se vuelve azul fijo como modo de espera.
Comunicación Wiegand y deslizamiento de una tarjeta autorizada.	Buzz una vez. El indicador parpadea en verde una vez y luego se vuelve azul fijo como modo de espera.
Comunicación Wiegand y deslizamiento de una tarjeta no autorizada.	Zumbido tres veces. El indicador parpadea en rojo una vez y luego se vuelve azul fijo como modo de espera.
Actualización de software o esperando actualización en BOOT.	El indicador parpadea en azul hasta que se completa la actualización.

5.2 Modelo de huellas dactilares

Figure 5-2 Descripción del mensaje de luz y sonido

Situación	Aviso de luz y sonido
El dispositivo está encendido	Buzz una vez. El indicador es azul fijo.

Situación	Aviso de luz y sonido
Extracción del dispositivo.	Zumbido largo durante 15 segundos.
Enlace de alarma activado por el controlador.	Zumbido largo durante 15 segundos.
485 comunicación y deslizar una tarjeta autorizada.	Buzz una vez. El indicador parpadea en verde una vez y luego se vuelve azul fijo como modo de espera.
485 comunicación y pasar una tarjeta no autorizada	Buzz cuatro veces. El indicador parpadea en rojo una vez y luego se vuelve azul fijo como modo de espera.
Comunicación 485 anormal y deslizamiento de una tarjeta/huella digital autorizada o no autorizada.	Zumbido tres veces. El indicador parpadea en rojo una vez y luego se vuelve azul fijo como modo de espera.
485 comunicación y se reconoce una huella dactilar	Buzz una vez.
485 comunicación y pasar una huella digital autorizada	Buzz dos veces con un intervalo de 1 segundo. El indicador parpadea en verde una vez y luego se vuelve azul fijo como modo de espera.
485 comunicación y pasar una huella digital no autorizada	Buzz una vez, y luego cuatro veces. El indicador parpadea en rojo una vez y luego se vuelve azul fijo como modo de espera.
Operaciones de huellas dactilares, incluidas la adición, eliminación y sincronización	El indicador parpadea en verde.
Salir de las operaciones de huellas dactilares, incluidas la adición, eliminación y sincronización	El indicador es azul fijo.
Actualización de software o esperando actualización en BOOT	El indicador parpadea en azul hasta que se completa la actualización.

6 Actualización del dispositivo

6.1 SmartPSS CA

Use SmartPSS AC para actualizar el dispositivo a través del controlador de acceso.

