Asistencia independiente

Guía de inicio rápido

Versión 1.0.0

Prefacio

General

Este manual presenta la instalación y las operaciones básicas del dispositivo Attendance Standalone (en adelante, el "Dispositivo"). Lea atentamente antes de utilizar el dispositivo y guarde el manual para futuras consultas.

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.
TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
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 2022

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, huellas dactilares y número de matrícula. Debe cumplir con las leyes y normativas 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 Dispositivo, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el Dispositivo y cumpla con las pautas al usarlo.

Requerimientos de transporte

Transporte, utilice y almacene el Dispositivo en condiciones de humedad y temperatura permitidas.

Requisito de almacenamiento

Guarde el dispositivo en condiciones de humedad y temperatura permitidas.

Requisitos de instalación

- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- Cumpla estrictamente con los códigos y normas de seguridad eléctrica locales. Asegúrese de que el voltaje ambiental sea estable y cumpla con los requisitos de suministro de energía del dispositivo.
- No conecte el dispositivo a dos o más tipos de fuentes de alimentación, para evitar dañarlo.
- El uso inadecuado de la batería podría provocar un incendio o una explosión.

- El personal que trabaja en altura debe tomar todas las medidas necesarias para garantizar su seguridad personal, incluido el uso de casco y cinturones de seguridad.
- No coloque el dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- Instale el dispositivo sobre una superficie estable para evitar que se caiga.
- 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.
- Utilice los cables de alimentación recomendados para la región y que cumplan con las especificaciones de potencia nominal.
- 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 dispositivo.
- El dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectada a una toma de corriente con conexión a tierra.

Requisitos de funcionamiento

- Compruebe si la fuente de alimentación es correcta antes de usarlo.
- No desconecte el cable de alimentación del costado del dispositivo mientras el adaptador esté encendido.
- Utilice el dispositivo dentro del rango nominal de entrada y salida de energía.
- Utilice el dispositivo en las condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquidos sobre el dispositivo y asegúrese de que no haya ningún objeto lleno de

líquido en el dispositivo para evitar que fluya líquido hacia él.

- No desmonte el dispositivo sin instrucción profesional.
- Este producto es un equipo profesional.
- Este equipo no es adecuado para su uso en lugares donde es probable que haya niños presentes.

Tabla de contenido

Prefacio..... I **Medidas de seguridad y advertencias importantes**..... III **1 Descripción general del producto**..... 1

2 dimensiones..... 2

3 Cableado..... 3

4 Instalación..... 4

4.1 Instalación (modelo GL)..... 4

4.2 Instalación (modelo E y modelo ES)..... 5

5 Operaciones locales..... 7

5.1 Introducción al teclado..... 7

5.2 Encendido..... 10

5.3 Creación de una cuenta de administrador..... 10

5.4 Iniciar sesión..... 10

6 Operaciones de SmartPSS Lite..... 12

6.1 Instalación..... 12

6.2 Inicialización..... 12

6.3 Iniciar sesión..... 13

Apéndice 1 Puntos importantes de las instrucciones para el registro de huellas dactilares..... 15

Apéndice 2 Método de entrada..... 17

Apéndice 3 Preguntas frecuentes..... 18

Apéndice 4 Recomendaciones de ciberseguridad..... 19

1 Descripción general del producto

El dispositivo se puede utilizar para controlar la asistencia de las personas. Las personas pueden registrar su entrada y salida mediante huella dactilar, contraseña y tarjeta. El deslizamiento de tarjeta solo está disponible en algunos modelos.

2 dimensiones

Figura 2-1 Dimensiones (modelo GL) (mm [pulgadas])

