Módulo de 1 botón

Manual del usuario

Versión 1.0.0

Prefacio

General

Este manual presenta las funciones y operaciones del módulo de 1 botón (en adelante denominado "el dispositivo").

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
Versión 1.0.0	Primer lanzamiento.	Diciembre de 2024

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 torniquete, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el torniquete, cumpla con las pautas al usarlo y guarde el manual en un lugar seguro para futuras consultas.

Requerimientos de transporte

Transporte el dispositivo en condiciones de humedad y temperatura permitidas.

Requisito de almacenamiento

Conservar el dispositivo en condiciones de humedad y temperatura permitidas.

Requisitos de instalación

- No conecte el adaptador de corriente al torniquete 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 torniquete.
- No conecte el torniquete a dos o más tipos de fuentes de alimentación, para evitar dañarlo.

- Instale el torniquete sobre una superficie estable para evitar que se caiga.
- No coloque el torniquete en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el torniquete alejado de la humedad, el polvo y el hollín.
- Instale el dispositivo en un lugar bien ventilado y no bloquee su ventilación.
- Utilice un adaptador o una fuente de alimentación de armario proporcionada por el fabricante.
- 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 torniquete.
- El torniquete es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del torniquete esté conectada a una toma de corriente con conexión a tierra de protección.

Requisitos de funcionamiento

- Asegúrese de que la fuente de alimentación sea correcta antes de usar.
- No desconecte el cable de alimentación del costado del torniquete cuando el adaptador esté encendido.
- Utilice el torniquete dentro del rango nominal de entrada y salida de energía.

- Transporte, utilice y almacene el dispositivo en condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquidos sobre el torniquete y asegúrese de que no haya ningún objeto lleno de líquido sobre el torniquete que impida que el líquido fluya hacia él.
- No desmonte el torniquete sin instrucción profesional.

Requisitos de mantenimiento

- Después de la instalación, retire la película protectora y limpie el torniquete.
- Realice periódicamente un mantenimiento del torniquete para garantizar que funcione correctamente.
- Si el torniquete se instala cerca de lugares con mala calidad del aire, como la entrada de una piscina, a menos de 50 km del mar o un sitio de construcción, entonces se debe realizar un mantenimiento con mayor frecuencia en la cubierta de acero inoxidable.
- No utilice disolvente de pintura ni ningún otro agente orgánico durante el mantenimiento.
- Cuando utilice un componente de reconocimiento facial, aplique sellador de silicona impermeable en la posición de instalación.

Precauciones

- Las mujeres embarazadas, las personas mayores y los niños deben estar acompañados al pasar por el torniquete.
- Los niños que midan menos de 1 m deben pasar el torniquete en brazos o al lado de un adulto.
- No permanecer ni jugar en el pasillo.
- Asegúrate de que tu maleta pase por delante o a tu lado.
- Solo puede pasar una persona a la vez. No siga de cerca a otra persona, no se quede en el paso ni lo interrumpa.
- Un impacto violento podría dañar el núcleo de la máquina y acortar la vida útil del torniquete.
- Asegúrese de que el torniquete esté correctamente conectado a tierra para evitar lesiones personales.
- No utilice el torniquete cuando haya tormentas.

- Al autorizar el paso de una persona por el Torniquete, no debe haber ninguna persona en el lado opuesto del Torniquete, de lo contrario las barreras permanecerán desbloqueadas hasta que la persona del lado opuesto salga.
- Pase por el torniquete lo antes posible después de la autorización. Si la persona no ingresa en el tiempo especificado, el sistema cerrará automáticamente las barreras.
- Cuando entran varias personas, pueden pasar con autorización continua cuando el modo de memoria está habilitado. Sin embargo, se recomienda que el intervalo entre autorizaciones continuas sea de 2 a 5 s.
- Preste atención al estado del indicador al verificar la identidad de una persona. El rojo indica que no se ha verificado la identidad de la persona. El verde indica que se ha verificado correctamente su identidad y que la persona puede pasar.
- No intente pasar a la fuerza por el pasillo. Este torniquete cuenta con un sistema inteligente anti-intrusión y anti-entrada inversa. Si intenta pasar a la fuerza, el sistema se bloqueará automáticamente y cerrará el pasillo. Esto puede provocar lesiones a una persona.
- El torniquete no reconocerá correctamente la tarjeta autorizada si se utiliza junto con otras tarjetas.
- Conserve bien la tarjeta autorizada para asegurarse de su correcto funcionamiento.

- No pase artículos a través del torniquete, de lo contrario, el torniquete considerará el artículo como no autorizado.

