Traducido del inglés al español - www.onlinedoctranslator.com

Módulo de extensión de control de acceso

Manual de usuario

V1.0.0

Prefacio

General

Este manual presenta las funciones, la conexión en red y las preguntas frecuentes del Módulo de extensión de control de acceso (en lo sucesivo, "el Módulo de extensión"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Sentido
DANGER	Indica un peligro de alto 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, reducción del rendimiento o resultados impredecibles.
TIPS	Proporciona métodos para ayudarlo a resolver un problema o ahorrar tiempo.
NOTE	Proporciona información adicional como suplemento al texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	marzo 2022

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otros, como su rostro, 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 proporcione la información de contacto requerida.

Sobre el Manual

- El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas sufridas 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 reglamentos de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, use nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Se pueden encontrar 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. Actualizaciones de Producto

podría dar lugar a 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 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 con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de compañías en el 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 se produce algún problema durante el uso del dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del módulo de extensión, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el módulo de extensión y cumpla con las pautas cuando lo use.

Requisito de transporte

Transporte, use y almacene el módulo de extensión en condiciones de humedad y temperatura permitidas.

Requisito de almacenamiento

Guarde el módulo de extensión en las condiciones de humedad y temperatura permitidas.

requerimientos de instalación

 WARNING

- No conecte el adaptador de corriente al módulo de extensión 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 módulo de extensión.
- No conecte el módulo de extensión a dos o más tipos de fuentes de alimentación para evitar daños al módulo de extensión.
- El uso inadecuado de la batería puede provocar un incendio o una explosión.

- El personal que trabaje en alturas debe tomar todas las medidas necesarias para garantizar su seguridad personal, incluido el uso de casco y cinturones de seguridad.
- No coloque el módulo de extensión en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el módulo de extensión alejado de la humedad, el polvo y el hollín.
- Instale el módulo de extensión en una superficie estable para evitar que se caiga.
- Instale el módulo de extensión en un lugar bien ventilado y no bloquee su ventilación.
- Utilice un adaptador o una fuente de alimentación de gabinete proporcionada por el fabricante.
- Utilice los cables de alimentación recomendados para la región y cumpla 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 la fuente de alimentación están sujetos a la etiqueta del módulo de extensión.
- El Módulo de Extensión es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del módulo de extensión esté conectada a una toma de corriente con protección a tierra.

Requisitos de operación

- Compruebe si la fuente de alimentación es correcta antes de usar.
- No desenchufe el cable de alimentación del lateral del módulo de extensión mientras el adaptador está alimentado.

en.

- Opere el módulo de extensión dentro del rango nominal de entrada y salida de energía.
- Utilice el módulo de extensión en las condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquido sobre el módulo de extensión y asegúrese de que no haya ningún objeto lleno de líquido sobre el módulo de extensión para evitar que el líquido fluya hacia él.
- No desmonte el módulo de extensión sin instrucción profesional.