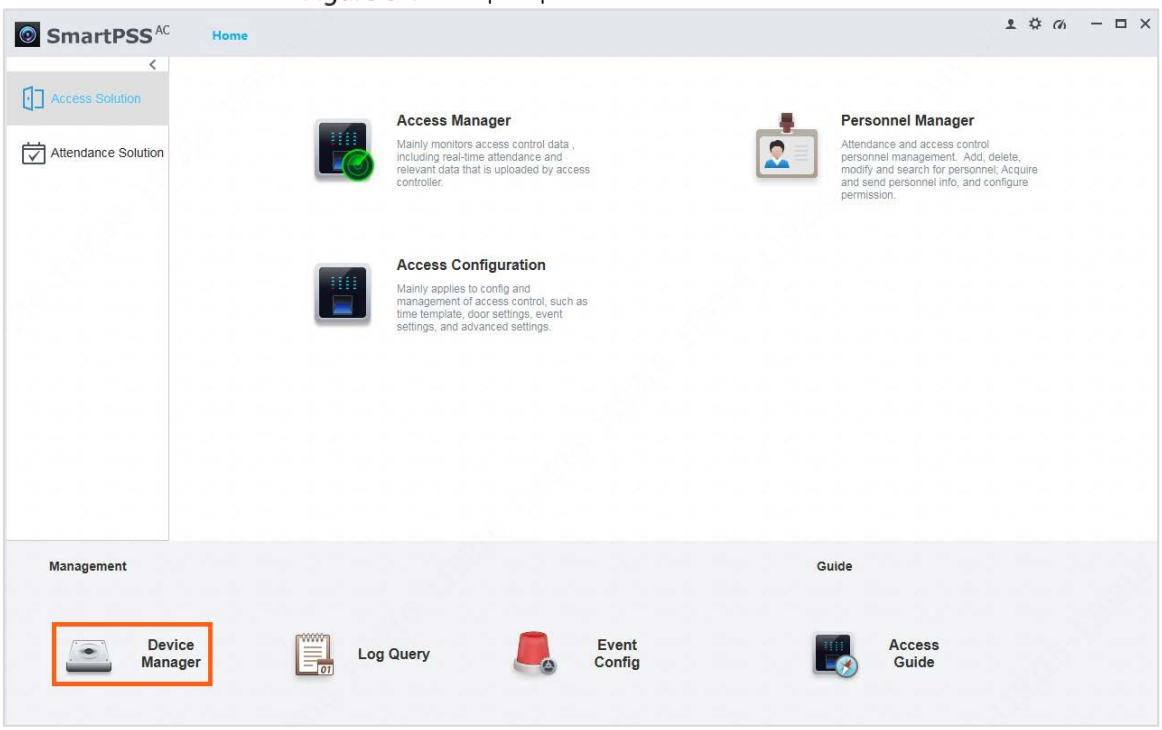
requisitos previos

- El dispositivo y el controlador de acceso están conectados y encendidos.
- SmartPSS AC está instalado en su PC.

Procedimiento

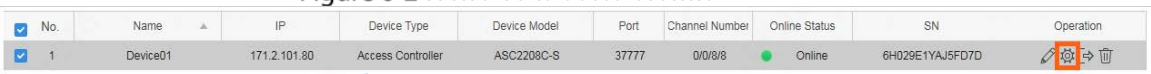
Step 1 Inicie sesión en SmartPSS AC y luego seleccione**Administrador de dispositivos**.

Figure 6-1 Menú principal de SmartPSS AC



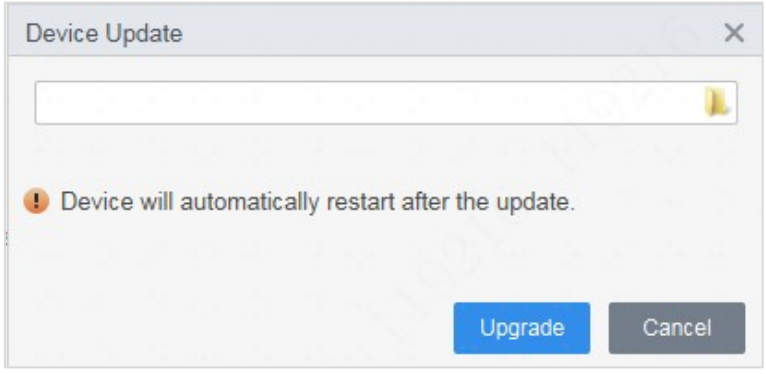
Step 2 Hacer clic .

Figure 6-2 Seleccione el controlador de acceso



Step 3 Hacer clic y para seleccionar el archivo de actualización.

Figura 4-3 Actualización del dispositivo



Step 4 Hacer clic**Mejora.**

El indicador del dispositivo parpadea en azul hasta que se completa la actualización y luego el dispositivo se reinicia automáticamente.

6.2 Herramienta de configuración

Utilice la herramienta de configuración para actualizar el dispositivo a través del controlador de acceso.

