

# **Lector de registro de huellas dactilares**

## **Manual de usuario**








# Prefacio

## General

Este manual presenta las funciones y operaciones del lector de registro de huellas dactilares (en lo sucesivo, "el Dispositivo").

### Instrucciones de seguridad

Las siguientes palabras de advertencia categorizadas con un significado definido pueden aparecer en el manual.

Palabras de advertencia	Sentido
 <b>PELIGRO</b>	Indica un peligro de alto potencial que, si no se evita, provocará la muerte o lesiones graves.
 <b>ADVERTENCIA</b>	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 <b>PRECAUCIÓN</b>	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
 <b>PUNTAS</b>	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
 <b>NOTA</b>	Proporciona información adicional como énfasis y complemento del texto.

## Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	octubre 2020

## Sobre el Manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por las operaciones que no cumplen con el manual.
- El manual se actualizaría de acuerdo con las últimas leyes y reglamentos de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar 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.
- Todavía puede haber desviación en los datos técnicos, descripción de funciones y operaciones, o errores en la impresión. 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 comerciales registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio al cliente si ocurre algún problema al usar el dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

## Medidas de seguridad y advertencias importantes

Este capítulo presenta el contenido que cubre el manejo adecuado del dispositivo, la prevención de riesgos y la prevención de daños a la propiedad. Lea este contenido detenidamente antes de utilizar el Dispositivo, respételo cuando lo utilice y guarde bien el manual para futuras consultas.

- No toque el sensor de huellas dactilares con objetos duros.
- Mantenga su dedo limpio antes de agregar la huella digital. Si su dedo está mojado, séquelo y luego agregue su huella digital. Del mismo modo, si su dedo está demasiado seco, humedézcalo, séquelo y luego agregue su huella digital.
- Mantenga limpia el área de recolección de huellas dactilares. Si es necesario, use un paño suave para limpiarlo suavemente. Utilice el dedo con una huella dactilar clara y completa.
- Al recolectar huellas dactilares, aplique la presión adecuada durante aproximadamente 1 segundo para obtener el mejor resultado. Demasiada presión distorsionará la huella dactilar y afectará el resultado.
- Mantenga el dispositivo alejado del agua. Corte la energía inmediatamente en caso de daños por agua. Encienda el dispositivo cuando esté completamente seco, pero es posible que no funcione correctamente.
- Conecte a tierra correctamente la fuente de alimentación; de lo contrario, el dispositivo podría dañarse o representar un riesgo para la seguridad.

# Tabla de contenido

<b>Prólogo</b> .....	<b>YO Medidas de seguridad y advertencias importantes</b> .....	<b>II 1</b>
<b>Introducción</b> .....		<b>1</b>
1.1 Características .....		1
1.2 Dimensiones .....		1
<b>2 Funcionamiento del dispositivo</b> .....		<b>2</b>
2.1 Expedición de la tarjeta .....		2
2.2 Recogida de huellas dactilares .....		7
<b>3 Instrucciones para la recogida de huellas dactilares</b> .....		<b>11</b>
<b>4 Actualización del dispositivo</b> .....		<b>13</b>
<b>Appendix 1 Recomendaciones de ciberseguridad</b> .....		<b>14</b>

# 1. Introducción

Este dispositivo integra las funciones de emisión de tarjetas y recolección de huellas dactilares. Es plug-and-play usando un cable USB para conectarse a la PC. Es aplicable a zonas industriales, edificios de oficinas, escuelas, fábricas, estadios, CBD, áreas residenciales, propiedades gubernamentales y más.

## 1.1 Características

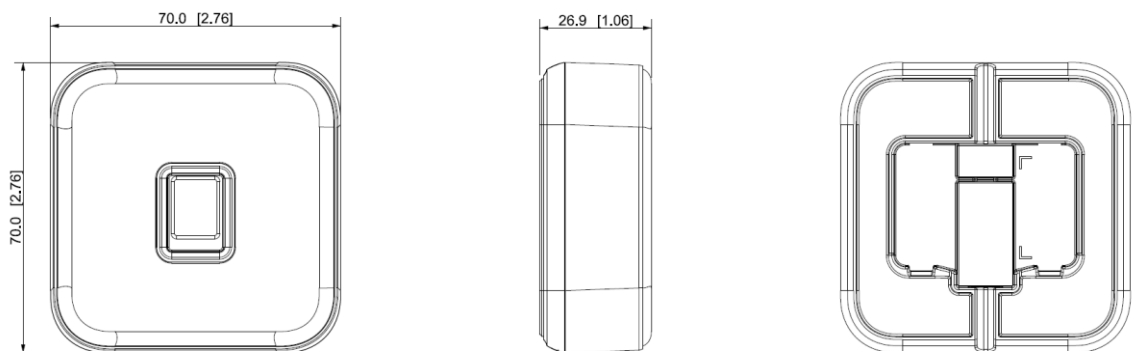
- Panel frontal de material PC y acrílico con diseño ultrafino.
- Conexión y reproducción USB 2.0.
- Problema con IC (Mifare)/tarjeta de identificación.
- Recoger huellas dactilares.
- Zumbador incorporado y luz indicadora.
- Vigilancia integrada para garantizar la estabilidad del dispositivo.
- Seguro y estable con protección contra sobrecorriente y sobretensión.



Las funciones varían con los diferentes modelos. Prevalecerá el producto real.