Tabla de contenido

1 Introducción del producto

El módulo modular VTO de 1 botón (con cubierta frontal de metal) admite llamadas al presionar un botón.

2 puertos

Figura 2-1 Puerto

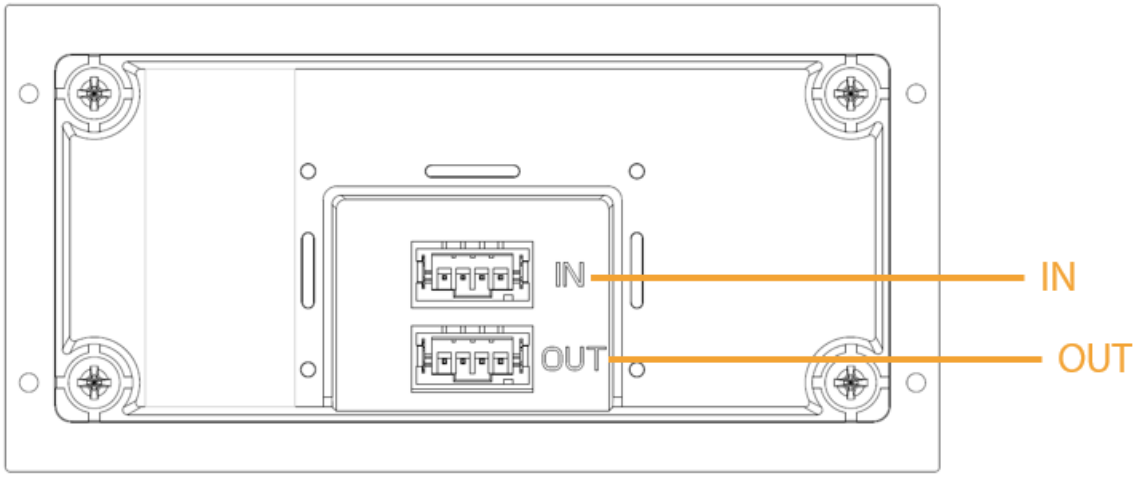


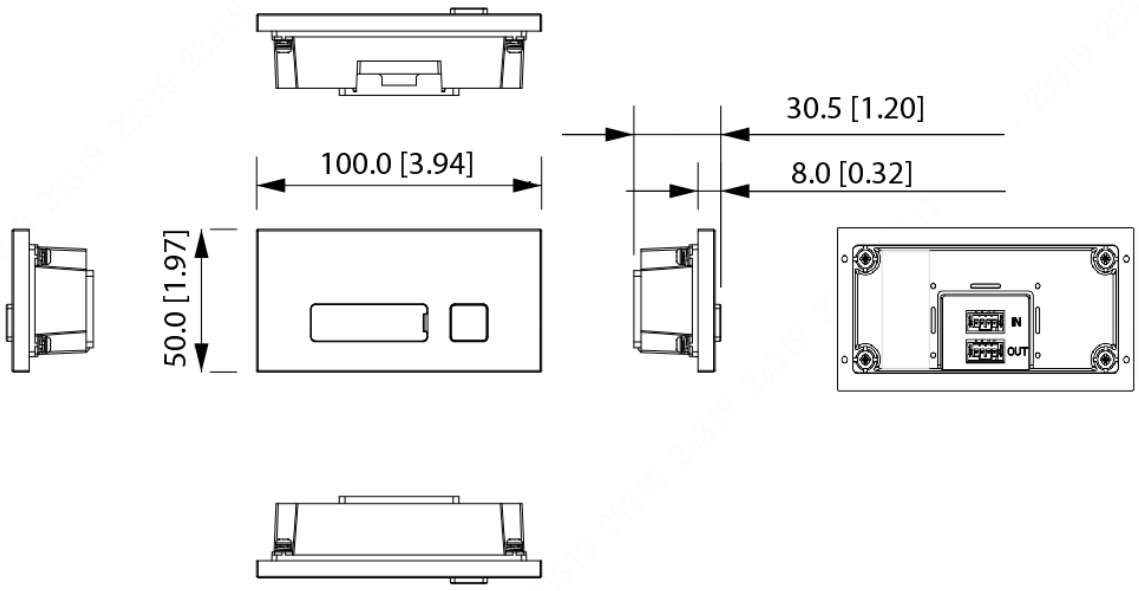
Tabla 2-1 Descripción del puerto

Puerto	Descripción
EN	Puerto de enlace ascendente
AFUERA	Puerto de enlace descendente

3 dimensiones

A continuación se muestra la dimensión del módulo.

Figura 3-1 Dimensiones (unidad: mm [pulgadas])



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 adecuadamente 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 se produce 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).