

Estación de recolección de datos

Guía de inicio rápido



Prefacio

General

Este manual presenta las funciones y operaciones de la estación de recopilación de datos (en lo sucesivo, "la Estación").

Las instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Significado
 PELIGRO	Indica un peligro de alto potencial que, si no se evita, provocará la muerte o lesiones graves.
 ADVERTENCIA	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, reducción del rendimiento o resultados impredecibles.
 CONSEJOS	Proporciona métodos para ayudarlo a resolver un problema o ahorrar tiempo.
 NOTA	Proporciona información adicional como suplemento al texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.2	<ul style="list-style-type: none">● Pantalla de inicio actualizada.● Se agregó "3.1 Iniciar sesión".	noviembre 2021
V1.0.1	Actualizado "1.1 Introducción".	mayo 2021
V1.0.0	Primer lanzamiento.	marzo 2021

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. Las actualizaciones del producto pueden 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 de la estación, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar la estación, cumpla con las pautas al usarla y guarde el manual en un lugar seguro para futuras consultas.

Requisito de operación

- No coloque ni instale la Estación en un lugar expuesto a la luz solar o cerca de una fuente de calor.
- Mantenga la estación alejada de la humedad, el polvo o el hollín.
- Mantenga la Estación instalada horizontalmente en un lugar estable para evitar que se caiga.
- No deje caer ni salpique líquido sobre la estación y asegúrese de que no haya ningún objeto lleno de líquido sobre la estación para evitar que el líquido fluya hacia la estación.
- Instale la estación en un lugar bien ventilado y no bloquee la ventilación del escáner.
- Opere la estación dentro del rango nominal de entrada y salida de energía.
- No desmonte la estación.
- Transporte, use y almacene la Estación en las condiciones de humedad y temperatura permitidas.

Seguridad ELECTRICA

- Reemplácelas siempre con el mismo tipo de baterías.
- Utilice los cables de alimentación recomendados en la región y cumpla con la especificación de potencia nominal.
- Utilice el adaptador de corriente proporcionado con la Estación; de lo contrario, podría provocar lesiones personales y daños en el dispositivo.
- 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 dispositivo.
- Conectar la Estación (estructura tipo I) a la toma de corriente con puesta a tierra de protección.
- El acoplador del aparato es un dispositivo de desconexión. Cuando use el acoplador, mantenga el ángulo para facilitar la operación.

Tabla de contenido

Prefacio.....	I Medidas de seguridad y advertencias importantes
general	III 1. Información
1.1 Introducción	1
1.2 Apariencia del producto	2
1.2.1 Módulo de control	2
1.2.2 Aspecto de los módulos de recopilación de datos	4
1.3 Descripción de los botones	5
1.4 Encendido.....	6
1.5 Conexión del dispositivo	6
1.5.1 Conexión del módulo de control y el módulo de recopilación de datos	6
1.5.2 Conexión de la cámara corporal y el módulo de recopilación de datos	6
2 Instalación de la unidad de disco duro	10
3 Configuración y funcionamiento	13
3.1 Acceso	14
3.2 Gestión de archivos	15
3.2.1 Recopilación de archivos	15
3.2.2 Ver archivos	15
3.3 Usuario	15
3.3.1 Gestión de usuarios	dieciséis
3.3.2 Adición de Enforcer.....	17
3.3.3 Restablecimiento de la contraseña	17
Appendix 1 Recomendaciones de ciberseguridad	18

1. Información general

1.1 Introducción

Al trabajar con una cámara corporal, la Estación puede adquirir los datos de las cámaras corporales y cargarlas. La estación puede reconocer automáticamente y conectar la cámara corporal conectada a través del puerto USB. Al trabajar con la plataforma, la Estación puede autorizar la cámara corporal, adquirir automáticamente la evidencia electrónica (video, audio e instantánea). La estación contiene un módulo de control y un módulo de recopilación de datos. Un módulo de control puede admitir 4 módulos de recopilación de datos como máximo. Se presenta con:

- Recargue y recopile datos de un máximo de 32 cámaras corporales al mismo tiempo Actualice
- las cámaras corporales de forma automática o manual.
- Cree automáticamente un archivo y luego guarde los datos electrónicos recopilados.
- Sube automáticamente la evidencia a FTP oa la plataforma.
- Sincroniza automáticamente la hora.
- Cuando hay más de 1 módulo de recolección de datos, la Estación recolectará datos de la cámara corporal en los muelles fijos de cada módulo de recolección de datos en prioridad.
- Puede buscar, editar, transcodificar, reproducir, ver, eliminar y administrar todos los datos de la estación.