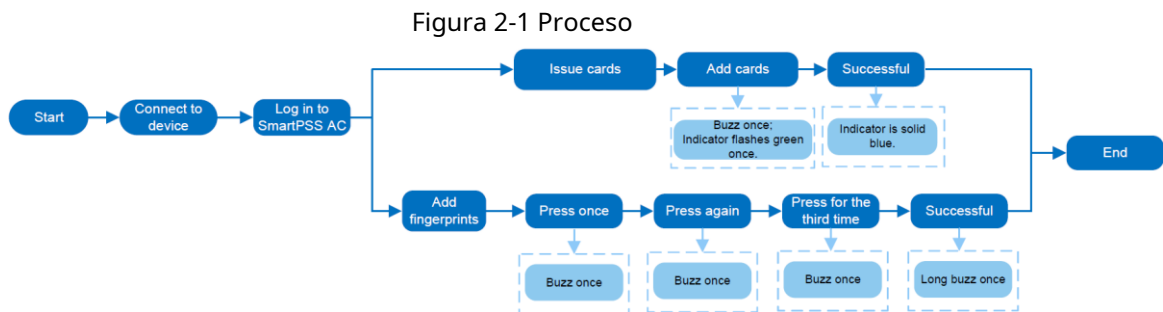
## 1.2 Dimensiones

Figura 1-1 Dimensiones (mm [pulgadas])



## 2 Operación del dispositivo

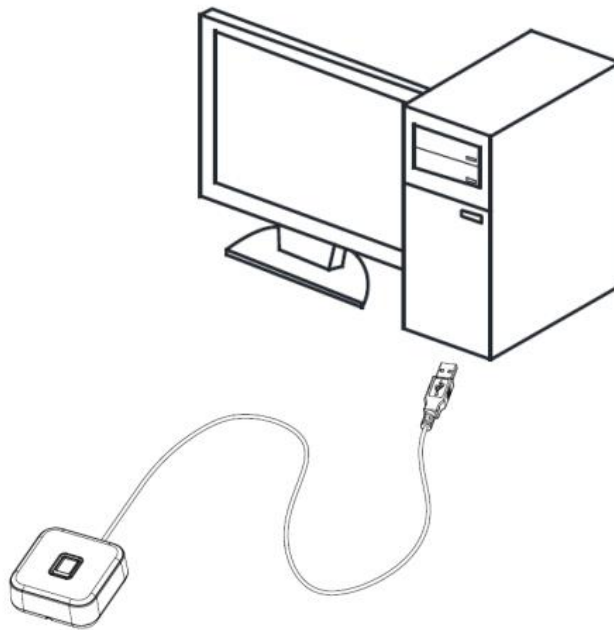
Antes de emitir tarjetas, debe instalar DSS Pro o SmartPSS AC en su PC y luego seguir el proceso a continuación. Tome SmartPSS AC como ejemplo.



### 2.1 Tarjeta emisora

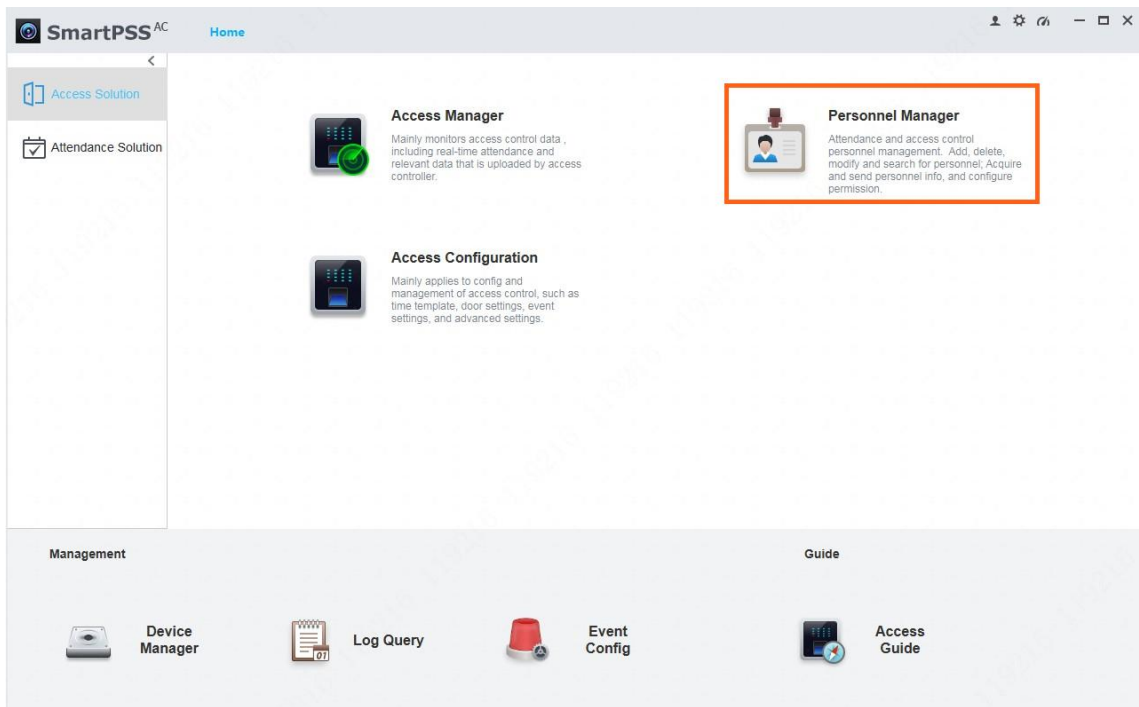
Step 1 Conecte el cable USB del Dispositivo a la PC, y luego el indicador del Dispositivo será azul fijo.