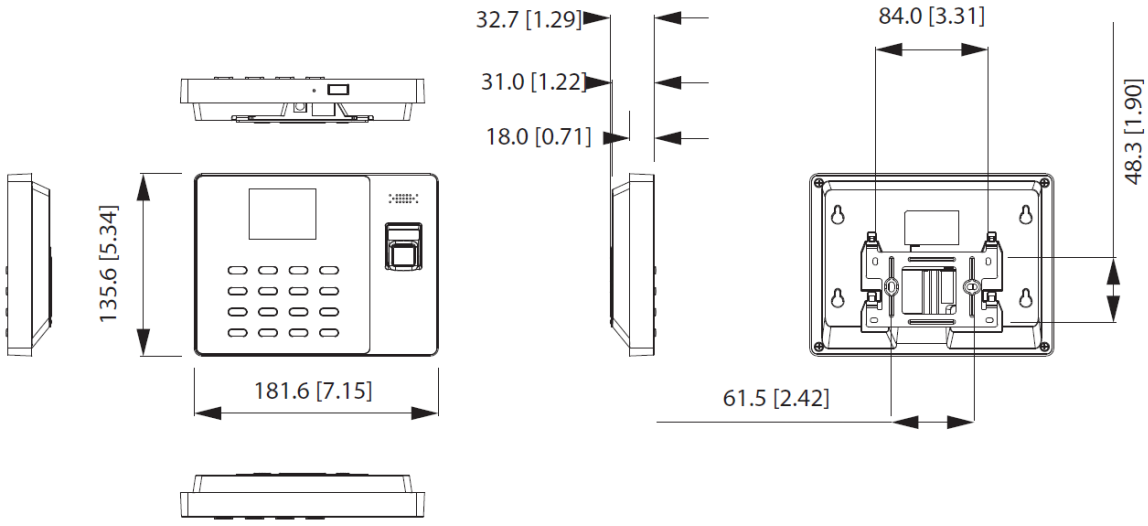
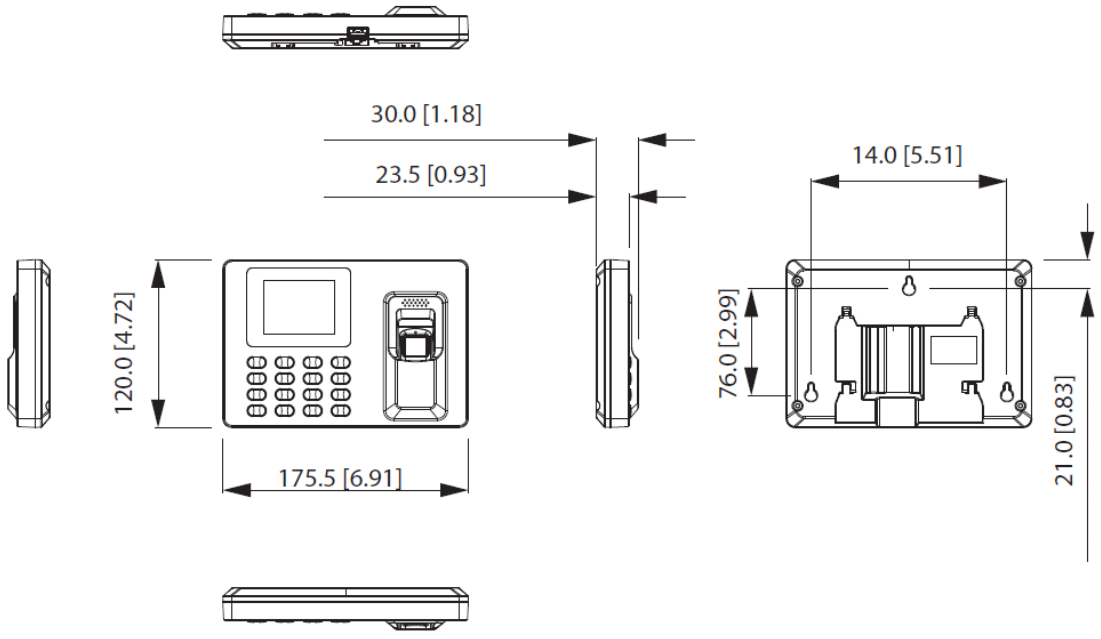
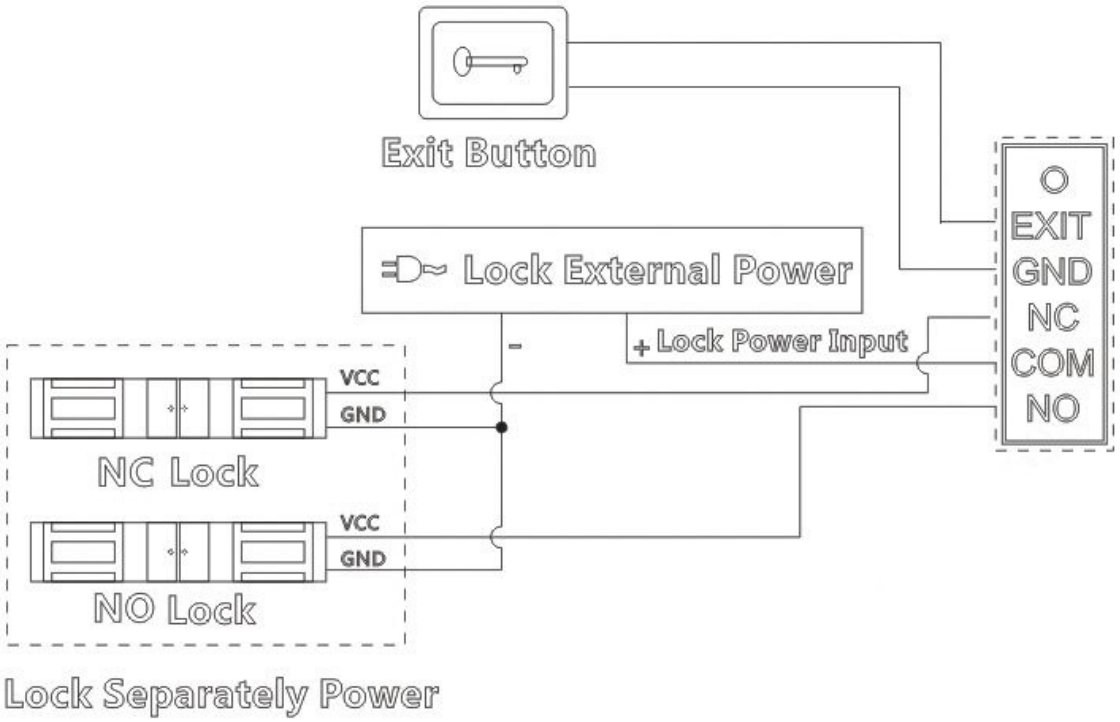


