



Soporte móvil B100 para estación de recopilación de datos

Guía de inicio rápido



Prefacio

General

Este manual presenta las funciones y operaciones del soporte móvil B100 para la estación de recopilación de datos (en lo sucesivo, "el soporte"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para futuras consultas. Lea detenidamente antes de usar el soporte y guarde el manual en un lugar seguro para futuras consultas.

Las instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Significado
 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 stand, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el soporte y cumpla con las pautas cuando lo use. Lea atentamente antes de usar el soporte y cumpla con las pautas cuando lo use.

requerimientos de instalación

- Una instalación incorrecta puede causarle daño a usted o al dispositivo.
- Si no está seguro de cómo instalar el soporte, confíe la instalación a profesionales.
- Si alguna parte o componente del soporte está dañado, no instale el soporte.
- El soporte está diseñado para soportar la estación de recolección de datos. No utilice el soporte para otros fines.
- Peso neto: 55 kg; capacidad de carga: 100 kg. Para garantizar la seguridad, no utilice el soporte para soportar una carga que supere su capacidad de carga.
- Si desconoce la capacidad de carga, no instale el soporte.

Tabla de contenido

Prefacio.....	YO Medidas de
seguridad y advertencias importantes.....	III 1. Introducción
.....	1
1.1 Resumen.....	1
1.2 Apariencia.....	1
1.3 Componentes.....	1
1.4 Accesorios.....	2
2 Instalación.....	3
2.1 Cómo asegurar los posavasos.....	3
2.2 Soporte de fijación.....	3
2.3 Viga transversal de conexión.....	4
2.4 Fijación del soporte de montaje en pared.....	5
2.5 Apariencia después de la instalación.....	6
2.5.1 1 Módulo de Control + 1 Módulo de Toma de Datos.....	6
2.5.2 1 Módulo de Control + 2 Módulos de Toma de Datos.....	7
2.5.3 1 Módulo de Control + 3 Módulos de Toma de Datos.....	8
2.5.4 1 Módulo de Control + 4 Módulos de Toma de Datos.....	8
Apéndice 1 Recomendaciones sobre ciberseguridad.....	10

1. Introducción

1.1 Resumen

El dispositivo es un soporte móvil para la estación de recolección de datos. Es fácil de instalar en proyectos y aplicable para usos en escenarios como seguridad pública, policía de tránsito, electricidad, energía, parques industriales y exposiciones.

1.2 Apariencia

Figura 1-1 Apariencia



1.3 Componentes

Figura 1-2 Base y soporte vertical

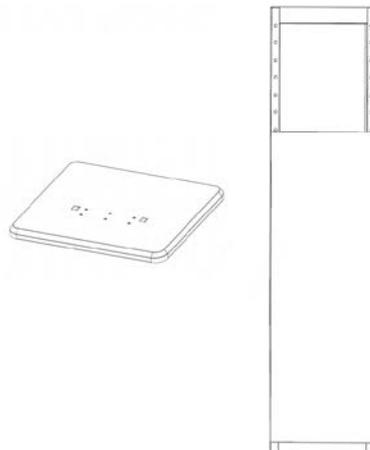


Figura 1-3 Travesaño y conector

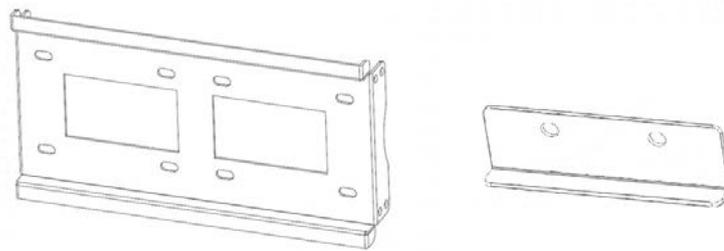


Figura 1-4 Soporte de montaje en pared y posavasos giratorio



1.4 Accesorios

Tabla 1-1 Lista de accesorios

Accesorio	Dimensiones	Cantidad	Descripción
Tornillo	M5 × 110 mm (parcialmente roscado)	3	Fije los tornillos en la parte inferior del soporte de montaje en pared entre el módulo de control y el último módulo de recopilación de datos.
	Hexágono interior M8 × 20	36	Use los tornillos para asegurar: <ul style="list-style-type: none"> ● Portavasos. ● Base y soporte vertical. ● Travesaño y conector.
	Hexágono exterior M8 × 25	26	Asegure la viga transversal y el soporte de montaje en pared.
Empaquetadura	M8	56	Utilice las juntas junto con los tornillos M8.
Tuerca	M8 (brida)	26	Utilice las tuercas junto con los tornillos M8.
Llave inglesa	Llave hexagonal interior (M8)	1	herramienta de instalación.
	Llave hexagonal exterior (M5)	1	
	Llave hexagonal interior y exterior	1	

2 Instalación

2.1 Cómo asegurar los posavasos

Use tornillos M8 × 20 mm para asegurar los cuatro posavasos en las esquinas de la base.

