Acceso al lector

Manual del usuario



V1.1.4

Prefacio

General

Este manual presenta las funciones y operaciones del lector Access (en adelante, el lector de tarjetas). Lea atentamente antes de utilizar el dispositivo y guarde el manual para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de señal	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.
NOTE	Proporciona información adicional como complemento al texto.

Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
V1.1.4	Se agregaron requisitos de cableado.	Septiembre de 2024
V1.1.3	Se agregó la descripción del cableado.	Abril de 2024
V1.1.2	Se actualizó el cableado descripción.	Abril de 2024
Versión 1.1.1	Se actualizó el manual.	Diciembre de 2023

Aviso de protección de la privacidad

Como usuario del dispositivo o responsable del tratamiento de datos, es posible que recopile 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 de la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del manual

- El manual es solo de referencia. Pueden 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 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 solo para referencia. Pueden encontrarse 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 provocar 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 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 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 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 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.

Requerimientos de transporte



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

Requisito de almacenamiento



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

Requisitos de instalación



- No conecte el adaptador de corriente al lector de tarjetas mientras el adaptador esté encendido.
- Cumpla estrictamente con los códigos y estándares de seguridad eléctrica locales. 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 dañar el lector de tarjetas.
- El uso inadecuado de la batería podría provocar un incendio o una explosión.



- 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 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 en 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 una fuente de alimentación de armario 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 en la norma IEC 62368-1 y no 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 conexión a tierra.

Requisitos de funcionamiento



- Compruebe si la fuente de alimentación es correcta antes de usarlo.
- No desconecte el cable de alimentación del costado del lector de tarjetas mientras el adaptador esté encendido.
- Utilice el lector de tarjetas dentro del rango nominal de entrada y salida de energía.
- Utilice el lector de tarjetas en las condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquidos sobre el lector de tarjetas y asegúrese de que no haya ningún objeto lleno de líquido sobre el lector de tarjetas que evite que el líquido fluya hacia él.
- No desmonte el lector de tarjetas sin instrucciones profesionales.

Tabla de contenido

Prólogo..... I

Medidas de seguridad y advertencias importantes..... III

1 Descripción general.....1

1.1 Apariencia..... 1

1.2 Diagrama de red..... 2

2 Requisitos de cableado.....3

3 Instalación..... 4

Apéndice 1 Recomendaciones de seguridad.....5

1 Descripción general

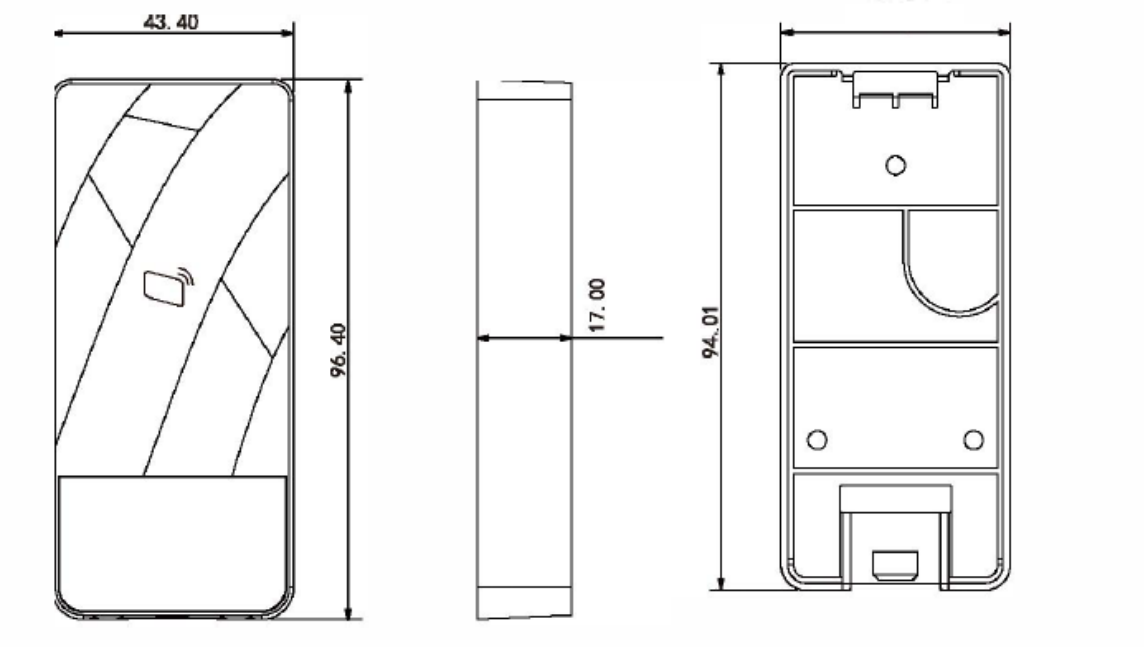
En la mayoría de los sistemas de control de acceso, un lector de tarjetas de control de acceso es un sistema de seguridad que requiere pasar una tarjeta de identificación para verificar que la persona que ingresa a la habitación o espacio está autorizada. Es adecuado para una amplia variedad de escenarios, como edificios de oficinas, escuelas, complejos, comunidades, fábricas, lugares públicos, centros comerciales 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 de < 0,3 s.
- Admite el protocolo Wiegand y el protocolo RS-485. La velocidad en baudios del protocolo RS485 es de 9600 bps.
- Admite función de vigilancia.
- Todos los puertos tienen protección contra sobrecorriente y sobretensión.
- Nivel de protección: IP67. Apto para instalación en exteriores. La temperatura de funcionamiento es de -30 °C a +60 °C y la humedad de funcionamiento es ≤95 %.
- Admite zumbador y luz indicadora.

