

Lector de acceso

Manual del usuario



Prefacio

General

Este manual describe las funciones y el funcionamiento del lector de acceso (en adelante, lector de tarjetas). Léalo atentamente antes de usar el dispositivo y guarde este manual para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras clave podrían aparecer en el manual.

Palabras de señalización	Significado
 DANGER	Indica un peligro potencial elevado que, de no evitarse, provocará la muerte o lesiones graves.
 WARNING	Indica un riesgo potencial medio o bajo que, de no evitarse, podría provocar lesiones leves o moderadas.
 CAUTION	Indica un riesgo potencial que, de no evitarse, podría ocasionar daños materiales, pérdida de datos, disminución del rendimiento o resultados impredecibles.
 NOTE	Proporciona información adicional como complemento al texto.

Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
V1.0.4	Requisitos de cableado adicionales.	Septiembre de 2024
V1.0.3	Se ha actualizado el método de desbloqueo.	Marzo de 2023
V1.0.2	Se han añadido métodos de desbloqueo y actualización del sistema.	Diciembre de 2022
V1.0.1	Modelos de dispositivos actualizados.	Diciembre de 2021
V1.0.0	Primer lanzamiento.	Octubre de 2020

Aviso de protección de la privacidad

Como usuario del dispositivo o responsable del tratamiento de datos, usted podría recopilar datos personales de terceros, como su rostro, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para salvaguardar 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 facilitar la información de contacto requerida.

Acerca del manual

- El manual es solo para consulta. Pueden existir pequeñas diferencias entre el manual y el producto.

- No nos hacemos responsables de las pérdidas ocasionadas por el uso del producto de forma que no se ajuste al manual.
- El manual se actualizará de acuerdo con las leyes y regulaciones más recientes de las jurisdicciones correspondientes. Para obtener información detallada, consulte el manual de usuario impreso, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo de referencia. Pueden existir pequeñas diferencias entre la versión electrónica y la impresa.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden generar algunas diferencias entre el producto real y el manual. Para obtener la versión más reciente del programa y la documentación complementaria, póngase en contacto con el servicio de atención al cliente.
- Es posible que existan errores de impresión o discrepancias en la descripción de las funciones, el funcionamiento y los datos técnicos. En caso de duda o controversia, nos reservamos el derecho a la interpretación final.
- Si no puede abrir el manual (en formato PDF), actualice el software de lectura o pruebe con otro software de lectura convencional.
- Todas las marcas comerciales, marcas registradas y nombres de empresas que aparecen en este 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 surge algún problema al utilizar el dispositivo.
- En caso de incertidumbre o controversia, nos reservamos el derecho a dar la explicación final.

Medidas de seguridad y advertencias importantes

Esta sección incluye información sobre el manejo adecuado del lector de tarjetas, la prevención de riesgos y la prevención de daños materiales. Lea atentamente antes de usar el lector de tarjetas y siga las instrucciones al utilizarlo.

Requisito de transporte



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

Requisitos de almacenamiento



Guarde el lector de tarjetas en condiciones de humedad y temperatura permitidas.

Requisitos de instalación



WARNING

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



- El personal que trabaje en altura debe tomar todas las medidas necesarias para garantizar su seguridad personal, incluyendo el uso de casco y cinturones de seguridad.
- No coloque el lector de tarjetas en un lugar expuesto a la luz solar ni cerca de fuentes de calor.
- Mantenga el lector de tarjetas alejado de la humedad, el polvo y el hollín.
- Instale el lector de tarjetas sobre una superficie estable para evitar que se caiga.
- Instale el lector de tarjetas en un lugar bien ventilado y no obstruya su ventilación.
- Utilice un adaptador o una fuente de alimentación para gabinetes proporcionada por el fabricante.
- Utilice los cables de alimentación recomendados para la región y que cumplan con las especificaciones de potencia nominal.
- La fuente de alimentación debe cumplir con los requisitos de ES1 de la norma IEC 62368-1 y no debe ser superior a PS2. Tenga en cuenta que los requisitos de la fuente de alimentación están sujetos a la etiqueta del lector de tarjetas.
- El lector de tarjetas es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del lector de tarjetas esté conectada a una toma de corriente con toma de tierra de protección.

Requisitos de operación



- Compruebe que la fuente de alimentación sea la correcta antes de usarla.
- No desconecte el cable de alimentación del lateral del lector de tarjetas mientras el adaptador esté encendido.
- Utilice el lector de tarjetas dentro del rango nominal de entrada y salida de potencia.
- Utilice el lector de tarjetas dentro de las condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquido sobre el lector de tarjetas y asegúrese de que no haya ningún objeto lleno de líquido sobre el lector de tarjetas para evitar que el líquido fluya hacia él.
- No desmonte el lector de tarjetas sin la instrucción de un profesional.

Tabla de contenido

Prólogo.....	I Medidas de seguridad y advertencias importantes.....	III 1
Introducción.....		1
1.1 Características.....		1
1.2 Apariencia.....		1
1.2.1 86 Modelo de caja.....		1
1.2.2 Modelo Slim.....		2
1.2.3 Modelo de huella dactilar.....		2
2 Requisitos de cableado.....		3
3 Instalación.....		5
3.1 Instalación del modelo de caja 86.....		5
3.2 Instalación del modelo Slim.....		6
3.3 Instalación del modelo de huella dactilar.....		8
4 Indicador de sonido y luz.....		12
4.1 86 Modelos Box y Slim.....		12
4.2 Modelo de huella dactilar.....		12
5. Desbloqueando la puerta.....		14
6 Actualización del sistema.....		15
6.1 Actualización a través de SmartPSS Lite.....		15
6.2 Actualización mediante la herramienta de configuración.....		15
Apéndice 1 Recomendación de seguridad.....		16

1 Introducción

1.1 Características

- Fabricado en policarbonato y panel acrílico con un diseño delgado e impermeable.
- Admite la lectura de tarjetas sin contacto.
- Admite la lectura de tarjetas IC (Mifare), la lectura de tarjetas de identificación (solo para lectores de tarjetas con función de lectura de tarjetas de identificación) y la lectura de códigos QR (solo para lectores de tarjetas con función de lectura de códigos QR).
- Admite la 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).
- Admite actualizaciones en línea.
- Admite alarma antisabotaje.
- Zumbador y luz indicadora incorporados.
- Sistema de vigilancia integrado para garantizar la estabilidad del lector de tarjetas.
- Seguro y estable, con protección contra sobrecorriente y sobretensión.



