Acceso independiente

Manual del usuario

Versión 1.0.0

Prefacio

General

Este manual presenta las funciones y el funcionamiento del Access Standalone (en adelante, el "Dispositivo"). Léalo detenidamente antes de usarlo y consérvelo para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de señal	Significado
DANGER	Indica un peligro potencial alto que, si no se evita, provocará la muerte o lesiones graves.
WARNING	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
CAUTION	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, reducciones en el rendimiento o resultados impredecibles.
ESD	Dispositivos sensibles a la electrostática. Indica un dispositivo que es sensible a la descarga electrostática.
ELECTRIC SHOCK	Indica alto voltaje peligroso. Tenga cuidado de no entrar en contacto con la electricidad.
LASER RADIATION	Indica un peligro de radiación láser. Tenga cuidado de evitar la exposición a un rayo láser.
TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
NOTE	Proporciona información adicional como complemento al texto.

Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
Versión 1.0.0	Primer lanzamiento.	Abril de 2024

Aviso de protección de la privacidad

Como usuario del dispositivo o responsable del tratamiento de datos, podría recopilar datos personales de terceros, como su rostro, audio, huellas dactilares y número de matrícula. Debe cumplir con las leyes y normativas 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

- Este manual es solo de referencia. Podrían existir ligeras diferencias entre el manual y el producto.
- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas que no cumplan con el manual.
- El manual se actualizará según las últimas leyes y regulaciones de las jurisdicciones pertinentes. Para obtener información detallada, consulte el manual de usuario impreso, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. Este manual es solo de referencia. Podrían existir ligeras diferencias entre la versión electrónica y la versión impresa.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto podrían generar diferencias entre el producto real y el manual. Para obtener el programa más reciente y la documentación complementaria, póngase en contacto con el servicio de atención al cliente.
- Podría haber errores de impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. En caso de duda o controversia, nos reservamos el derecho de ofrecer una explicación definitiva.
- 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 registradas y nombres de empresas en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o 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 explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta información sobre el manejo adecuado del Dispositivo, la prevención de riesgos y la prevención de daños materiales. Lea atentamente antes de usar el Dispositivo y siga las instrucciones al usarlo.

Requisito de transporte

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

Requisito de almacenamiento

Guarde el dispositivo en condiciones de humedad y temperatura permitidas.

Requisitos de instalación

- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- Cumpla estrictamente con las normas y códigos de seguridad eléctrica locales. Asegúrese de que el voltaje ambiente sea estable y cumpla con los requisitos de alimentación del dispositivo.
- No conecte el dispositivo a dos o más tipos de fuentes de alimentación, para evitar dañarlo.
- 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 de SELV (voltaje extra bajo de seguridad) y no exceder los estándares ES-1.
    - Cuando la potencia del dispositivo no supere los 100 W, la fuente de alimentación debe cumplir 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 suministro de energía (como el voltaje nominal) están sujetos a la etiqueta del dispositivo.

- El personal que trabaja en altura debe tomar todas las medidas necesarias para garantizar su 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 que 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.