Figura 2-2 Conecte el dispositivo a la PC



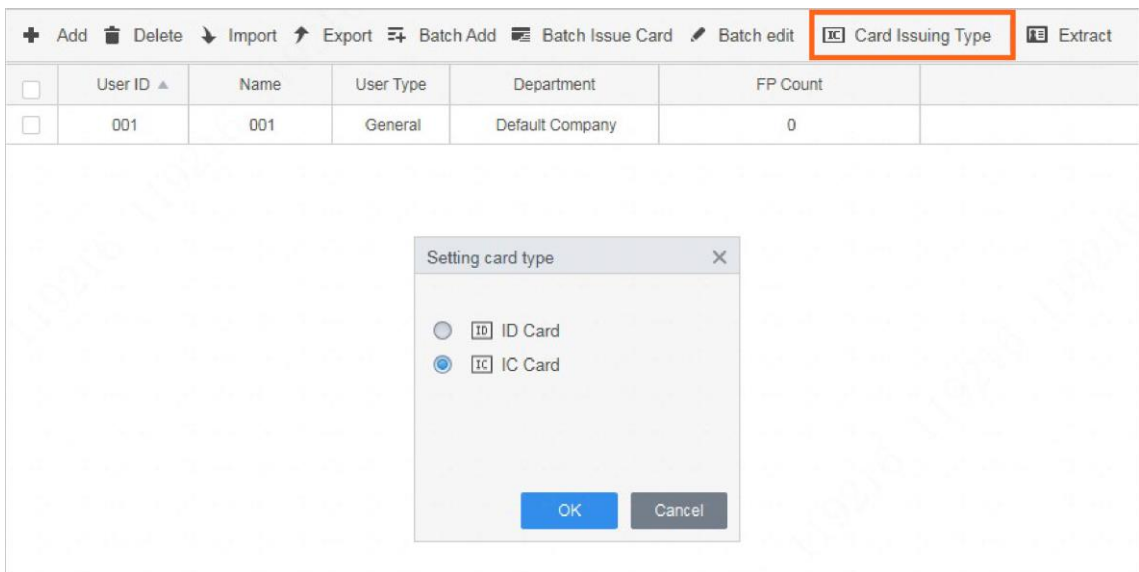
Step 2 Ejecute el cliente SmartPSS AC en la PC y haga clic en **Solución de acceso > Administrador de personal**.

Figura 2-3 SmartPSS CA



**Step 3** Hacer clic **Tipo de emisión de tarjeta** luego seleccione el tipo según sea necesario.

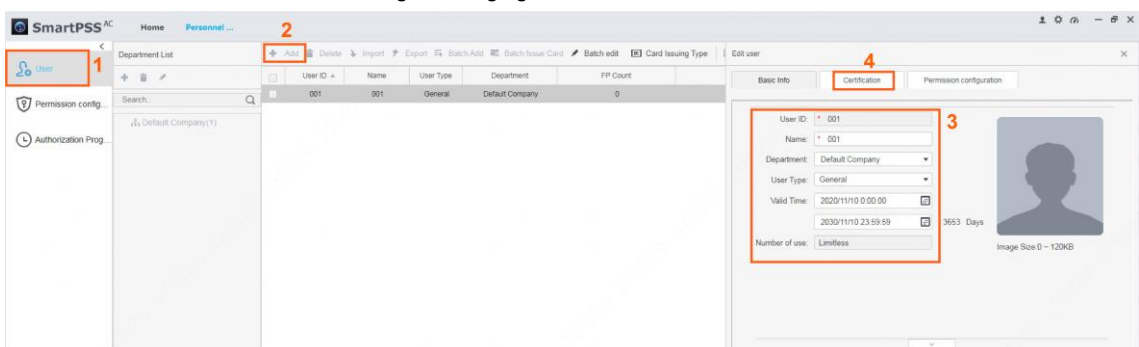
Figura 2-4 Tipo de emisión de tarjeta



**Step 4** Hacer clic **Usuario** en el menú de la izquierda.

- Si necesita agregar un nuevo usuario, haga clic en **Agregar**, ingrese la información básica y luego haga clic en **Certificación**.

Figura 2-5 Agregar un usuario




- Para un usuario existente, haga clic en  a la derecha y luego haga clic en **Certificación**.


Figura 2-6 Editar información de usuario



User ID	Name	User Type	Department	FP Count	Operation
001	001	General	Default Company	0	


**Step 5** A la derecha de la **Tarjetas** sección, haga clic en , seleccione el lector de tarjetas y luego haga clic en **OK**.