1.1 Apariencia

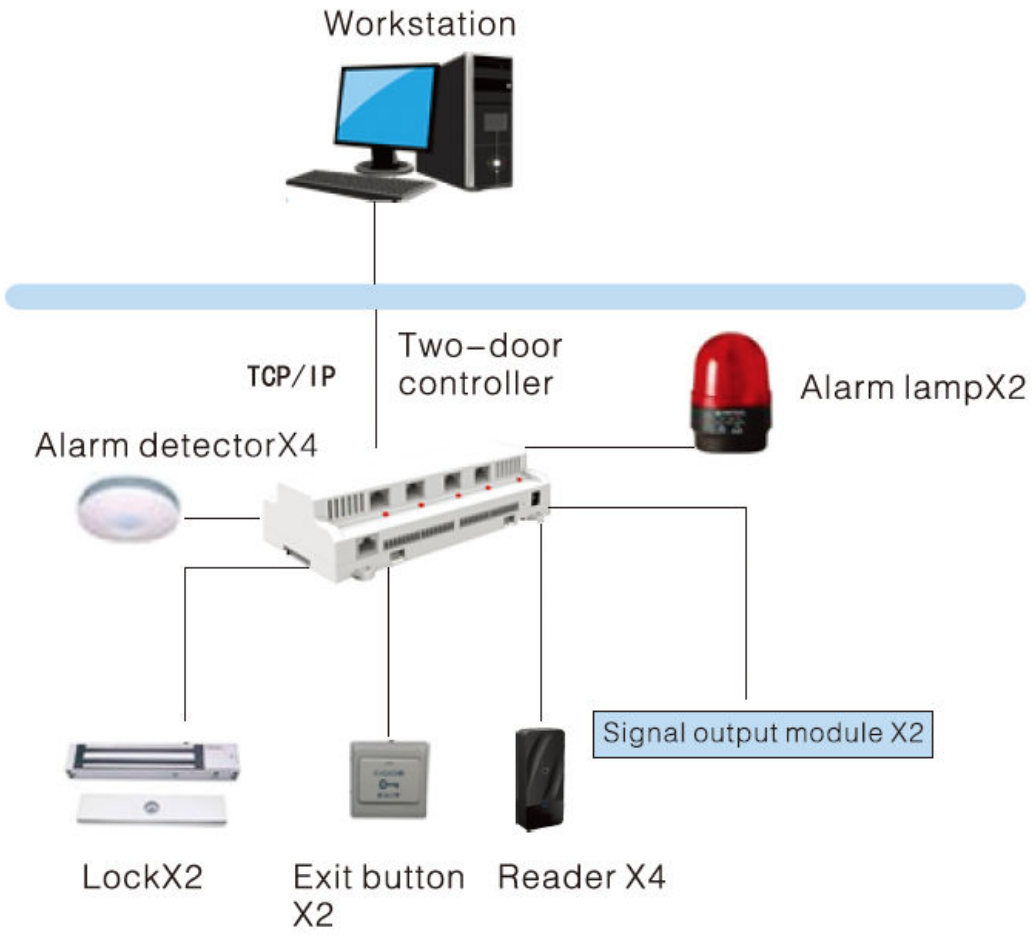
Figura 1-1 Dimensiones (mm)



1.2 Diagrama de red

El diagrama de red es sólo para referencia.

Figura 1-2 Diagrama de red



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 de los cables.