Figura 2-1 Posavasos seguros (1)

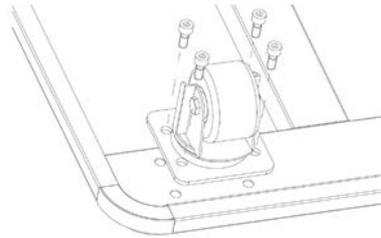


Figura 2-2 Posavasos seguros (2)

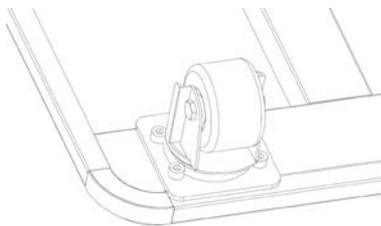
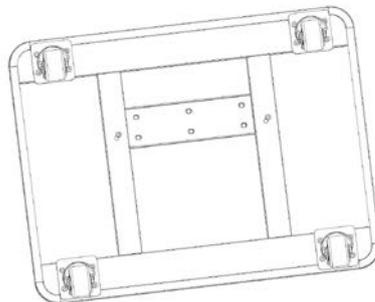


Figura 2-3 Posavasos seguro (3)



2.2 Soporte de fijación

Asegure el soporte vertical a la base y luego use ocho tornillos M8 × 20 mm para fijar la base.

Figura 2-4 Soporte de seguridad (1)

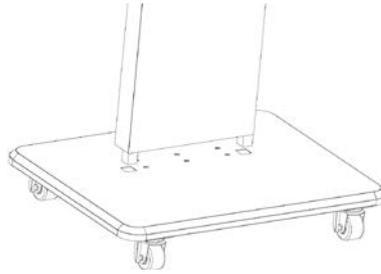


Figura 2-5 Soporte de seguridad (2)

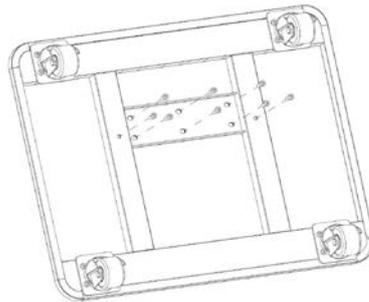


Figura 2-6 Soporte de seguridad (3)

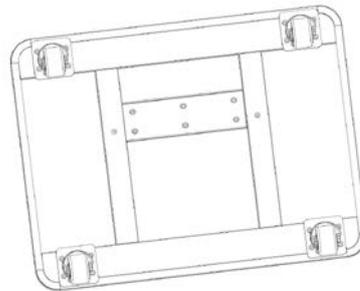
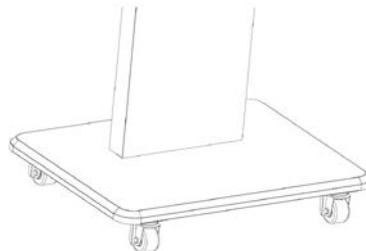


Figura 2-7 Soporte de seguridad (4)



2.3 Viga transversal de conexión

El número de travesaños está determinado por el número de módulos de control y recopilación de datos conectados.

