Producto antirrobo para supermercados

Manual del usuario

Versión 1.0.0

Prefacio

Este manual presenta la introducción y el funcionamiento del producto antirrobo para supermercados. Lea atentamente antes de utilizar el producto y guarde el manual para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de señal categorizadas con un significado definido pueden aparecer en el manual.

Palabras de señal	Descripciones
	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
	Indica equipo sensible a la electrostática.
	Indica peligro de alto voltaje.
	Indica fuerte radiación láser.
	Indica piezas móviles peligrosas, manténgase alejado de las aspas del ventilador en movimiento.
	Indica que partes del equipo causarán heridas mecánicas a las personas.
	Proporciona métodos para ayudarle a resolver un problema o ahorrarle tiempo.
	Proporciona información adicional como énfasis y complemento al texto.

Historial de revisiones

Versión	Contenido de la revisión	Fecha de lanzamiento
Versión 1.0.0	Primer lanzamiento.	Noviembre de 2024

Aviso de protección de la privacidad

Como usuario del producto 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 sobre 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 detector, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el detector y cumpla con las pautas al usarlo.

Requisitos de transporte

- Transporte el detector en las condiciones de humedad y temperatura permitidas.
- Embale el controlador con el embalaje proporcionado por su fabricante o un embalaje de la misma calidad antes de transportarlo.

Requisitos de almacenamiento

-Guarde el detector en las condiciones de humedad y temperatura permitidas.

Requisitos de instalación

- Instale el detector en un lugar bien ventilado y no bloquee la ventilación del detector.

- Se recomienda que el dispositivo se instale a 2 metros de distancia de equipos de tipo motor grande (como ascensores, fuentes de alimentación conmutadas de alta potencia) para evitar interferencias.

Requisitos de funcionamiento

-Utilice el detector en las condiciones de humedad y temperatura permitidas.

Requisitos de mantenimiento

- Utilice los cables de alimentación recomendados en la región y que cumplan con la especificación de potencia nominal.
- Utilice únicamente el adaptador de corriente estándar del dispositivo; de lo contrario, el usuario será responsable de lesiones personales o daños al dispositivo.
- La fuente de alimentación deberá cumplir con los requisitos de la norma de voltaje extra bajo de seguridad (SELV) y suministrar energía con un voltaje nominal que cumpla con la norma de potencia limitada.

Requisito de fuente según（IEC60065）o（IEC60950-1.) Tenga en cuenta que los requisitos de alimentación están sujetos a la etiqueta del dispositivo.

- Debe estar estrictamente conectado a tierra y alimentado de forma independiente. Se recomienda no trabajar con otros equipos eléctricos.

- Evite que los líquidos salpiquen o goteen sobre el dispositivo. Asegúrese de que no haya objetos que contengan líquido sobre el dispositivo para evitar que los líquidos fluyan hacia él.
- No presione con fuerza, no vibre violentamente ni sumerja el dispositivo.
- Realice bien el trabajo de conexión a tierra para mejorar la capacidad antiinterferencia del dispositivo.

Tabla de contenido

Prólogo..... I
Medidas de seguridad y advertencias importantes.....III 1
Descripción general..... 6
1.1 Introducción..... 6
2 Instalación..... 7
2.1 Lista de verificación 7
2.2 Asuntos que requieren atención.....7
Appendix 1 Recomendaciones de ciberseguridad..... 8

1.1 Introducción

Los productos antirrobo para supermercados, combinados con sus propias ventajas y características, pueden desempeñar un papel de alarma en el proceso de robo de productos, no limitado a la iluminación y el sonido, previniendo el robo de productos y desempeñando un papel importante en la prevención de pérdidas para varios minoristas. Los productos antirrobo para supermercados son adecuados para varios escenarios, como supermercados, centros comerciales, tiendas de ropa, etc.

2 Instalación

2.1 Lista de verificación

Después de recibir el producto del transportista, abra la caja y consulte la hoja siguiente. Si hay algún problema, póngase en contacto con su distribuidor local o con un técnico de servicio para obtener ayuda.