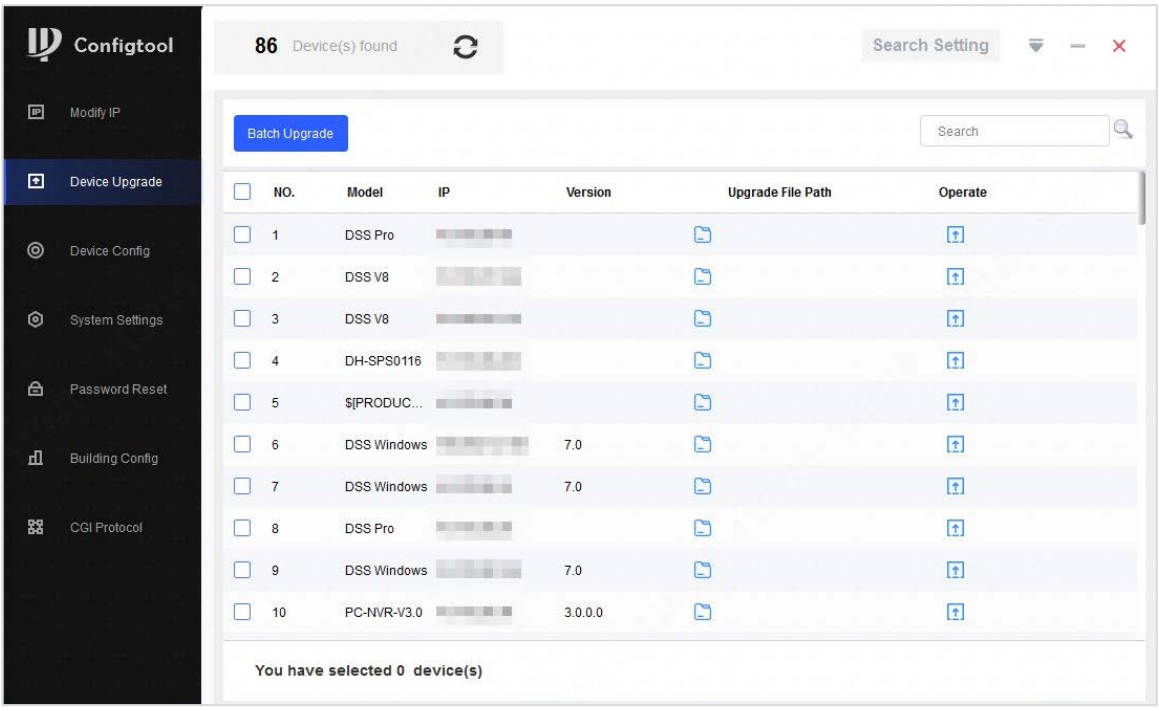
requisitos previos

- El dispositivo y el controlador de acceso están conectados y encendidos. El
- Configtool está instalado en su computadora.

Procedimiento

Step 1 Abra la herramienta de configuración y luego seleccione**Actualización de dispositivo**.