Tabla de contenido

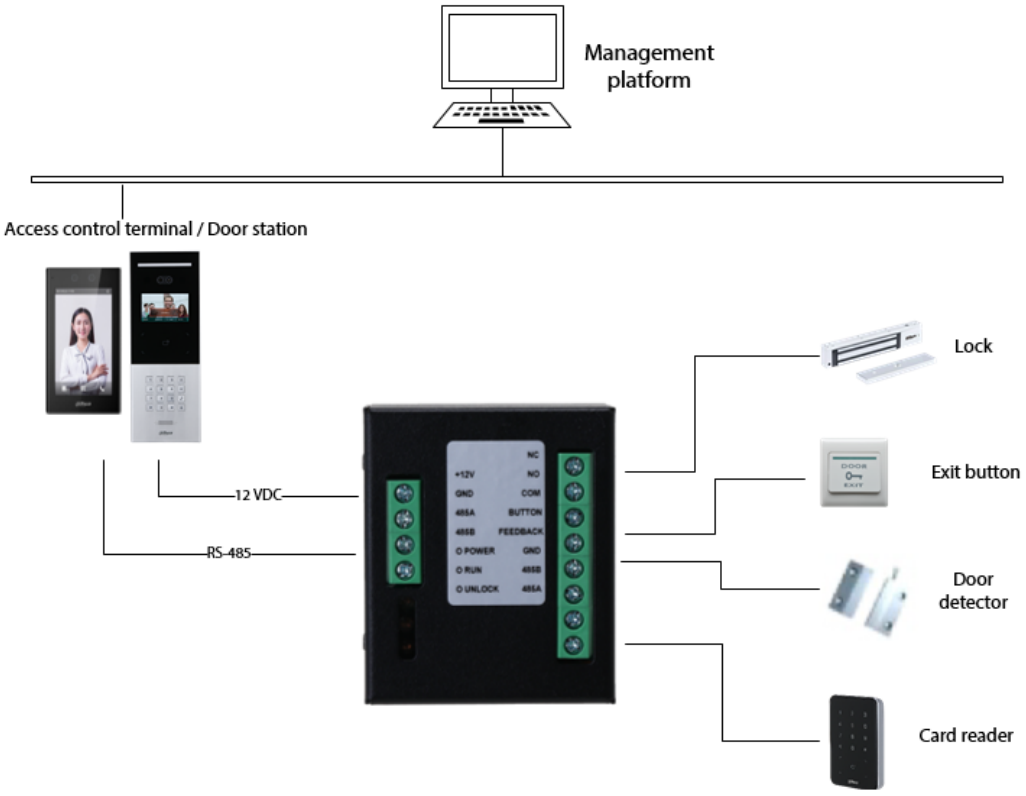
1 Introducción del producto

1.1 Resumen del producto

El módulo de extensión de control de acceso puede funcionar con el terminal de control de acceso o la estación de puerta. El Módulo de Extensión se comunica con el terminal de control de acceso o estación de puerta a través del BUS RS-485, y se conecta con detector de puerta, botón de salida, lector de tarjetas y cerradura. El módulo de extensión transmite información de tarjeta, información de puerta abierta y alarmas a la terminal de control de acceso o estación de puerta, mejorando la seguridad del control de acceso.