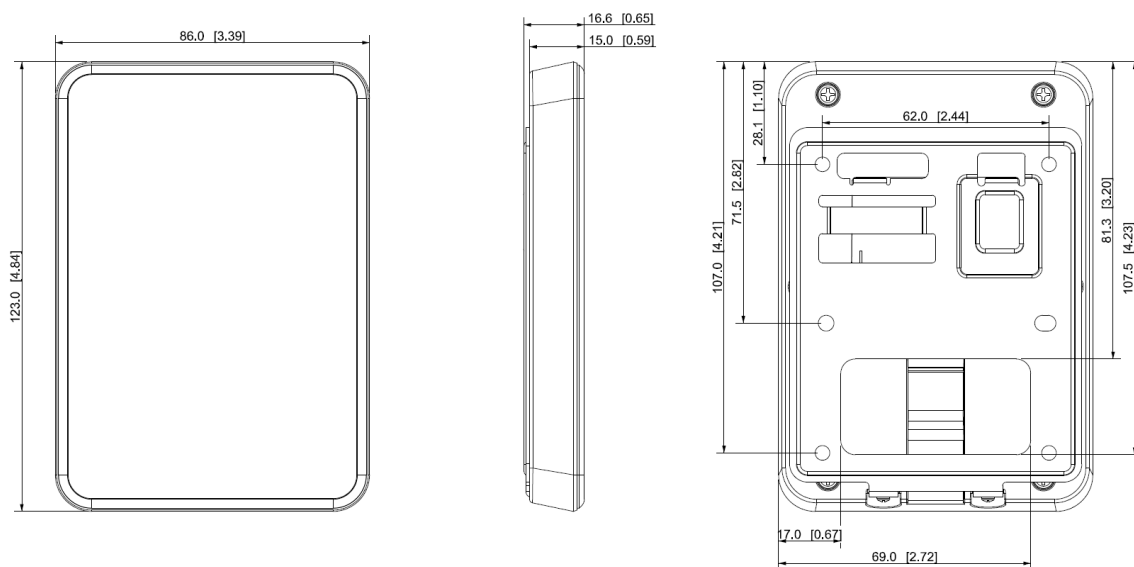
Las funciones pueden variar según los diferentes modelos.

1.2 Apariencia

El lector de tarjetas se puede clasificar, según su apariencia, en modelo de caja 86, modelo delgado y modo de huella dactilar.

1.2.1 Modelo de caja 86

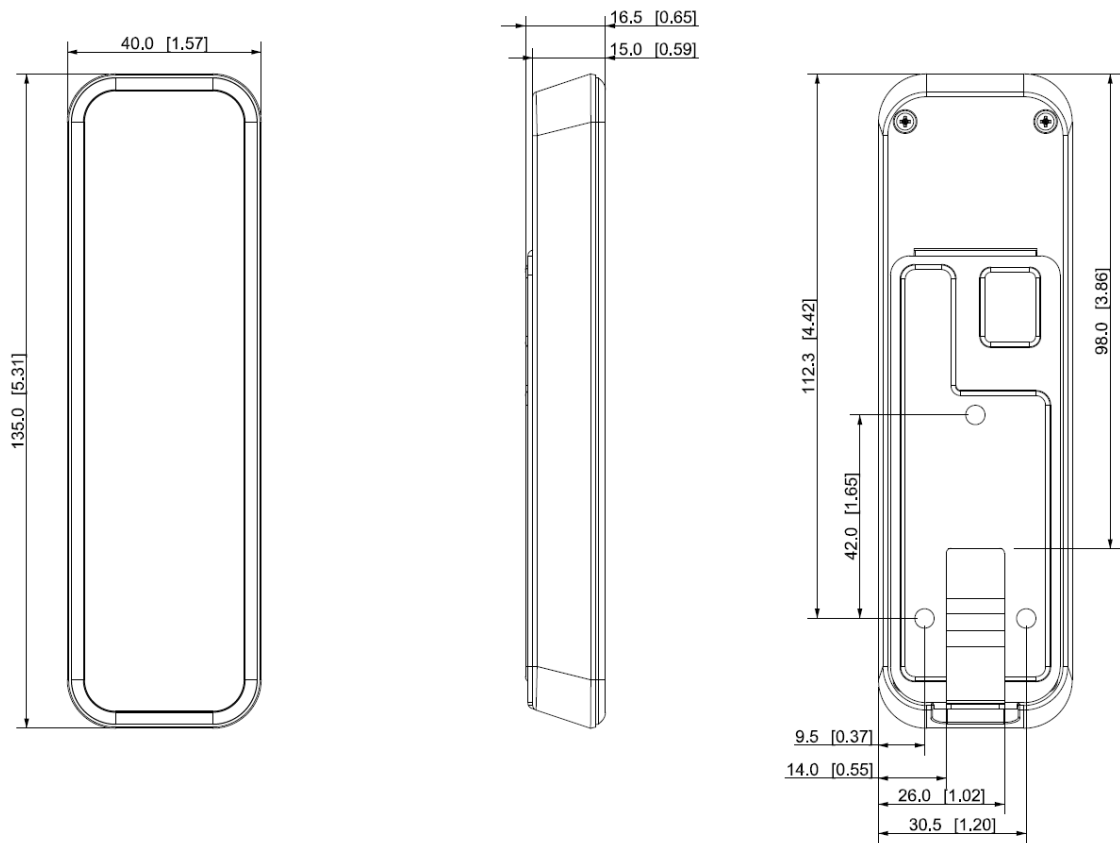
Figura 1-1 Dimensiones del modelo de caja 86 (mm [pulgadas])



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

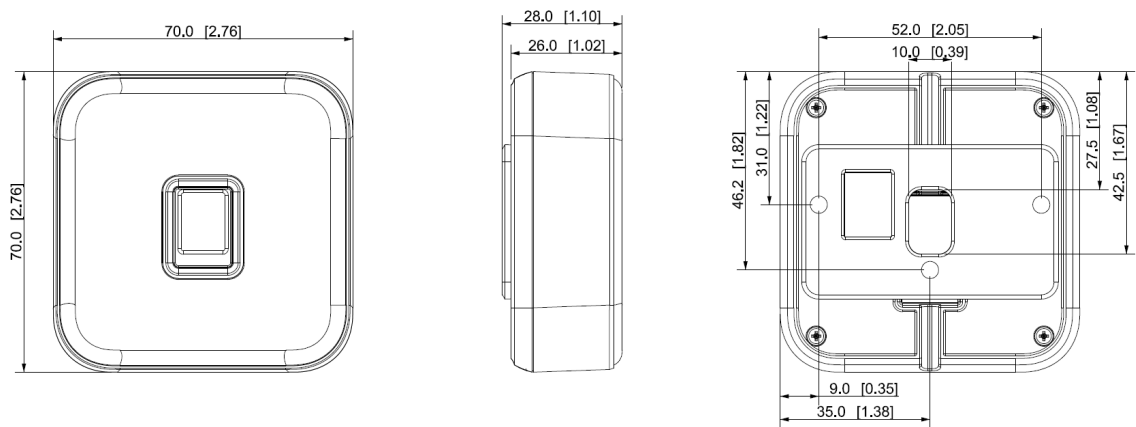
1.2.2 Modelo delgado

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



1.2.3 Modelo de huellas dactilares

Figura 1-3 Dimensiones del modelo de huella dactilar (mm [pulgadas])



2 Requisitos de cableado

- Conecte el lector de tarjetas a los puertos Wiegand o a los puertos RS-485, según el tipo de lector de tarjetas.
- Seleccione los cables adecuados según los requisitos del fabricante.