Tabla 2-1 Descripción del cableado

Color	Puerto	Descripción
Rojo	12 voltios	Fuente de alimentación (12 VCC)
Negro	Tierra	Cable de puesta a tierra
Azul	CASO	Señal de alarma de manipulación La función no está disponible actualmente.
Blanco	D1	Señal de transmisión Wiegand (efectiva solo cuando se utiliza el protocolo Wiegand)
Verde	D0	
Marrón	CONDUJO	Señales sensibles a Wiegand (efectivas solo cuando se utiliza el protocolo Wiegand)
Amarillo	RS485-	Cable negativo RS-485 (efectivo solo cuando se utiliza el protocolo RS-485) No se admite la actualización del dispositivo a través de RS-485.
Púrpura	RS485+	Cable positivo RS-485 (efectivo solo cuando se utiliza el protocolo RS-485) No se admite la actualización del dispositivo a través de RS-485.

Tabla 2-2 Requisitos de cableado del lector de tarjetas

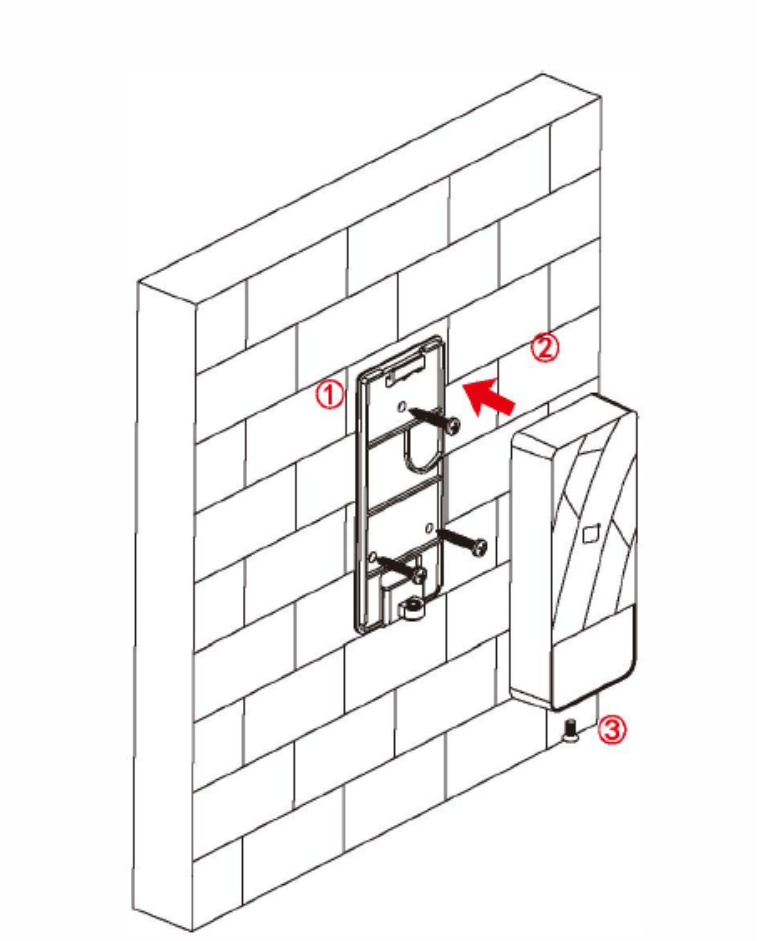
Tipo	Requisitos de impedancia	Requisitos de longitud
Lector de tarjetas RS485	Conecta cables RS-485 y la impedancia de un solo cable debe ser ≤ 10 Ω.	≤ 100 metros. Por encima de UL1061 24AWG Los cables blindados son recomendado.
Lector de tarjetas Wiegand	Conecta cables Wiegand y la impedancia de un solo cable debe ser ≤ 2 Ω.	≤ 80m. Por encima de UL1061 18AWG Los cables blindados son recomendado.

3 Instalación

Procedimiento

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

Figura 3-1 Instalación



Paso 2 Coloque la tapa frontal en el gancho que se encuentra en la parte superior de la tapa

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

Apéndice 1 Recomendaciones 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 de forma predeterminada. Se recomienda mantenerla habilitada para proteger la seguridad de la cuenta. Después de varios intentos fallidos de ingresar la contraseña, se bloquearán la cuenta correspondiente y la dirección IP de origen.

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 actores maliciosos, si hay algún cambio en la información, modifíquela a tiempo. Al configurar las preguntas de seguridad, se recomienda no utilizar respuestas fáciles de adivinar.

Configuración del servicio

1.**Habilitar HTTPS**

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

2.**Vinculación de dirección 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, particione 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 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 realizar el seguimiento.

Seguridad del software

1.**Actualizar el firmware a tiempo**

De acuerdo con las especificaciones operativas estándar de la industria, el firmware de los dispositivos debe actualizarse a la última versión a tiempo para garantizar que el dispositivo tenga las últimas funciones y seguridad. Si el dispositivo está conectado a la 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.**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).