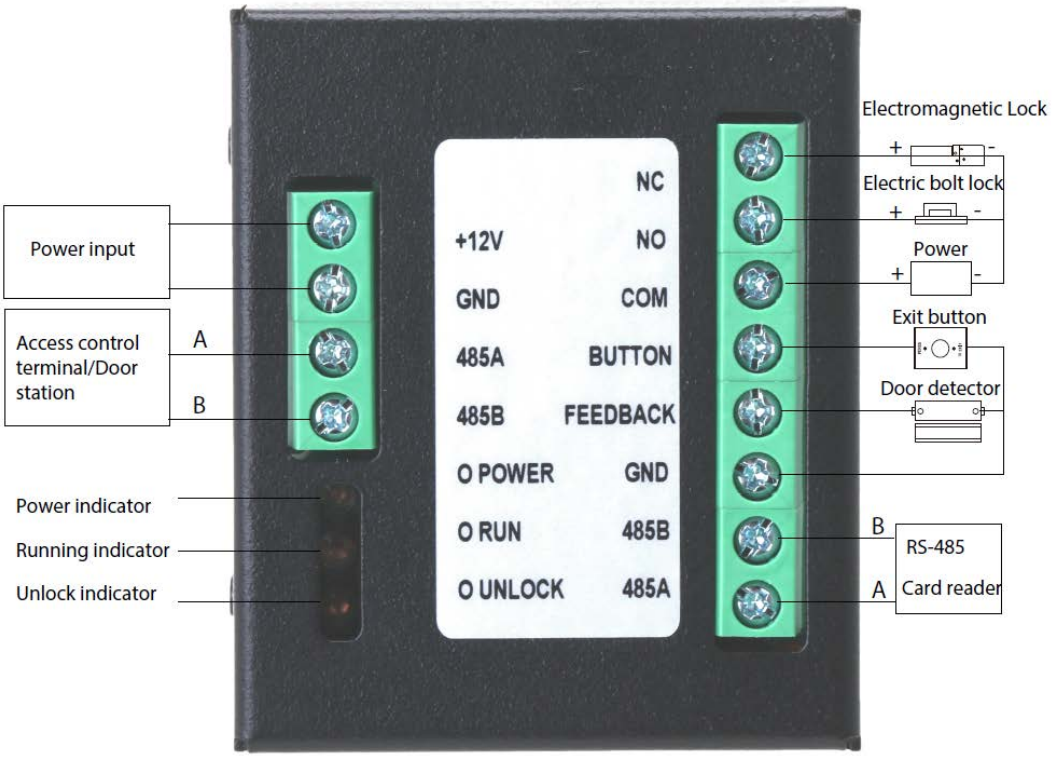
1.2 Diagrama de red

Figura 1-1 Diagrama de red



Descripción de 2 puertos

Figura 2-1 Puertos



3 preguntas frecuentes

1:**La puerta no se puede abrir cuando paso la tarjeta.**

- Consulta los datos de la tarjeta en la plataforma de gestión. Es posible que su tarjeta esté vencida o no autorizada, o que el pase de tarjeta solo esté permitido en los horarios definidos.
- La tarjeta está dañada.
- El módulo de extensión no está correctamente conectado al lector de tarjetas.
- El detector de puerta del dispositivo está dañado.

2.**El módulo de extensión no puede funcionar correctamente después de la red.**

Compruebe si la función del módulo de seguridad está activada en la interfaz web del terminal de control de acceso, o compruebe si la función de segundo bloqueo está activada en la interfaz web de la estación de puerta.

3.**La puerta no se puede abrir con el botón de salida.**

Compruebe si el botón de salida y el Módulo de extensión están bien conectados. 4.**La cerradura permanece abierta durante mucho tiempo después de que se abre la puerta.**

- Compruebe si la puerta está cerrada.
- Compruebe si el detector de puerta está bien conectado. Si no hay detector de puerta, compruebe si la función de detector de puerta está activada.

5:**Tengo otros problemas que siguen sin resolver.** Pida ayuda al soporte técnico.

4 Lista de embalaje

Verifique los artículos en la caja de embalaje de acuerdo con la lista de empaque.

Tabla 4-1 Lista de embalaje

Artículo	Cantidad
Módulo de extensión de control de acceso	1
Manual de usuario	1

Apéndice 1 Recomendaciones sobre ciberseguridad

Acciones obligatorias a realizar 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 caracteres; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos.
- No contenga el nombre de la cuenta o 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 de "verificación automática 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 "agradables de 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 un gabinete y una sala de computadoras especiales, e implemente una administración de claves y permisos de control de acceso bien hechos para evitar que personal no autorizado realice contactos físicos, como dañar el hardware, conexión no autorizada de equipos extraíbles (como un disco flash USB, puerto), etc

2.**Cambie las contraseñas regularmente**

Le sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinadas o descifradas.

3.**Establecer y actualizar contraseñas Restablecer información a tiempo**

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 de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección de contraseña, se sugiere no utilizar aquellas que se pueden adivinar fácilmente.

4.**Habilitar bloqueo de cuenta**

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

5.**Cambiar 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 ajenas puedan adivinar qué puertos está utilizando.

6.**Habilitar HTTPS**

Le sugerimos que habilite 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, así

reduciendo el riesgo de falsificación de ARP.

8.**Asigne cuentas y privilegios de manera razonable**

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios razonablemente 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 los 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 encriptación WPA2-PSK y configure contraseñas seguras.

10**Transmisión encriptada de audio y video**

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 robo de datos de audio y video durante la transmisión.

Recordatorio: la transmisión encriptada causará cierta pérdida en la eficiencia de la transmisión.

11**Auditoría segura**

- Verifique a los usuarios en línea: le sugerimos que verifique a los usuarios en línea regularmente para ver si el dispositivo está conectado sin autorización.
- Verifique el registro del equipo: al ver los registros, puede conocer las direcciones IP que se usaron para iniciar sesión en sus dispositivos y sus operaciones clave.

12**Registro de red**

Debido a la limitada capacidad de almacenamiento del equipo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, se recomienda habilitar la función de registro de red para asegurarse de que los registros críticos se sincronizan con el servidor de registro de red para su seguimiento.

13**Construir un entorno de red seguro**

Para garantizar mejor la seguridad de los equipos 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 una red externa.
- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere usar VLAN, GAP de red 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 que pueden acceder al dispositivo.