Requisitos de operación

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

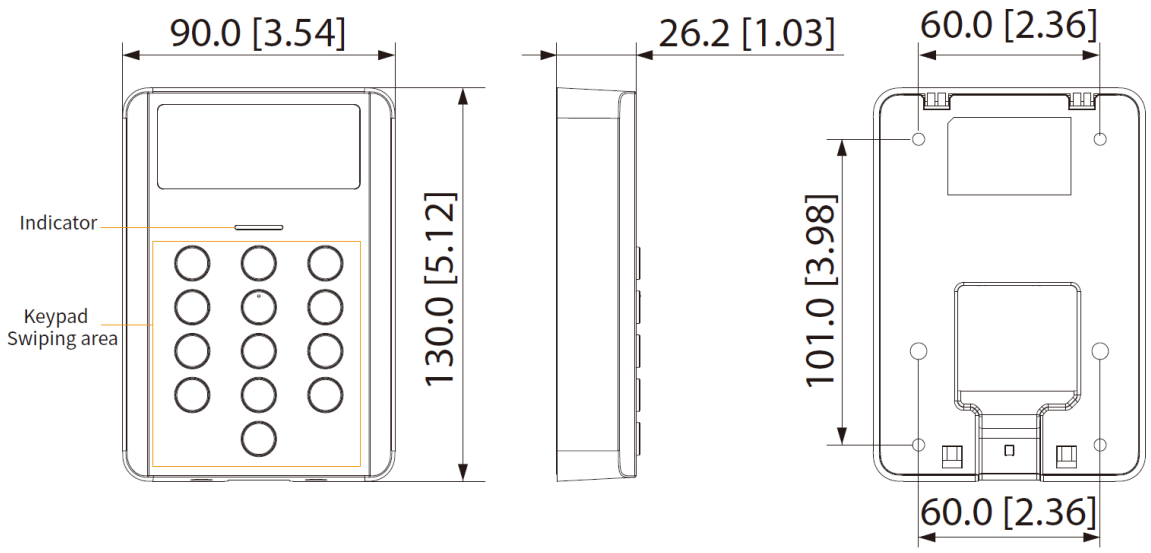
Tabla de contenido

1 Descripción general del producto

Este producto es un equipo de control de acceso que integra lectura, configuración y ejecución de tarjetas. Su diseño es sencillo y moderno, ideal para edificios de oficinas, escuelas, parques, comunidades, fábricas, espacios públicos, centros comerciales, edificios gubernamentales y otras aplicaciones.

2 Apariencia y dimensiones

Figura 2-1 Aspecto y dimensiones (unidad: mm [pulgadas])



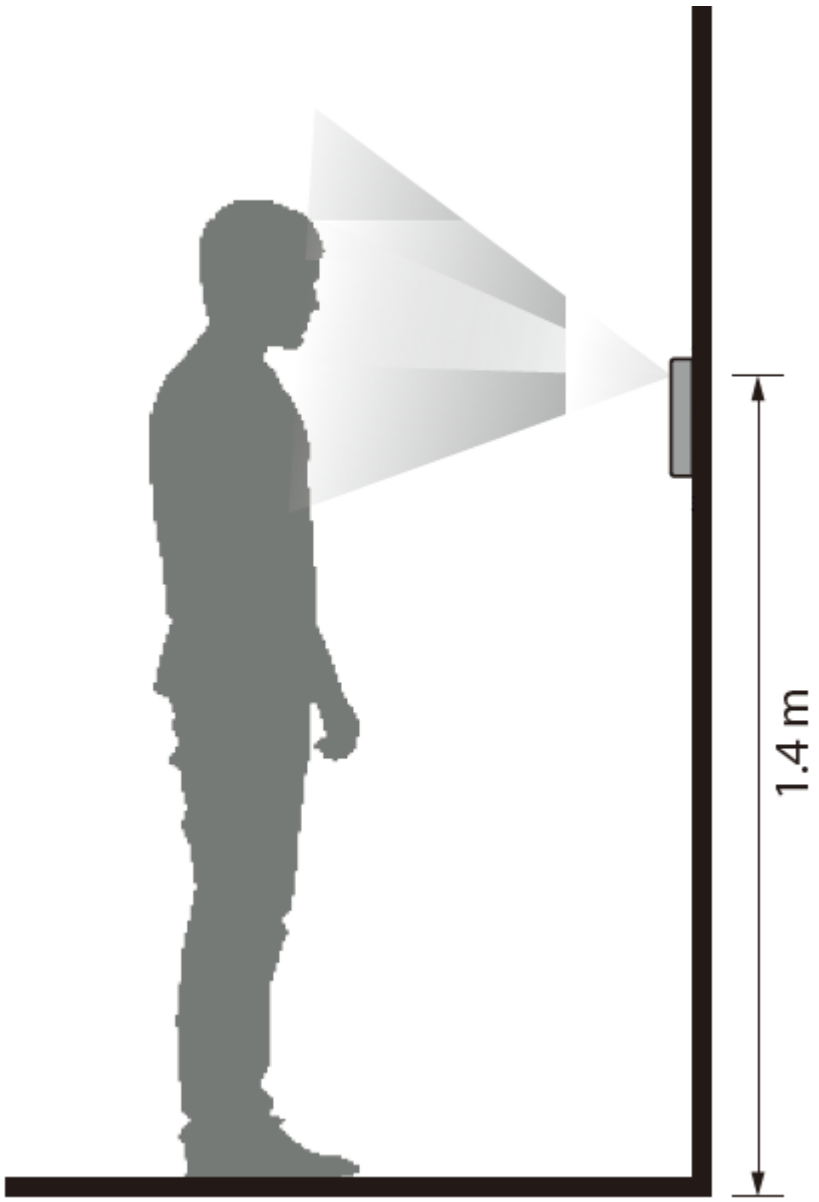
3. Escurrir e instalar

3.1 Entorno de instalación

- La luz a 0,5 metros de distancia del Access Standalone no debe ser inferior a 100 Lux.
- Le recomendamos instalar el Access Standalone en interiores, al menos a 3 metros 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 3-1 Requisito de altura de instalación