Tabla 2-1 Número de travesaños

Número de módulos de control	Número de módulos de recopilación de datos	Número de vigas transversales
1	1	1
1	2	2
1	3 o 4	3

Figura 2-8 Conexión de la viga transversal (1)

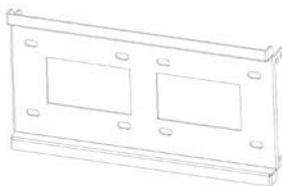


Figura 2-9 Conectar la viga transversal (2)

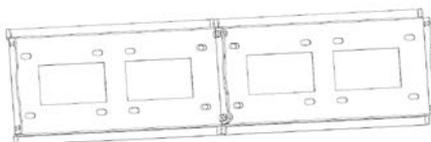


Figura 2-10 Conexión de la viga transversal (3)

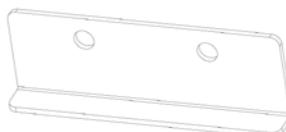
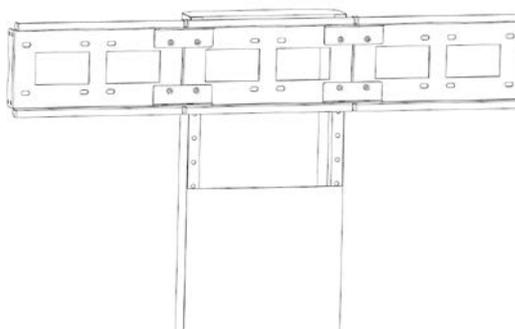


Figura 2-11 Conexión de la viga transversal (4)



2.4 Fijación del soporte de montaje en pared

Use tornillos M8 para asegurar el soporte de montaje en pared al módulo de control y luego fije el soporte con tuercas hexagonales exteriores M8 × 25.

Figura 2-12 Soporte de montaje en pared seguro (1)



Figura 2-13 Soporte de montaje en pared seguro (2)

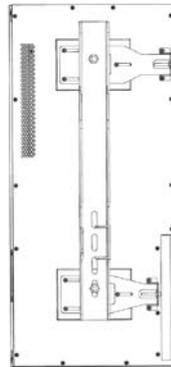
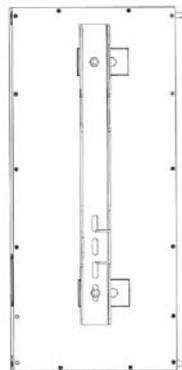


Figura 2-14 Soporte de montaje en pared seguro (3)



2.5 Apariencia después de la instalación

2.5.1 1 Módulo de Control + 1 Módulo de Toma de Datos

- Paso 1** Prepare una viga transversal.
- Paso 2** Instale primero el módulo de control y luego el módulo de recopilación de datos.
- Paso 3** Conecte los dos módulos y luego apriete los tornillos en las posiciones superior e inferior. Instale
- Paso 4** tornillos M5 en la parte inferior de los módulos.

Figura 2-15 1 módulo de control + 1 módulo de recopilación de datos (1)

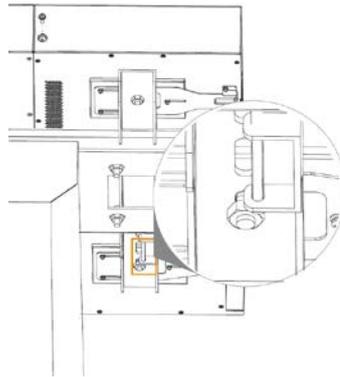
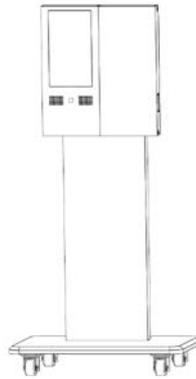


Figura 2-16 1 módulo de control + 1 módulo de recopilación de datos (2)



2.5.2 1 Módulo de Control + 2 Módulos de Toma de Datos

- Paso 1** Prepare dos vigas transversales.
- Paso 2** Instale un módulo de recopilación de datos en el medio y luego instale otros módulos en dos lados.
- Paso 3** Conecte los tres módulos y luego apriete los tornillos en las posiciones superior e inferior. Instale tornillos M5 en la parte inferior de los módulos más a la izquierda y más a la derecha.
- Paso 4**

Figura 2-17 1 módulo de control + 2 módulos de recopilación de datos (1)

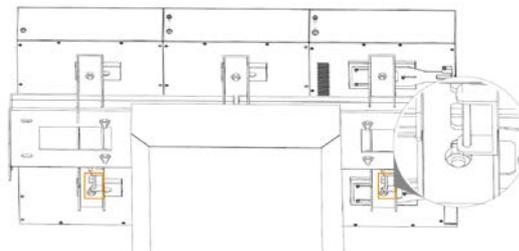
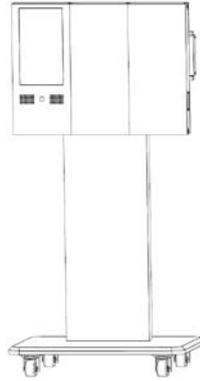


Figura 2-18 1 módulo de control + 2 módulos de recopilación de datos (2)



2.5.3 1 Módulo de Control + 3 Módulos de Toma de Datos

Paso 1 Prepare tres vigas transversales.