Los modelos de huella dactilar y de código QR solo son compatibles con RS-485.

Cables de 8 núcleos para los modelos 86 Box y Slim.

Tabla 2-1 Descripción de la conexión del cable (1)

Color	Puerto	Descripción
Rojo	RD+	PWR (12 V CC)
Negro	RD-	GND
Azul	CASO	Señal de alarma de manipulación
Blanco	D1	Señal de transmisión Wiegand (eficaz solo cuando se utiliza el protocolo Wiegand)
Verde	D0	
Marrón	CONDUJO	Señal sensible a Wiegand (eficaz solo cuando se utiliza el protocolo Wiegand)
Amarillo	RS-485_B	
Púrpura	RS-485_A	

Cables de 5 núcleos para el modelo de huella dactilar

Tabla 2-2 Descripción de la conexión del cable (2)

Color	Puerto	Descripción
Rojo	RD+	PWR (12 V CC)
Negro	RD-	GND
Azul	CASO	Señal de alarma de manipulación
Amarillo	RS-485_B	
Púrpura	RS-485_A	

Tabla 2-3 Requisitos de cableado del lector de tarjetas

Tipo	Requisitos de impedancia	Requisitos de longitud
Lector de tarjetas RS485	Conecta cables RS-485, y la impedancia de cada cable debe ser $\leq 10 \Omega$.	≤ 100 m. Por encima de UL1061 24AWG Los cables blindados son recomendado.

Tipo	Requisitos de impedancia	Requisitos de longitud
lector de tarjetas Wiegand	Conecta cables Wiegand, y la impedancia de un solo cable debe ser $\leq 2 \Omega$.	≤ 80 m. Por encima de UL1061 18AWG Los cables blindados son recomendado.

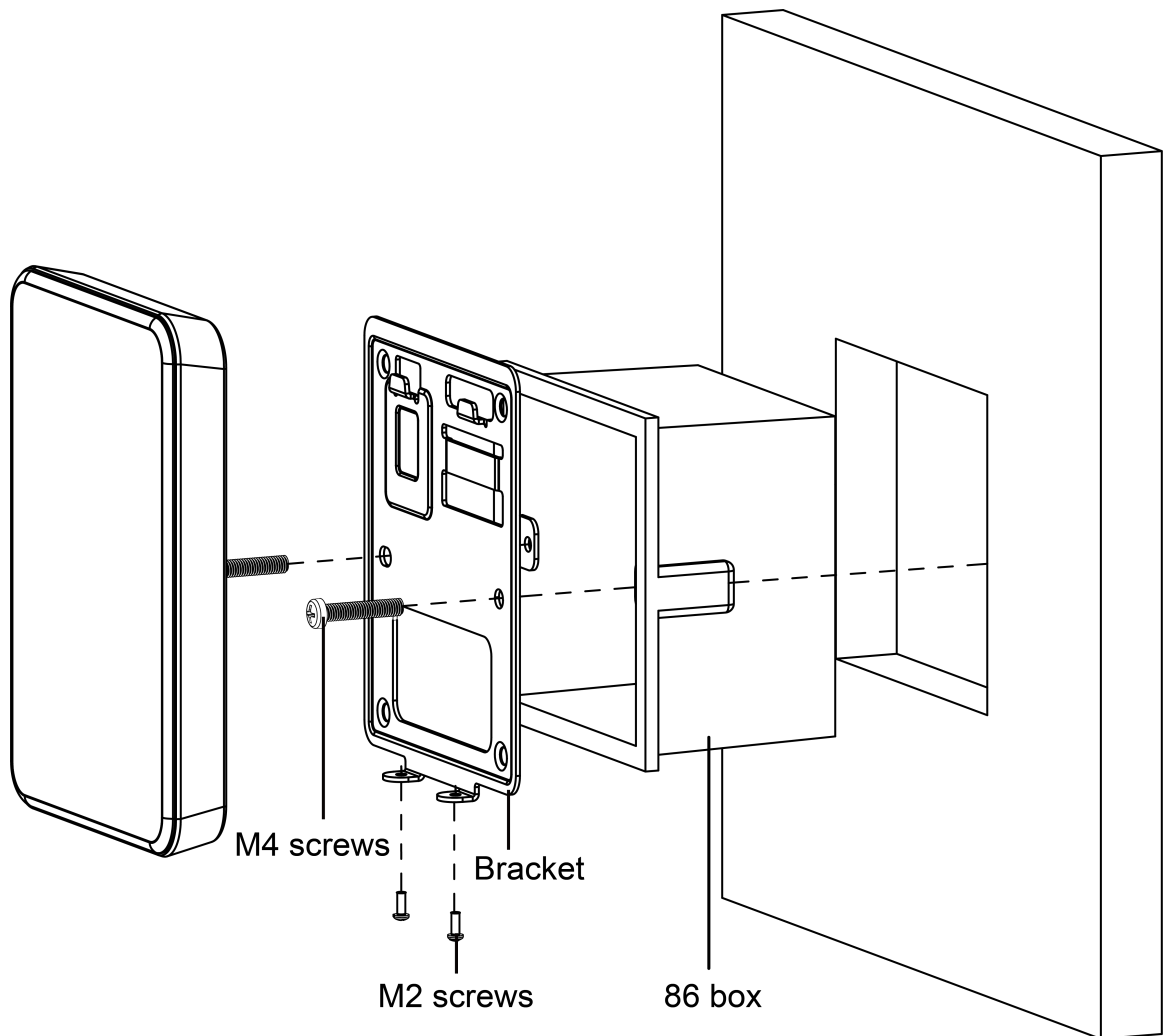
3 Instalación

3.1 Instalación del modelo de caja 86

Montaje en caja

1. Monte la caja 86 en la pared.
2. Conecte el lector de tarjetas y coloque los cables dentro de la caja 86.
3. Utilice dos tornillos M4 para fijar el soporte a la caja 86.
4. Fije el lector de tarjetas al soporte de arriba hacia abajo.
5. Atornille 2 tornillos en la parte inferior del lector de tarjetas.