1.2 Apariencia del producto

1.2.1 Módulo de control

Figure 1-1 Panel frontal y panel trasero

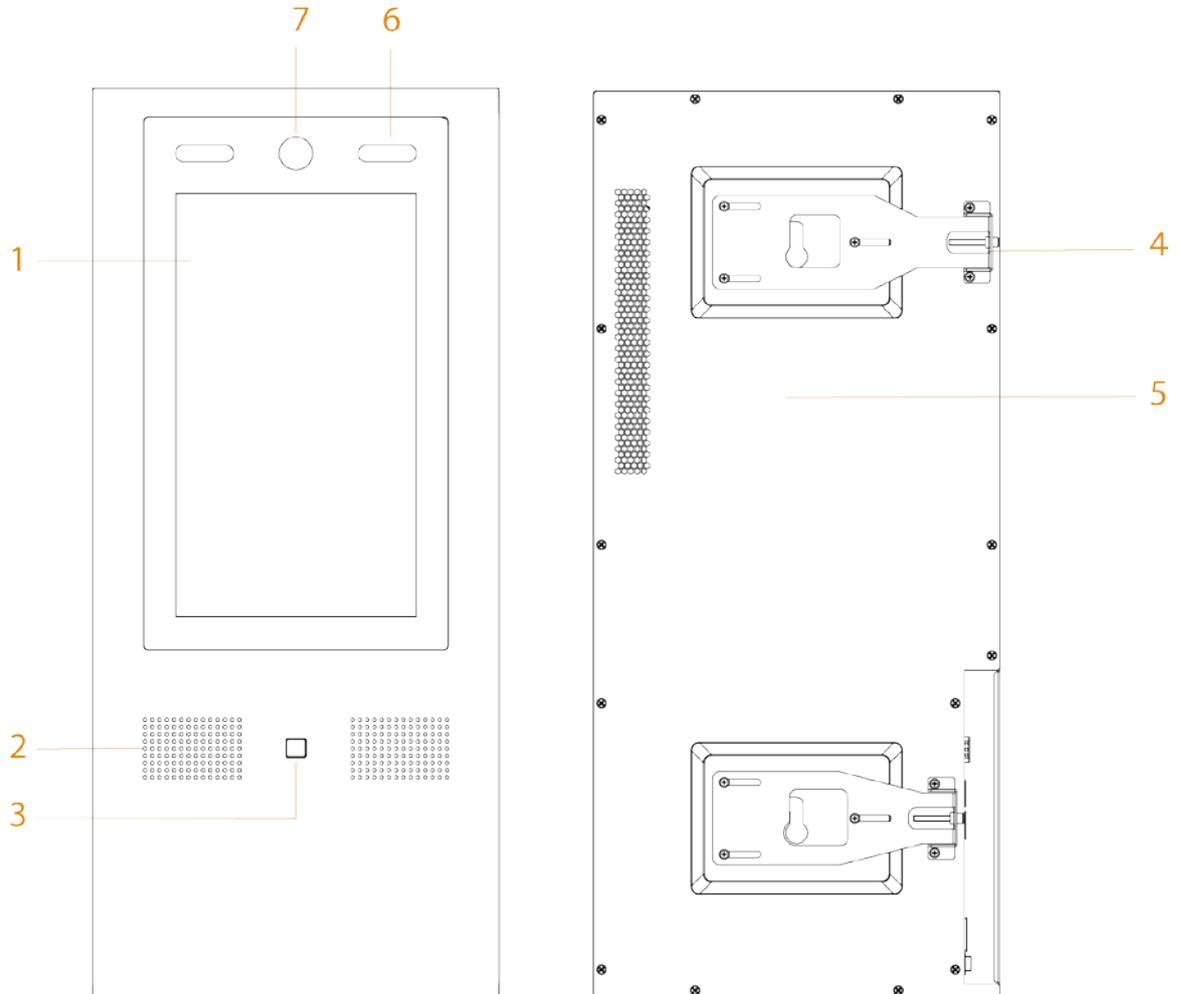


Figure 1-2 Panel lateral

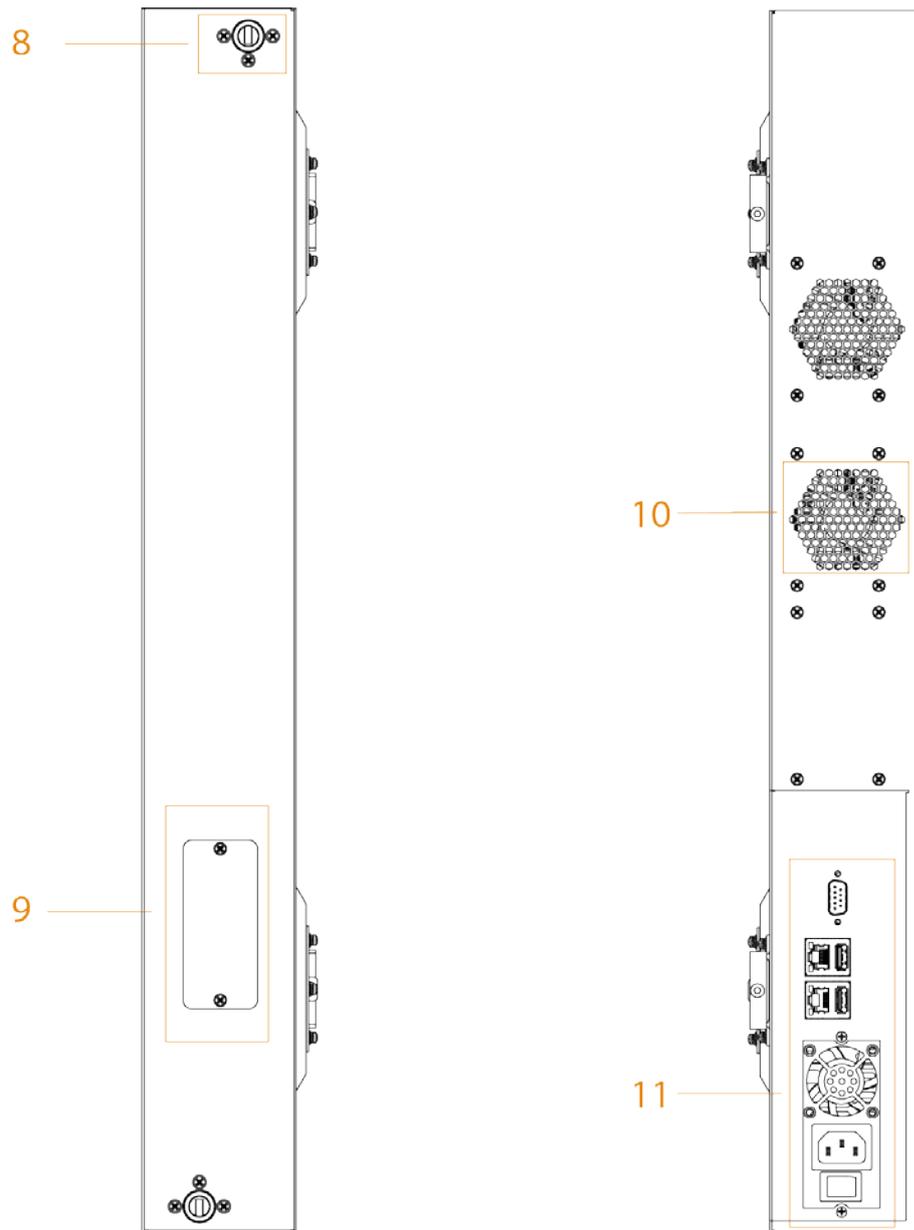


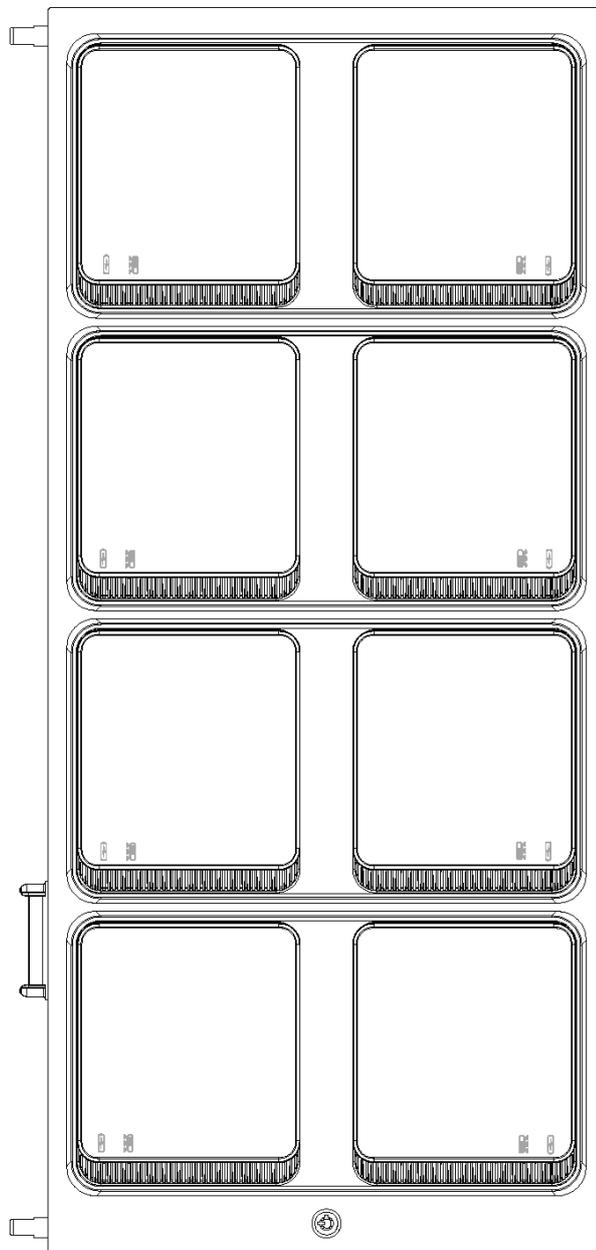
Tabla 1-1 Descripción de la apariencia

No.	Nombre	Descripción
1	Pantalla táctil	Pantalla táctil de 13,3 pulgadas.
2	Vocero	Salida de audio.
3	Sensor de huellas dactilares	Agrega datos de huella o desbloqueo por huella. Se pueden agregar como máximo 3 huellas dactilares para cada usuario.
4	Tablero de ajuste	Retire el módulo de control cuando conecte el módulo de control y los módulos de recopilación de datos.
5	Cubierta trasera	—
6	luz blanca	<ul style="list-style-type: none"> ● Proporciona luz adicional al reconocer rostros. Proporciona luz adicional a la cámara en condiciones de oscuridad.
7	Cámara	Reconoce la información de la cara. Puede desbloquear la estación a través del reconocimiento facial.
8	carcasa del eje.	Conecta el módulo de control y los módulos de recopilación de datos. Uno está en la parte superior y el otro en la parte inferior.