Paso 2 Instale un módulo de recopilación de datos en el medio y luego instale otros módulos en dos lados.

Paso 3 Conecte los cuatro módulos y luego apriete los tornillos en las posiciones superior e inferior. Instale tornillos

Paso 4 M5 en la parte inferior de los módulos más a la izquierda y más a la derecha.

Figura 2-19 1 módulo de control + 3 módulos de recopilación de datos (1)

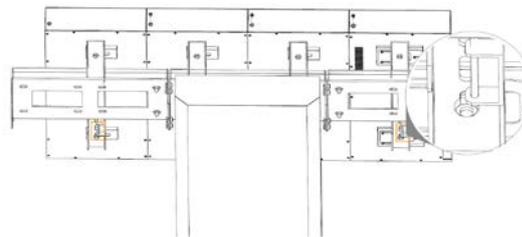
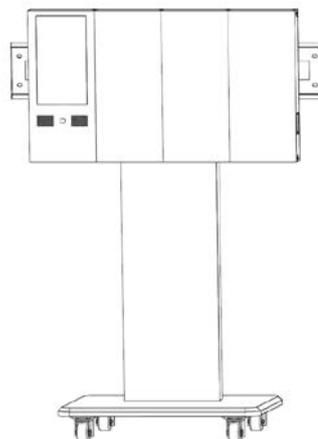


Figura 2-20 1 módulo de control + 3 módulos de recopilación de datos (2)



2.5.4 1 Módulo de Control + 4 Módulos de Toma de Datos

Paso 1 Prepare tres vigas transversales. Instale los

Paso 2 módulos de izquierda a derecha.

Paso 3 Conecte los cinco módulos y luego apriete los tornillos en las posiciones superior e inferior. Instale tornillos

Paso 4 M5 en la parte inferior de los módulos más a la izquierda y más a la derecha.

Figura 2-21 1 módulo de control + 4 módulos de recopilación de datos (1)

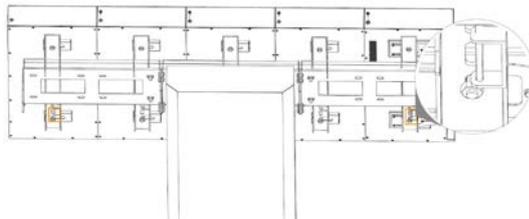
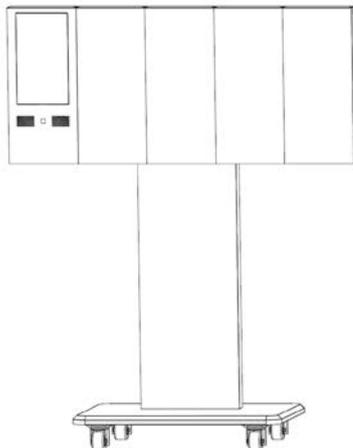


Figura 2-22 1 módulo de control + 4 módulos de recopilación de datos (2)



Apéndice 1 Recomendaciones sobre ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que pertenece a todos los dispositivos que están conectados a Internet. La videovigilancia IP no es inmune a los riesgos cibernéticos, pero tomar medidas básicas para proteger y fortalecer las redes y los dispositivos en red los hará menos susceptibles a los ataques. A continuación se presentan algunos consejos y recomendaciones de Dahua sobre cómo crear un sistema de seguridad más seguro.

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 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 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 está conectado a la red pública, se recomienda habilitar la función de "comprobación 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 dispositivo:

1. Protección Física

Le sugerimos que realice una protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala y gabinete de computadoras especiales, e implemente un permiso de control de acceso y una administración de claves bien hechos para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de un dispositivo extraíble (como un disco flash USB), puerto serie), 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

1024-65535, 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 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 dispositivo, reduciendo así el riesgo de suplantación de identidad 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 dispositivo:** 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 capacidad de almacenamiento limitada del dispositivo, 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 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 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 a la

dispositivo.

Más información

Visite el centro de respuesta a emergencias de seguridad del sitio web oficial de Dahua para conocer los anuncios de seguridad y las recomendaciones de seguridad más recientes.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883