Figura 3-1 Montaje en pared

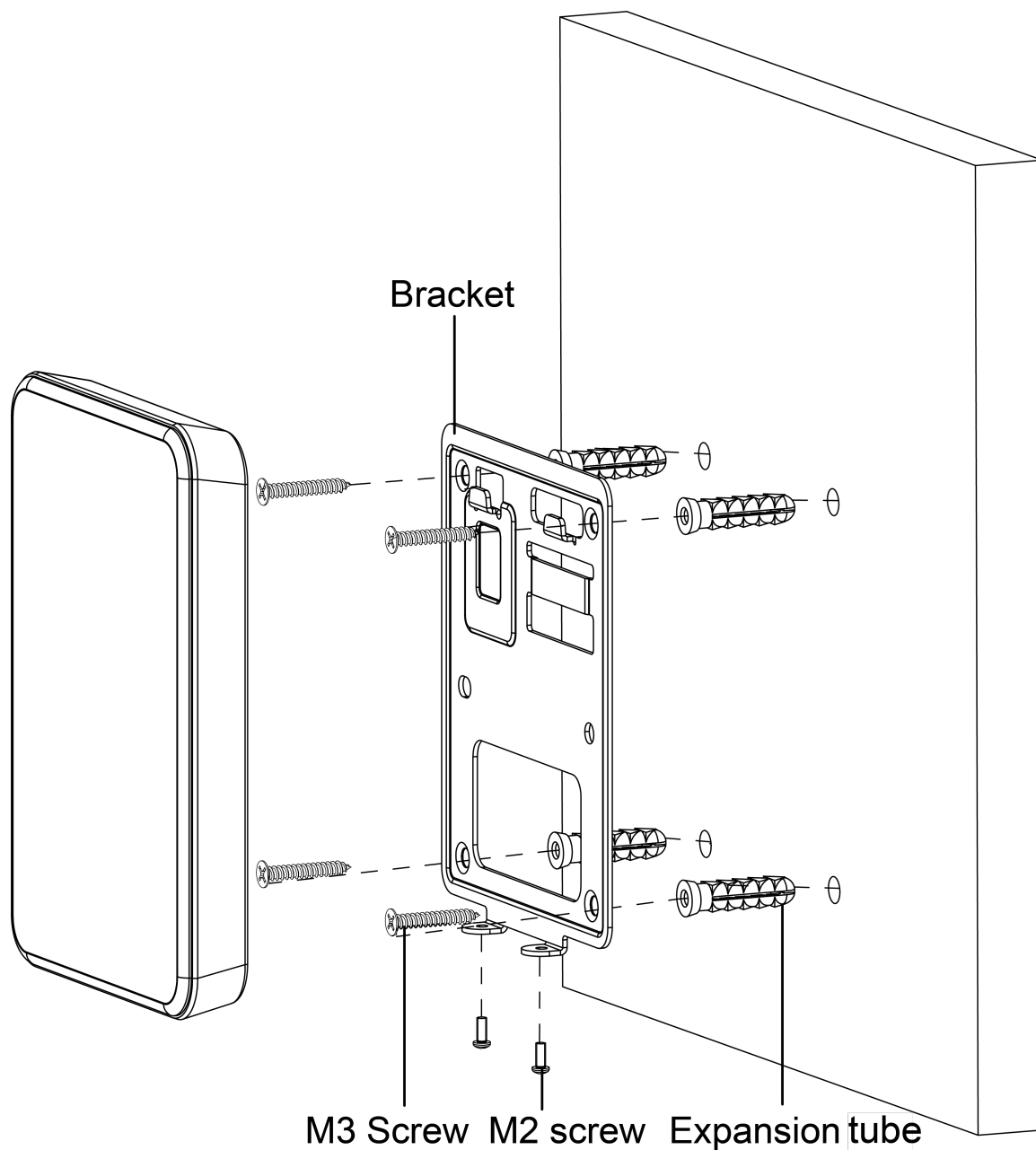


Montaje en pared

1. Taladre agujeros en la pared.
2. Coloca 4 pernos de expansión en los agujeros.
3. Pase el lector de tarjetas a través de la ranura del soporte.

4. Utilice dos tornillos M3 para fijar el soporte a la pared.
5. Fije el lector de tarjetas al soporte de arriba hacia abajo.
6. Atornille 2 tornillos en la parte inferior del lector de tarjetas.

Figura 3-2 Montaje en pared



3.2 Instalación del modelo Slim

Procedimiento

- Paso 1** Taladre 4 agujeros y una salida para cable en la pared.



Para el cableado en superficie, no se requiere una salida de cable.

- Paso 2** Coloca 3 pernos de expansión en los agujeros.

- Paso 3** Conecte los cables del lector de tarjetas y páselos por la ranura del soporte.

- Paso 4 Utilice tres tornillos M3 para fijar el soporte a la pared. Coloque el
- Paso 5 lector de tarjetas en el soporte de arriba hacia abajo. Atornille un
- Paso 6 tornillo M2 en la parte inferior del lector de tarjetas.

