Lector de acceso

Manual de usuario

V1.1.1

Prefacio

General

Este manual presenta las funciones y operaciones del Lector de Acceso (en adelante denominado Lector de Tarjetas). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para consultarlo en el futuro.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Significado
DANGER	Indica un alto riesgo potencial 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.
TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
NOTE	Proporciona información adicional como complemento al texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.1.1	Actualizado el manual.	diciembre 2023

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otras personas, como su rostro, audio, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: Proporcionar una identificación clara y visible para informar a las personas sobre la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del Manual

- El manual es sólo para referencia. Pueden encontrarse ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas incurridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es sólo para referencia. Es posible que se encuentren ligeras diferencias entre la versión electrónica y la versión en papel.

- Todos los diseños y software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones de productos pueden provocar que aparezcan algunas diferencias entre el producto real y el manual. Comuníquese con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Pueden existir errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en este manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de dar una explicación final.

Salvaguardias y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del lector de tarjetas, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el lector de tarjetas y cumpla con las pautas al usarlo.

Requisito de transporte

Transporte, utilice y almacene el Lector de Tarjetas bajo las condiciones permitidas de humedad y temperatura.

Requisito de almacenamiento

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

requerimientos de instalación

- 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 el voltaje ambiental sea estable y cumpla con los requisitos de suministro de energía del controlador de acceso.
- No conecte el lector de tarjetas a dos o más tipos de fuentes de alimentación para evitar daños al lector de tarjetas.
- El uso inadecuado de la batería podría provocar un incendio o una explosión.

- El personal que trabaja en alturas debe tomar todas las medidas necesarias para garantizar la seguridad personal, incluido el uso de casco y cinturones de seguridad.
- No coloque el Lector de Tarjetas en un lugar expuesto a la luz solar o 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 bloquee su ventilación.
- Utilice un adaptador o fuente de alimentación de gabinete proporcionado por el fabricante.
- Utilice los cables de alimentación recomendados para la región y cumplan con las especificaciones de potencia nominal.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en el estándar IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de suministro de energía 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 conexión a tierra de protección.

Requisitos de operación

- Compruebe si la fuente de alimentación es correcta antes de su uso.
- No desenchufe el cable de alimentación en el costado del lector de tarjetas mientras el adaptador esté encendido.
- Opere el lector de tarjetas dentro del rango nominal de entrada y salida de energía.
- Utilice el lector de tarjetas en las condiciones permitidas de humedad y temperatura.
- 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 instrucción profesional.

Tabla de contenido

1. Información general

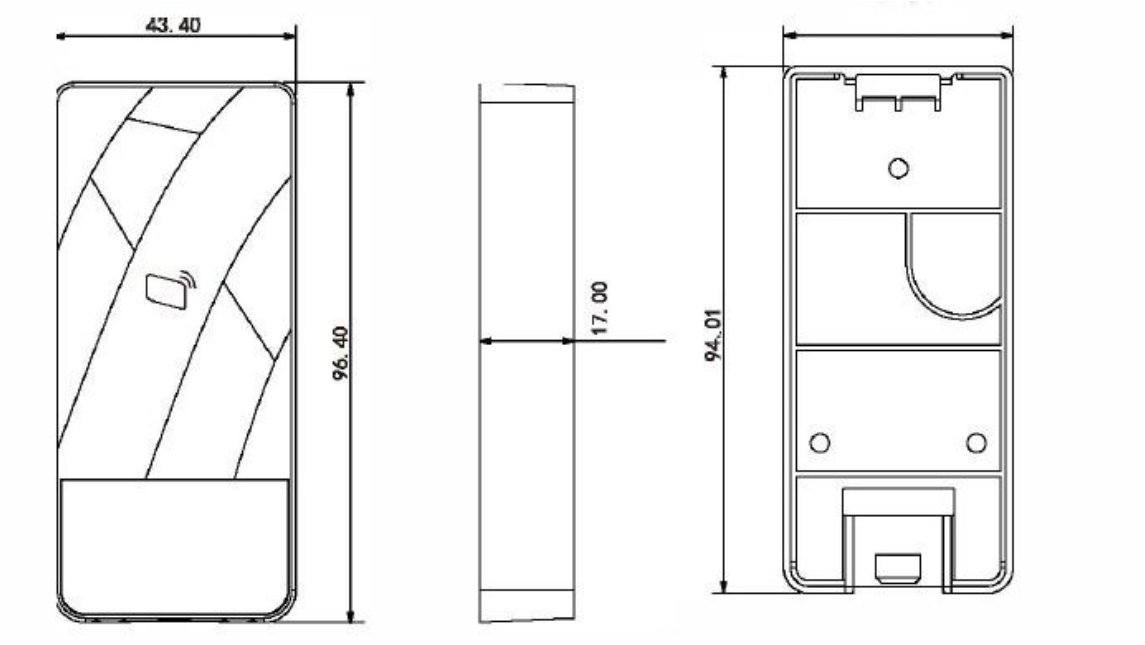
En la mayoría de los sistemas de control de acceso, un lector de tarjetas de control de acceso es un sistema de seguridad que requiere deslizar una tarjeta de credencial para verificar que la persona que ingresa a la habitación/espacio esté libre. Es adecuado para una amplia variedad de escenas, como edificios de oficinas, escuelas, complejos, comunidades, fábricas, lugares públicos, centros de negocios y edificios gubernamentales.