Figura 2-7 Seleccione un lector de tarjetas

Basic Info Certification Permission configuration

**Password** Add  For the 2nd-generation access controller, it is the personnel password; otherwise it is card password.

**Card** Add  The card number must be added if not the 2nd generation access controller is used. 

**Fingerprint** 

Card Reader Management

Card Reader: Card issuer

OK Cancel

**Step 6** Hacer clic **Agregar**. El dispositivo emite un zumbido y el indicador parpadea en verde.

**Step 7** Deslice la tarjeta en el dispositivo y suena una vez.

El sistema lee el número de tarjeta y el indicador parpadea en verde. Hacer clic

**Step 8** **OK** para terminar el proceso.

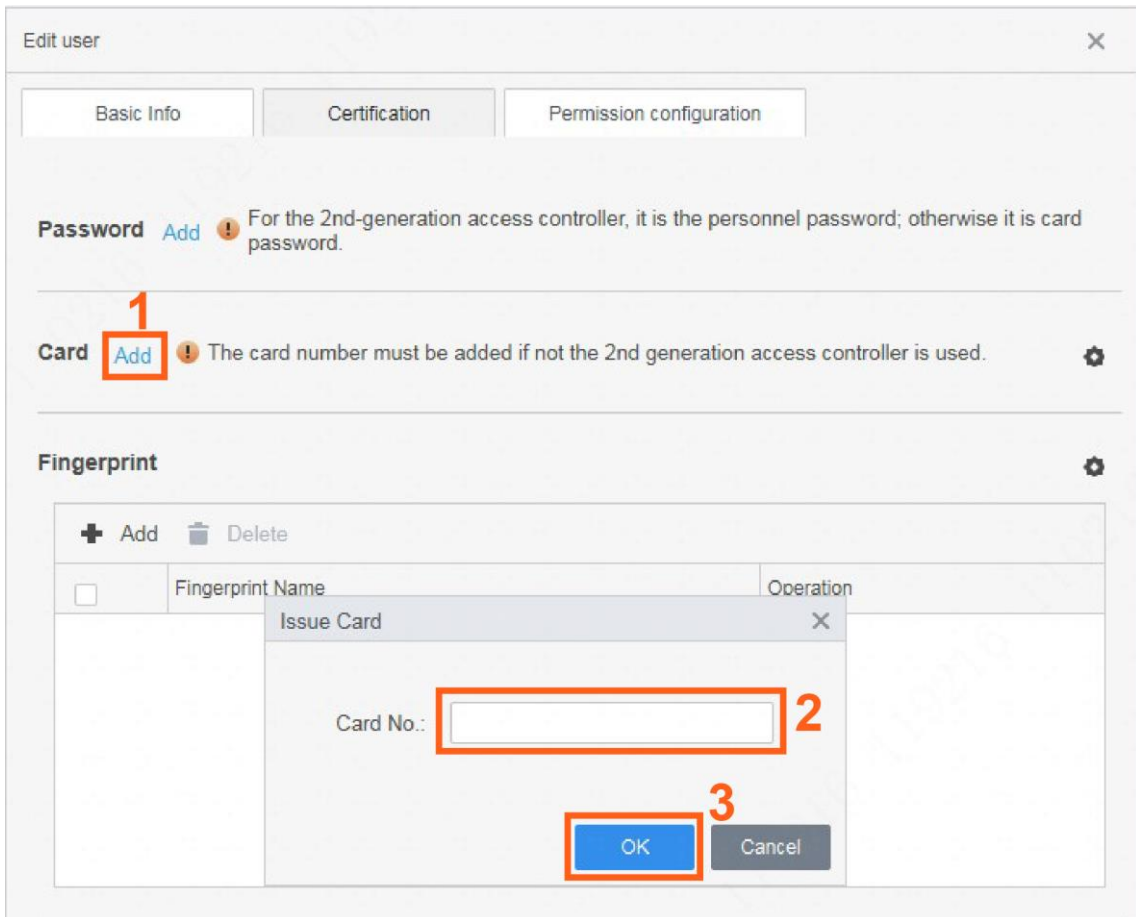
El indicador del dispositivo se vuelve azul fijo como modo de espera.



- El lector de tarjetas solo puede leer una tarjeta a la vez. Cuando se apilan varias cartas juntos, no puede funcionar correctamente. Cada
- usuario puede tener cinco tarjetas como máximo.



Figura 2-8 Agregar una tarjeta



### Operaciones relacionadas

Hacer clic **Usuario**, seleccione los usuarios según sea necesario y luego haga clic en **Tarjeta de emisión por lotes**.

Figura 2-9 Tarjeta de emisión en lotes

+ Add    - Delete    ↘ Import    ↗ Export    ⇄ Batch Add <b>Batch Issue Card</b> ✎ Batch edit    [IC] Card Issuing Type    [E] Extract						
<input checked="" type="checkbox"/>	User ID ▲	Name	User Type	Department	FP Count	
<input checked="" type="checkbox"/>	001	001	General	Default Company	0	
<input checked="" type="checkbox"/>	002	002	General	Default Company	0	
<input checked="" type="checkbox"/>	003	003	General	Default Company	0	

● Leer automáticamente el número de tarjeta.

1) Seleccionar **Emisor de la tarjeta**.

2) Haga clic **Tema**.

3) Pase las tarjetas en el orden de la lista de usuarios y el sistema leerá automáticamente los números de tarjeta. Puede configurar la información para cada usuario, incluida la hora de inicio y finalización.

Hacer clic **OK**.

Figura 2-10 Tarjeta de emisión en lotes

Batch Issue Card

Device:  **1**  **2**

ID:  Name:

Card No.:  **3** Department:

Start Time:  End time:

Card List

User ID	Name	Card No.	Operation
001	001	12345678	<input type="button" value="🗑"/>
002	002		<input type="button" value="🗑"/>
003	003		<input type="button" value="🗑"/>

**4**

- Introducir números de tarjeta manualmente.