No.	Nombre	Descripción
9	Conector.	Transfiere los datos del módulo de control y los módulos de recopilación de datos
10	Disipación de calor agujero	—
11	Puertos	Incluye puerto de entrada de alimentación, puertos USB, puertos Ethernet y puerto RS-232. Para obtener más información, consulte la Tabla 1-2.

1.2.2 Aspecto de los módulos de recopilación de datos

Figure 1-3 Aspecto de los módulos de recopilación de datos.





- Coloque cámaras corporales en los muelles para la recopilación de datos. Cuando hay más de 1 recogida de datos módulos, se recogerán primero los datos de las cámaras corporales en los dos muelles de la primera fila.
- Hay dos iconos debajo del muelle:  indica recarga;  indica la recopilación de datos.
- Cuando no se puede abrir un muelle, puede abrirlo con la llave.

1.3 Descripción de Botones

Figure 1-4 Puertos

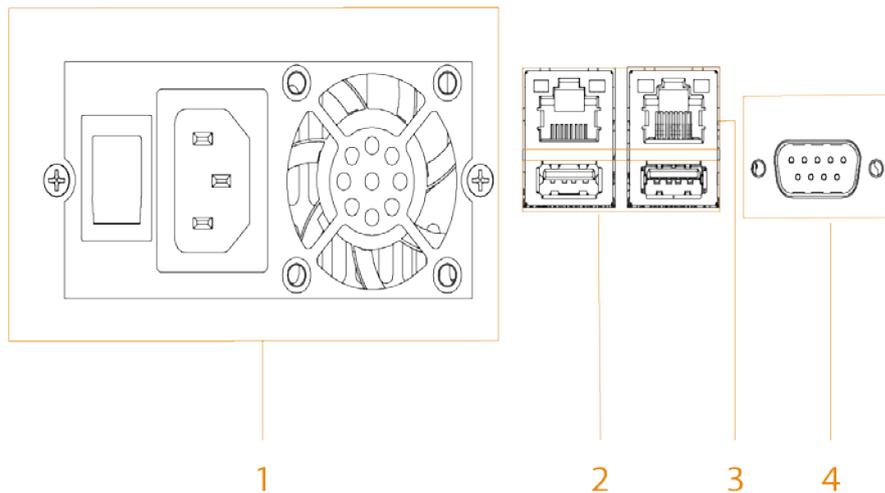


Tabla 1-2 Descripción del puerto

No.	Nombre	Descripción
1	Entrada de alimentación	Entradas de alimentación de 100 a 240 VCA para la estación.  Después de apagar la Estación, el ventilador funcionará durante un período para enfriar la Estación.
2	puertos USB	Conéctese a dispositivos de almacenamiento USB (USB 2.0 y USB 3.0), mouse y más.
3	ethernet	2 puertos Gigabit.  Cuando usa dos puertos al mismo tiempo, solo un puerto puede obtener la puerta de enlace automáticamente. Para la otra tarjeta Ethernet, deshabilite la función de obtener la dirección IP automáticamente.
4	RS-232	Se utiliza para la depuración serial común, la configuración de direcciones IP y la transmisión de datos de serial transparente.

1.4 Encendido



La cubierta de la Estación tiene electricidad estática, lo que podría provocar una descarga eléctrica. Para evitar la electricidad choque, asegúrese de que la estación esté bien conectada a tierra.

Step 1 Conecte el cable de alimentación y el cable de red.

Step 2 Presiona el botón de poder.

Todo el proceso tomará un período de tiempo. Por favor sea paciente.

1.5 Conexión del dispositivo

1.5.1 Conexión del módulo de control y el módulo de recopilación de datos



- Puede conectar 4 módulos de recopilación de datos al módulo de control como máximo.
- Para los detalles de instalación, consulte las instrucciones en el mapa de posicionamiento.

Step 1 Fije el módulo de control en la pared.

Step 2 Pegue el mapa de posicionamiento del módulo de recopilación de datos en la pared.

Step 3 Fije el módulo de recopilación de datos de acuerdo con las instrucciones en el mapa de posicionamiento.

1.5.2 Conexión de la cámara corporal y el módulo de recopilación de datos

Después de iniciar la estación, conecte las cámaras corporales a la estación y luego podrá recopilar datos de las cámaras corporales y recargarlas.



Asegúrese de que la conexión de las cámaras corporales y el módulo de recopilación de datos sea correcta, y que el cuerpo las cámaras están colocadas en las ranuras correctamente. Si las cámaras corporales no se colocan correctamente en las ranuras, el las cámaras pueden caerse cuando se abren las bases o las bases no se pueden abrir.



Las ranuras son especiales para la cámara corporal MPT220 por defecto. Si desea utilizar la cámara corporal MPT210, use la ranura separada en el paquete de accesorios.

Step 1 Abra la base a través de la pantalla táctil o la tecla y luego saque el cable de datos.



No arrastre el cable de datos con demasiada fuerza. De lo contrario, podría resultar en un resorte no válido o aflojamiento de conexión de puerto!