Figura 4-4 Menú principal de Configtool

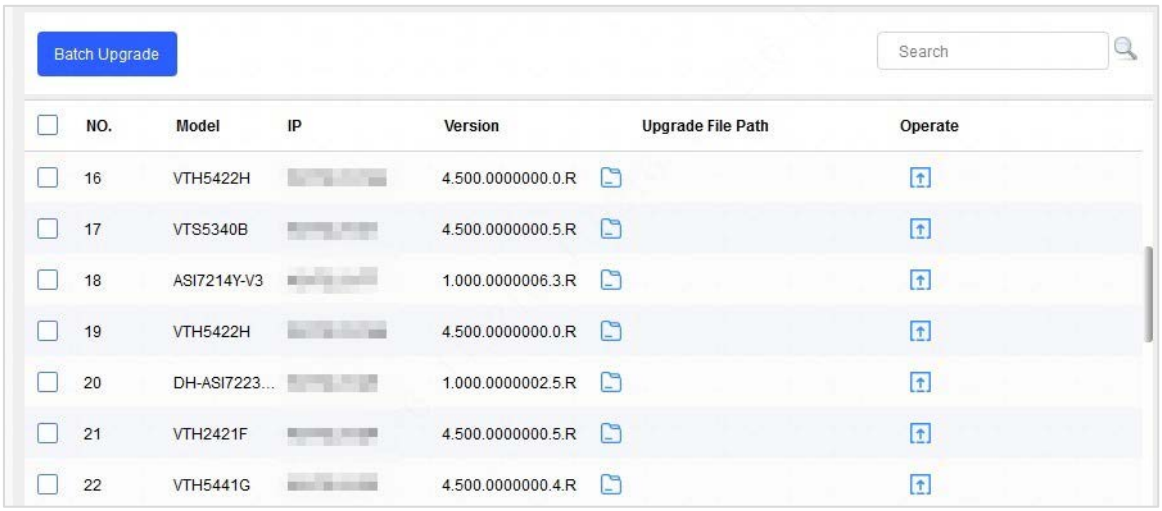


Step 2 Hacer clic y seleccione el archivo de actualización para cada controlador de acceso, y luego haga clic en .

Step 3 Hacer clic**Actualización por lotes.**

El indicador del dispositivo parpadea en azul hasta que se completa la actualización y luego el dispositivo se reinicia automáticamente.

Figura 4-5 Actualización por lotes



Appendix 1 Instrucción de recolección de huellas dactilares

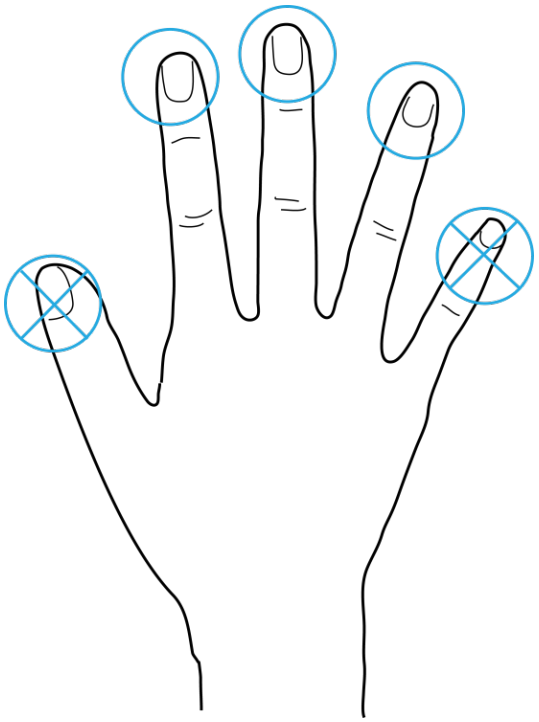
Precauciones

- Asegúrese de que sus dedos estén limpios y secos antes de tomar sus huellas dactilares. No
- exponga el escáner de huellas dactilares a altas temperaturas y humedad.
- Si sus huellas dactilares están desgastadas o no están claras, use otros métodos, incluida la contraseña y la tarjeta.