Seleccione cada usuario e ingrese el número de tarjeta correspondiente, y luego haga clic en **OK**.

Figura 2-11 Introducir números de tarjeta manualmente

Batch Issue Card

Device: Card issuer Issue

ID: 001 Name: 001

Card No.: 12345678 2 Department: Default Company

Start Time: 2020-11-10 00:00:00 End time: 2030-11-10 23:59:59

Card List

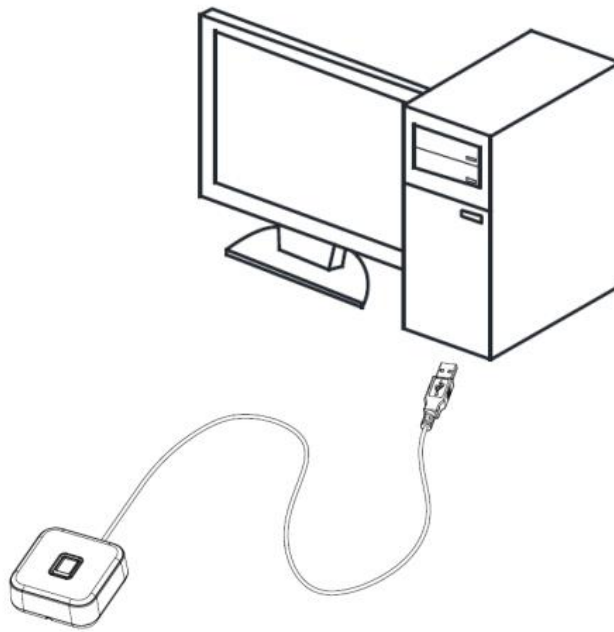
User ID	Name	Card No.	Operation
001	001	12345678	<span>1</span>
002	002		
003	003		

3 OK Cancel

## 2.2 Recogida de huellas dactilares

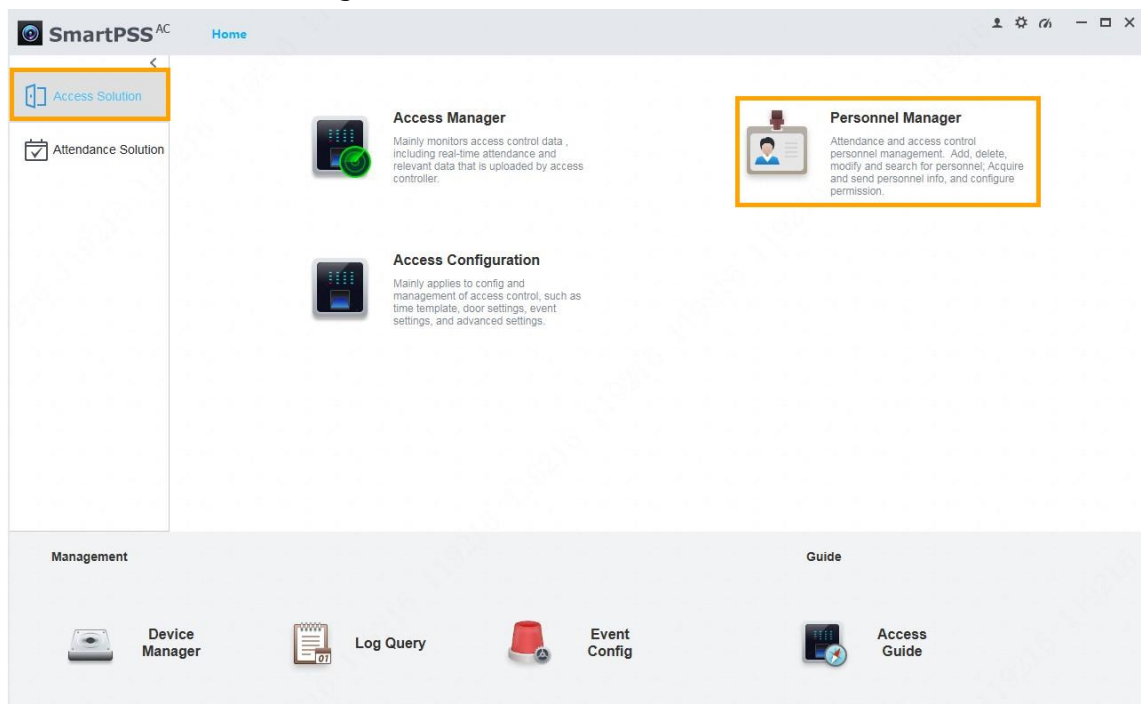
Step 1 Conecte el cable USB del Dispositivo a la PC, y luego el indicador del Dispositivo será azul fijo.