Figure 1-5 Saque el cable de datos (ranura MPT220)



Figure 1-6 Saque el cable de datos (ranura MPT210)



Step 2 Conecte el cable de datos a la cámara corporal hasta que aparezca el cuadro de diálogo de conexión exitosa de la estación.

Figure 1-7 Conectar dispositivo (ranura MPT220)



Figure 1-8 Conectar dispositivo (ranura MPT210)



Step 3 Después de la conexión, coloque la cámara corporal en la base y luego podrá recopilar datos y recargar la cámara corporal.



- Para la cámara corporal MPT220, inserte el dispositivo en la ranura.
- Para la cámara corporal MPT210, inserte el clip en la ranura. Solo cámara corporal MPT210 con el último clip se puede insertar en la ranura. Consulte la Figura 1-8.

Figure 1-9 Recopilación de datos (ranura MPT220)



Figure 1-10 Recopilación de datos (ranura MPT210)



Instalación de 2 discos duros

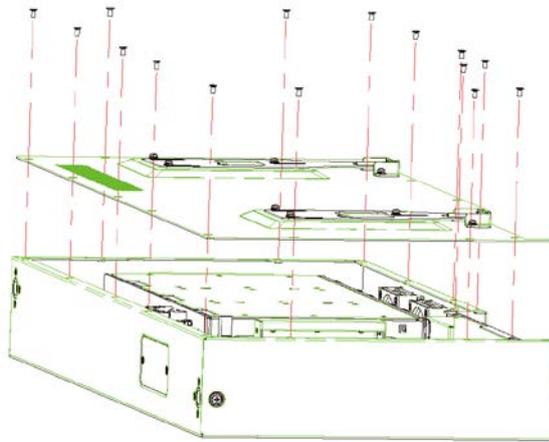
Puede instalar seis HDD 10T (unidades de disco duro).



- Para evitar espacio de almacenamiento insuficiente, se recomiendan discos duros de más de 2T.
- Para reducir la presión de escritura de cada HDD, le recomendamos que instale al menos 2 HDD con la misma capacidad de recogida de datos y recarga.

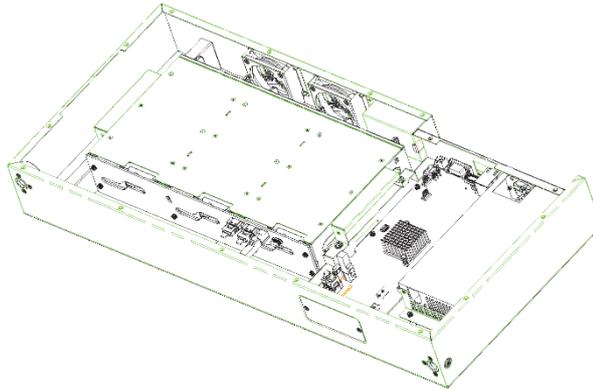
Step 1 Afloje los tornillos de la cubierta trasera y luego retire la cubierta trasera.

Figure 2-1 Retire la cubierta trasera



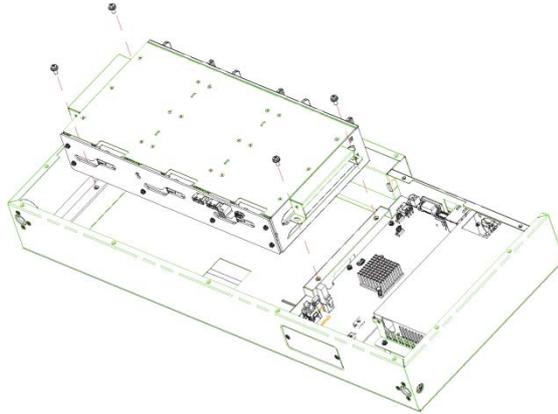
Step 2 Desconecte los cables entre la placa principal y la placa HDD.

Figure 2-2 Afloje el cable



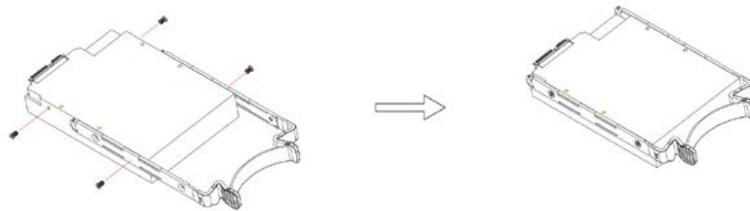
Step 3 Afloje los cuatro tornillos fijos en la caja del disco duro y luego saque la caja.

Figure 2-3 Saque la caja del disco duro



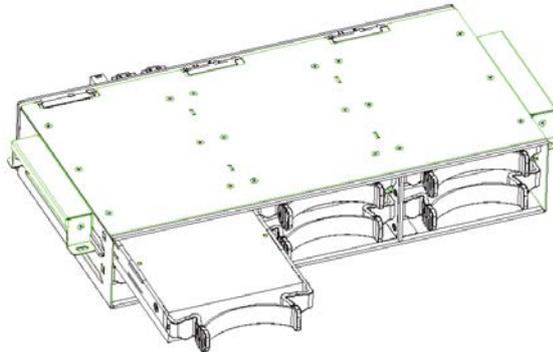
Step 4 Reparar discos duros

Figure 2-4 Reparar disco duro



Step 5 Instalar discos duros. Empuje los HDD fijos en la caja HDD.