Figura 3-3 Cableado dentro de la pared

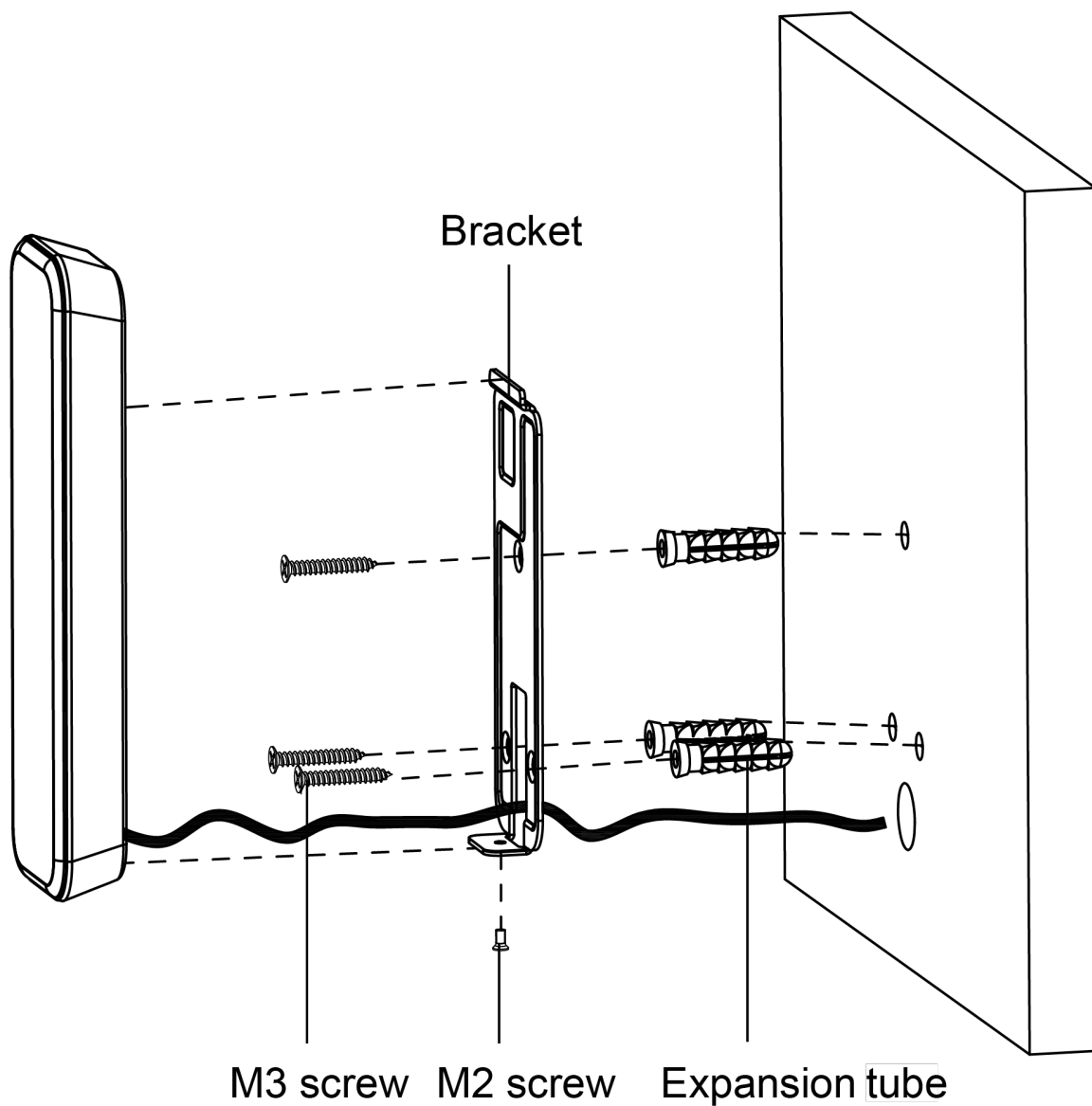
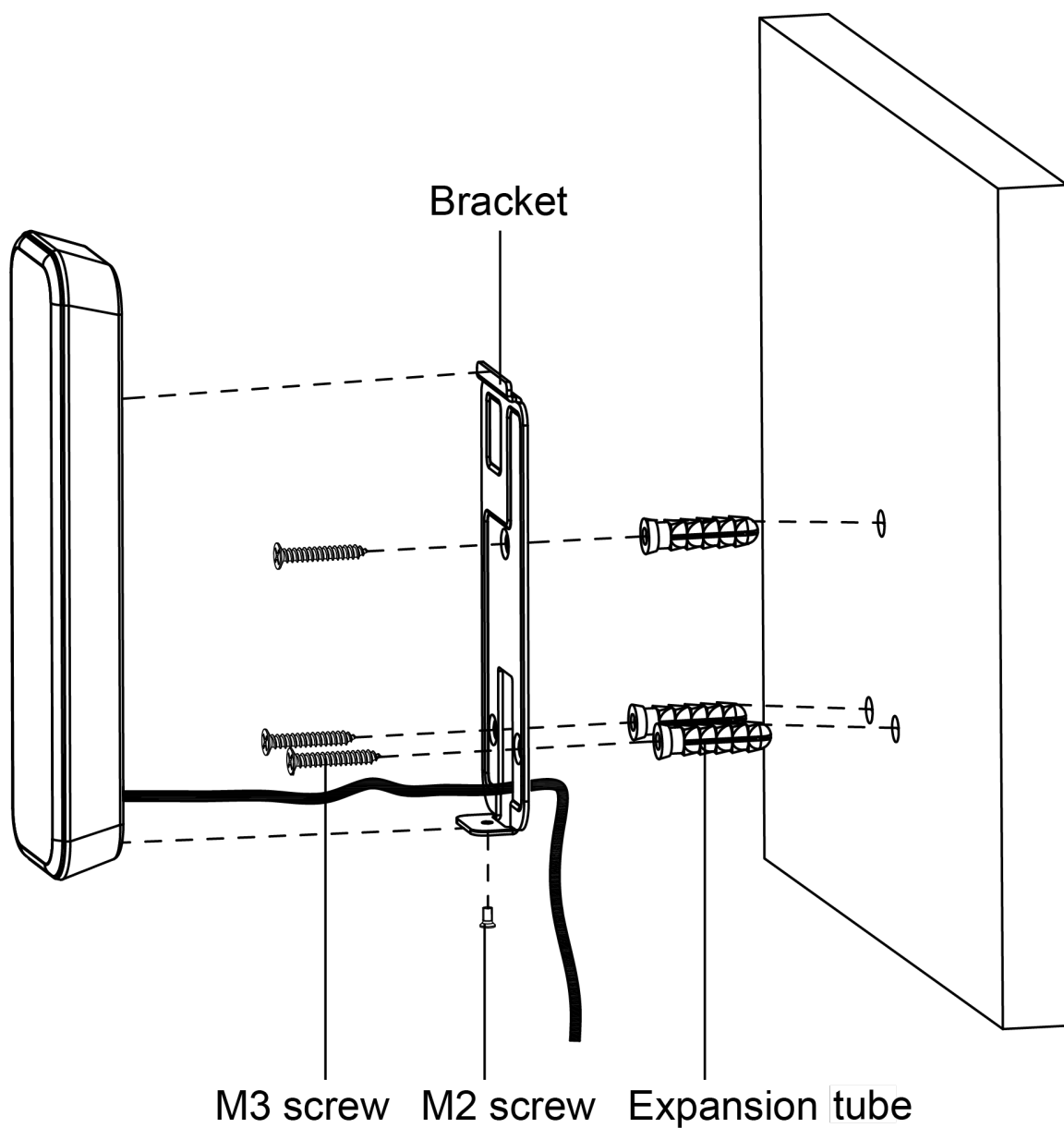


Figura 3-4 Cableado de montaje en superficie



3.3 Instalación del modelo de huella dactilar

Procedimiento

Paso 1 Taladre 4 agujeros y una salida para cable en la pared.



Para el cableado en superficie, no se requiere una salida de cable.

Paso 2 Coloca 3 pernos de expansión en los agujeros.

Paso 3 Utilice tres tornillos M3 para fijar el soporte a la pared.

Paso 4 Cableado del lector de tarjetas.

Paso 5 Fije el lector de tarjetas al soporte de arriba hacia abajo.