Figura 2-12 Conecte el dispositivo a la PC



**Step 2** Ejecute el cliente SmartPSS AC en la PC y seleccione **Solución de acceso > Administrador de personal**.

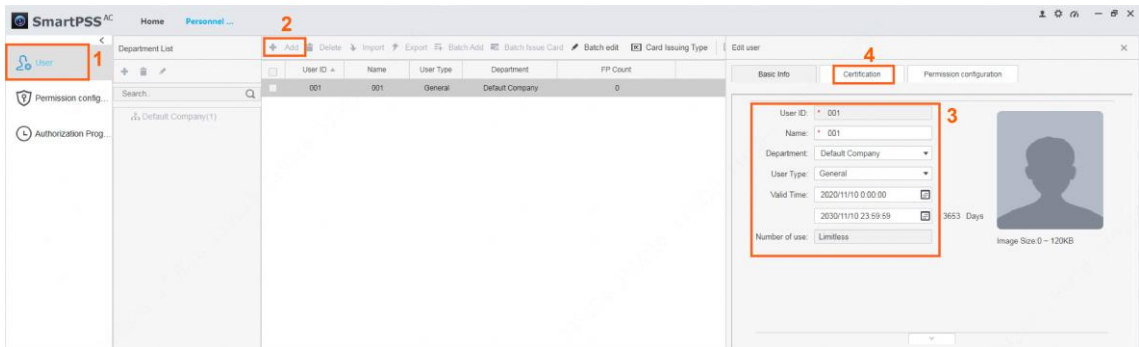
Figura 2-13 Cliente SmartPSS AC



**Step 3** Hacer clic **Usuario** en el menú de la izquierda.

- Si necesita agregar un nuevo usuario, haga clic en **Agregar**, ingrese la información básica y luego haga clic en **Certificación**.

Figura 2-14 Agregar un usuario




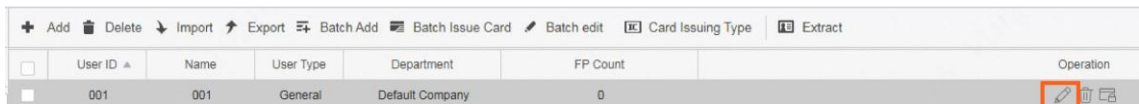
● Para un usuario existente, haga clic en  a la derecha y luego haga clic en **Certificación**.

Figura 2-15 Editar información de usuario




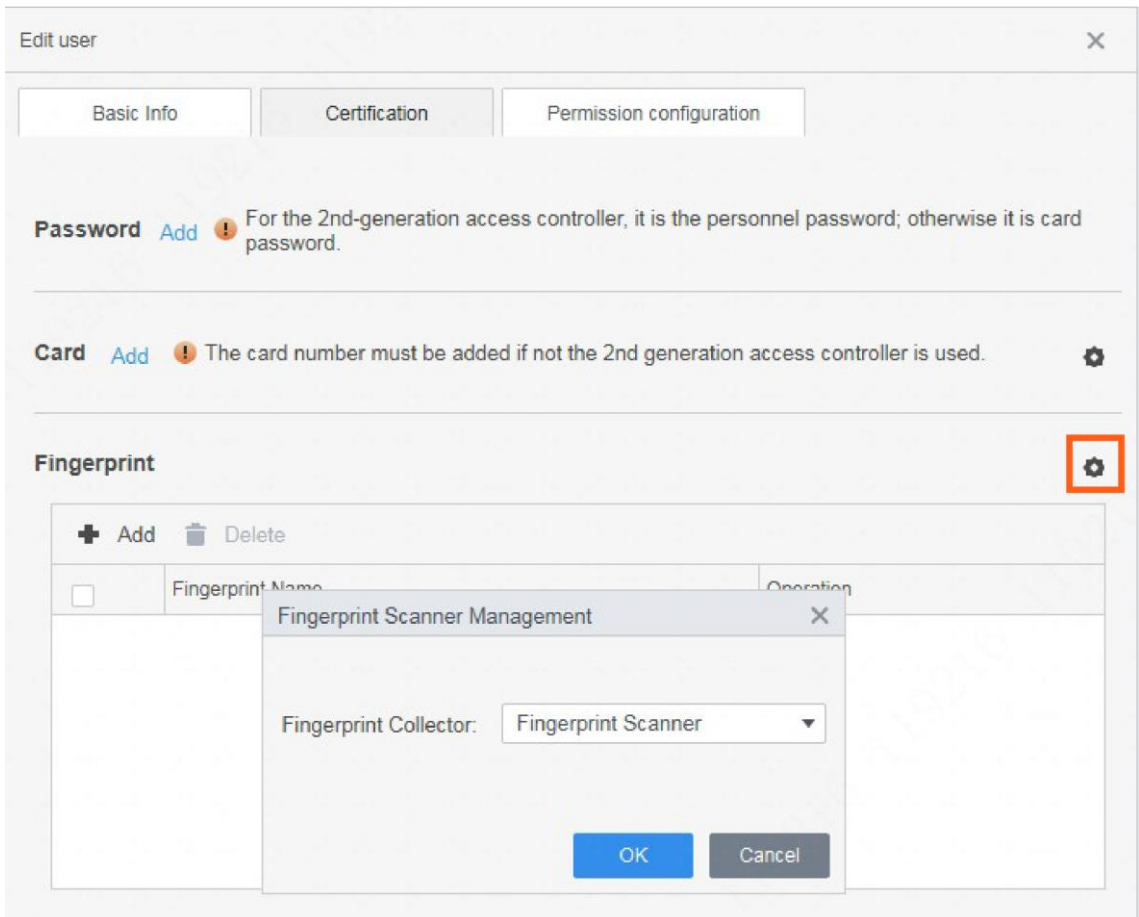
**Step 4** A la derecha de la **Huella dactilar** sección, haga clic en , Seleccione **Escáner de huellas dactilares**, y entonces en **OK**.