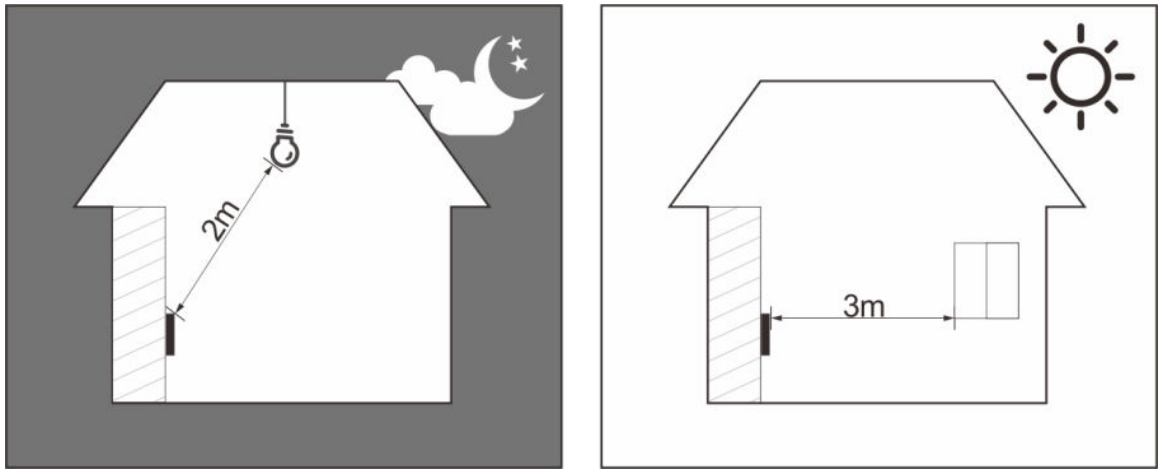


Requisitos de iluminación ambiental

Figura 3-2 Requisitos de iluminación ambiental

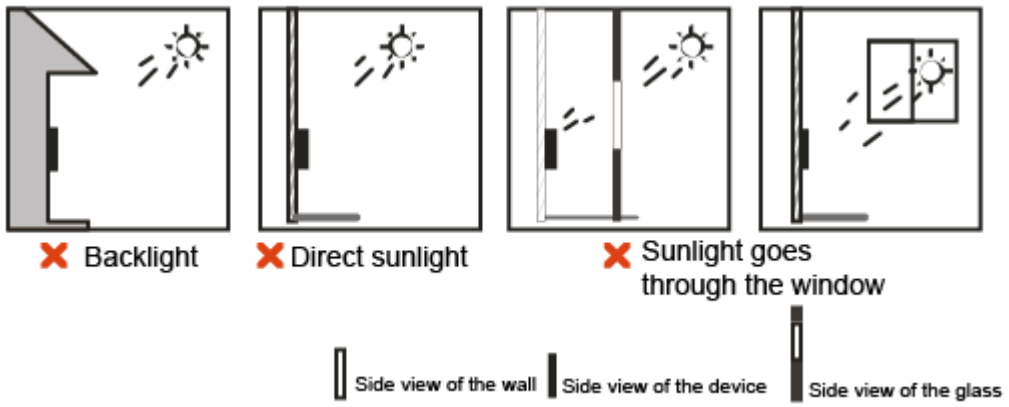
Ubicaciones de instalación recomendadas

Figura 3-3 Ubicaciones de instalación recomendadas



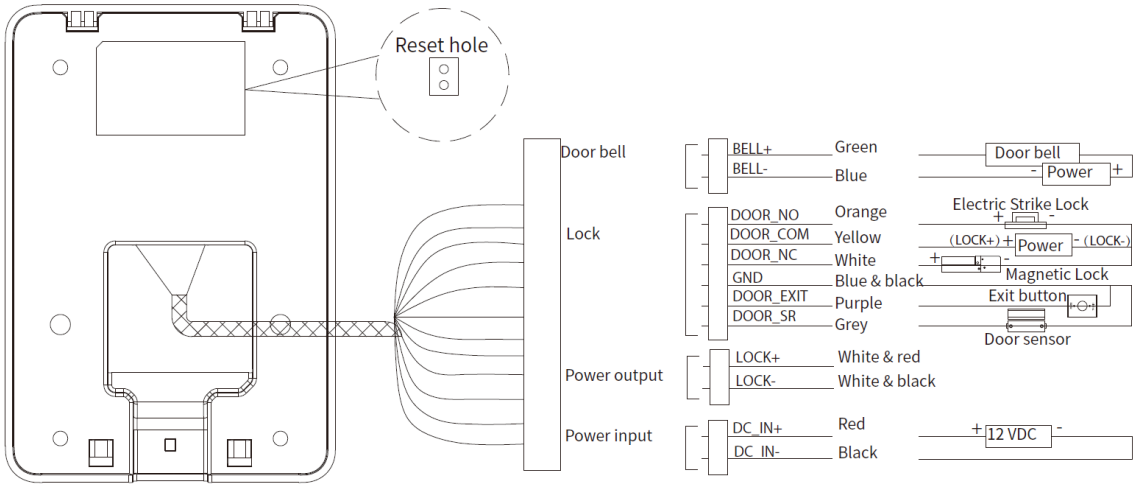
Ubicaciones de instalación no recomendadas

Figura 3-4 Ubicaciones de instalación no recomendadas



3.2 Cableado

Figura 3-5 Cableado



El dispositivo (que conecta los polos + y - de la cerradura) o una fuente de alimentación independiente suministra energía a la cerradura. Si la distancia de alimentación supera los 30 m, se recomienda suministrar energía a la cerradura mediante una fuente de alimentación independiente.

- Restablecimiento de fábrica del hardware: dentro de los 5 minutos posteriores a que se inicie el dispositivo, use pinzas para cortocircuitar el orificio de reinicio.
  - ◇ Si el tiempo de cortocircuito es inferior a 5 segundos, el dispositivo se restaura a la configuración de fábrica y se conserva la información del usuario. Todo se restaura a la configuración de fábrica, excepto el usuario y la contraseña pública.
  - ◇ Si el tiempo de cortocircuito no es inferior a 5 segundos, el dispositivo se restaura a la configuración de fábrica y se restaura toda la información.