Figura 2-2 Dimensiones (modelo E y modelo ES) (mm [pulgadas])



3 Cableado

Figura 3-1 Montaje en pared (modelo GL) (mm [pulgadas])



4 Instalación

4.1 Instalación (modelo GL)

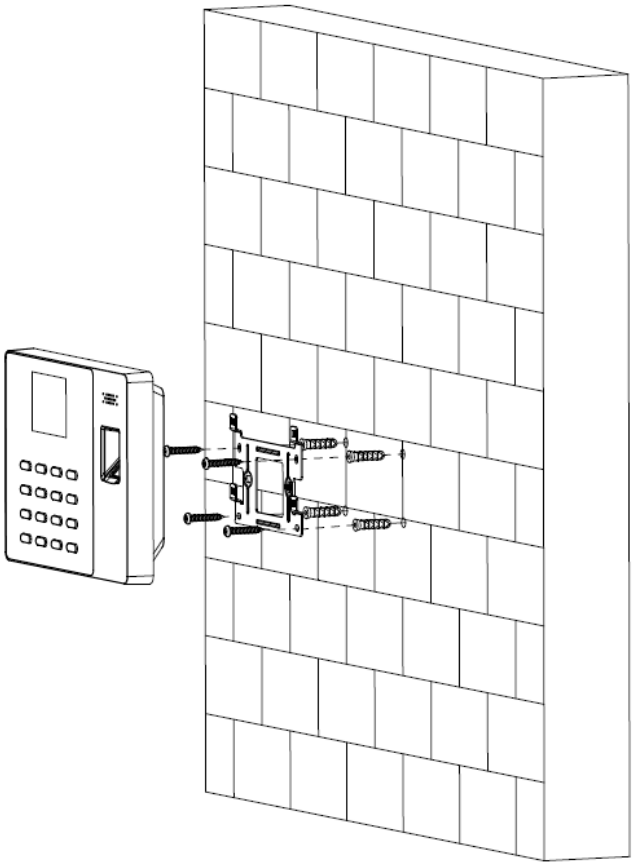
Montaje en pared

1. De acuerdo con la posición de los orificios del soporte, taladre 4 orificios y 1 salida de cable en la pared. Coloque pernos de expansión en los orificios.

   La salida de cable no es necesaria para el cableado montado en superficie.

2. Utilice los 4 tornillos para fijar el soporte a la pared.
3. Conecte el controlador de acceso. Para obtener más información, consulte "3 Cableado".
4. Coloque el controlador de acceso en el soporte.

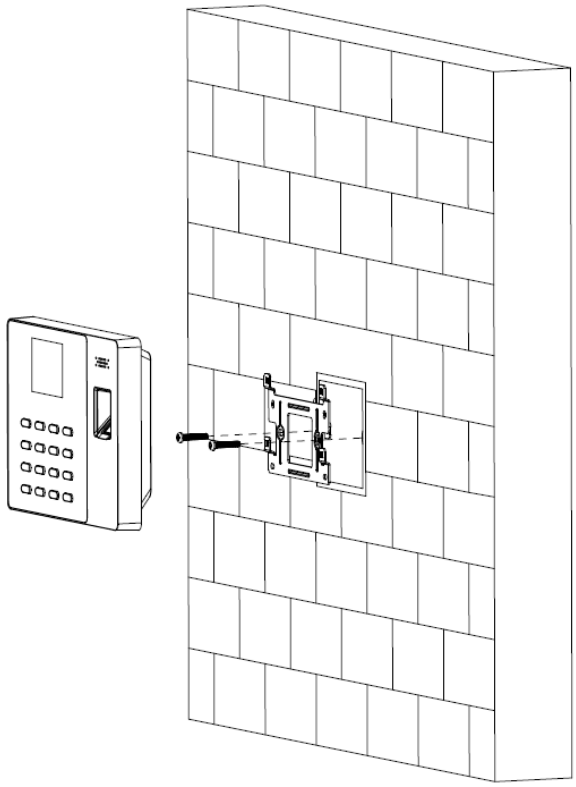
Figura 4-1 Montaje en pared (modelo GL) (mm [pulgadas])



Montaje en caja

1. Coloque una caja 86 en la pared a una altura adecuada.
2. Fije el soporte a la caja 86 con 2 tornillos.
3. Conecte el controlador de acceso. Para obtener más información, consulte "3 Cableado".
4. Conecte el controlador de acceso al soporte.

Figura 4-2 Montaje de caja 86 (modelo GL) (mm[pulgadas])



4.2 Instalación (modelo E y modelo ES)

Procedimiento

Paso 1 Coloque el papel de montaje en la pared. Taladre 3 agujeros en la pared según la posición de los agujeros en el papel.

La salida de cable es necesaria para el montaje en la pared.

Paso 2 Martille los pernos de expansión en los orificios.

Paso 3 Atornille 3 tornillos en los pernos de expansión.

Paso 4 Conecte el controlador de acceso.

Paso 5 Conecte el controlador de acceso al soporte.