Dedos recomendados

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

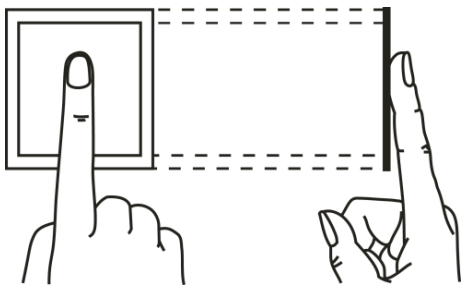
Apéndice Figura 1-1 Dedos recomendados



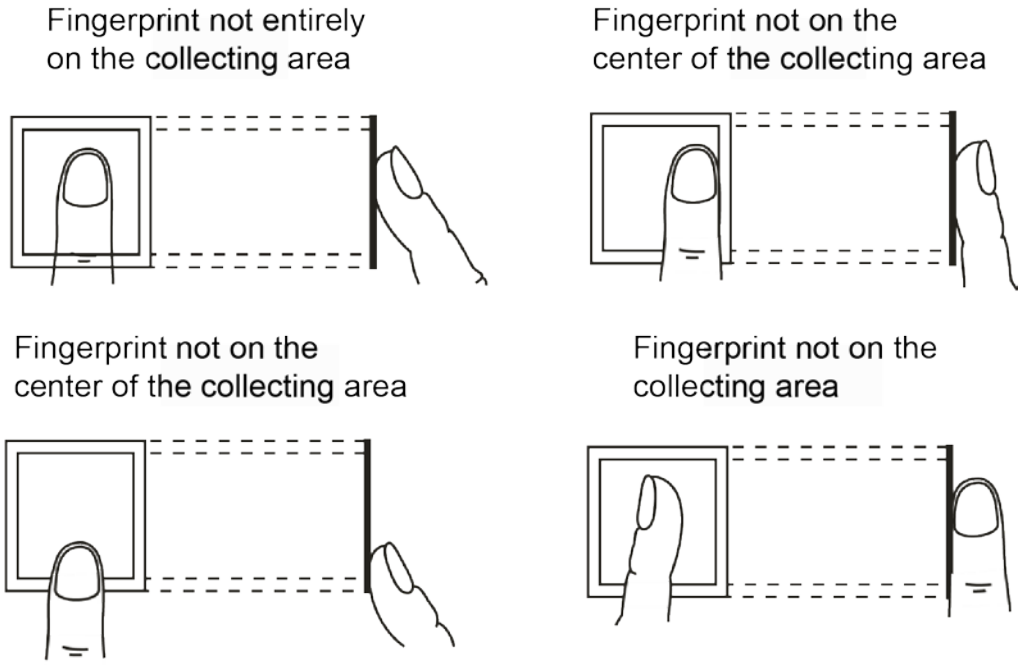
Manera correcta de presionar el dedo

Presione su dedo en el área de recolección de huellas digitales y alinee el centro de su huella digital con el centro del área de recolección.