Figura 3-6 Cableado de la fuente de alimentación de la cerradura

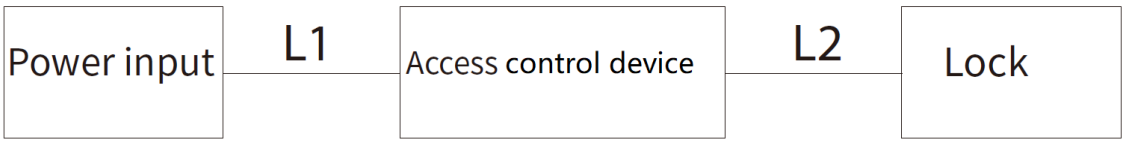


Tabla 3-1 Selección de cables

No.	Nombre	Modelo recomendado y especificación	Distancia máxima de alimentación (cable 17 AWG, impedancia ≤ 2 Ω por metro)
L1	Cable de alimentación	Cable de 2 núcleos de 17 AWG	• El dispositivo: L1 no puede superar los 100 m. • El Dispositivo y la cerradura: L1+L2 no más de 30 m.
L2	Alambre de bloqueo	Cable de 2 núcleos de 17 AWG, Cable de 4 núcleos de 17 AWG, o cable de categoría 5e	

- Si la cerradura se alimenta mediante el dispositivo, se recomienda que su corriente máxima no supere los 1000 mA. La cerradura admite un amplio rango de voltaje, y el voltaje mínimo permitido no debe superar los 10 V.
- La distancia de cableado de L1 y L2 se ve afectada por el voltaje de la fuente de alimentación y las especificaciones de los cables. En la construcción real, el voltaje de la fuente de alimentación no debe ser inferior al voltaje de funcionamiento mínimo permitido del dispositivo de control de acceso y la cerradura.
- Utilice cable de categoría 5e (impedancia por kilómetro ≤ 9 Ω) para alimentar la cerradura. Salvo las líneas de señal, el resto de las líneas deben distribuirse uniformemente para alimentar la cerradura y minimizar la pérdida de potencia.