Figura 3-5 Cableado dentro de la pared

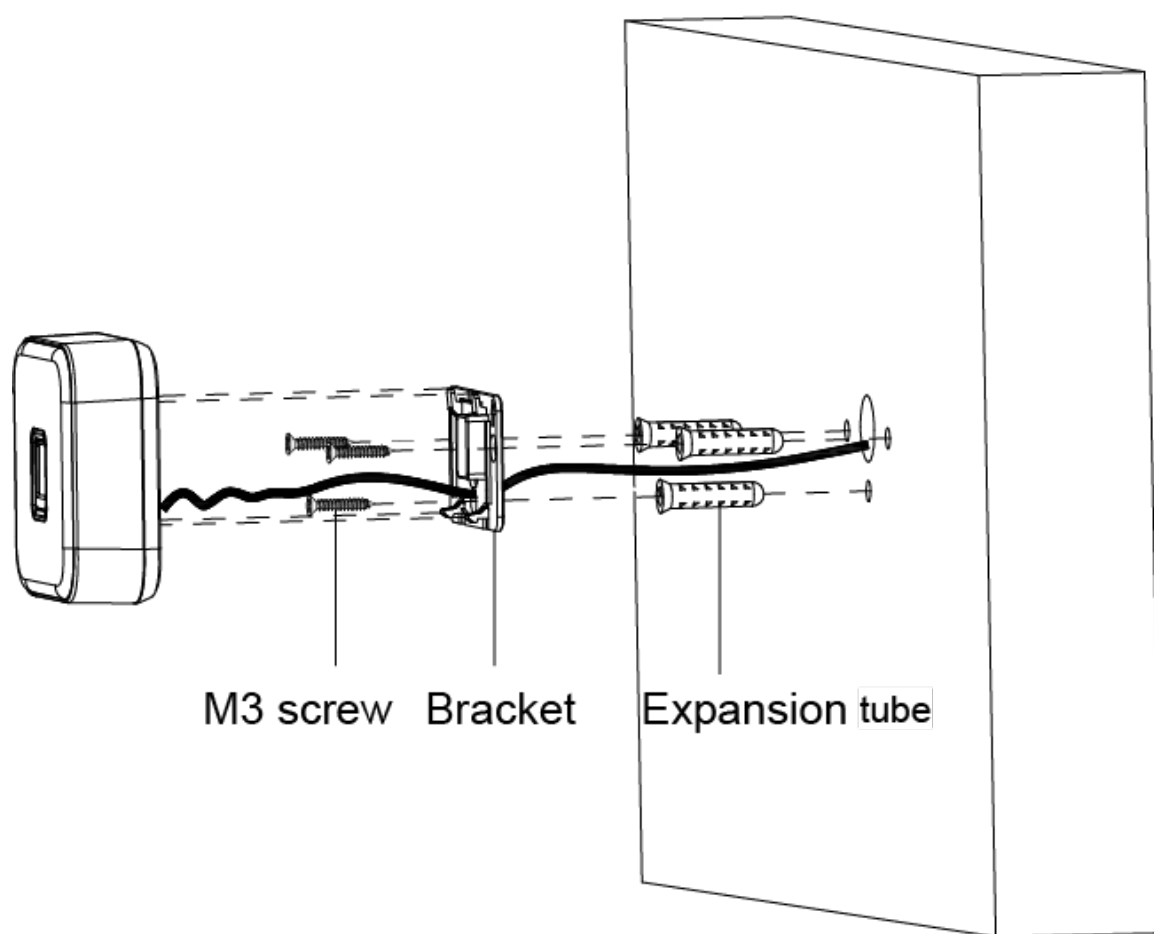
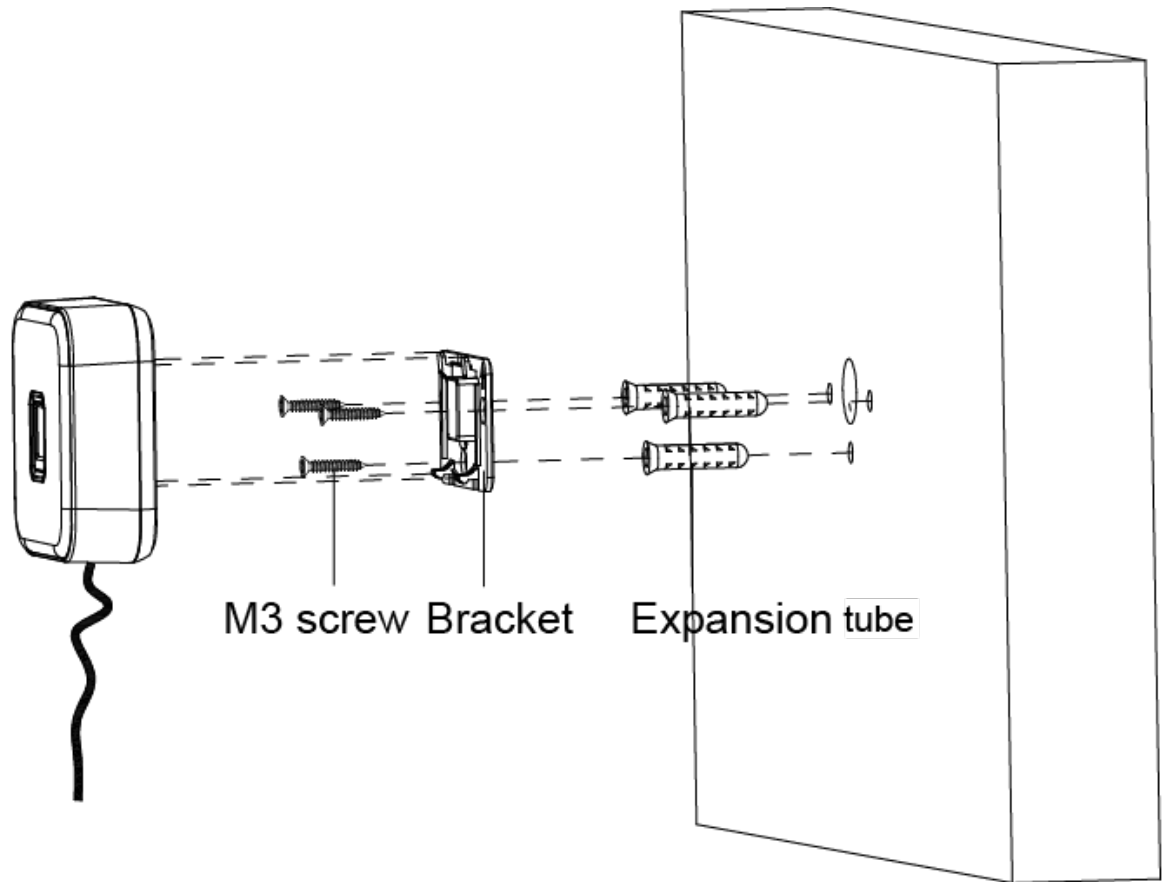
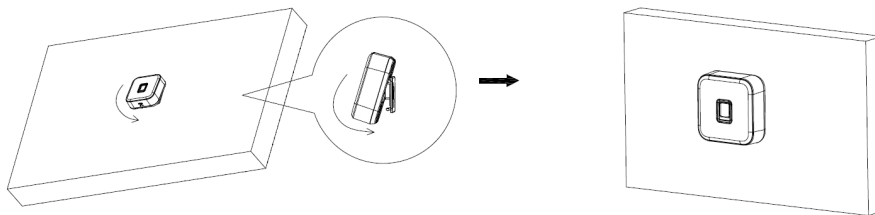


Figura 3-6 Cableado de superficie



Paso 6 Presione el lector de tarjetas hacia adelante hasta que escuche un "clic" y la instalación se completará.