Figura 4-3 Cableado de montaje en superficie

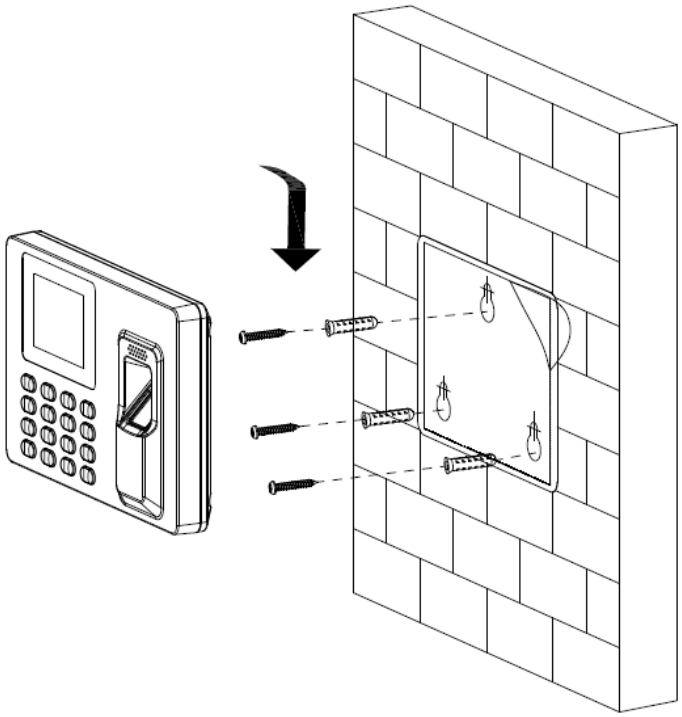
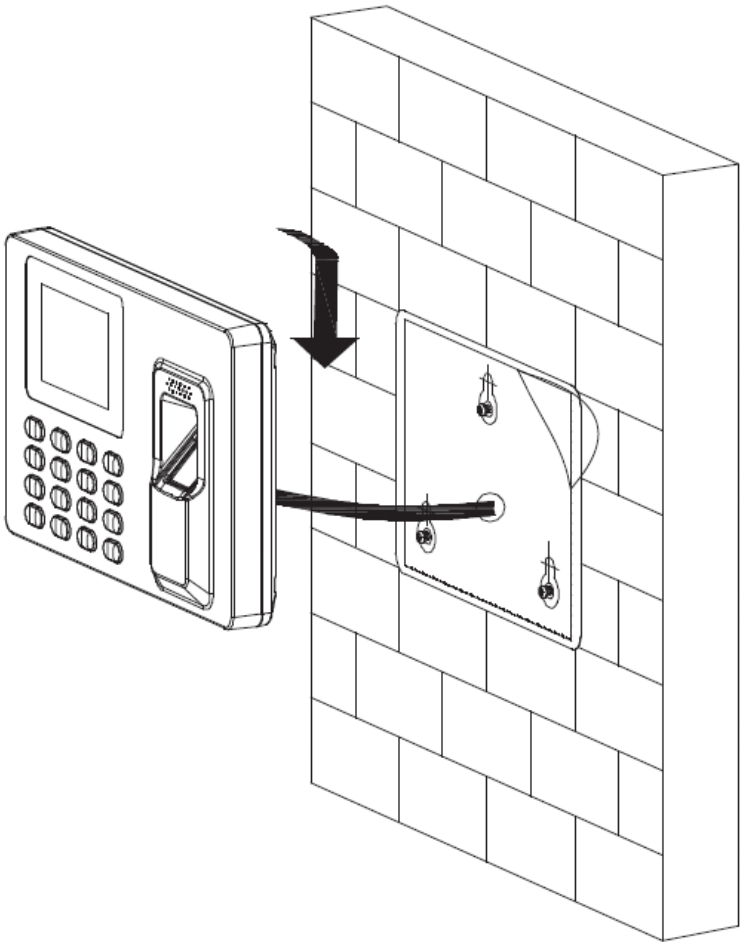


Figura 4-4 Cableado en la pared



5 Operaciones locales

El teclado varía ligeramente según el modelo del dispositivo. En esta sección se utiliza el modelo GL como ejemplo.

5.1 Introducción al teclado

Figura 5-1 Apariencia (GL)

Tabla 5-1 Descripción de parámetros

Parámetro	Descripción
0–9	Teclas numéricas para ingresar números y letras.
ESC/F1	● Salir o ir a la pantalla anterior. ● Tócalo en la pantalla de espera para registrar tu entrada.
∧/F2	● Tócalo en la pantalla de espera y BREAK OUT se mostrará en la pantalla. ● Toque para subir las opciones.
∨/F3	● Tócalo en la pantalla de espera y aparecerá BREAK IN en la pantalla. ● Tócalo para desplazarte por las opciones.
Aceptar/F4	● Confirme su configuración. ● En la pantalla de espera, tóquelo para marcar su salida.
#	● Borrar. ● Atajo para revisar registros.

Parámetro	Descripción
	● Manténgalo presionado durante más de 3 segundos para encender/apagar el dispositivo. ● En la pantalla de espera, tóquelo para ingresar al menú principal mediante huellas dactilares, contraseñas o tarjetas.  Sólo los administradores pueden ingresar al menú principal. ● Tócalo para cambiar los tipos de entrada (números, letras y símbolos).