3.3 Proceso de instalación

3.3.1 Montaje en pared

Procedimiento

Paso 1 Afloje un tornillo en la parte inferior del dispositivo y retire el panel posterior.

Paso 2 Según la posición del orificio del panel posterior, taladre 4 orificios en la pared e inserte tubos de expansión en los orificios.

Para el cableado dentro de la pared, es necesario perforar otro orificio en la pared para realizar el cableado.

Paso 3 Utilice los cuatro tornillos autorroscantes (ST3) para fijar el panel posterior a la pared.

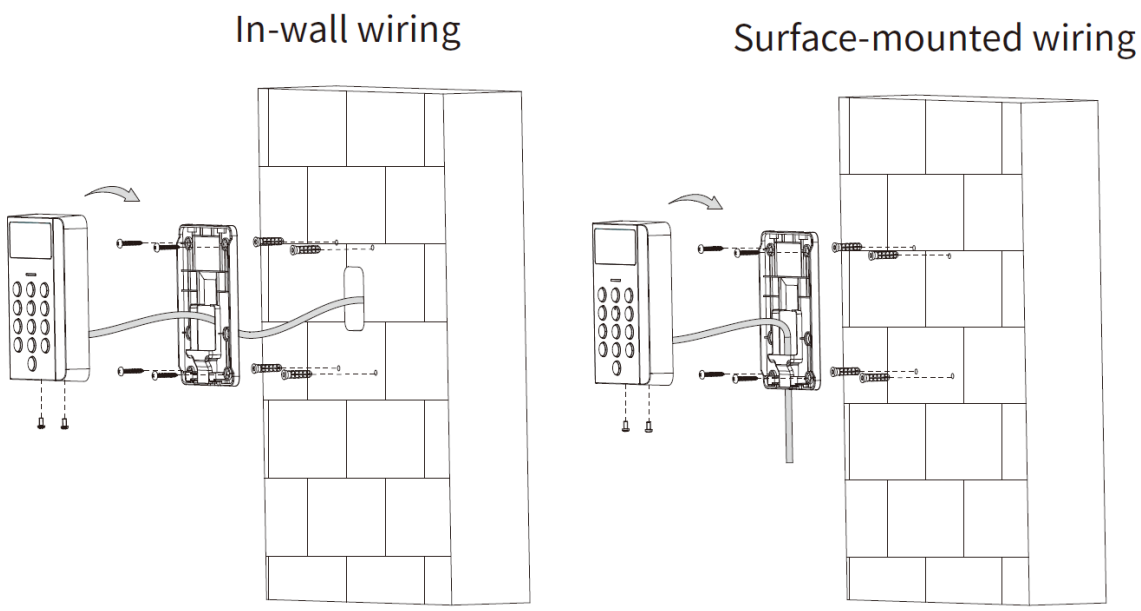
Para el cableado montado en superficie, pase el cable a través del panel posterior antes de fijar el panel posterior a la pared.

Paso 4 Conecte el dispositivo. Para más detalles, consulte "3.2

Paso 5 Cableado". Conecte el dispositivo al panel trasero.

Paso 6 Atornille firmemente dos tornillos desde la parte inferior del dispositivo.

Figura 3-7 Montaje en pared



3.3.2 86 Montaje en caja

Procedimiento

Paso 1 Afloje un tornillo en la parte inferior del dispositivo y retire el panel trasero.