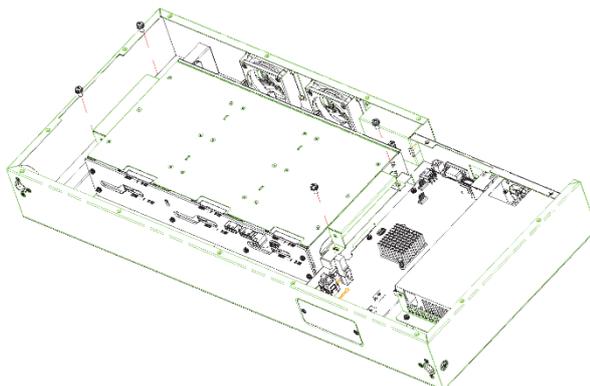
Figure 2-5 Instalar disco duro



Empuje los discos duros en la dirección que muestran el puerto del disco duro y el puerto de la placa principal.

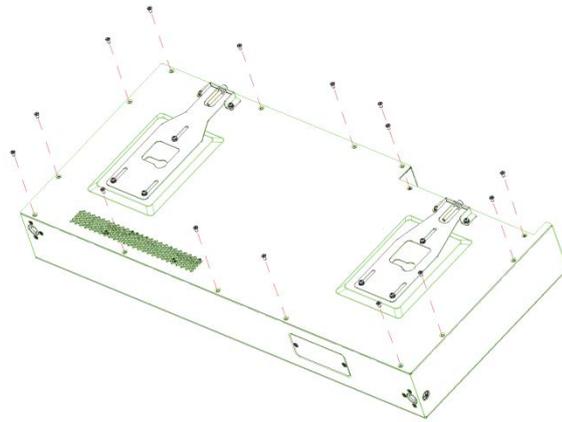
Step 6 Fije la caja HDD en el chasis.

Figure 2-6 Instale la caja de disco duro



- Step 7** Conecte el cable entre la placa principal y la placa HDD. Arregla la
Step 8 cubierta.