Figura 5-2 Aspecto (modelo E)

Figura 5-3 Aspecto (modelo ES)

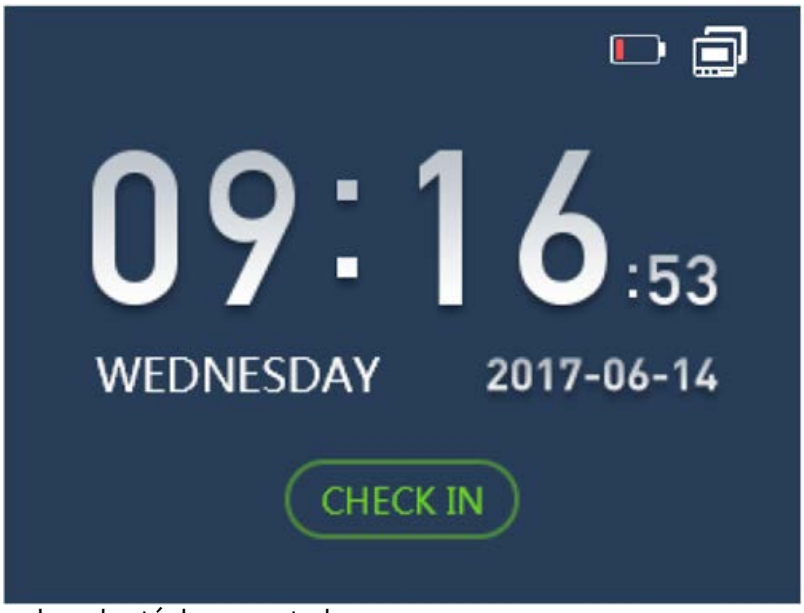
Tabla 5-2 Descripción de parámetros

Parámetro	Descripción
0～9	Tecla numérica para ingresar números y letras.
ESC	Regresar o salir.
∧	Tócalo para subir las opciones.
∨	Tócalo para desplazarte por las opciones.
DE ACUERDO	Ingresar o confirmar
#	Retroceso
	Ingrese al menú principal o cambie el método de entrada.

5.2 Encendido

Después de encender el dispositivo, se muestra la pantalla de espera.

Figura 5-4 Pantalla de espera



- indica que la red está desconectada.
- indica que la red está conectada.
- Indica el estado de la batería. Cuando se enciende el dispositivo por primera vez, el nivel de batería es del 25 % (puede durar aproximadamente 1 hora).

5.3 Creación de una cuenta de administrador

Cuando se inicia el dispositivo por primera vez, cualquier persona puede ingresar al menú principal y configurarlo. Para la seguridad de la cuenta, recomendamos crear primero la cuenta de administrador y, luego, solo los administradores podrán ingresar al menú principal.

Procedimiento

Paso 1 Grifo para ingresar a la pantalla del menú principal.

Paso 2 Seleccionar**1 usuario**>**Agregar nuevo usuario**

Paso 3 Introduzca la información del usuario.

Paso 4 Seleccionar**Administrador**de**Nivel de usuario**1.

Seleccione**Nivel de usuario**y luego toque**Aceptar/F4**.

2. Seleccionar∧/**F2**o∨/**F3**Para seleccionar**Administrador**.

3. Toque**Aceptar/F4**.

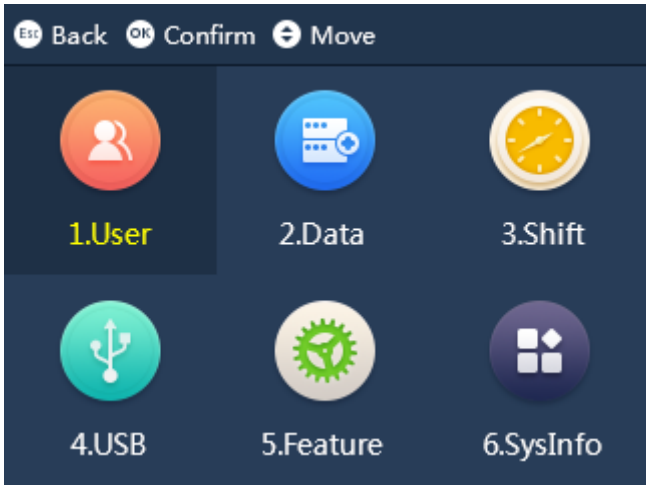
5.4 Iniciar sesión

Después de crear la cuenta de administrador, puede ingresar al menú principal después de haber verificado su

Identificaciones mediante huella dactilar, contraseña o tarjeta.

La función de deslizar tarjeta solo está disponible en modelos seleccionados.

Figura 5-5 Menú principal



Grifo y luego ingrese al menú principal después de que se haya verificado su identidad.

- Coloque su dedo sobre el sensor de huellas dactilares.
- Introduzca el ID y la contraseña del administrador.
- Pase la tarjeta por el lector de tarjetas.

6 Operaciones de SmartPSS Lite

Solo algunos modelos admiten configuraciones en SmartPSS Lite. Para obtener más información, consulte el manual del usuario de SmartPSS Lite.

6.1 Instalación

Comuníquese con el soporte técnico o descargue ToolBox para obtener SmartPSS Lite.

- Si obtiene el paquete de software de SmartPSS Lite, instale y ejecute el software de acuerdo con las instrucciones de la página.
- Si obtiene el software mediante ToolBox, ejecute SmartPSS Lite según las instrucciones de la página.