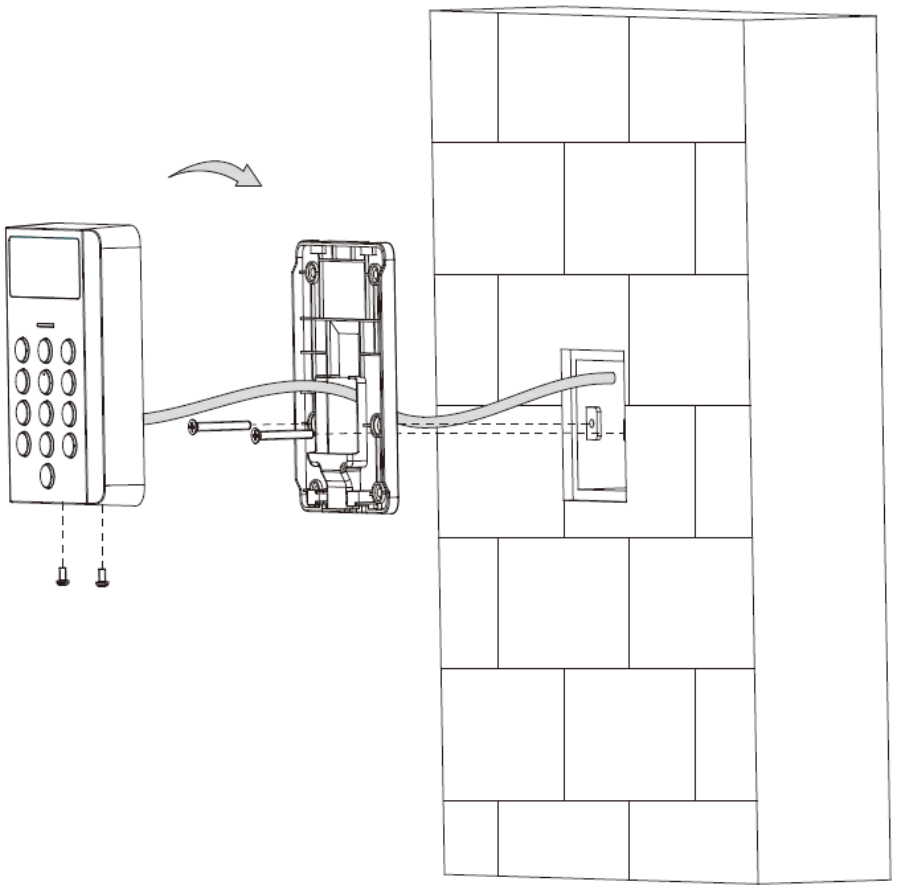
Paso 2 Monte el panel trasero en la caja 86 con dos tornillos M4.

Paso 3 Cableado del dispositivo. Para más detalles, consulte "3.2

Paso 4 Cableado". Conecte el dispositivo al panel trasero.

Paso 5 Atornille firmemente 2 tornillos desde la parte inferior del dispositivo.

Figura 3-8 Montaje de 86 cajas



4 Configuración

4.1 Inicialización

Tras encender el dispositivo por primera vez, deberá configurar la contraseña de administrador. Esta contraseña se utiliza para acceder al menú principal.

Procedimiento

Paso 1 Encienda el dispositivo y la luz indicadora parpadeará lentamente en rojo.

Paso 2 Presione**#**, ingrese la contraseña de administrador y luego presione**#**.

La contraseña debe tener entre 1 y 8 caracteres.

Si la luz indicadora está en azul fijo, significa que el dispositivo está inicializado.

4.2 Menú principal

Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

- El indicador parpadea en azul y significa que has ingresado al menú principal.
- El indicador parpadea en rojo una vez, el zumbador genera un pitido y luego el indicador se vuelve azul fijo, lo que significa que la contraseña es incorrecta.

4.3 Indicaciones

- El indicador parpadea en verde una vez y el zumbador emite un pitido, lo que significa que la operación o la verificación del control de acceso es exitosa.
- El indicador parpadea en rojo una vez y el zumbador emite tres pitidos, lo que significa que la operación o la verificación del control de acceso falló.
- Si el indicador parpadea en rojo lentamente significa que el dispositivo no está inicializado.
- Si el indicador está en azul fijo, significa que el dispositivo está en estado de espera.
- El indicador parpadea en azul, significa que el dispositivo ingresa al menú principal.

4.4 Gestión de usuarios

4.4.1 Agregar usuarios

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadeará en azul.

Paso 2 Presione**1**y**#**para agregar usuarios.

Paso 3 Después de pasar la tarjeta, presione**#**Para agregar la tarjeta,

Paso 4 ingrese la contraseña de usuario y luego presione**#**.

Si no necesita configurar la contraseña de usuario, presione**#**Para saltártelo.

La contraseña puede tener entre 1 y 8 caracteres.

Paso 5 Repetir Paso 3 a Paso 4 para agregar más usuarios.

Después de agregar el usuario, presione ***** para volver al menú principal y luego presione ***** para volver al estado de espera.

4.4.2 Eliminación de usuario

Procedimiento

Paso 1 Prensa **#**, ingrese la contraseña de administrador y luego presione **#**.

Ingrese al menú principal y el indicador parpadeará en azul.

Paso 2 Presione **2** y **#**.