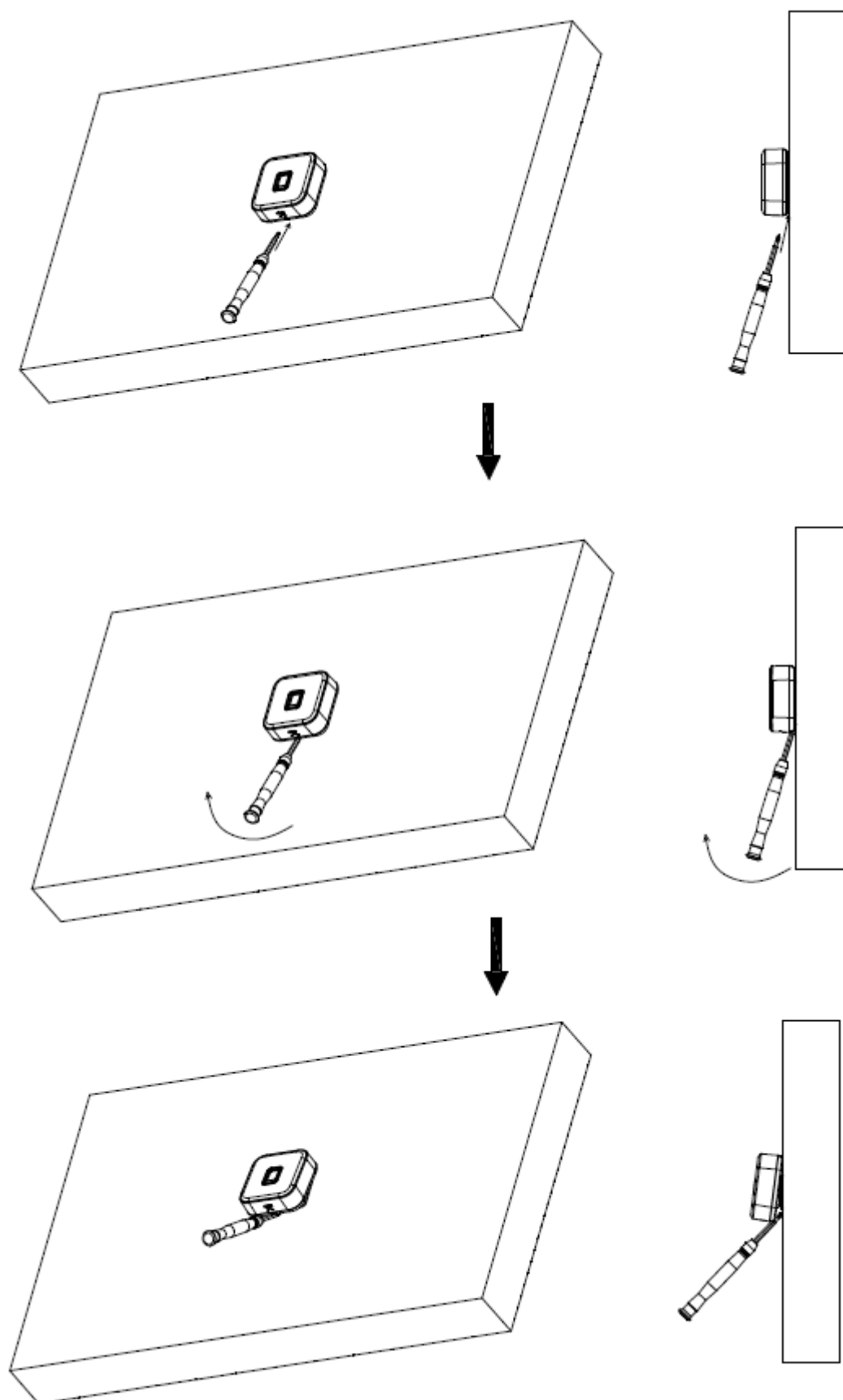
Figura 3-7 Asegure el lector de tarjetas



Operaciones relacionadas

Para extraer el lector de tarjetas de la pared, utilice un destornillador para hacer palanca y abrirlo desde la parte inferior hasta que oiga un "clic".

Figura 3-8 Retire el lector de tarjetas



4. Indicaciones sonoras y luminosas

4.1 86 Modelos Box y Slim

Tabla 4-1 Descripción de las indicaciones sonoras y luminosas

Situación	Indicaciones sonoras y luminosas
Encendido.	Pulsa una vez. El indicador es de color azul sólido.
Retirar el lector de tarjetas.	Zumbido prolongado durante 15 segundos.
Presionar botones.	Un zumbido breve una vez.
Alarma activada por el controlador.	Zumbido prolongado durante 15 segundos.
Comunicación RS-485 y deslizamiento de una tarjeta autorizada.	Pulsa una vez. El indicador parpadea en verde una vez y luego se ilumina en azul fijo, indicando el modo de espera.
Comunicación RS-485 y uso de una tarjeta no autorizada.	Suena cuatro veces. El indicador parpadea en rojo una vez y luego se ilumina en azul fijo, en modo de espera.
Comunicación anómala 485 y deslizamiento de una tarjeta autorizada/no autorizada.	Suena tres veces. El indicador parpadea en rojo una vez y luego se ilumina en azul fijo, en modo de espera.
Comunicación Wiegand y deslizamiento de una tarjeta autorizada.	Pulsa una vez. El indicador parpadea en verde una vez y luego se ilumina en azul fijo, indicando el modo de espera.
Comunicación Wiegand y uso de una tarjeta no autorizada.	Suena tres veces. El indicador parpadea en rojo una vez y luego se ilumina en azul fijo, en modo de espera.
El software se está actualizando o está esperando una actualización en BOOT.	El indicador parpadea en azul hasta que finaliza la actualización.

4.2 Modelo de huellas dactilares

Tabla 4-2 Descripción de las indicaciones sonoras y luminosas

Situación	Indicaciones sonoras y luminosas
El lector de tarjetas está encendido.	Pulsa una vez. El indicador es de color azul sólido.
Retirar el lector de tarjetas.	Zumbido prolongado durante 15 segundos.