Figura 2-16 Seleccione un escáner de huellas dactilares

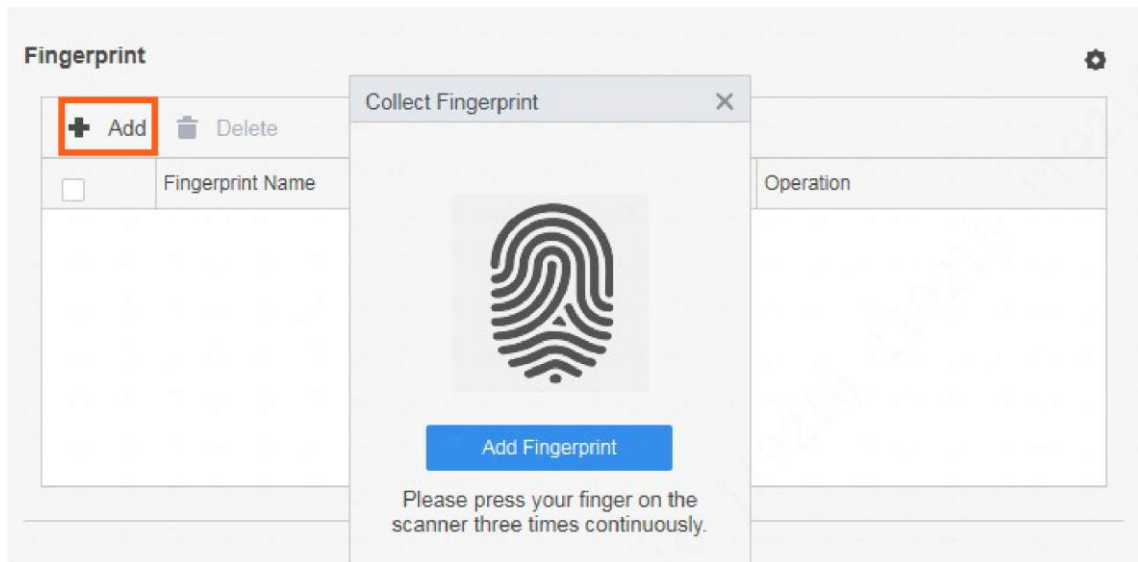


**Step 5** Hacer clic **Agregar**.



Cada usuario puede tener tres huellas dactilares como máximo.

Figura 2-17 Recolectar una huella digital



**Step 6** Hacer clic **Agregar huella digital** y luego siga las instrucciones para presionar su dedo tres veces en el área de recolección de huellas dactilares del dispositivo.

Tabla 2-1 Descripción del mensaje de sonido al recopilar huellas dactilares

Situación	Aviso de sonido
Presione el dedo una vez	Éxito: Buzz una vez; Tiempo de espera: Buzz tres veces.
Presione el dedo por segunda vez	Éxito: Buzz una vez; Tiempo de espera: Buzz tres veces.
Presione el dedo por tercera vez	Éxito: Buzz una vez; Tiempo de espera: Buzz tres veces.
Resultado	Éxito: Zumbido largo una vez; Fallo: Buzz tres veces.

### 3 Instrucción de recolección de huellas dactilares

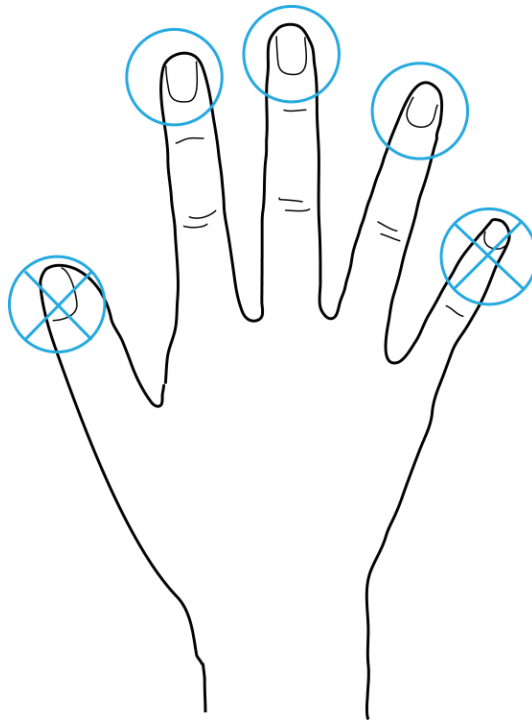
#### Aviso

- Asegúrese de que sus dedos estén limpios y secos antes de tomar sus huellas dactilares.
- No exponga el escáner de huellas dactilares a altas temperaturas y humedad.
- Si sus huellas dactilares están desgastadas o no son claras, utilice otros métodos, como la contraseña y la tarjeta.

#### Dedos recomendados

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

Figura 3-1 Dedos recomendados



#### Manera correcta de presionar el dedo

Presione su dedo en el área de recolección de huellas digitales y alinee el centro de su huella digital con el centro del área de recolección.