Paso 3 Eliminar un usuario.

- Pase la tarjeta y luego presione **#**.

  Si pasa una tarjeta que no ha sido agregada, la eliminación fallará.
- Ingrese 0000 y luego presione **#** para eliminar todos los usuarios.

Después de eliminar, presione ***** para volver al menú principal y luego presione ***** para salir del menú principal.

4.5 Configuración del modo de desbloqueo de puertas

Procedimiento

Paso 1 Prensa **#**, ingrese la contraseña de administrador y luego presione **#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione **3** y **#**.

Paso 3 Seleccione el modo de desbloqueo.

- Prensa **0** y **#** para configurar el desbloqueo con tarjeta.
- Prensa **1** y **#** para configurar el desbloqueo mediante tarjeta y contraseña de usuario.

Paso 4 Prensa ***** para salir del menú principal.

4.6 Configuración de la duración del desbloqueo

La puerta permanece abierta después de un tiempo definido después de desbloquearse, lo que permite el paso de personas.

Procedimiento

Paso 1 Prensa **#**, ingrese la contraseña de administrador y luego presione **#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione **4** y **#**.

Paso 3 Introduzca la hora y luego presione **#**.

El valor varía de 1 s a 600 s. El valor predeterminado es 3 s. Pulse *****

Paso 4 para salir del menú principal.

4.7 Configuración del sensor de puerta

Tras activar el sensor de puerta, la alarma de tiempo de espera se activa simultáneamente de forma predeterminada. Si la puerta permanece abierta después del tiempo de espera establecido, el zumbador del dispositivo genera alarmas.

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione**5**y**#**.

Paso 3 Habilitar o deshabilitar el sensor de puerta.

El sensor de puerta está deshabilitado de forma predeterminada.

- Prensa**0**y**#**para habilitar el sensor de la puerta.
- Prensa**1**y**#**para desactivar el sensor de la puerta.

Paso 4 Prensa*****para salir del menú principal.

4.8 Gestión de contraseñas

4.8.1 Cambiar la contraseña del administrador

Para garantizar la seguridad del dispositivo, le recomendamos que cambie la contraseña de administrador de vez en cuando.

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione**0**y**#**.

Paso 3 Ingrese la nueva contraseña y luego presione**#**Ingrese

Paso 4 nuevamente la nueva contraseña y luego presione**#**. Prensa

Paso 5 *****para salir del menú principal.

4.8.2 Agregar contraseña pública

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione**6**y**#**.

Paso 3 Ingrese la contraseña pública y luego presione**#**.

La contraseña puede tener entre 1 y 8 caracteres.

Puedes agregar hasta 500 contraseñas públicas. Repite el paso 3 para agregar más. No se pueden repetir las contraseñas públicas.

Paso 4 Prensa*****para salir del menú principal.

4.8.3 Eliminación de la contraseña pública

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione**7**y**#**.

Paso 3 Ingrese la contraseña pública y presione**#**.

Repita el paso 3 si desea eliminar más contraseñas públicas.

Paso 4 Presione*****para salir del menú principal.

4.9 Gestión de la tarjeta principal

4.9.1 Agregar tarjeta principal

Después de agregar la tarjeta principal, puede agregar y eliminar rápidamente otras tarjetas de usuario a través de la tarjeta principal.

Información de fondo

La tarjeta principal no se puede utilizar para desbloquear la puerta.

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione**8**y**#**.

Paso 3 Pase la tarjeta y luego presione**#**.

Las tarjetas de usuario que se hayan agregado también se pueden configurar como tarjeta principal.

- Si una tarjeta de usuario está configurada como tarjeta principal, no podrá desbloquear la puerta.
- Solo admite una tarjeta principal. Si se añade una nueva, se sobrescribirá la anterior.

Paso 4 Prensa*****para salir del menú principal.

4.9.2 Eliminación de la tarjeta principal

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadeará en azul.

Paso 2 Presione**9**y**#**.

Paso 3 Pase la tarjeta y presione**#**. Prensa

Paso 4 *****para salir del menú principal.

4.9.3 Gestión de tarjetas de usuario a través de la tarjeta principal

Si no se realiza ninguna operación durante 3 segundos después de pasar la tarjeta principal, el dispositivo entra en modo de tarjeta principal y determinará la función correspondiente según las veces que se haya pasado. En modo de tarjeta principal, el indicador parpadea en rojo y azul alternativamente. Si no se realiza ninguna operación durante 10 segundos o se vuelve a pasar la tarjeta principal una vez, vuelve al modo de espera.