Tabla 2-1 Lista de verificación

No.	Artículo		Descripción
1	En general embalaje	Apariencia	No hay daños evidentes.
		Embalaje	No distorsionado ni roto.
		Accesorio	No falta ninguna.
2	Anfitrión	Apariencia	No hay daños evidentes.
		Modelo	Coincide con la orden de compra.
		Etiquetas en el Dispositivo	No roto. No arranque ni tire las etiquetas, ya que de lo contrario se pueden perder los servicios de garantía. Debe proporcionar el número de serie del dispositivo cuando llame al servicio posventa.

2.2 Asuntos que requieren atención

- Mantener alejado de objetos metálicos grandes y estáticos.
- Manténgase alejado de fuentes de interferencia electromagnética y de fuentes de radiación electromagnética. El
- dispositivo debe estar estrictamente conectado a tierra.

  Para garantizar la seguridad personal y del dispositivo, mejorar la capacidad antiinterferencias del dispositivo y mejorar la distancia de detección, el dispositivo debe estar conectado a tierra de manera confiable de acuerdo con las regulaciones.
- Mantenga separados los cables eléctricos y electrónicos.
- Lo eléctrico y lo electrónico son propensos a influenciarse mutuamente y causar problemas de seguridad, por lo que los dos cableados deben estar separados.

  Las siguientes pueden ser fuentes de interferencia EM y fuentes de radiación EM que afectan al producto: gabinetes de control eléctrico, dispositivos de RF, computadoras y dispositivos periféricos, monitores de video, motores de alta potencia, transformadores de alta potencia, cables de CA, circuitos de tiristores (fuente de alimentación conmutada de alta potencia, máquinas de soldar con inversor), motores, máquinas con motor y lámparas fluorescentes con balastos electrónicos convencionales.

Appendix 1 Recomendaciones de ciberseguridad

Acciones obligatorias que se deben tomar para la seguridad básica de la red del dispositivo:

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 caracteres; 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 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 esté conectado a la red pública, se recomienda habilitar la función de "comprobación automática de actualizaciones" para obtener información oportuna sobre las actualizaciones de firmware publicadas por el fabricante.

- Le sugerimos que descargue y utilice la última versión del software del cliente.

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

Le sugerimos que proteja físicamente el dispositivo, especialmente los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras y un gabinete especiales e implemente un control de acceso y una gestión de claves bien hechos para evitar que personal no autorizado realice contactos físicos, como dañar el hardware, conectar sin autorización dispositivos extraíbles (como un disco flash USB, un puerto serial), etc.

2. Cambie las contraseñas periódicamente

Le sugerimos que cambie sus contraseñas periódicamente para reducir el riesgo de que sean adivinadas o descifradas.

3. Establezca y actualice la información de restablecimiento de contraseñas de manera oportuna

El dispositivo admite la función de restablecimiento de contraseña. Configure a tiempo la información relacionada con el restablecimiento de contraseña, incluido el buzón de correo del usuario final y las preguntas de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar las preguntas de protección de contraseña, se recomienda no utilizar aquellas que se puedan adivinar fácilmente.

4. Habilitar bloqueo de cuenta

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

5. Cambiar el 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 externas puedan adivinar qué puertos está utilizando.

6. Habilitar HTTPS

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

7. Vinculación de direcciones MAC

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

8. Asignar cuentas y privilegios de manera razonable

Según los requisitos comerciales y de gestión, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

9. Desactivar los servicios innecesarios y elegir 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 autenticación seguras.
- SMTP: Elija TLS para acceder al servidor de buzón.
- FTP: Elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

10. Transmisión de audio y vídeo encriptados

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 que los datos de audio y video sean robados durante la transmisión.

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

11. Auditoría segura

- Comprobar usuarios en línea: le sugerimos que compruebe periódicamente los usuarios en línea para ver si el dispositivo ha iniciado sesión sin autorización.
- Comprobar el registro del dispositivo: 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 dispositivo, el registro almacenado es limitado. Si necesita guardar el registro durante un período prolongado, se recomienda que habilite 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.

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 la red externa.
- La red debe estar dividida y aislada de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se recomienda utilizar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establecer 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 a los que se les permite acceder al dispositivo.