6.2 Inicialización

Inicialice SmartPSS Lite cuando inicie sesión por primera vez. Deberá establecer una contraseña para iniciar sesión y sus preguntas de seguridad para restablecer la contraseña.

Procedimiento

Paso 1 Haga doble clic en SmartPSSLite.exe o haga clic en**Abierto**Junto al icono del software en la caja de

Paso 2 herramientas, seleccione el idioma de la lista desplegable y seleccione**He leído y acepto el acuerdo de software.**y luego haga clic en**Próximo**.

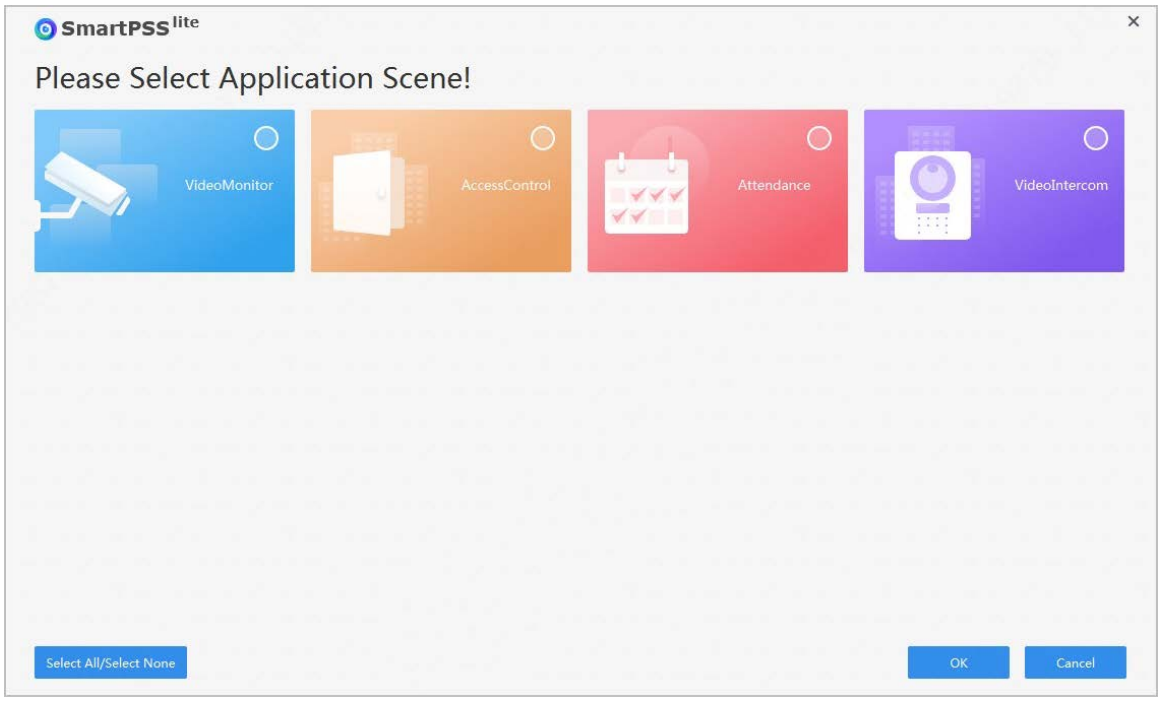
Paso 3 Hacer clic**Navegar**para seleccionar la ruta de instalación y luego haga clic en**Instalar**

Paso 4 Haga clic en**Finalizar**para completar la instalación.

Seleccionar**Ejecutar SmartPSSLite**para iniciar SmartPSS Lite.

Paso 5 Seleccione las escenas de aplicación que desea agregar y luego haga clic en**DE ACUERDO**.

Figura 6-1 Seleccionar escenas de aplicación



Paso 6 Hacer clic**Aceptar y continuar**estar de acuerdo**Acuerdo de licencia de software**y**Política de privacidad del producto**.

Paso 7 Establecer contraseña en el**Inicialización**página y luego haga clic en**Próximo**.

Tabla 6-1 Parámetros de inicialización

Parámetro	Descripción
Contraseña	La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos 2 tipos de caracteres, incluidas letras mayúsculas, letras minúsculas, números y caracteres especiales.
Fuerza de la contraseña	Muestra la seguridad de una contraseña frente a ataques de fuerza bruta y de adivinación. El color verde significa que la contraseña es segura y el rojo, que es demasiado débil. Establezca una contraseña de alta seguridad utilizando el indicador de seguridad de contraseña como ayuda.
confirmar Contraseña	Ingrese la contraseña nuevamente para confirmarla.
Inicio de sesión automático después del registro	Permitir**Inicio de sesión automático después del registro**para que SmartPSS Lite inicie sesión automáticamente después de la inicialización; de lo contrario, se muestra la página de inicio de sesión.

Paso 8 Establezca preguntas de seguridad y luego haga clic en**Finalizar**.

6.3 Iniciar sesión

Procedimiento

Paso 1 Haga doble clic en SmartPSSLite.exe o haga clic en**Abierto**Junto al icono del software en la caja de herramientas,

Paso 2 introduzca el nombre de usuario y la contraseña y, a continuación, haga clic en**Acceso**.