Apéndice Figura 1-2 Forma correcta



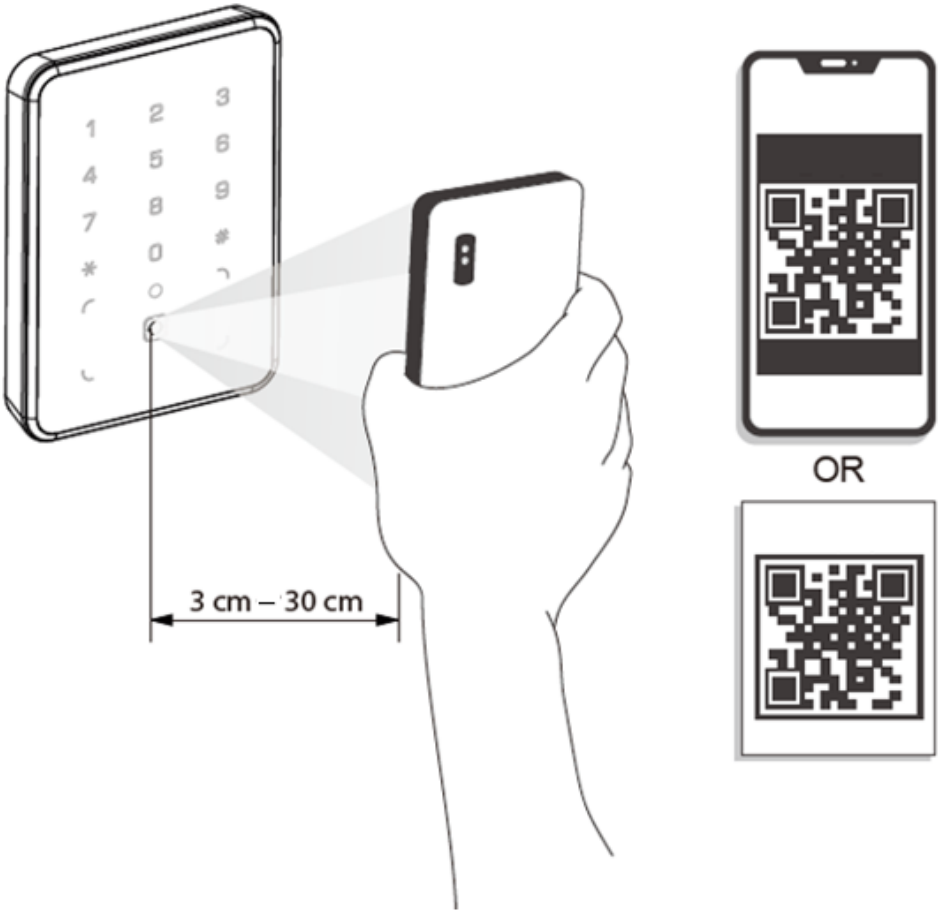
Apéndice Figura 1-3 Formas incorrectas



Appendix 2 Requisitos para escanear códigos QR

- Para garantizar un mejor rendimiento de escaneo de códigos QR, se requieren buenas condiciones de iluminación y se requiere que el iluminador brinde luz durante la noche o en días nublados.
- La distancia entre el código QR y la lente de escaneo del lector es de 3 cm a 30 cm. El
- tamaño del código QR no debe ser inferior a 30 mm × 30 mm.
- La capacidad de bytes del código QR debe ser inferior a 100 bytes, y el papel de código bidimensional tiene que ser plano.
- La película de privacidad adherida al teléfono puede afectar el rendimiento del escaneo.

Apéndice Figura 2-1 Requisito de distancia



Appendix 3 Recomendaciones de ciberseguridad

Acciones obligatorias que se deben tomar para la seguridad básica de la red del dispositivo: 1. Use contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres.
- Incluya al menos dos tipos de caracteres; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos.
- No contenga el nombre de la cuenta o el nombre de la cuenta en orden
- inverso. No utilice caracteres continuos, como 123, abc, etc.
- No utilice caracteres superpuestos, como 111, aaa, etc.

2. Actualice el firmware y el software del cliente a tiempo

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su dispositivo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el dispositivo está conectado a la red pública, se recomienda habilitar la función de "verificación automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones "agradables de tener" para mejorar la seguridad de la red de su dispositivo: 1. Protección física

Le sugerimos que realice una protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala y gabinete de computadoras especiales, e implemente un permiso de control de acceso y una administración de claves bien hechos para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de un dispositivo extraíble (como un disco flash USB). , puerto serie), etc.

2. Cambie las contraseñas regularmente

Le sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinadas o descifradas.

3. Establezca y actualice la información de restablecimiento de contraseñas a tiempo

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

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

Le sugerimos que cambie el HTTP predeterminado y otros puertos de servicio a cualquier conjunto de números entre 1024 y 65535, lo que reduce el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.

6. Habilitar HTTPS

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

7. Enlace de dirección MAC

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

8. Asigne cuentas y privilegios de manera razonable

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios razonablemente y asígneles un conjunto mínimo de permisos.

9. Deshabilite los servicios innecesarios y elija modos seguros

Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir los riesgos.

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

- SNMP: elija SNMP v3 y configure contraseñas de cifrado y contraseñas de autenticación seguras.

- SMTP: Elija TLS para acceder al servidor de buzones.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de encriptación WPA2-PSK y configure contraseñas seguras.

10. Transmisión encriptada de audio y video

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

Recordatorio: la transmisión encriptada causará cierta pérdida en la eficiencia de la transmisión.

11. Auditoría segura

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

12. Registro de red

Debido a la capacidad de almacenamiento limitada del dispositivo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, se recomienda habilitar la función de registro de red para asegurarse de que los registros críticos se sincronizan con el servidor de registro de red para su seguimiento.

13. Construya un entorno de red seguro

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

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