Situación	Indicaciones sonoras y luminosas
La activación de la alarma la realiza el controlador.	
Comunicación 485 y deslizamiento de una tarjeta autorizada.	Pulsa una vez. El indicador parpadea en verde una vez y luego se ilumina en azul fijo, indicando el modo de espera.
Comunicación 485 y uso de una tarjeta no autorizada.	Suena cuatro veces. El indicador parpadea en rojo una vez y luego se ilumina en azul fijo, en modo de espera.
Comunicación 485 anómala y deslizamiento de una tarjeta/huella dactilar autorizada o no autorizada.	Suena tres veces. El indicador parpadea en rojo una vez y luego se ilumina en azul fijo, en modo de espera.
485 comunicación y se reconoce una huella digital.	Pulsa una vez.
Comunicación 485 y escaneo de una huella dactilar autorizada.	Pulsa dos veces con un intervalo de 1 segundo. El indicador parpadea en verde una vez y luego se ilumina en azul fijo, indicando el modo de espera.
Comunicación 485 y toma de huellas dactilares no autorizada.	Pulsa una vez, y luego cuatro veces. El indicador parpadea en rojo una vez y luego se ilumina en azul fijo, en modo de espera.
Operaciones de huella digital, incluyendo añadir, eliminar y sincronizar.	El indicador parpadea en verde.
Finalizar las operaciones de huellas dactilares, incluyendo añadir, eliminar y sincronizar.	El indicador es de color azul sólido.
El software se está actualizando o está esperando una actualización en BOOT.	El indicador parpadea en azul hasta que finaliza la actualización.

5. Desbloquear la puerta

Deslice la tarjeta por el lector para abrir la puerta. Si el lector tiene teclado, también puede desbloquearlo introduciendo el nombre de usuario y la contraseña.

- Desbloquea la puerta mediante contraseña pública: Introduce la contraseña pública y, a continuación, pulsa#.
- Desbloquea la puerta mediante contraseña de usuario: Introduce el ID de usuario y pulsa#y luego ingrese la contraseña de usuario y toque#.
- Desbloquea la puerta con tarjeta y contraseña: desliza la tarjeta, introduce la contraseña y pulsa.#.

Si la contraseña es correcta, el indicador se ilumina en verde y suena el zumbador una vez. Si la contraseña es incorrecta, el indicador se ilumina en rojo y suena el zumbador 4 veces (comunicación RS-485) o 3 veces (comunicación Wiegand o si no hay ninguna línea de señal conectada).

6. Actualización del sistema

6.1 Actualización a través de SmartPSS Lite

Requisitos previos

- El lector de tarjetas se añadió al controlador de acceso mediante cables RS-485.
- El controlador de acceso y el lector de tarjetas están encendidos.

Procedimiento

Paso 1 Instale e inicie sesión en SmartPSS Lite y luego seleccione **Administrador de dispositivos**.

Paso 2 Clic . 

Figura 6-1 Seleccione el controlador de acceso

No.	Name	IP	Device Type	Device Model	Port	Channel Number	Online Status	SN	Operation
1	Device01	172.16.1.100	Access Controller	ASC2208C-S	37777	0/0/8/8	Online	7D	  

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

Paso 4 Hacer clic **Mejora**.

El indicador del lector de tarjetas parpadea en azul hasta que finaliza la actualización, momento en el que el lector de tarjetas se reinicia automáticamente.

6.2 Actualización mediante la herramienta de configuración

Requisitos previos

- El lector de tarjetas se añadió al controlador de acceso mediante cables RS-485.
- El controlador de acceso y el lector de tarjetas están encendidos.

Procedimiento

Paso 1 Instale y abra Configtool y luego seleccione **Actualización del dispositivo**.

Paso 2 Haga clic en un controlador de acceso y luego haga clic en 

Paso 3 Haga clic **Mejora**.

El indicador del lector de tarjetas parpadea en azul hasta que finaliza la actualización, momento en el que el lector de tarjetas se reinicia automáticamente.

Apéndice 1 Recomendación de seguridad

Gestión de cuentas

1. Utilice contraseñas complejas

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de caracteres: 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 consecutivos, como 123, abc, etc.
- No utilice caracteres repetidos, como 111, aaa, etc.

2. Cambie las contraseñas periódicamente

Se recomienda cambiar periódicamente la contraseña del dispositivo para reducir el riesgo de que sea adivinada o pirateada.

3. Asigne las cuentas y los permisos adecuadamente.

Agregue usuarios según corresponda, en función de los requisitos de servicio y administración, y asígneles los permisos mínimos necesarios.

4. Habilitar la función de bloqueo de cuenta

La función de bloqueo de cuenta está activada por defecto. Se recomienda mantenerla activada para proteger la seguridad de la cuenta. Tras varios intentos fallidos de contraseña, la cuenta y la dirección IP correspondientes se bloquearán.

5. Establezca y actualice la información de restablecimiento de contraseña de manera oportuna.

El dispositivo admite la función de restablecimiento de contraseña. Para reducir el riesgo de que ciberdelincuentes utilicen esta función, modifique su información de inmediato si hay algún cambio. Al configurar las preguntas de seguridad, se recomienda no usar respuestas fáciles de adivinar.

Configuración del servicio

1. Habilitar HTTPS

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

2. Transmisión cifrada de audio y vídeo

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

3. Desactive los servicios no esenciales y utilice el modo seguro.

Si no son necesarios, 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, que incluyen, 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 correo.
- FTP: Elija SFTP y configure contraseñas complejas.
- Punto de acceso: seleccione 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 ciberdelincuentes lo adivinen.

Configuración de red

1. Habilitar lista de permitidos

Se recomienda activar la función de lista de permitidos y permitir el acceso al dispositivo únicamente a las direcciones IP incluidas en dicha lista. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la del dispositivo compatible a la lista de permitidos.

2. Enlace de dirección MAC

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

3. Construir un entorno de red seguro

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

- Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa;
- Según las necesidades reales de la red, divida la red: si no hay demanda de comunicación entre las dos subredes, se recomienda utilizar VLAN, puerta de enlace y otros métodos para dividir la red y lograr el aislamiento de la red;
- Implementar 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. Comprobar usuarios en línea

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

2. Consultar el registro del dispositivo

Al consultar los registros, podrá obtener información sobre las direcciones IP que intentan iniciar sesión en el dispositivo y las operaciones clave realizadas por los usuarios que han iniciado sesión.

3. Configurar el registro de red

Debido a la limitada capacidad de almacenamiento de los dispositivos, 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 se sincronicen con el servidor de registro de red para su posterior seguimiento.

Seguridad del software

1. Actualiza el firmware a tiempo.

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

2. Actualizar el software del cliente a tiempo

Se recomienda descargar y utilizar la última versión del software cliente.

Protección física

Se recomienda implementar medidas de protección física para los dispositivos (especialmente los de almacenamiento), como colocar el dispositivo en una sala de máquinas y un armario dedicados, y contar con control de acceso.

y un sistema de gestión de claves para evitar que personal no autorizado dañe el hardware y otros equipos periféricos (por ejemplo, unidades flash USB, puertos serie).