Tabla 6-2 Parámetros de inicio de sesión

Parámetro	Descripción
Recordar Contraseña	Permitir**Recordar contraseña**para que no tengas que volver a introducir la contraseña la próxima vez que inicies sesión.

Parámetro	Descripción
Inicio de sesión automático	Permitir**Inicio de sesión automático**para que SmartPSS Lite inicie sesión automáticamente la próxima vez que utilice la misma cuenta.
Olvidó ¿contraseña?	Hacer clic**¿Has olvidado tu contraseña?**para restablecer la contraseña cuando la olvidas.

Apéndice 1 Puntos importantes de la toma de huellas dactilares

Instrucciones de registro

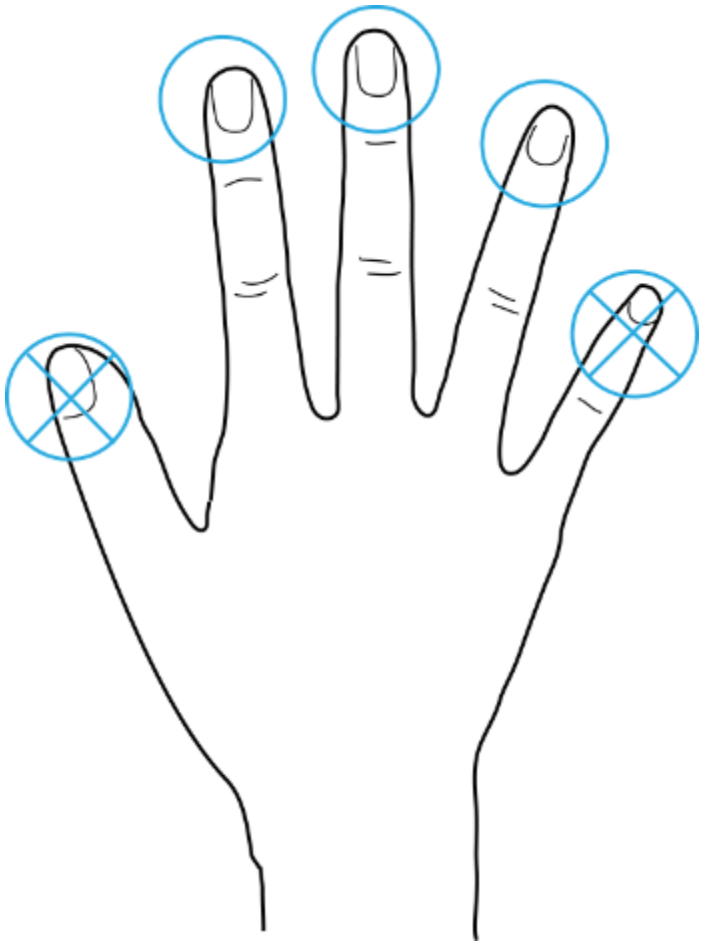
Al registrar la huella dactilar, preste atención a los siguientes puntos:

- Asegúrese de que sus dedos y la superficie del escáner estén limpios y secos.
- Presione su dedo en el centro del escáner de huellas dactilares.
- No coloque el sensor de huellas dactilares en un lugar con luz intensa, alta temperatura y alta humedad.
- Si sus huellas dactilares no están claras, utilice otros métodos de desbloqueo.

Se recomiendan los dedos

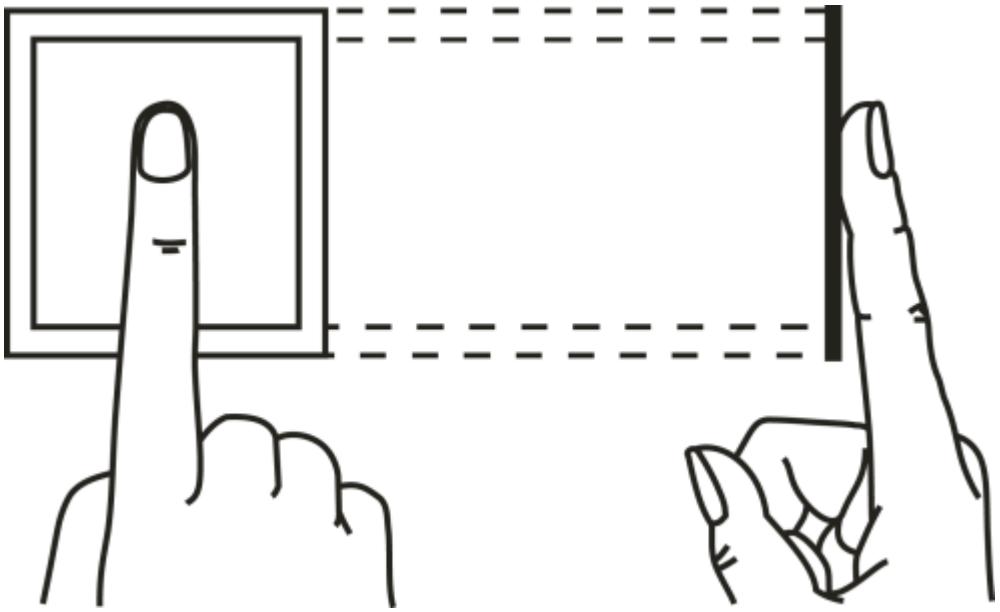
Se recomiendan los dedos índice, medio y anular. Los pulgares y meñiques no se pueden colocar fácilmente en el centro de la grabación.