Las características principales son las siguientes.

- El lector sin contacto (solo lectura) tiene una distancia de lectura de 2,5 cm a 5,5 cm y un tiempo de respuesta <0,3 s.
- Soporta protocolo Wiegand y protocolo RS-485. La velocidad en baudios de RS485 es de 9600 bps.
- Admite la función de vigilancia.
- Todos los puertos tienen protección contra sobrecorriente y sobretensión.
- Nivel de protección: IP67. Apto para instalación en exteriores. La temperatura de trabajo es de -30 °C a +60 °C y la humedad de trabajo es≤95%.
- Soporta zumbador y luz indicadora.

1.1 Apariencia

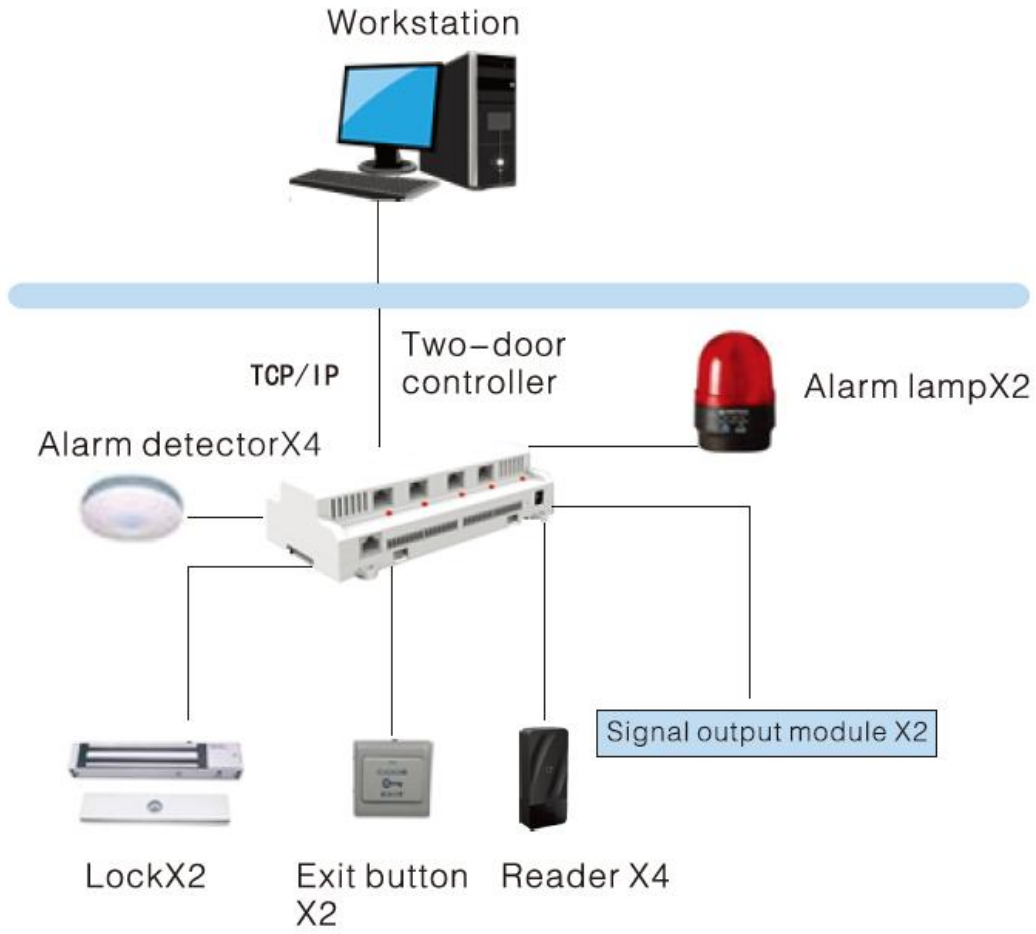
Figura 1-1 Dimensiones (mm])



1.2 Diagrama de red

El diagrama de red es solo como referencia.