Figure 2-7 arreglar la cubierta



3 Configuración y Operación

Figure 3-1 Pantalla de inicio

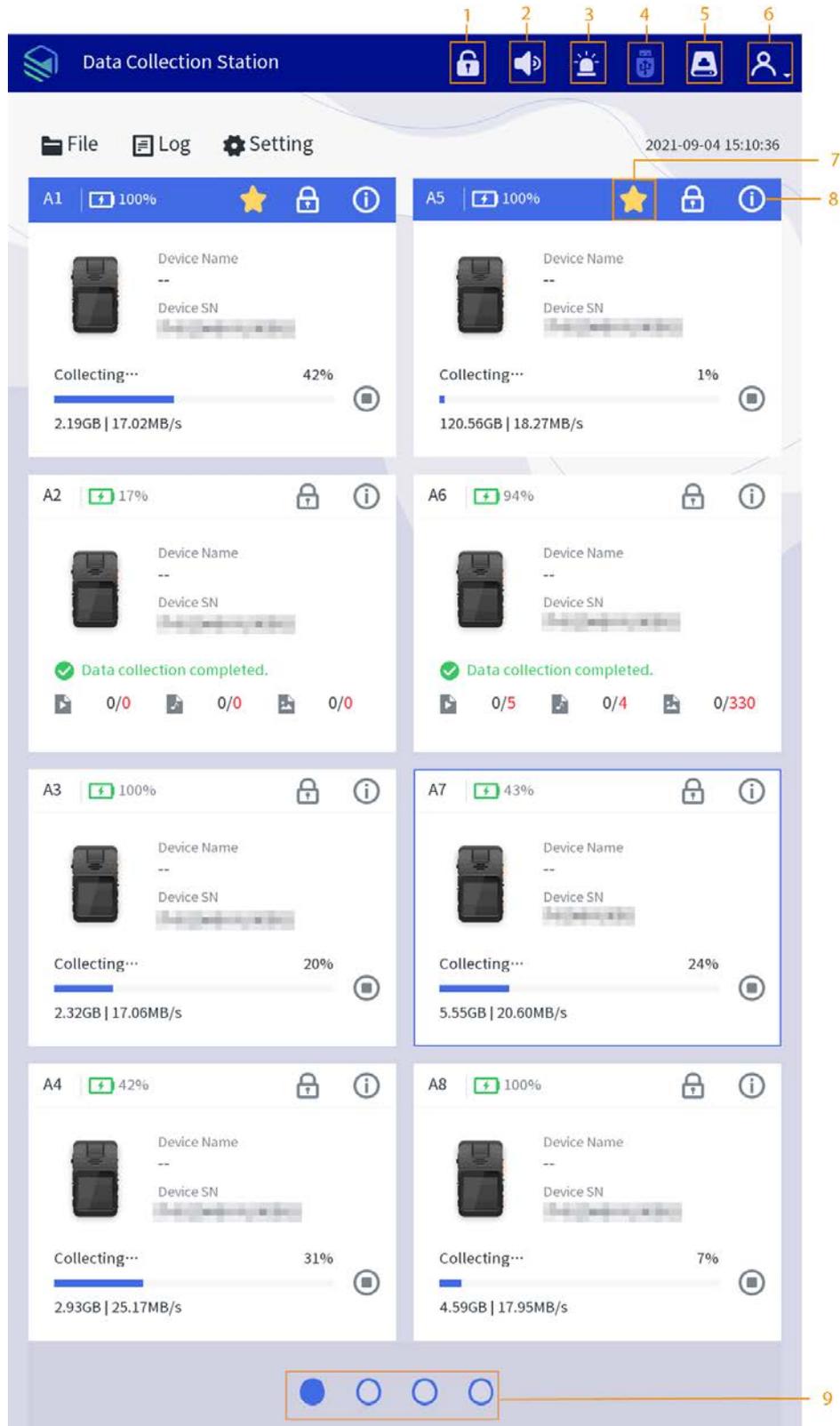


Tabla 3-1 Descripción de la pantalla de inicio

No.	Descripción
1	Desbloquee el muelle con un toque.

No.	Descripción
2	Alarma. Tóquelo y la melodía de la alarma se desactivará.
3	Pantalla de información de alarma. La luz roja parpadea cuando hay alarma.
4	Dispositivo de almacenamiento USB externo. Gris significa que no hay ningún dispositivo de almacenamiento USB conectado.
5	Ver la capacidad del disco duro.
6	Iniciar sesión, cerrar sesión, reiniciar, apagar y editar la información del usuario.
7	<p> indica la recopilación de datos en prioridad, lo que puede mejorar la velocidad de recopilación del muelle correspondiente.</p> <p></p> <p>Para habilitar esta función, debe conectar al menos dos módulos de recopilación de datos. Él La función es compatible con los dos muelles de la primera fila en cada módulo de recopilación de datos.</p>
8	<p>Ver métodos de actualización de la estación y cámaras corporales.</p> <p></p> <p>Tocar obligar a hacer cumplir sobre el información del dispositivo pantalla, ingrese el nombre del ejecutor y el No. del ejecutor, hacer clic Búsqueda, a continuación, seleccione el ejecutor que desea vincular.</p>
9	Cambiar pantallas de módulos de recopilación de datos. Admite 4 pantallas como máximo.

3.1 Acceso



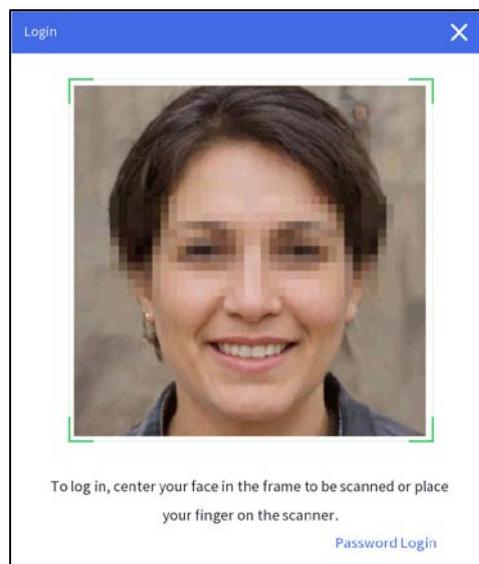
Antes de usar el inicio de sesión con rostro o con huella digital, debe completar las configuraciones relacionadas. Para detalles, consulte "3.3 Usuario".

Inicio de sesión facial

Después de que comience la estación, coloque su rostro en el cuadro de detección.

Una vez desbloqueada, la estación muestra la pantalla de inicio.

Figure 3-2 Inicio de sesión facial



Inicio de sesión con huella digital

Después de que se inicie la estación, coloque su dedo en el escáner.

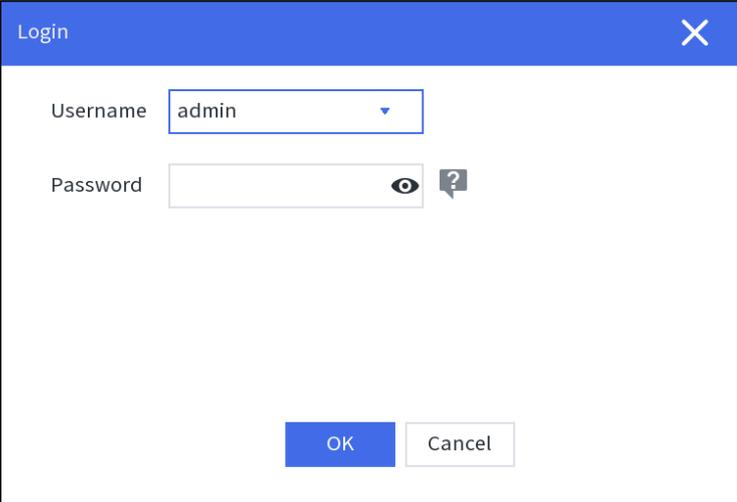
Una vez desbloqueada, la estación muestra la pantalla de inicio.

Contraseña de acceso

Después de que comience la estación, toque **Contraseña de acceso** en la esquina inferior derecha de la **Acceso** pantalla y, a continuación, introduzca el nombre de usuario y la contraseña.

Una vez desbloqueada, la estación muestra la pantalla de inicio.