Apéndice Figura 1-1 Dedos recomendados

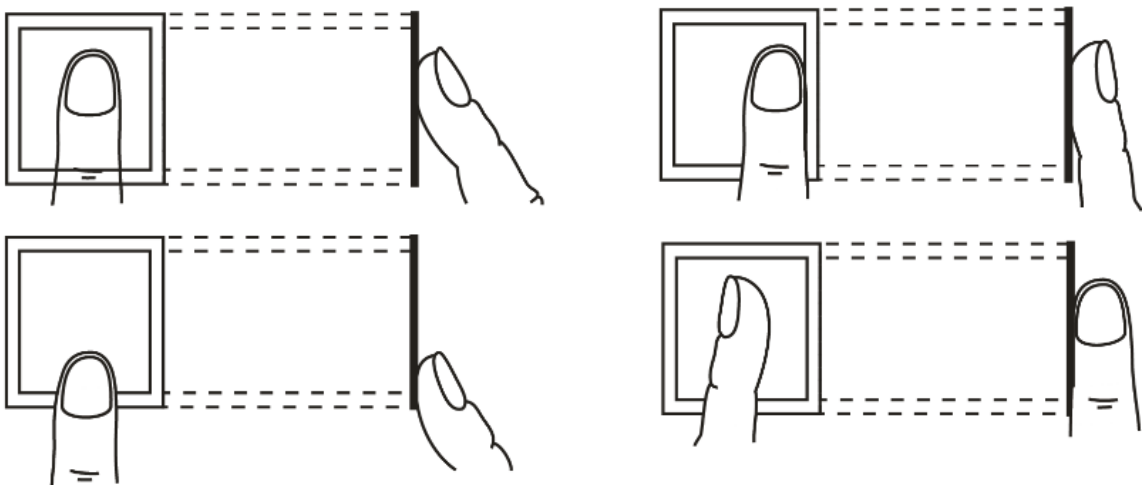


Cómo presionar su huella digital en el escáner

Apéndice Figura 1-2 Colocación correcta



Apéndice Figura 1-3 Colocación incorrecta



Apéndice 2 Método de entrada

Puede escribir letras, números y símbolos en inglés.

Números

1. Toque  para cambiar los métodos de entrada hasta**123**se muestra en la pantalla.
2. Introduzca números.
3. Toque**Aceptar/F4**Para confirmar.

Letras

1. Toque  para cambiar los métodos de entrada hasta**abecedario**se muestra en la pantalla.
2. Introduzca letras.
3. Toque**Aceptar/F4**Para confirmar.

Símbolos

1. Toque  para cambiar los métodos de entrada hasta**:-)**se muestra en la pantalla.
2. Toque∧/**F2**o∨/**F3**para seleccionar símbolos.
3. Toque**Aceptar/F4**Para confirmar.

Apéndice 3 Preguntas frecuentes

- P: El dispositivo me solicita que lo haga nuevamente después de haber colocado mi dedo sobre el sensor.
  R: Verifique si sus huellas dactilares han sido registradas.
- P: La campana no suena.
  A: Verifique si el timbre está configurado correctamente y el interruptor de volumen de transmisión está activado.
- P: No puedo actualizar el dispositivo a través del USB.
  A: Verifique si el dispositivo es reconocido exitosamente por el dispositivo y verifique el nombre del archivo de actualización.
- P: No se pudo exportar mediante una unidad flash USB. R:
  Utilice una unidad USB en formato FAT32.
- P: Olvidé la contraseña de administrador. R:
  Comuníquese con el fabricante.
- P: ¿Cómo buscar el registro de asistencia del usuario?
  A: En la pantalla de espera, toque**#**, y luego coloque el dedo sobre el sensor de huellas dactilares, o ingrese el ID de usuario y la contraseña, o deslice la tarjeta.

Apéndice 4 Recomendaciones de ciberseguridad

Acciones obligatorias a tomar para la seguridad básica de la red de equipos:

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 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 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 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 sus equipos:

1.**Protección física**

Le sugerimos que realice una protección física de los equipos, especialmente de los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en una sala de computadoras y un gabinete especiales, e implemente un control de acceso y una gestión de claves adecuados para evitar que personal no autorizado realice contactos físicos, como dañar el hardware, conectar sin autorización equipos extraíbles (como memorias USB, puertos seriales), etc.

2.**Cambie las contraseñas periódicamente**

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

3.**Establecer y actualizar contraseñas Restablecer información oportunamente**

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 puerto 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 dirección MAC**

Le recomendamos vincular la dirección IP y MAC del gateway al equipo, reduciendo así el riesgo de suplantación de ARP.

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

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios de manera razonable y asigne un

conjunto mínimo de permisos para ellos.

9.**Desactivar 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.
- Consultar log de equipos: Al consultar los logs podrás conocer las direcciones IP que se utilizaron para iniciar sesión en tus dispositivos y sus operaciones claves.

12.**Registro de red**

Debido a la capacidad de almacenamiento limitada del equipo, 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.**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 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.