Figura 3-2 Forma correcta

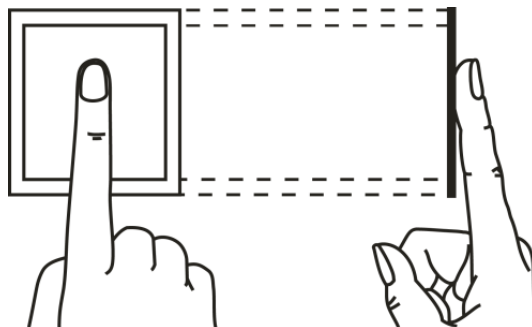
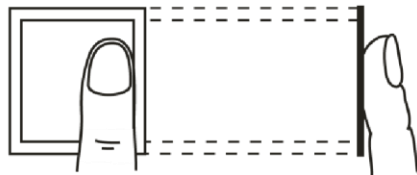


Figura 3-3 Formas incorrectas

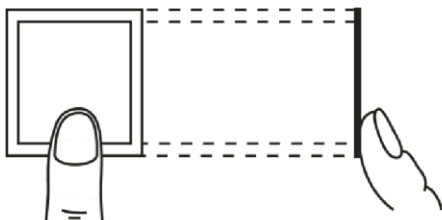
Fingerprint not entirely on the collecting area



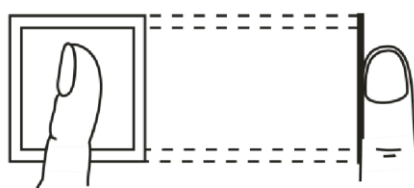
Fingerprint not on the center of the collecting area



Fingerprint not on the center of the collecting area



Fingerprint not on the collecting area





## Actualización de 4 dispositivos

Utilice la herramienta de actualización USB para actualizar el programa del dispositivo.

### requisitos previos

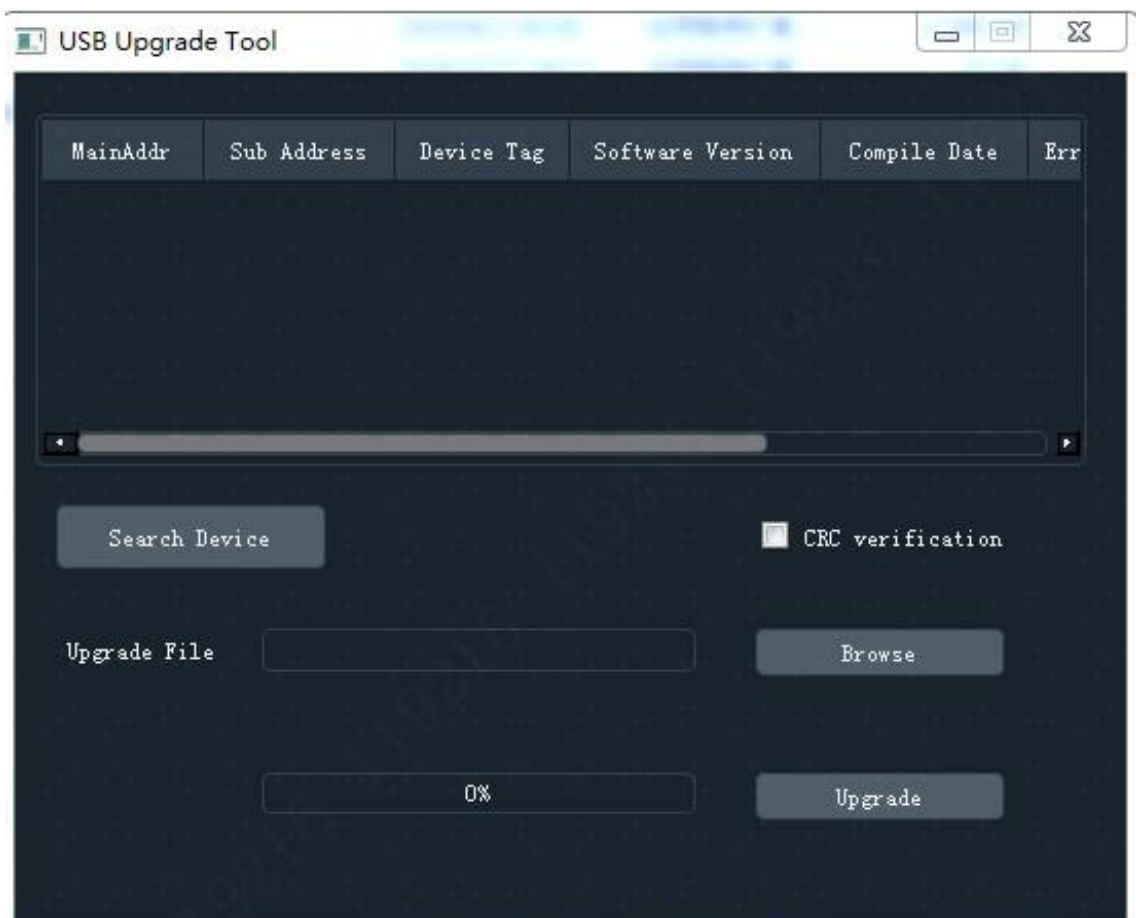
- Descargue la herramienta de actualización USB a su PC.
- Utilice un cable USB para conectar el dispositivo a su PC.

### Procedimiento

**Step 1** Haga doble clic para ejecutar el programa. Hacer

**Step 2** clic **Dispositivo de búsqueda**.

Figura 4-1 Herramienta de actualización de USB



**Step 3** Hacer clic **Navegarey** luego seleccione el archivo de actualización. Seleccione el dispositivo

**Step 4** según sea necesario y luego haga clic en **Mejora**. Cuando la barra de progreso alcanza el 100 %, la actualización se completa.

# Appendix 1 Recomendaciones de 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 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. 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 un gabinete y una sala de computadoras especiales, e implemente un control de permisos y administración de claves bien hecho 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, un dispositivo en serie). puerto), 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 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. 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.