- Añadir tarjeta de usuario: Deslice la tarjeta principal una vez y, a continuación, la tarjeta de usuario para añadirla. Se pueden añadir tarjetas de usuario continuamente.
- Eliminar la tarjeta de usuario: Deslice la tarjeta principal dos veces y, a continuación, deslice la tarjeta de usuario para eliminarla. Las tarjetas de usuario se pueden eliminar continuamente.
- Borrar todas las tarjetas de usuario: Pase la tarjeta principal 5 veces seguidas.

4.10 Configuración del período de tiempo de espera de la puerta

Una vez habilitado el sensor de puerta, si la puerta permanece abierta después del tiempo establecido, el zumbador del dispositivo emitirá una alarma.

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadea en azul.

Paso 2 Presione**10**y**#**.

Paso 3 Ingrese el período de tiempo de espera de la puerta y luego presione**#**.

El rango de valores va de 1 s a 9999 segundos. El valor predeterminado es 60 segundos. Pulse

Paso 4 *****para salir del menú principal.

4.11 Restaurar la configuración de fábrica

Procedimiento

Paso 1 Prensa**#**, ingrese la contraseña de administrador y luego presione**#**.

Ingrese al menú principal y el indicador parpadeará en azul.

Paso 2 Presione**11**y**#**.

Paso 3 Restaurar el dispositivo a la configuración de fábrica.

- Prensa**00**y**#**para restaurar la configuración de fábrica (conservar la información del usuario).
- Prensa**000**y**#**para restaurar la configuración de fábrica (restaurar toda la información).

4.12 Desbloqueo de la puerta

4.12.1 Desbloqueo con tarjeta

Pase la tarjeta de usuario para desbloquear la puerta.

Si una tarjeta de usuario está configurada como tarjeta principal, no podrá desbloquear la puerta.

4.12.2 Desbloqueo con Tarjeta + Contraseña

Si configura el modo de desbloqueo en**Tarjeta + Contraseña**,Deslice la tarjeta de usuario e ingrese la contraseña de usuario y luego presione**#**Para desbloquear la puerta.

4.12.3 Desbloqueo mediante contraseña pública

Ingrese la contraseña pública y luego presione**#**Para abrir la puerta. Para más detalles sobre cómo configurar contraseñas públicas, consulte "4.8.2 Añadir contraseña pública".

La contraseña pública se puede utilizar para desbloquear la puerta en cualquier modo de desbloqueo.

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 contenga el nombre de la cuenta ni el nombre de la cuenta en orden inverso;
- No utilice caracteres continuos, como 123, abc, etc.;
- No utilice caracteres 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 descifrada.

3.**Asignar cuentas y permisos de forma adecuada**

Agregue usuarios de forma adecuada 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 por defecto. Se recomienda mantenerla habilitada para proteger la seguridad de la cuenta. Tras varios intentos fallidos de contraseña, la cuenta y la dirección IP de origen correspondientes 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 cibercriminales, si se produce algún cambio en la información, modifíquela a tiempo. 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 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 encriptada para reducir el riesgo de que sus datos de audio y video sean interceptados durante la transmisión.

3.**Desactiva los servicios no esenciales y utiliza el modo seguro**

Si no es necesario, se recomienda desactivar algunos servicios como SSH, SNMP, SMTP, UPnP, AP hotspot, 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 buzón.
- 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 ser adivinado por actores de amenazas.

Configuración de red

1.**Habilitar lista de permitidos**

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

2.**Vinculación de direcciones 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.**Construir 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 intranet desde la red externa;
- De acuerdo con 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 particionar la red para lograr el aislamiento de la red;
- Establecer un sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso ilegal a terminales de la red privada.

Auditoría de seguridad

1.**Comprobar usuarios en línea**

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

2.**Comprobar 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 un periodo 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 seguimiento.

Seguridad del software

1.**Actualizar el firmware a tiempo**

Según las especificaciones operativas estándar de la industria, el firmware de los dispositivos debe actualizarse a la última versión oportunamente para garantizar que cuenten con las funciones y la seguridad más recientes. Si el dispositivo está conectado a la red pública, se recomienda activar 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.**Actualice el software del cliente a tiempo**

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

Protección física

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

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