Figure 3-3 Contraseña de acceso



The image shows a 'Login' dialog box with a blue header bar containing the text 'Login' and a close button (X). Below the header, there are two input fields. The first is labeled 'Username' and has a dropdown menu with 'admin' selected. The second is labeled 'Password' and has a text input field, an eye icon for visibility, and a question mark icon. At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

3.2 Gestión de archivos

3.2.1 Colección de archivos

Después de recopilar los archivos de datos de las cámaras corporales, la Estación cargará los archivos en la plataforma de acuerdo con la configuración en **Almacenamiento**.

3.2.2 Visualización de archivos

Toque dos veces un archivo para ver los detalles y podrá realizar las operaciones de reproducción rápida, reproducción lenta, acercar o alejar.

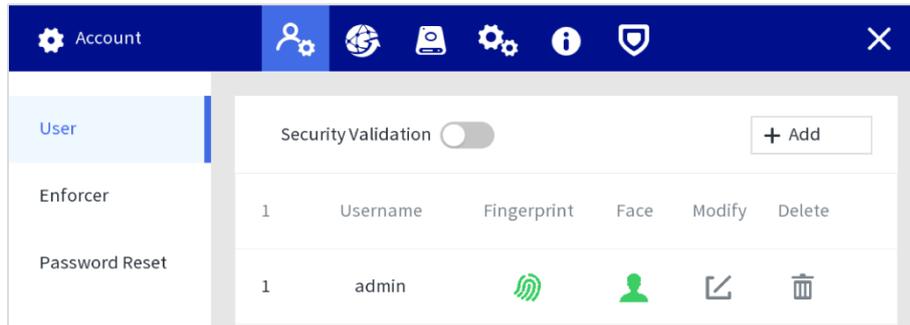
3.3 Usuario

El administrador puede agregar usuarios, eliminar usuarios y editar permisos de usuario según sea necesario.

3.3.1 Gestión de usuarios

Step 1 Seleccione **Configuración > Cuenta > Usuario**.

Figure 3-4 Gestión de usuarios



Step 2 Tocar **Agregar** para agregar usuarios.

1) Puede agregar caras y huellas dactilares, y configurar permisos de usuario. Todos los permisos están habilitados de forma predeterminada.

-

Figure 3-5 Agregar usuarios

The 'Add' user form contains the following fields and options:

- Username:** Input field with the value 'abc'.
- Password:** Input field.
- Confirm Password:** Input field.
- Password Requirement:** Text indicating the password must be 8 to 32 characters, including at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters (Characters like ' " ; : & cannot be included in).
- Face:** '+ Add' button.
- Fingerprint:** '+ Add' button.
- Permission:** A list of permissions, all of which are checked:
 - All
 - SYSTEM INFO
 - Export File
 - FILE MANAGEMENT
 - System Settings
 - ACCOUNT
 - Unlock All

At the bottom right, there are 'OK' and 'Back' buttons.

3.3.2 Adición de Enforcer

Seleccione **Configuración > Cuenta > Enforcer** y luego toque **Agregar** para agregar usuarios. Ingrese el departamento del ejecutor, el número del ejecutor, el nombre del ejecutor, la contraseña y confirme la contraseña, y agregue la cara y la huella digital según sea necesario.

Figure 3-6 Agregar ejecutor

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The form contains the following fields and elements:

- Enforcer Dept:** A dropdown menu with a blurred selection.
- Enforcer No:** A text input field containing "111".
- Enforcer Name:** A text input field containing "fr".
- Password:** A text input field with masked characters (dots).
- Confirm Password:** An empty text input field.
- Password Strength:** A progress bar below the password field, with the first segment highlighted in red.
- Instructions:** Text below the confirm password field: "Password must be 8 to 32 characters, including at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters (Characters like ' ; : & cannot be included in)."
- Face:** A section with a "+ Add" button.
- Fingerprint:** A section with a "+ Add" button.

3.3.3 Restablecimiento de contraseña

Seleccione **Configuración > Cuenta > Restablecimiento de contraseña** e ingrese la dirección de correo electrónico de recuperación y las preguntas de seguridad.

Figure 3-7 Restablecimiento de contraseña

The screenshot shows a configuration screen for "Password Reset". The interface includes a sidebar on the left with the following items:

- User
- Enforcer
- Password Reset (highlighted)

The main content area is titled "Password Reset" and contains the following elements:

- Enable:** A toggle switch that is currently turned on.
- Reserved Email:** An empty text input field.
- Security Question:** A section with a "Reset" button and the text: "Set successfully. Please reset first if you need to modify securi".
- Question 1:** A dropdown menu with the text "What is your favorite children's book?".
- Answer:** A masked text input field.
- Question 2:** A dropdown menu with the text "What was the first name of your first boss?".
- Answer:** A masked text input field.
- Question 3:** A dropdown menu with the text "What is the name of your favorite fruit?".
- Answer:** A masked text input field.

Appendix 1 Recomendaciones de ciberseguridad

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

dispositivo: 1. Use 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 "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

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. Establezca y actualice la información de restablecimiento de contraseñas 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 dispositivo, reduciendo así

el riesgo de suplantación 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 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. 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 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.