Figura 1-2 Diagrama de red



2 cableado

Tabla 2-1 Descripción del cableado

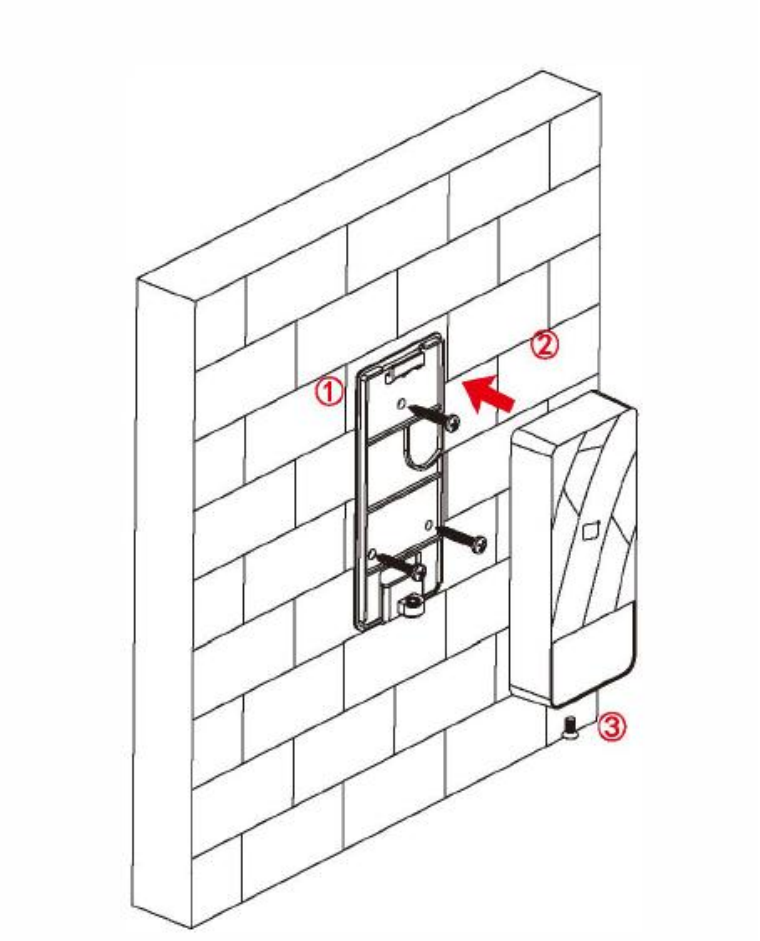
Color	Puerto	Descripción
Rojo	12 voltios	Fuente de alimentación (12 VCC)
Negro	Tierra	Cable de tierra
Azul	CASO	Señal de alarma de manipulación
Blanco	D1	Señal de transmisión Wiegand (efectivo sólo cuando se utiliza el protocolo Wiegand)
Verde	D0	
Marrón	CONDUJO	Señales de respuesta Wiegand (efectivas solo cuando se utiliza el protocolo Wiegand)
Amarillo	RS485-	Cable RS485 negativo (efectivo sólo cuando se utiliza el protocolo RS-485)
Púrpura	RS485+	Cable RS485 positivo (efectivo sólo cuando se utiliza el protocolo RS-485)

3 Instalación

Procedimiento

Paso 1 Fije la cubierta trasera a la pared con tornillos autorroscantes.

Figura 3-1 Instalación



Paso 2 Coloque la cubierta frontal en el gancho en la parte superior de la cubierta

Paso 3 trasera. Atornille un tornillo en la parte inferior del lector de tarjetas.

Apéndice 1 Recomendaciones de ciberseguridad

Acciones obligatorias a tomar 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 incluya 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 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 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 “autoverificación 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 "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 y un gabinete especiales, e implemente permisos de control de acceso y administración de claves bien hechos para evitar que personal no autorizado lleve a cabo contactos físicos como daños en el hardware, conexión no autorizada de equipos extraíbles (como discos flash USB). , puerto serie), etc.

2.**Cambie las contraseñas con regularidad**

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de que las adivinen o las descifren.

3.**Establecer y actualizar contraseñas Restablecer información oportunamente**

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 sobre protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar preguntas de protección con contraseña, se sugiere no utilizar aquellas que puedan adivinarse fácilmente.

4.**Habilitar bloqueo de cuenta**

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

5.**Cambiar HTTP predeterminado y otros puertos de servicio**

Le sugerimos que cambie 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 habilitar 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 equipo, reduciendo así el riesgo de suplantación de ARP.

8.**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.

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 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 cifrado WPA2-PSK y configure contraseñas seguras.

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

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

Recordatorio: la transmisión cifrada provocará cierta pérdida en la eficiencia de la transmisión.

11.**Auditoría segura**

- Verifique los usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo inició sesión 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.

12.**Registro de red**

Debido a la capacidad de almacenamiento limitada del equipo, 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 estén sincronizados con el servidor de registro de red para su seguimiento.

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

Para garantizar mejor la seguridad de los equipos y reducir los posibles riesgos cibernéticos, recomendamos:

- Deshabilite la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa.
- La red debe dividirse y aislarse según las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere utilizar 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.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts permitidos para acceder al dispositivo.